An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Combatting scam calls and texts

Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications

Response to Consultation and Decisions

Reference:	ComReg 24/24
Decisions:	D09/24, D10/24, D11/24, D12/24, D13/24, D14/24, D15/24
Date:	03/04/2024

Content

Section **Page**

Annex

Section Page

Table of Figures and Tables

Table of Figures

Section **Page**

Table of Tables

Section **Page**

Executive Summary

Introduction and summary

1. Scams, or nuisance communications, have rapidly become not just a blight on society but the cause of significant financial and economic harm to consumers, business, and public bodies. Unfortunately, most of us know someone who has been scammed and had money stolen by unscrupulous fraudsters whose criminal actions cause significant stress and financial harm or even ruin.

2. Moreover, we can all identify with the considerable stress and anxiety these scams can cause our vulnerable loved ones. Our loved ones receive these unwanted communications and can become confused about whether to respond or not, out of fear of being scammed. These scams are an undesirable development that have damaged legitimate communications by breaking trust. The total quantifiable harm to Ireland's society arising from scam calls and texts is conservatively estimated **at over €300 million per annum**.

3. In June 2023, ComReg launched its public consultation that proposed a package of interventions to combat scam calls and texts. ComReg's response, set out in this document, assesses the response of interested parties and provides ComReg's final decision on the necessary interventions that must be implemented within the prescribed timeframes.

4. Responses were largely positive, and operators have broadly welcomed the

proposed interventions. However, some were of the view that certain interventions were unnecessary and, if anything, should be implemented over a longer timeframe. Others suggested that ComReg should adopt a 'wait and see' approach whereby some interventions should be implemented but others only introduced on foot of a further assessment.

5. Helpfully, ComReg notes that Mr. Torlach Denihan of the Telecommunications Industry Ireland ("TII") – IBECs representative body for the electronic communications industry in Ireland, recently confirmed[1] on national television that "*we are awaiting a decision from ComReg … once we hear from them, once we get the greenlight, we will implement with maximum haste those interventions*". ComReg welcomes this TII statement and hopes that operators will indeed act with haste to implement the interventions speedily. Rapidly implementing these interventions provides operators with a prime opportunity to demonstrate their commitment to protecting their consumers from criminals and ensuring that the services they provide over their networks can once again be trusted and used without worry.

6. Having carefully considered the views of respondents and the available evidence before it, ComReg has now confirmed its **current package of six interventions** to mitigate the ongoing scourge of nuisance communications. Real-world experience of the success of these interventions in other countries is heartening and provides convincing evidence of their effectiveness, with significant reductions measured in the rates of scam calls and texts following their introduction.

7. ComReg estimates that the **overall benefit of the package of interventions implemented is around €1.2 billion** over the next seven years.

Harm caused by scam calls and texts to consumers.

8. To appreciate why this package of interventions is required, it is first necessary to understand the extent of the harm caused by scam calls and texts. There has been much debate regarding their harm to society, but it was only recently that the full extent of this was revealed. ComReg published research and analysis it commissioned from B&A[2] and Europe Economics[3] which provided the first detailed insight into the harm caused in Ireland. The results paint a bleak picture of a menace that targets us all and leaves many picking up the pieces from the aftermath of financial harm and mental

[1] RTE1, Upfront With Katie Hannon – 18 December 2023
[2] ComReg 23/52b, Behavior & Attitudes "*Research on Nuisance Communications - Consumer*", 16 June 2023. Link and ComReg 23/52c, Behavior & Attitudes "*Research on Nuisance Communications - Business*", 16 June 2023. Link
[3] Europe Economics Report "*Scam calls and texts in Ireland – costs and benefits of interventions*", 16 June 2023. Link

distress.

9. Scam calls and texts now pervade society with over 90 per cent of adults in Ireland having received a scam call to their mobile phone in the last year, while 84 per cent have received some form of scam text. The scammers strategy involves bombarding us with a large number of scams in the hope that some of us can be scammed. **Overall, Irish consumers receive around 59 million scam calls and over 47 million scam SMS messages annually**. This points to an average of approximately 161,000 scam calls and 129,000 scam SMS being received by Irish consumers each and every day.

10. We also now know that in Ireland around **1,000 people are defrauded of money every single day**. That is 1,000 people who are left angry and distraught by scammers who have no concern for the mental or financial wellbeing of their victims. Importantly, not every instance of fraud is the same, with the financial harm ranging from small to relatively large amounts. Clearly, the high number of cases continues to be a cause of concern. Of the 365,000 cases of financial fraud every year, it is estimated that 175,000 people were defrauded after receiving scam calls, while 190,000 people lost money after receiving scam texts.

11. These scams impact all walks of life, rich or poor, young or old, and given our collective reliance on telecommunications services, we are all potential targets and victims. Financial fraud affects all demographics but young people under 25 years are by far the most likely to be defrauded, accounting for 40% of all fraud cases. Older people are less likely to be defrauded but suffer larger financial impacts when they are swindled. They also show significantly higher levels of concern about being scammed, and this instils fear and anxiety when engaging in calls where the number or service is unfamiliar to them. Indeed, we are all familiar by now with our older loved ones seeking advice about calls and texts and worrying about whether they responded safely or not.

12. It is estimated that scam calls and texts in the last year were responsible for up to **89 million annoying/irritating communications and 31 million distressing communications**. Scams take a steep emotional toll on people, and the research shows that scams impact individuals' health and well-being, regardless of whether they have experienced financial loss or not. Constant scam attempts can increase stress levels and negatively impact people's mental health. This is even more insidious when the fraudsters target those most vulnerable who are often older, lonely or managing an illness.

Harm caused by to business and public authorities.

13. Of course, there is also significant harm caused to businesses by nuisance

communications. Scam calls and texts are polluting the channels used by business to communicate with consumers. Both calls and SMS remain very important channels for a broad range of businesses, being the only communication applications that are available on every single mobile phone.

14. It is estimated that over **5,000 businesses have been the victim of fraud** after receiving scam calls and texts in the past year. These scams impose costs on business due to the time and resources spent resolving customer problems, responding to customer queries and implementing scam prevention measures – be that new software/programmes, staff training, moving to alternative communications channels, etc.

15. Government departments (e.g., Dept. of Social Welfare, Revenue), public agencies (e.g., HSE, An Garda Síochána) suffer many harms as a direct consequence of scams. Scam calls and texts reduce or remove consumers trust in SMS and Voice calls, channels which are used by many public bodies to provide information, schedule appointments or otherwise communicate with Irish citizens. Many consumers may simply ignore texts that claim to be from public bodies, resulting in missed appointments or information regarding critical services. This harm is likely to be most acute precisely when such communications are most vital, as fraudsters target notable events (e.g., Covid-19 scams, An Post Christmas scams). In this way, fraudsters may exacerbate the impact of negative events on consumers, frustrating the effort of public bodies to ameliorate the effect of various events or crises.

16. Overall, the total quantifiable harm to Ireland's society arising from scam calls and texts **is conservatively estimated at over €300 million per annum** (See Chapter 3).

Importance of trust and why it's being lost.

17. People need to trust that those contacting them are genuine; otherwise, avoidance will result in legitimate and important calls and texts going unanswered. People answer calls and read text messages in the anticipation that the caller or sender is someone they know or with a genuine reason to contact them, perhaps a business providing services of value to them (for example banking and parcel delivery). Until recently, we generally trusted that the calls and text messages we received were legitimate. Irish numbers and Sender IDs should provide consumers with information they value and can trust (e.g., geographic location/ name organisation), absent trust the likelihood that the call will be answered or that the text will be read is reduced or eliminated. Nobody wants to be hoodwinked by the fraudster.

18. The B&A research paints a disturbing picture of how trust in calls and texts has been critically damaged. For example:

- Around half of consumers now require some confirmation of the legitimacy from the caller or sender of a text or they will cease the voice or text exchange.
- Over **40% of consumers that use SMS services**[4] **have lost trust in these communications** and increasingly pay less attention to them.

19. As we have noted, this loss of trust also has serious consequences for the delivery of public services. The HSE and An Garda Síochána, among others, have outlined to ComReg the serious repercussions that this lack of trust brings, increasing incidence of missed health appointments for example and the diversion of scarce public service resources to deal with the repercussions. Those respondents who commented on trust all agreed that scam calls and texts are eroding trust in Irelands voice and SMS platforms.

What actions has ComReg mandated?

20. Regrettably, existing telecommunications infrastructure has little capability to see and recognise nuisance communications; indeed, if nuisance communications could be readily recognised from valid communications, then the current issues could be more readily addressed. This is not a phenomenon exclusive to Ireland, but rather represents how telecommunications have developed, where the focus has tended to be squarely on the delivery of calls and texts rather than on their scrutiny or prohibition.

21. ComReg has been engaging with the telecoms industry through the auspices of its Nuisance Communications Industry Taskforce ("NCIT"). ComReg established the NCIT in 2022, to develop interventions that the telecommunications industry can adopt to tackle the problem. Some, but unfortunately not all, operators have already implemented a number of these measures to tackle nuisance communications. ComReg is grateful to these operators and for the telecoms industry commitment in the fight against fraudsters, but there is a great deal more to be done.

22. Notwithstanding some of the voluntary measures taken by some operators, ComReg is of the view that certain network-based interventions must be implemented across the entire industry (the "Interventions"). This package has been designed, mindful of the evidence that scammers will always try to find new ways of targeting consumers and businesses. Importantly, any package of interventions must be cognisant of the ability of fraudsters to readily switch across scams, platforms, and territories.

[4] Such services include information/reminders about health appointments, banking and utility bill.

23. For example, scams in the main initially originated abroad but have since evolved and Ireland based fraudsters are growing in scale and scope. This means that while interventions targeting calls from abroad (e.g., blocking calls based on call line identification ("CLI")[5]) are required to fight scams from overseas, they have no impact on scams that originate here at home. If ComReg mandated interventions that only targeted telecommunications traffic from abroad, it would leave consumers exposed to these domestic based scams. Therefore, an effective package of interventions must target scams regardless of where they originate.

24. ComReg is mandating a package of Voice and SMS interventions which it considers would best deal with the ongoing scourge of nuisance communications at this time. This package should therefore significantly reduce, though not fully eliminate scams and their harm, not least because fraudsters will inevitably try to circumvent any interventions imposed by ComReg.

Voice Interventions

25. ComReg is mandating five measures to reduce harm and improve trust in voice communications. The first four interventions **are to be put in place within six months of ComReg's Decisions**, and each is designed to address obvious vulnerabilities and reduce fraud in an expedited fashion.

    I. **A Do Not Originate ("DNO") list** refers to phone numbers which are never used for outgoing calls. For example, certain banks provide numbers for consumers to contact them, but they never contact a consumer using that same number. Consequently, any calls that appear to come from these numbers are spoofed and therefore should be automatically blocked.

    II. **A Protected Numbers ("PN") list** refers to phone numbers that have not been assigned by ComReg to any operator or business and so any calls that presents with them are spoofed and should therefore be blocked.

    III. **Mobile CLI Call Blocking** would identify and block nuisance calls stemming from international networks which present with Irish mobile caller IDs unless the mobile caller is genuine and known to be abroad. These scam calls attempt to deceive customers into thinking a call is coming from someone in Ireland on their mobile.

[5] Calling Line Identification (CLI) is the number presented or displayed by the party making a telephone call to the recipient of that call.

IV. **Fixed CLI Call Blocking** operates in the same way as mobile CLI call blocking but blocks nuisance calls that are spoofing geography specific numbers[6] (e.g., 01, 061) and the non-geographic numbers[7] that businesses use (e.g., 0818).

26. These initial interventions should help reduce nuisance calls, however of themselves they will not be enough to combat scam calls which can still originate from valid numbers within Ireland rather than abroad (e.g., primarily using pre-pay phones). Further, scams are likely to become increasingly sophisticated as scammers adapt to the implementation of ComReg's initial interventions. In particular, warnings have already been sounded regarding Artificial Intelligence ("AI") as it becomes increasingly advanced and harder to detect. AI can now generate highly impressionable scripts and convincingly replicate people's voices, further broadening the threat landscape. Therefore, ComReg is also mandating the introduction of a **Voice Firewall over a period of 18 months.**

27. Unlike the initial interventions which are static in nature, a Voice Firewall is a dynamic intervention and can be updated in real time to account for fraudsters' ever-adapting strategies to reach consumers by exploiting newly discovered vulnerabilities in networks and changes to consumer behaviour. A Voice Firewall acts in the same way as any firewall, assessing all terminating call traffic to decide which are allowed to pass through and which are likely to be from fraudsters. Typically, voice firewalls are designed with advanced real-time call data analytics, using machine learning and AI techniques to detect and act upon unusual patterns of call signalling data and traffic volumes.

SMS interventions

28. ComReg is mandating the establishment of a Sender ID Registry which will allow businesses to register their Sender ID with ComReg. Telecommunications providers can block any message bearing a Sender ID from any source other than those in the registry. In this way, fraudsters would be unable to pose as legitimate businesses to mislead consumers. **ComReg is introducing the Sender ID Registry over a period of 18 months**. This should be effective in reducing the prevalence of scam SMS that use Sender IDs to impersonate businesses and organisations.

29. ComReg also consulted on a SMS Scam Filter in order to target other SMS

[6] These are known as "Geographic Numbers".
[7] These are known as "Non-Geographic Numbers".

based scams. A SMS Scam Filter[8] operates like the spam filters that are applied to email inboxes, by detecting and blocking harmful links or content, with all inbound messages being routed through the firewall, to be analysed, classified and where necessary blocked. There was strong support for the SMS Scam Filter expressed, particularly from those whose customers are most likely to be victims of scams. In particular, both Bank of Ireland and Revolut who are at the coalface of contending with scams, expressed firm support for the SMS Scam Filter. The financial industry representative group – the BPFI, noted that SMS Scam Filters are already in place in other jurisdictions, and Irish businesses and consumers have experienced the effectiveness on comparable spam filters on email inboxes. BPFI supported legislative changes and offered every assistance.

30. ComReg cannot mandate the introduction of the SMS Scam Filter as it requires a legislative basis[9]. ComReg has and continues to engage with its parent department, the Department of the Environment, Climate and Communications ("DECC") in regard to tackling nuisance communications, and specifically a proposed SMS Filter equivalent or similar legislation as is already in place in Belgium and Poland[10]. ComReg continues to provide DECC with the necessary technical information to assist it in making a determination on the merits of its proposal. ComReg understands from DECC that once this phase is complete, it will be in a position to assess what, if any, legislative avenues may be required to proceed with the proposal.

31. ComReg remains conscious that the absence of a dynamic intervention such as the SMS Scam Filter, exposes consumers to the risk of harm from scam SMS, an issue that might exacerbate further as other avenues for fraudsters are removed. Europe Economics has conservatively estimated that a 1-year delay in implementing the SMS Scam Filter would result in c.€90 million of additional harm to Irish consumers and businesses.

32. Ireland is also part of the *anglosphere* and as such is markedly more susceptible to text-based scams that use the English language than its European counterparts. Furthermore, as SMS Scam Filters are already in place in the United States, United Kingdom, Canada and Australia, Ireland is now potentially more exposed to fraud via SMS.

[8] Without content scanning only a rudimentary evaluation of SMS is possible. Otherwise a SMS Scam Filter cannot detect common scams, such as those that use harmful links or content that encourages you to click on the link and then install malware or enter personal information, that is used in turn to commit fraud using that consumer's details.

[9] A fully effective SMS Scam Filter requires anti-scam software to scan the content and location data of an SMS to identify potentially suspicious or malicious content (e.g., fraudulent URLs). Such an intervention requires a legislative basis.

[10] ComReg also notes that the Spanish Ministry of Economy, Commerce and Business launched a consultation in February of this year about a range of interventions similar to ComReg's and this includes consideration of replicating the Belgium and Poland scam filter precedents.

33. Consequently, and in order to address the SMS gap, ComReg will commence a separate consultation during the summer to consider the options available to it to address SMS scams and thereby protect Irish consumers.

34. Notwithstanding, there is of course no impediment to any mobile operator acting independently of ComReg and implementing an SMS Scam Filter lawfully by way of customer opt-in in if they choose.

Cost and benefits of the package of interventions

35. The relatively modest costs of the mandated interventions will primarily be borne by the telecoms operators that implement them. However, as some operators have readily acknowledged, interventions to curtail scam calls and texts should increase trust in those services, safeguarding operators' long run commercial interests, by being able to offer services and networks worthy of consumers' trust. As their continuing commitment to ComReg's NCIT confirms, operators are very aware of the damage fraudulent calls and texts can do to their business and reputation.

36. ComReg also notes that some operators have defended their recently announced annual price increases (second increase due in April 2024) based on generating revenues to finance investment in the upgrade of networks and services. It is inconceivable that such upgrades would not include measures to protect their customers from criminals who are committing fraud using the very same services provided over their networks.

37. Finally, ComReg notes that analysis conducted by Europe Economics shows that the overall benefit of the package of interventions proposed in 23/52 would be in the order of **€1.2 billion** over the next seven years[11]**.** In summary, the benefits to society for each euro spent on the interventions is substantial and highlights the importance of their early implementation. When combined, ComReg's package of interventions should bring **€55 euros in economic and social benefit for every €1 spent by operators securing their networks.**

Responses to ComReg Consultation 23/52

38. ComReg received thirty-one responses to Consultation 23/52. These responses spanned a wide range of commercial interests and experiences, again highlighting how widespread the impact of scam calls and texts are felt across the economy. These responses acknowledged the significant harm caused by nuisance communications and generally speaking offer support for

[11] This includes the benefits of the SMS Scam Filter.

the interventions. While ComReg remains of the view that each of the interventions are necessary, ComReg has made a number of modifications and clarifications in response to issues raised by respondents. These modifications should better ensure the more effective implementation of each of the interventions maximising the benefit to society.

Next Steps

39. ComReg will now put in place two main workstreams in order monitor implementation of the interventions and address any remaining gaps that scammers could exploit to target Irish consumers and businesses.

40. **First**, ComReg will reformulate the NCIT to primarily focus on the implementation of the Decision Instruments. The Decision Instruments published as part of this consultation have mandated a package of interventions with various deadlines for implementation. The work of the NCIT will now focus on implementing these interventions in line with the mandated timelines and in a manner that best ensures their most effective operation. To this end, an overarching Steering Group and two technical working groups will be established.

    - The Steering Group will primarily be responsible for ensuring the successful implementation of the interventions by the operators. In doing so, it will provide terms of reference and guidance to the two technical working groups who will report into the Steering Group from time to time, as matters arise, and on their overall implementation recommendations. The Steering Group will also consider more overarching matters concerning efforts to combat scam calls and texts.
    - There will be two separate technical working groups – a Voice Working Group and an SMS Working Group.
        - The Voice Working Group will primarily focus on the implementation of each of the Voice Interventions (e.g. Fixed and Mobile CLI and the Voice Firewall) by the operators. Industry will need to agree certain technical specifications regarding the implementation of the Voice Interventions and provide these to the Steering Group for consideration.
        - The SMS Working Group will, initially at least, focus on the implementation of the Sender ID Registry intervention. ComReg will first present a Design and Project Plan to industry for comment and discussion. This Working Group may also need to consider any interventions or measures that result from the SMS Scam Filter consultation that ComReg will publish during the summer.

41. Both Working Groups may also be asked by the Steering Group to consider other matters, from time to time, as they relate to scam calls and SMS to address any emerging or remaining gaps that scammers could exploit.

42. ComReg will publish an Information Notice soon after the publication of this response to consultation, setting out:

    - the details of the Steering Group and the Working Groups; and
    - how industry can participate in the work of the Steering Group and its Working Groups.

43. **Second**, and as noted earlier, ComReg will publish a consultation during the summer assessing the options available to it to address SMS scams and protect Irish consumers. This will include consideration of the potential to implement the SMS Scam Filter via an “Opt-In” process, which would not raise privacy concerns or require enabling legislation.

44. ComReg looks forward to the successful implementation of the package of interventions considered in this document.

Chapter 1

1 Introduction

1.1 Background

1.1 The purpose of this document is to set out the Commission for Communications Regulation's ("ComReg") response to Consultation 23/52, and the Decision Instruments concerning the Interventions, which telecommunications operators must implement to combat scam calls and texts.

1.2 In Consultation 23/52[12], ComReg set out its preliminary views on the package of interventions which it considered would best deal with the ongoing scourge of Nuisance Communications. ComReg formed these preliminary views in light of the relevant material before it, including, among other things, the report by Europe Economics (the "Europe Economics' Report" or ComReg 23/52a)[13] and the surveys conducted by B&A of Irish Consumers (the "B&A Consumer survey" or ComReg 23/52b)[14] and Businesses (the "B&A Business survey" or ComReg 23/52c)[15].

1.3 In Consultation 23/52, ComReg consulted on the Decision Instruments for each of its proposed interventions. ComReg also created a guidance document for each intervention, a Draft Functional Requirement, which provided operators with further information as to ComReg's views on the correct implementation and functioning of each intervention. For security reasons, the Draft Functional Requirements were only shared with relevant operators upon request.

1.4 Furthermore, Consultation 23/52 also consulted on the envisaged updates to the Numbering Conditions of Use and Application Process document ("Draft Updates to Numbering Conditions") in support of the proposed interventions, alongside an updated version of the Numbering Conditions (ComReg 23/52d)[16].

1.5 Consultation 23/52 was published on 16 June 2023 and invited views from

[12] Consultation 23/52, "*Combatting scam calls and texts Consultation on network based interventions to reduce the harm from Nuisance Communications*", 16 June 2023. Link
[13] Europe Economics Report "*Scam calls and texts in Ireland – costs and benefits of interventions*", 16 June 2023. Link
[14] ComReg 23/52b, Behavior & Attitudes "*Research on Nuisance Communications - Consumer*", 16 June 2023. Link
[15] ComReg 23/52c, Behavior & Attitudes "*Research on Nuisance Communications - Business*", 16 June 2023. Link
[16] ComReg 23/52d, "*Draft Numbering Conditions of Use and Application Process*", 16 June 2023. Link

interested parties on all aspects of this Consultation in the six-week period to 28 July 2023. Recognising the breadth of issues covered in this consultation, ComReg gave an additional two weeks over the normal four weeks identified in ComReg's Consultation Procedures[17].

1.2 IBEC Request and Consultation Extension

1.6 Four weeks after the publication of Consultation 23/52, ComReg received a request from the lobby and business representative group IBEC[18] (See Annex 1) for an extension of the 28 July deadline to the end of August 2023 – an additional four weeks, bringing the total duration of the consultation period to 10 weeks. IBEC also requested engagement from ComReg on questions that it would provide to ComReg.

1.7 Given the scope of the proposed interventions, ComReg considered it appropriate, on an exceptional basis, to provide an opportunity for interested parties to request clarification on any aspect of these interventions. Further, and in the interests of transparency and non-discrimination, ComReg provided the opportunity for all interested parties to submit Clarification Questions, and not just IBEC. On foot of IBEC's request, ComReg extended the deadline for its Consultation to 31 August 2023[19] and requested that interested parties submit any clarification questions they may have with regard to Consultation 23/52[20].

1.8 On 10 August, ComReg published the questions submitted by operators alongside ComReg's answers to same[21]. In total, ComReg provided responses to 32 questions submitted by interested parties.

1.3 Responses to Consultation 23/52

1.9 ComReg received 31 submissions from a wide variety of interested parties. Respondents are grouped as follows below for ease of reference.

[17] ComReg 11/34 "ComReg Consultation Procedures" 6 May 2011. Link
[18] Telecommunications Industry Ireland ("TII") are the IBEC representative body for the electronic communications industry in Ireland. Member companies are involved in broadband, broadcasting, cable, data centres, fixed, mobile, satellite and wireless internet as well as equipment manufacturers and network providers.
[19] ComReg Document 23/67, "*Extension of Consultation 23/52 (Consultation on combatting Nuisance Communications)*", 20 June 2023. Link
[20] ComReg made it clear that such questions were to be strictly limited to those requesting clarification on the matters discussed in the consultation (e.g., the proposed interventions and/or the associated updates to the Numbering Conditions). Any questions beyond this scope which, for example, related to the merits or otherwise of the proposed interventions and/or the updates of the Numbering Conditions would not be considered. ComReg made clear that such questions could only be considered as part of ComReg's formal response to submissions received on Consultation 23/52.
[21] ComReg Document 23/75, "*Clarification Questions and Answers on Consultation 23/52*", 10 August 2023. Link

- **Domestic ECS providers** - Eircom Limited ('Eir'), British Telecom ("BT"), Imagine, Tesco Mobile Ireland Limited ('Tesco'), Three Ireland (Hutchison) Limited ("Three"), Vodafone Ireland Limited ("Vodafone"), Viatel Ireland Limited ("Viatel"), Virgin Media Ireland Ltd ("Virgin") and Sky Ireland Limited ("Sky").

- **International ECS providers** - Magrathea, Microsoft, Twilio, Verizon and Voxbone.

- **Vendors** - Cellusys, Ericsson, Hiya, NetNumber, Openmind, Tanla and XConnect

- **Telecoms associations** - ALTO[22], IBEC, i3Forum[23] and Mobile Ecosystem Forum ("MEF")[24].

- **Financial Bodies** – Revolut, Bank of Ireland and Banking & Payments Federation Ireland ("BPFI")[25].

- **Other parties** - Commsrisk[26]; and two members of the public.

1.10 ComReg would like to thank all respondents for their submissions. ComReg notes that respondents are generally supportive of the preliminary views as set out in Consultation 23/52, with any incongruity centred in the main on certain points in relation to the implementation of the interventions.

1.11 ComReg has published the non-confidential versions of the submissions as ComReg Document 24/24s. Having carefully considered the submissions, the points made therein and other relevant information, this document, among other things, sets out ComReg's views in relation to the matters raised by both respondents. ComReg also provides its Regulatory Impact Assessments and Decisions.

1.12 ComReg has also published a response by Europe Economics to submissions to Consultation 23/52 which commented on their work and/or findings (the "Europe Economics Response") (24/24a).

1.13 In addition, ComReg has commissioned Plum Consulting ("Plum")[27] to

[22] ALTO is an association of national and international operators in the fixed, wireless, mobile and cable sectors.
[23] i3Forum is a trade association for international telecommunications service providers.
[24] MEF is a trade association for providers of mobile services such as messaging, content, advertising and IoT.
[25] BPFI is a trade association for banking and payments service providers in Ireland.
[26] Commsrisk is a website that reports on, among other things, the risks faced by electronic communications providers and their customers. Commsrisk is affiliated with Risk & Assurance Group (RAG) a nonprofit association that provides free information, advice and events for communications risk and assurance professionals.
[27] Plum is a leading independent consulting firm, focused on the telecommunications, media, technology, and adjacent sectors.

produce a report on the implementation timelines for each of the interventions (the "Plum Report") (24/24b). Plum was tasked with assessing the appropriateness of the timelines proposed by ComReg in Consultation 23/52, in light of the submissions received. In providing its advice Plum considered Consultation 23/52 and the responses to same, and other relevant factors, including:

- the resources that would be required and capability of operators to implement the proposed interventions.
- the views of respondents to Consultation 23/52 on the timelines;
- the implementation of equivalent or similar interventions in other jurisdictions.
- the need for operators to implement some interventions simultaneously using the same or equivalent resources.
- the views of external service providers (e.g., vendors) on the resources and time required to implement the proposed interventions.

1.4 Update since publication of Consultation 23/52

1.14 In this Section, ComReg provides an update on relevant information since the publication of Consultation 23/52 under the following headings:

1. The recent work of the NCIT[28] and ComReg.
2. Legislation required to support a SMS Scam Filter.
3. ComReg's on-going engagement with other NRAs.

1.4.1 The recent work of NCIT and ComReg

1.15 In its Electronic Communications Strategy Statement for 2023 to 2025 (Document 23/34)[29], ComReg set out its intention to undertake a number of tasks in relation to the work of NCIT including:

> "◉ *delivering on agreed* [NCIT] *member's implementation roadmaps to ensure that the interventions are implemented by the appropriate network and/or service providers as quickly as possible;*

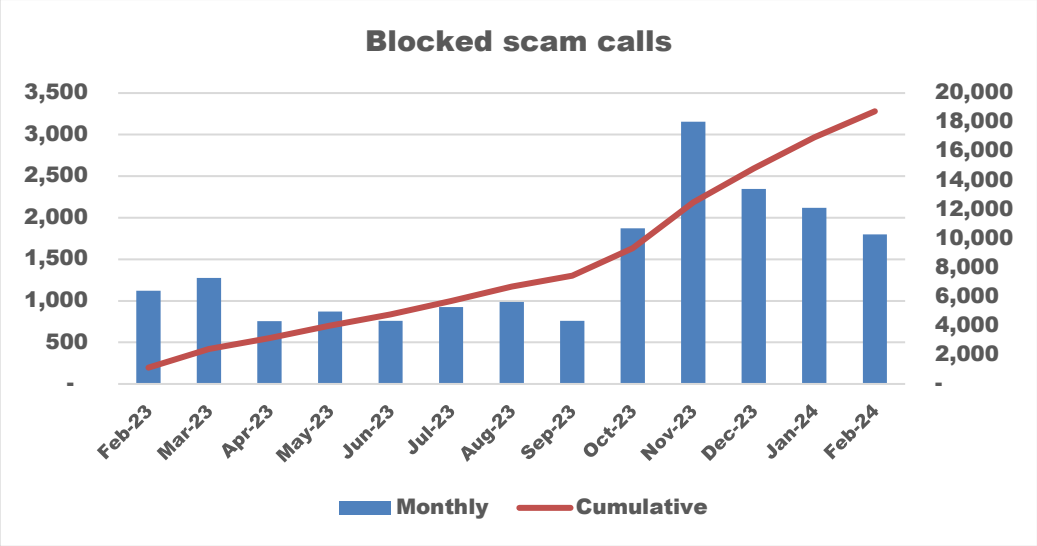
[28] On 17 December 2021, and to address nuisance communications, ComReg established the Nuisance Communications Industry Taskforce, to bring together representatives of the electronic communications industry. See ComReg documents 21/129, 22/77 and 23/12 at www.comreg.ie for further information.
[29] ComReg Document 23/34, "*Electronic Communications Strategy Statement 2023 – 2025*", 13 April 2023 Link.

providing metrics as per agreed technical specifications and in line with the expected timelines of the deliverable of the taskforce."

1.16 ComReg wishes to acknowledge the valuable contribution of members of the NCIT to date[30]. This has been fundamental to developing the NCIT interventions, and the subsequent implementation of certain of those interventions by some NCIT members. This work continues and the NCIT has met on 26 occasions to date.

1.17 The work of the NCIT members has begun to have an impact with the monthly number of scam calls blocked noticeably increasing in recent months as more operators implement the DNO, PN and Fixed CLI Call Blocking (see Figure 1 below). Participating operators report having blocked approximately 18 million scam calls in 2023[31].

Figure 1: Scam calls and texts blocked by Irish telecommunication operators, February 2023-2024



Source: Blocked scam calls reported by operators.

1.4.2 Legislation required to support a SMS Scam Filter

1.18 In Consultation 23/52, ComReg noted that a SMS Scam Filter could be implemented in a number of ways, including.

- All mobile consumers by default ("All-In");

[30] ComReg is grateful for the continuing and active support of Minister Ossian Smyth, Minister of State at the Department of Public Expenditure and Reform, and the Department of the Environment, Climate and Communications in this endeavour.
[31] For reference, Europe Economics estimated that Irish consumer received over 59 million calls in 2022.

- All mobile consumers, except where the consumer wishes not to avail of the service (i.e., the consumer may "Opt-out"). This could, for example, include automatic enrolment, wherein a notification SMS would be sent to mobile users, with an opt-out option at the end stating e.g., "Send STOP to unsubscribe".

- All mobile consumers that indicate their wish to avail of the service (i.e., the consumer may "Opt-In"). This could, for example, be achieved by a notification SMS offering the service being sent to mobile users, with an Opt-In option at the end stating e.g., "Reply 'YES' to subscribe".[32]

1.19 The draft 'Scam Filter' Regulatory Impact Assessment ("RIA") was framed on the basis that all consumers would benefit from the SMS Scam Filter (i.e., the "All-In" approach). This approach would likely maximise the net benefit of the SMS Scam Filter in terms of combatting scams through increasing the number of subscribers covered and reducing the cost and complexity of implementation for the relevant operators. An important finding of the Europe Economics Report was that the SMS Scam Filter alone could account for up to €500 Million in benefit from the proposed package of interventions, driven mainly by its ability to cover all inbound SMS and dynamically adapt to scammers changing tactics.

1.20 However, ComReg also noted that there were legal impediments to this approach, noting that the imposition of the SMS Scam Filter as an "All-In" or an "Opt-Out" introduces potential legal issues on the protections of end user rights in relation to interception and data protection as provided in the ePrivacy Directive[33] and the General Data Protection Regulation ("GDPR")[34]. It is ComReg's understanding that a change to the current legislation to allow for the SMS Scam Filter is necessary.

1.21 Consequently, ComReg has engaged with its parent department, the DECC[35] with a view to providing such a legislative amendment in line with laws passed in other EU member states to enable SMS Scam Filters (e.g., Belgium[36] and Poland[37]). Furthermore, the Spanish Ministry of Economy, Commerce and Business launched a consultation in February of this year about a range of interventions similar to ComReg's which also includes consideration of replicating the Belgium and Poland scam filter precedents.

[32] For a description of SMS Opt-in in a different context, see this explained from Twilio, an international SMS aggregator: Opt-In and Opt-Out Text Messages: Definition, Examples, and Guidelines (twilio.com).
[33] This 2002 ePrivacy Directive is an legal instrument for privacy in the digital age, and more specifically the confidentiality of communications. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058
[34] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[35] Indeed, ComReg is entirely dependent on a Government Department to progress this matter.
[36] Justel: 2005-06-13/32 (fgov.be)
[37] USTAWA z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (sejm.gov.pl)

1.22 Such legislation would enable ComReg to meaningfully consult on implementing a SMS Scam Filter via an "All-In" approach, to maximise the benefits to consumers. At the time of publication, and notwithstanding continuing engagement with the DECC[38], there is as yet no confirmation that legislation to support the SMS Scam Filter will be introduced and consequently it is not listed in the current legislative programme.

1.23 As ComReg cannot proceed with the SMS Scam Filter intervention based on legislation at this time, it will instead publish a consultation during the summer assessing the options available to it to address SMS scams and protect Irish consumers. This will include consideration of the potential to implement the SMS Scam Filter via an "Opt-In" process, which would not raise privacy concerns or require enabling legislation.

1.24 There is of course no impediment to any mobile operator acting independently of ComReg and implementing an SMS Scam Filter lawfully by way of customer opt-in in if they choose. Any Irish mobile operator that was to implement a SMS Scam Filter via an Opt-in process of their own accord, would clearly demonstrate their commitment to combatting the harm of scam texts and protecting their customers.

1.25 Although such alternatives may appear sub-optimal from a harm-mitigation perspective by comparison with the legislative enabled approach, ComReg must nevertheless ensure that telephone numbers are not misused and thus cannot countenance a situation where consumers continue to be so egregiously harmed. Trust in telephone numbers and the ubiquitous messaging services that relies upon them is being lost to the detriment of consumers, businesses, important public sector services such as health and taxation and telecommunications service providers themselves.

1.4.3 ComReg's contribution to global efforts to combat scams and engagement with other NRAs.

1.26 In its Electronic Communications Strategy Statement for 2023 to 2025, ComReg set out its intention to undertake a number of tasks in relation to nuisance communications to, among other things:

> "◉ *contributing to international regulatory initiatives to promote an international approach, as appropriate."*

1.27 Nuisance Communications is a global scourge which is not unique to Ireland. Many other countries have experienced similar increases in scam calls and

[38] ComReg continues to engage with DECC on this matter.

texts since 2021[39]. Unsurprisingly, an increasing number of National Regulatory Authorities ("NRAs") are now taking action to combat scams, using a variety of interventions. This reinforces the importance of Ireland implementing its own interventions without delay as scammers will likely switch away from countries with higher defences, as Europe Economics note, in favour of those that are more facilitative of criminal activity. Clearly, any country that does not match its neighbours' defences risks becoming an even greater target itself.

1.28 NRAs can learn from each other's work in combatting scam calls and there is therefore an opportunity for NRAs to collaborate to better protect their citizens from fraudsters. Through close cooperation, NRAs can assess the effectiveness of interventions introduced in other jurisdictions and adjust as needed to improve outcomes for consumers. For example, ComReg has closely followed the work of policymakers in Belgium and Poland who have enacted legislation to enable a SMS Scam Filter and Spain which seems primed to follow, and also those in the UK and Germany who have implemented same under existing legislation, an option not open to Ireland.

1.29 ComReg has also engaged with NRAs in Finland and Singapore pioneering the use of full SMS Sender ID Registry and the Mobile CLI Call Blocking using roamer check. ComReg also enjoys close working relationships with other English speaking countries including Australia, Canada, New Zealand and the United States.

Table 1: Regulators that ComReg has held meetings with to discuss combatting scams

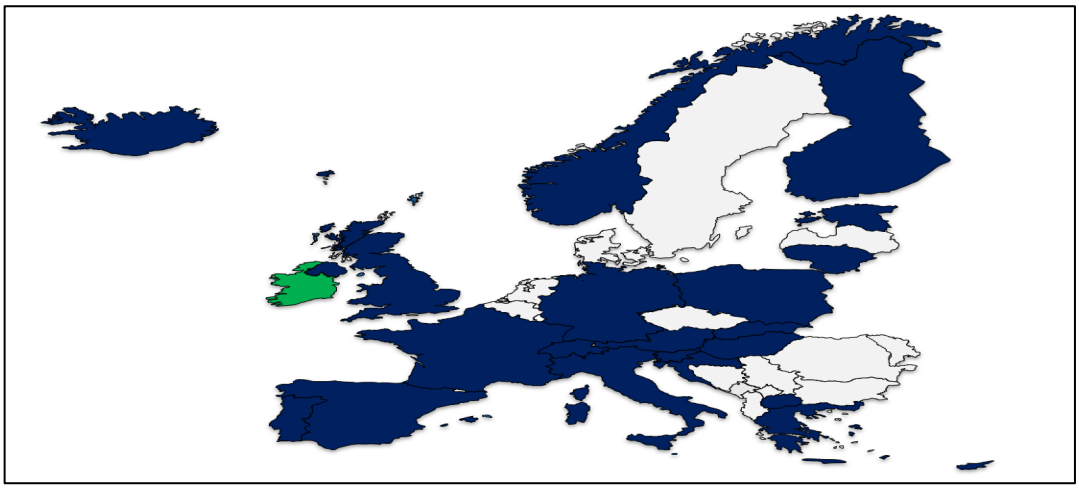
Country	Regulator
Australia	Australian Communications and Media Authority ("ACMA")
Belgian	Belgian Institute for Postal services & Telecommunications ("BIPT")
Canada	Canadian Radio-Television & Telecommunications Commission ("CRTC")
Finland	Transport and Communications Agency ("Traficom")
Germany	Bundesnetzagentur ("BnetzA")
Iceland	Fjarskiptastofa
Italy	Autorita per le Garanzie nelle Comunicazioni ("AGCOM")
Spain	Ministry of Digital
Singapore	Infocomm Media Development Authority ("IMDA")
UK	The Office of Communications ("OFCOM").
USA	Federal Communications Commission ("FCC")

[39] See Figure 13 in ComReg 23/52.

1.30 Furthermore, ComReg has issued a number of questionnaires, or Requests for Information ("RFI"), to members of the Independent Regulatory Group ("IRG")[40] (the "IRG RFIs"), to record, compile and distribute the latest information on what interventions other European jurisdictions are implementing or considering to implement to deal with this serious issue.

1.31 In total, between bilateral meetings and the IRG RFIs, ComReg has engaged with the communication regulator or relevant government department of 24 other European countries.

Figure 2: European NRAs that ComReg has engaged with.



1.32 Moreover, since the publication of Consultation 23/52, ComReg has communicated its findings to other NRAs, both in bilateral meetings and by presenting its findings and proposed approach in various international regulatory fora, such as the IRG. There are early indications that other NRAs are converging on a suite of preferred interventions[41], essentially those that ComReg proposed in Consultation 23/52. Since June of last year, a number of other NRAs have announced plans to examine or implement some of the newer or more novel interventions that ComReg included as part of its Proposed Package. This includes:

[40] The IRG was established in 1997 as a group of NRAs to share experiences and points of views among its members on important issues relating to the regulation and development of the European telecommunications market.
[41] Noting that many NRAs may not actively combat scams or may have had no less need to intervene as their MNOs may have taken action.

- **Fixed and/or Mobile CLI Call Blocking** – UK[42], Spain[43], [✂ ✂][44], [✂ ✂][45], [✂ ✂][46], Lithuania[47], Malta[48]
- **Voice Firewall** – India.[49]
- **SMS Sender Registry** – Denmark[50], Australia[51], Hong Kong[52], Spain, Finland[53].
- **SMS Scam Filter** – [✂ ✂][54], Spain, Lithuania, Poland[55]

1.33 Inter-agency cooperation to combat scams will constitute an on-going area of ComReg's international work, given the potential benefits from NRAs cooperating to develop "best-practice" and the inherent dynamism required to fight scammers with maximal effectiveness. After all, what constitutes "best-practice" will necessarily evolve over time as fraudsters adapt to the actions of NRAs implement. As outlined in Annex 1, this is a very specific and lucrative type of crime, and so fraudsters have a strong incentive not to give up and a proven record of identifying and exploiting new and emerging vulnerabilities in ECS.

1.34 In that regard, ComReg is in the process of entering into a number of Memorandum of Understanding with other NRAs. These MoUs formalise the existing and ongoing collaboration between ComReg and other NRAs, with whom we will continue to work with, both bilaterally, and in other international groups.

1.35 Through these MoUs ComReg hopes to enhance cooperation and mutual information exchanges in areas such as regulatory frameworks and technical and policy solutions related to nuisance communications in Ireland and these

[42] Ofcom recently announce it would begin blocking calls from outside the UK bearing UK mobile and fixed presentation CLIs. Ofcom, 2024. "*Consultation: Tackling scam calls – expecting providers to block more calls with spoofed numbers*." Link
[43] Ministerio de Economía, Comercio y Empresa "Consulta Pública sobre iniciativas normativas y mecanismos técnicos y operativos para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos" Link
[44] IRG RFI. The country is redacted as this has not been published or finalised.
[45] IRG RFI. The country is redacted as this has not been published or finalised.
[46] IRG RFI. The country is redacted as this has not been published or finalised.
[47] the RRT resolution was adopted in July 2023 No. TN-347 (https://www.e-tar.lt/portal/lt/legalAct/37d1cd002c7b11ee9de9e7e0fd363afc)
[48] Consultation paper on preventative measures to mitigate CLI Spoofing and vishing scams (mca.org.mt)
[49] TRAI website TRAI issues Direction for deploying Artificial Intelligence and Machine Learning based UCC Detect system under TCCCPR, 2018 | Telecom Regulatory Authority of India
[50] Denmark to Introduce SMS Sender ID Registration to Counter Smishing | Commsrisk
[51] The SMS Sender ID Registry | ACMA
[52] Office of the Communications Authority - Short Message Service (SMS) Sender Registration Scheme (ofca.gov.hk)
[53] https://www.telecompaper.com/news/traficom-invites-organisations-to-apply-for-sms-sender-id-verification-to-avoid-scams--1481969
[54] This information was provided ComReg but treated as confidential as it relates to potential legal proceedings.
[55] https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm

countries. This inter-agency cooperation will prove invaluable to ComReg in fighting scammers targeting Irish consumers and businesses.

1.5 Overview of planned work

1.36 For the benefit of interested parties, ComReg provides some further information below on its envisaged workstreams. In particular, ComReg provides information on the following headings:

- The future of the NCIT; and
- The Scam SMS Consultation.

1.5.1 The future of the NCIT

1.37 Following the publication of the Decision Instruments, the focus of the work of ComReg and industry will shift primarily to implementing all of the Interventions by operators. This will require an even greater focus on the practical implementation of the interventions by operators, not least in light of the additional interventions and the need for operators to coordinate on certain interventions.

1.38 Therefore, while the NCIT in its current form has served its purpose well to this point, it now needs to reflect the current state of progress so as to facilitate more detailed discussion of matters by the relevant technical experts including developing the Functional Specifications for each intervention. The Functional Requirements documents will provide operators with Guidance as to the effective implementation of the Interventions, codifying the approach that operators should take to fulfil the Decision Instruments.

1.39 ComReg will reformulate the NCIT to primarily focus on the implementation of the Decision Instruments. The Decision Instruments published as part of this consultation have mandated a package of interventions with various deadlines for implementation. The work of the NCIT will now shift to implementing these interventions in line with the mandated timelines and in a manner that best ensures the most effective operation of same. To this end, an overarching Steering Group and two technical working groups will be established.

- The Steering Group will primarily be responsible for ensuring the successful implementation of the interventions by the operators. In doing so, it will provide terms of reference and guidance to the two technical working groups who will report into the Steering Group from time to time, as matters arise, and on their overall implementation recommendations. The Steering Group will also consider more general matters concerning efforts to combat scam calls and texts.

- There will be two separate technical working groups – a Voice Working Group and an SMS Working Group.
    - The Voice Working Group will primarily focus on the implementation of each of the Voice Interventions (e.g. Fixed and Mobile CLI and the Voice Firewall) by the operators. Industry will need to agree certain technical specifications regarding the implementation of the Voice Interventions and provide these to the Steering Group for consideration.
    - The SMS Working Group will, initially at least, focus on the implementation of the Sender ID Registry intervention. ComReg will first present a Design and Project Plan to Industry for comment and discussion. This Working Group may also need to consider any interventions or measures that result from the SMS Scam Filter consultation which ComReg will commence during the summer.

1.40 Both Working Groups may also be asked by the Steering Group to consider other matters, from time to time, as they relate to scam calls and SMS to address any emerging or remaining gaps that scammers could exploit.

1.41 ComReg will publish an Information Notice soon after the publication of this response to consultation, setting out:

- the details of the Steering Group and the Working Groups; and
- how industry can participate in the work of the Steering Group and its Working Groups.

1.5.2 Scam SMS Consultation

1.42 ComReg is planning to publish a separate consultation on the SMS Scam issue later this year. ComReg must endeavour to meet with its obligations to ensure the efficient use of telephone numbers and avoid their misuse, being cognisant of the SMS gap and the continued harm being experienced by telecommunications consumers. This consultation would examine all potential solutions that are available, even in the absence of Scam Filter legislation, including an “Opt-In” Scam Filter which would involve consumers permitting operators to filter their text messages for scam texts.

1.6 Structure of this document

1.43 Submissions received on the Draft RIAs and Draft Decision Instruments (“Draft DIs”), Draft Functional Requirements and Draft Updates to the Numbering Conditions are each considered in separate Chapters. With that in mind, this document is structured in the following way:

- **Chapter 2** – Provides ComReg's response to submissions received on each of the Draft RIAs and Draft Decision Instruments.
- **Chapter 3** – Provides ComReg's response to submissions on the Draft Functional Requirements.
- **Chapter 4** – Provides ComReg's response on submissions to Draft Updates to the Number Conditions.
- **Chapter 5** – Provides ComReg's response on submissions on Know Your Customer (KYC).
- **Chapter 6** – Provides the updated and final Regulatory Impact Assessments.
- **Chapter 7** – Provides the updated Number Conditions.
- **Chapter 8** – Decision Instruments.
- **Annex 1** – Basic background on Nuisance Communications.
- **Annex 2** – Econometric analysis on victims of fraud.
- **Annex 3** – Provides information on ComReg's Legal Framework and Statutory Objectives.
- **Annex 4** – Glossary of Terms.

Chapter 2

2 Response to submissions on Draft Decision Instruments and Draft RIAs

2.1 In this chapter, ComReg considers the submissions on the draft RIAs and draft DIs as described in Chapter 5 and Chapter 7 of Consultation 23/52. ComReg then sets out its final position on the Proposed Package in light of the responses to Consultation 23/52 and other relevant material before it, including the views of Europe Economics in response to relevant submissions on Consultation 23/52 and the Plum Report.

2.2 While most submissions relate to individual interventions a number relate to either the proposed package of interventions ("Proposed Package") in their entirety or their shared economic analysis. For simplicity, ComReg assesses these submissions separately to those on individual interventions. Similarly, ComReg has grouped DNO, PN and Fixed CLI Call Blocking together, given the overlap between the comments received with regard to these particular interventions.

2.3 Accordingly, the views of respondents are grouped under the following headings, with the relevant references to Consultation 23/52 in brackets:

- The Proposed Package and overall approach (pages 193-197, 253-291);
- The economic analysis in the Draft RIAs (pages 193-197, 253-291);
- DNO, PN and Fixed CLI Call Blocking (pages 96-136, 253-265);
- Mobile CLI Call Blocking (pages 113-136, 265-270);
- Voice Firewall (pages 137-150, 271-275);
- SMS Sender ID Registry (pages 151-176, 276-281); and
- Alternative Interventions (pages 67-95).

2.1 Assessment of the submissions

2.1.1 The Proposed Package and overall approach.

Summary of ComReg's views in Consultation 23/52

2.4 In Consultation 23/52, ComReg proposed a package of Voice and SMS

interventions which it considered would best deal with the ongoing scourge of scam calls and texts. ComReg was of the preliminary view that the Proposed Package would most reduce and mitigate the harm caused by scam calls and texts, noting that scammers will persistently try to circumvent any interventions upon introduction.

2.5 These interventions are summarised in Section 6.2.2 (see Chapter 6).

View of respondents to Consultation 23/52

2.6 The views of respondents regarding the Proposed Package are summarised and then assessed by ComReg under the following headings.

- Support for the Proposed Package;
- The importance of network-based interventions;
- The need for regulation and enforcement;
- Further consultation on non-NCIT interventions;
- Implementation timelines;
- Blocking - the need for metrics;
- Blocking – inadvertent blocking (false positives);
- Blocking – the use of presentation CLIs;
- Periodic review;
- Alternative technologies; and
- Other issues.

Support for the Proposed Package

2.7 Ericsson, i3Forum, XConnect, the BPFI and CommsRisk expressed support for ComReg's Proposed Package in its entirety.

2.8 BPFI contends that ComReg's Proposed Package is of national importance in preventing scams and provides an important building block for the future of a national economic crime strategy in Ireland.

2.9 Commsrisk commends ComReg for the thorough research that has gone into developing an action plan to protect consumers from scam voice calls and SMS messages. In Commsrisk's view, ComReg distilled its research into the most sensible, cost-effective and actionable plan for tackling scam calls and messages of any national regulator.

The importance of Network Based interventions.

2.10 Ericsson agrees with ComReg's preliminary view that network-based interventions are more effective than those that require the use of a mobile application. Ericsson is of the view that solutions that do not rely on any action on the part of the consumer will result in a significantly higher success rate in blocking scam calls. Ericsson also contends that it is important that the solutions are capable of blocking scam calls on the widest range of devices, particularly those that might not be capable of hosting apps or downloading the device vendor's latest operating system.

2.11 Hiya, a leading provider of anti-scam solutions[56], which provides both app and network solutions, agrees with ComReg that there are critical limits on the effectiveness of app-based interventions.

The need for regulation and enforcement

2.12 ALTO welcomes appropriate regulation to enable these innovations to occur on a proportionate level.

2.13 Eir agrees that it is appropriate to codify the network interventions in order to ensure consistent implementation across Irish operators.

2.14 BT welcomes regulation and notes that absent same the investment of any operator could be 'totally wasted' were other operators not to reciprocate.

2.15 Relatedly, i3Forum observes that the effectiveness of any intervention is dependent on its enforcement.

2.16 i3forum opines that the different approaches being adopted by NRAs across the world creates confusion and allow loopholes to develop, allowing opportunities for future exploitation. i3forum contends that differences in the level of anti-scam defences between countries can create a "whack-a-mole" phenomenon, where scammers react to interventions by switching to target a different country.

2.17 Imagine agrees on the need for interventions but is concerned that operators could be viewed as being 'responsible' or 'negligent' for unfavourable outcomes.

2.18 Cellusys contends that Irish companies and individuals have been at the forefront of "*analysing and controlling signalling in telecommunications networks—the means to address the problem in hand*" and that it is disappointing that operators of local telecommunications networks have not

[56] Hiya provides both network and app based interventions to block scam calls.

been convinced to act to protect their customers from nuisance communications.

Further consultation on non-NCIT interventions

2.19 IBEC, Tesco and Virgin each opine that the interventions that are not "*NCIT interventions*" require industry engagement prior to implementation. Similarly, both Vodafone and Virgin contend that ComReg should evaluate the impact of the static measures before implementing any dynamic interventions. Vodafone is further of the view that ComReg should not impose additional measures above those proposed by the NCIT. Three and Eir both maintain that the Voice Firewall should not be implemented at this time but rather following a further consultation or industry engagement on a Voice Firewall held at some unspecified future date.

Implementation Timelines

2.20 IBEC contends that the number of interventions and timelines for implementation pose a difficulty for operators. Eir is of the view that what it terms the non-NCIT interventions are not sufficiently scoped to inform implementation timelines, and that the timelines are challenging for operators which have not yet started implementing interventions (e.g., non-NCIT members). Vodafone opines that ComReg should take account of what it terms *actual timelines* communicated via the NCIT and bilateral meetings when setting any formal Decision.

2.21 IBEC, Vodafone and Virgin each submit that ComReg should ensure that all proposed interventions are fully compliant with existing data protection law to ensure that each intervention can be implemented in a timely manner.

2.22 IBEC, Tesco Mobile, Three and Eir each contend that ComReg should also consider the regulatory burden of all regulatory initiatives on operators over the period of implementation.

Blocking – the need for metrics

2.23 Verizon and ALTO opine that ComReg should only seek metrics on a voluntary basis and that, in their view, it would be disproportionate to require operators with legacy infrastructure, which are unable to report blocking metrics, to make investments to provide metrics.

Blocking – inadvertent blocking (false positives)

2.24 Twilio maintains that it is essential for ComReg to acknowledge and address the risk of false positives in any formal regulatory measures and/or the technical and governance arrangements. Twilio further contends that an

agreed efficient process must be in place to address the situation where blocking proves to be unjustified or accidentally impedes a legitimate use case, in order to provide for blocking to be undone immediately. Twilio opines that ComReg should seek harmonisation with other jurisdictions in its approach to blocking.

2.25 Microsoft expresses its concern that the CLI Blocking DIs will block voice traffic that uses CLI spoofing[57] for what it terms legitimate purposes. Microsoft suggests that solutions should be designed to prevent illegitimate calls while allowing legitimate ones. Microsoft provides a number of examples of what it considers to be legitimate traffic which it believes may be at risk of being blocked, including:

- Cloud-based conferencing, where a call may originate and terminate in Ireland but transit internationally (e.g., leave and re-enter Ireland).
- One-way VoIP-to-PSTN calling services like "Skype to Phone", where users may assign their own number to their outbound calls.
- Where a general business CLI is applied to all individual's calls.
- Temporary assigned numbers, such as those used by ride-share apps.
- Local company numbers from global call centres.

2.26 Specifically, with regard to voice firewalls, Twilio and Microsoft both suggest that the procedures to enable unblocking need to be agreed and trialled prior to implementation.

2.27 Mr. Joseph Sheerin requests that interventions should not block legitimate traffic and verified IDs on VoIP services based outside Ireland.

Blocking – the use of presentation CLIs

2.28 Microsoft contends that ComReg should require operators applying the CLI Call Blocking interventions to block on the basis of the network CLI[58] and not the presentation CLI[59]. In this regard, Microsoft suggests that ComReg should adopt the approach taken in the UK by Ofcom in its Guidelines on CLI Call Blocking interventions. According to Microsoft, these permit operators to block on the basis of network CLI. Microsoft states that its next preferred approach is that operators are required to label international calls with domestic CLIs

[57] CLI spoofing refers to where the CLI has been faked by a fraudster and appears to be a call from a genuine number or business. In effect, it appears that an incoming call is coming from a local number that is already known and trusted to the receiver.
[58] While the presentation CLI and network CLI have equivalent SIP terms, the consultation will use the terms presentation and network CLI throughout.
[59] The presentation CLI enables a called party to view the calling party's number before answer and, if needed, use that CLI information to make a call-back.

"Anonymous", as it contends, is the case in Germany.

Periodic review

2.29 Eir submits that ComReg should periodically review the effectiveness of the technical interventions and that this should be specified in the Decision Instruments. In Eir's view, such reviews should be conducted every three years and ComReg should also allow for an ad hoc review at the request of the NCIT.

Alternative technologies

2.30 Tanla[60] opines that a Distributed Ledger Token (DLT) based network platform could, in theory, be used to apply DNO and PN, while also enabling call blocking interventions.

2.31 Cellusys maintains that a signalling-based firewall can incorporate DNO and PN, potentially via an API.

2.32 Ericsson states that a Voice Firewall can incorporate the static measures as part of its functionality. Similarly, Tanla and Cellusys claim that their respective technologies can implement SMS interventions, with Cellusys stating that a signalling-based firewall can incorporate both a Sender ID registry and SMS Scam Filter when accompanied by a blacklist and whitelist for Uniform Resource Locators (URLs) respectively.

Other issues

2.33 Revolut submits that, in its view, liability should lie with firms which are responsible for fraud, noting that some frauds occur as a result of scam calls and texts and may bypass financial institutions. Similarly, BPFI notes that scam calls and texts are upstream of the payment fraud that its members face, as by the time a consumer is making a payment, they have already been contacted and conned by the scammer.

2.34 Eir opines that the State should establish a fund to compensate it and other operators for any costs incurred while implementing the measures mandated by ComReg.

2.35 Tesco contends that Consultation 23/52 laid the blame on telecoms operators in relation to scams, which took off during the Covid-19 pandemic when operators were focussed on keeping consumers connected.

[60] Tanla Platforms Limited aims to facilitate streamlined and effective communication between enterprises and their clientele using channels like SMS, voice, email, Rich Communication Services (RCS), and OTT platforms like WhatsApp and FB Messenger, among others. See https://www.tanla.com/aboutus.html.

Views of Consultants

Europe Economics

The importance of network-based interventions

2.36 Europe Economics agrees with the view of Hiya that network based interventions are likely superior to app-based interventions, given the need for consumers to download apps, noting that:

> *"common sense and learnings from behavioural economics imply that solutions that do not rely on consumers' actions are indeed likely to be more effective. We agree with the experience of the operators that offer both network and app-based interventions and who thus are well-positioned to comment."*[61]

Plum

Implementation Timelines

2.37 As noted in Section 1.1, ComReg commissioned Plum to evaluate the appropriateness and proportionality of the timelines for the interventions. In summary, Plum found that the:

- Overall timeline for each individual intervention is appropriate;
- The time for the actions required to enable the overall timelines are appropriate; and
- The combined impact of multiple interventions for each intervention is not overly burdensome.

ComReg's assessment

Support for the entire Proposed Package.

2.38 ComReg acknowledges the support of Ericsson, i3Forum, XConnect, the BPFI and CommsRisk for the Proposed Package.

The importance of network-based interventions.

2.39 ComReg agrees with respondents' views on the preference for Network Based interventions over app-based solutions.

2.40 In particular, ComReg agrees that there are limits on the effectiveness of app-

[61] ComReg 24/24a, Europe Economics Response, page 4.

based solutions. Fundamentally, the scams from calls and texts (which are services operators provide to their consumers) originate through an operators' network but the use of Over-The-Top ("OTT") applications would place the burden of securing such services on consumers. Further, the use of app-based solutions would also lead to sub-optimal and asymmetric outcomes. For example:

- App-based solutions rely on consumers taking actions in terms of installing and/or paying for an OTT application that acts as a filter on scam calls and texts. While some consumers may decide to use app-based solutions, the current experience is that the vast majority of consumers do not and may not even be aware that such options are available. Importantly, the use of such solutions alone would do nothing to prevent the continuation of scams originating on an operator's network, with the app- based solution offering a solitary line of defence against such a proliferation.

- The effectiveness of different app solutions would likely vary across each operators chosen vendor. There are various app-based solutions available and the effectiveness of each is likely to vary depending on the filtering approach used by each vendor/operator. This would likely lead to a different consumer experience of scams – indeed even customers on the same network could experience scams in different ways, depending on the app being used.

- App-based solutions may not be available to all consumers depending on the device currently used, resulting in a lower level of protection overall. Feature phones[62] or older devices (typically owned by older persons) are unlikely to be able to support certain app-based solutions.

2.41 In summary, the use of app-based solutions would likely result in large sections of society continuing to be impacted by scam calls and texts, thereby providing scammers with incentives to continue targeting Ireland with scams. Alternatively, network-based interventions apply to all consumers from the date of implementation and do not require consumers to take any actions (e.g., installing apps).

2.42 Further, they provide the same high level of protection to all consumers regardless of their device, noting that any updates to the intervention (e.g., voice firewalls) would be undertaken at network level. Network-based interventions also ensure that operators are in control of the solutions that are

[62] Typically, a feature phone is a mobile phone that can complete basic functions but does not have all of the capabilities of a smartphone. These phones are usually created with cost-savings in mind and as a result, traditionally have buttons and a smaller display, but some have location capabilities and internet access.

designed to block or modify services provided to their consumers (which may not be the case under an app-based solution(s)).

The need for regulation and enforcement

2.43 ComReg agrees with the views of respondents that regulation is required to underpin the Proposed Package. ComReg considers that the publication of the Decision Instruments contained within this paper should enable operators to begin to implement the interventions with immediate effect. Furthermore, ComReg will monitor the implementation and operation of the interventions to ensure their effectiveness in combatting scams.[63]

2.44 ComReg agrees with i3forum that international coordination can help fight scammers. As noted in Section 1.4.3, ComReg has engaged with many international regulators to share our respective learnings on the potential interventions to combat scams. Ultimately, ComReg has responsibility for misuse of Irish numbers, and will take all necessary and proportionate actions to prevent their misuse. The need to act to protect Irish consumers from scams, is enhanced by the "*whack-a-mole*" problem described by i3forum, especially as an increasing number of NRAs are taking action to combat scams.

2.45 ComReg agrees with i3forum that international coordination can help fight scammers. ComReg has interacted with many international regulators to share our respective learnings on the potential interventions to combat scams and to improve the implementation of the proposed interventions. For example, ComReg has engaged extensively with the Singaporean regulator, the IMDA, with a view to better ensuring the smooth implementation of the Sender ID Registry, including the inclusion of "*Likely Scam*" SMS to diminish the rate of potentially valid SMS being blocked.

2.46 In relation to i3forum's view that there is a need for a "*whack-a-mole*" approach, ComReg agrees that any package of interventions must be cognisant of the ability of fraudsters to readily switch across scams, technologies, and territories. ComReg has specifically designed the package of interventions to reduce the risk of fraudster moving across technologies and scams in response to one or more interventions. Each intervention has in mind targeting the activities of fraudsters which are not covered by other interventions. In this way, ComReg can best reduce the harm caused to consumers and businesses.

2.47 More generally, ComReg notes the obligations on operators, under the

[63] This may include initiating enforcement which could result in the use of administrative fining powers under the Act of 2023 (which could involve a fine of up to €5 million or 10% annual turnover of the undertaking concerned).

Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 Under Part 2 Section 6. (1): "*Providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services*." Where 'security of networks and services' is defined as: "*the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services*." In particular, the implementation of network based interventions by the ECS/ECN is to mitigate compromises to the authenticity of the ECS/ECN.

Further consultation on non-NCIT interventions

2.48 In response to submissions that ComReg should hold a separate consultation on what is termed non-NCIT interventions (e.g., the Voice Firewall, roamer check, SMS Scam Filter), or that ComReg should fully evaluate the impacts of the NCIT interventions before moving forward, it is concerning that operators appear happy to implement a 'wait and see' approach when it is abundantly clear that the static interventions of themselves can only target a subset of scam calls. Therefore, such an approach would inevitably lead to consumers unnecessarily receiving scams from sources that ComReg identified previously (e.g., in Paragraph 5.152 of Consultation 23/52).

2.49 There is no reason to delay the implementation of the Voice Firewall or to consult separately on it. ComReg has already demonstrated that the Voice Firewall is an effective means of targeting such scam calls and respondents have not provided any reason why such an intervention would be ineffective. ComReg has assessed all submissions in relation to Consultation 23/52 and is satisfied that is has sufficiently consulted on these interventions. ComReg notes that the more detailed implementation issues can be taken forward in the relevant NCIT working group.

Implementation Timelines

2.50 In relation to concerns regarding the implementation timelines, it should be noted that ComReg did indeed consider the need for overlapping resources in Consultation 23/52. For example, ComReg was of the preliminary view that Voice Firewalls could be implemented within one year of any final decision but nonetheless provided an additional 6 months for a total of 18 months in recognition of the fact that overlapping resources will be required to implement both the static interventions and the Voice Firewall. (See Paragraph 4.44 of Consultation 23/52).

2.51 ComReg agrees with the findings of Plum that the timelines in the Decision Instruments are appropriate, proportionate and not overly burdensome.

2.52 In addition to the above, ComReg notes that the regulatory burden would not apply to all operators equally. Operators are responsible for ensuring that they have the resources to develop and maintain their networks in light of not only regulatory developments, but also technological and economic developments. In light of the serious harm scams are causing, ComReg would need more than a mere list of projects to even contemplate allowing such significant consumer harm to persist. An operator's ability to cope with multiple regulatory requirements is at least in part a function of operator's investment, in networks capability but also their staff.

2.53 Relatedly, ComReg notes that a more detailed technical specification will be developed in collaboration with industry in the NCIT steering groups.

2.54 In relation to the comments of IBEC and Virgin regarding data protection, ComReg is aware of the need for a legislative basis in order to implement certain interventions. In that regard, ComReg refers to its view at the outset of this consultation that there is a need to consult separately on the SMS Scam Filter. ComReg is unaware of any issue in relation to data protection law that would impede or delay any other interventions. ComReg notes that both IBEC's and Virgins' comments appear to be without basis in any specific concern, as certain interventions do not relate to personal data. In any event, and for completeness, ComReg notes that even if "*personal data*" is involved, and the General Data Protection Regulation is engaged, then the "*legitimate interests*" basis for processing under Article 6(1)(f) is likely to be engaged. As Recital 47 of the GDPR states: "*The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."*

Blocking - the need for metrics

2.55 Blocking metrics are critical to the functioning of the Interventions because they enable ComReg and operators to quickly identify emergent trends and assess the effectiveness of the interventions. Measuring the effectiveness of the proposed interventions is in the interests of all operators and ultimately consumers who are suffering significant harm (as identified in Consultation 23/52 and the Final RIA)

2.56 Providing metrics on a voluntary basis would inevitably lead to incomplete data on the number of blocked calls due to each intervention and impair the ongoing stewardship of the interventions. Neither ALTO nor Verizon have provided clear rationale as to why either considers the provision of metrics to be in some way disproportionate, or why, in the case of Verizon, it is unable to

report on these metrics due to the infrastructure that it currently uses.

Blocking – inadvertent blocking (false positives)

2.57 In relation to Microsoft's submission regarding the risk of false positives arising from the CLI Call Blocking intervention, ComReg notes that such risks should be small and decrease over time, once correctly implemented. CLI call blocking is a static intervention where specific types of traffic are deliberately blocked with certain well-defined exceptions. If the traffic types are well defined and operators apply the blocking correctly, such errors are avoidable. Furthermore, any inadvertent blocking would be the result of misapplication of the intervention by operators or the intervention protocol overlooking a certain traffic type. Therefore, for the static interventions, incorrect blocking is avoidable[64] and in any event should reduce after implementation as operators make adjustments as the intervention is rolled out.

2.58 In relation to Twilio's view that an agreed process for resolving the "*inadvertent blocking of legitimate traffic*" is necessary, ComReg considered the possibility of such errors in its draft RIAs at Para 4.41 and Para 4.86 of Consultation 23/52, wherein it noted that to minimise both false positives and false negatives, firewalls/scam filters often use a combination of filtering techniques, which analyse various aspects of the call, such as the sender, content, and behaviour, to determine whether it is legitimate or scam/fraudulent. By continuously updating their filtering rules and algorithms, firewalls/filters can improve their accuracy and reduce the occurrence of both false positives and false negatives.

2.59 For the dynamic interventions (i.e. firewalls), calls and texts are assessed based on their individual characteristics and blocked where deemed likely to be a scam. This inevitably involves a probabilistic prediction. The extent to which such errors arise depends on the configuration of the firewall/filter. A firewall/filter configured to block communications with a high probability of being a scam is unlikely to block valid calls/texts but may allow a small amount of scam calls/texts to be received by the user. Conversely, low probability configurations are likely to result in a higher rate of valid communications being blocked. Consequently, some level of false positives and false negatives is inevitable and will never be zero.

2.60 The configuration of the firewall/filter is typically managed by operators based on its preferences and the analytics available on a particular call/text. Probabilistic models need a pattern to emerge before recalibrating, and scams (particularly those that originate within Ireland) may arise temporarily from

[64] Indeed, discussions with NCIT members on interventions already implemented by NCIT members in bilateral meetings have not indicated any major issues with incorrect blocking.

time to time as scammers attempt new scams. However, it remains the case that the accuracy of firewalls/filter will continue to improve as more information and greater analytical capability becomes available. ComReg expects that these errors should fall over time as operators and service providers calibrate their models in light of their experience. Further, given that vendors and operators typically operate across multiple English-speaking jurisdictions, it is likely that some scams can be anticipated before they emerge in the Irish market reducing the false positives and false negatives.

2.61 Finally, ComReg notes that the Voice Firewall DI provides for modification of the CLI to warn consumers that calls may be "Likely Scams". This allows for some calls that might otherwise have been blocked to be assessed by consumers who may wish to verify the call status themselves by answering the call or through checking a voicemail. This functionality should further reduce the rate at which valid calls are blocked.

2.62 ComReg expects that discussions about other approaches for lessening both false negatives and false positives will feature as an item for discussion in the NCIT working group which will include procedures to enable unblocking and other related matters.

2.63 In relation to Mr. Joseph Sheerin's request, ComReg notes that, for compliant operators long-lining would generally appear to facilitate the types of calls to which he refers[65].

Blocking – the use of presentation CLIs

2.64 ComReg is of the view that because the presentation CLI is the number that consumers see on their handset, this clearly should be the number that must be controlled to prevent CLI Spoofing. Otherwise, scammers could still spoof any Irish number using any legitimate number (e.g., take a mobile SIM abroad and spoof numbers on the DNO, PN lists as well as Fixed CLIs). In relation to Microsoft's synopsis of Ofcom's policy in the UK, ComReg notes that since Microsoft responded, Ofcom has announced a consultation[66] on CLI Call blocking in which it "*propos*[es] *to update our Calling Line Identification (CLI) Guidance to confirm that providers are expected to identify and block calls from abroad that use a UK geographic or non-geographic telephone number as a Presentation Number, except in a limited number of legitimate use cases*".

2.65 In relation to the German approach, ComReg notes that calls blocked by the static voice interventions represent clearly illegitimate or incorrect use of Irish

[65] Extra-territorial calls bearing a Irish Fixed CLI.
[66] Closing 31st March 2024.

CLIs. ComReg has established protocols for dealing with well-defined exceptions (e.g., mobile roamers) and consequently there appears to be no valid reason to provide for CLI modification. This contrasts with dynamic interventions (e.g. firewalls) where there is less certainty that certain calls come from valid sources. In such scenarios, it may be more appropriate not to block certain calls but instead provide for a modification to the CLI.

Periodic review

2.66 In relation to Eir's view that ComReg should periodically review the effectiveness of the interventions, ComReg notes that it will monitor the effectiveness of the interventions on an on-going basis and update relevant parties through the NCIT working groups. This will occur far more frequently than the three years suggested by Eir. Indeed, ComReg notes that it will effectively be monitoring the progress of the interventions regularly in line with the availability of the reporting metrics as set of in each of the DIs. It is for this reason that ComReg set out the reporting requirements in each of the DIs and why all operators are required to comply with the requirement to gather and submit metrics for each individual static voice intervention. There does not appear to be any benefit from inserting a review period into the DI given that the requirement for providing metrics already exists and a decision for a more formal review is a matter for ComReg that would be take depending on the circumstances pertaining at the time.

Alternative technologies

2.67 ComReg welcomes these informative submissions that suggest alternative technologies/interventions that could combat nuisance communications. The interventions proposed by ComReg are required to be technologically neutral and may be implemented in a different number of ways, subject to meeting the requirement of the DI.

Other issues

2.68 In relation to the BPFI's comments, ComReg notes that in Consultation 23/52 it outlined the impacts of scam calls and texts on a wide variety of Irish businesses, which included banks and payment service providers. Indeed, Europe Economics interviewed such businesses to inform its views on the harm created by scam calls and texts.

2.69 In relation to Tesco's view that the ComReg consultation laid the blame on telecoms operators in relation to scams, ComReg disagrees. ComReg did not "*blame*" the operators for scams and there are no references at any point in Consultation 23/52 that would legitimately support this claim nor has Tesco pointed to any text which would support its contention.

2.70 ComReg is and has been focused on taking action to combat scams. Clearly, the blame for scam calls and text rests with the fraudsters, but there are interventions available to operators, and it is a simple matter of fact that only 16% of consumers think that operators have done enough to protect them from scam calls and texts, which is of concern. While several interventions have been introduced by some operators, implementation has not been universal, and more interventions are required to mitigate scams in the future. ComReg's decisions will address these matters.

2.71 Eir opines that the State should establish a fund to compensate operators for the implementation costs, While this is not a matter for it to address, ComReg has clearly identified the costs that would fall on operators in its RIAs, and it remains of the view that such costs are relatively modest compared to the harm to consumers and business.

2.72 Moreover, the costs are low in comparison to Eir's revenue growth, as since 2022, Eir has initiated annual increases in the price of its mobile products. These increases have been considerable, with an increase of 7.6% in April 2024 alone – or an additional €29.99 for an annual bill pay plan.[67] In light of Eir's large subscriber base, the price increases in April 2024 alone are likely to dwarf the entire cost to Eir of implementing the Interventions, noting that Europe Economics has estimated the one-off cost to Eir of implementing all the Interventions to be approximately €2-3 Million.

2.73 In summary, and when combined, ComReg's proposed interventions should bring €55 euros in economic and social benefit for every €1 spent securing networks. ComReg also notes that the successful implementation of these interventions would go a long way to restoring trust, demonstrating an operators commitment to protecting its customers, including businesses and organisations.

2.74 For its part, Revolut argues to the contrary that it is the telecommunication providers that are imposing cost of fraud on banks and payment providers (among others) by not preventing scams from proliferating (e.g., liability). Again, this is not a matter for ComReg, however it would note that all stakeholder's immediate attention should be focussed on ensuring the successful implementation of the Interventions. It is only through such proactive measures that consumers will ultimately be protected from fraudsters.

[67] Annual price change (eir.ie) "*Standalone Mobile Bill Pay Plan - If a customer just has a SIM Only mobile plan with a standard monthly price of €29.99. In April 2024, the monthly price will increase by €2.00.*"

2.1.2 The economic analysis in the Draft RIAs

Summary of ComReg's views in Consultation 23/52

2.75 Consultation 23/52 included four draft RIAs which considered, among other things, the likely effectiveness of each of the interventions and their associated costs. ComReg also considered the analysis conducted by Europe Economics which showed that the overall benefit of the Proposed Package would be in the order of €1.5 billion over the next seven years. Each intervention was codified in a separate draft Decision Instrument (see Chapter 7), each of which contained an deadline for their implementation.

2.76 These interventions are summarised in Section 6.2.2 (see Chapter 6).

View of respondents to Consultation 23/52

2.77 The views of respondents regarding the Proposed Package are summarised and then assessed by ComReg under the following headings.

- Identification of stakeholders;
- Estimated harms from scams;
- Estimated benefit of interventions;
- Estimated cost of interventions;
- Impact on competition; and
- Coverage.

View of respondents to Consultation 23/52

Identification of stakeholders

2.78 Twilio[68] contends that Cloud Service Providers should be included and assessed as a separate stakeholder within the draft RIAs.

Estimated harm from scams

2.79 BPFI outlines that it found in its most recent FraudSMART monitor that monies lost to fraud amounted to €88m for 2022 alone.

2.80 Tesco Mobile claims that it is inappropriate to include the HSE in the estimates of harm, given that it suffered greatly from a cybersecurity hack that

[68] Twilio provides programmable communication tools for making and receiving phone calls, sending and receiving text messages, and performing other communication functions using its web service APIs.

completely took down its systems.

2.81 Eir does not agree with ComReg's statement that "*Ireland, as an* English-*speaking country with a developed economy, is disproportionately targeted compared with our EU neighbours*". Eir references data from Hiya that it claims shows that Ireland is well down the league table in terms of scam and fraud call rates in Europe.

Estimated benefit of interventions

2.82 Three and Virgin both contend that the consultation does not address the migration of scams to Number Independent Interpersonal Communications Services ("NIICS"), which both state are also regulated by ComReg (e.g. WhatsApp). Relatedly, IBEC claims that ComReg overlooked NIICS and, in its view, scams should be expected to migrate to NIICS following the implementation of the interventions on Voice and SMS. BT also suggested that ComReg should review the regulation of number dependent and number independent services to avoid what it terms potential confusion.

Estimated cost of interventions

2.83 IBEC and Three both submit that the costs to industry have been underestimated.

2.84 Three contends that the draft RIAs significantly underestimate the financial costs and complexity of the proposed interventions. For example, Three notes that:

- [✂ ✂].

2.85 Three is also of the view that the estimates of time and expenditure set out in the consultation do not reflect its complexity.

2.86 Conversely, Cellusys, which designs and delivers signal solutions that give operators control over their systems, notably security, roaming, SMS monetisation and analytical applications contends that the costs of implementing interventions for MNOs and larger international gateway operators that transit international voice traffic into the state ("IGOs") are overstated by a small multiple.

2.87 Vodafone contends that in its RIA ComReg should use operator profits, and not revenues, to assess the impact of the cost of the Proposed Package on operators and consider operators "*investment challenges*" more broadly.

Impact on competition

2.88 IBEC contends that, in its view, that the proposals in Consultation 23/52 would have significant implications for the operation of the market as, the proposed interventions entail significant structural changes affecting the entire value chain.

2.89 IBEC also claims that ComReg did not consider the impact of the proposed interventions on competition.

Coverage

2.90 Sky supports ComReg's view that subscriber-based cut-offs are appropriate for certain interventions given the challenges entrants face entering the mobile market.

2.91 BT contends that the effectiveness of the interventions on international and originating traffic is dependent on these interventions being applied by all relevant operators[69]. BT contends that blocked scam calls can be re-routed within seconds to bypass any partial firewall and that it can demonstrate this happening during the implementation of the DNO and PN lists.

Views of Consultants

Europe Economics

Estimated harms from scams

2.92 Europe Economics reiterate that the inclusion of harms to the HSE are "*appropriate*" not least as the HSE was one of the organisations most impersonated by scammers. However, Europe Economics confirms that the cost of the cyber hack was not included in its estimated cost to the HSE. Rather, Europe Economics notes that it estimated the cost of a number of harms to the HSE including Do-Not-Attends.

Estimated benefit of interventions

2.93 In relation to the view that the migration of scams to other channels (OTT) will reduce the benefits of the interventions, Europe Economics notes that it

[69] From the context of the statement, ComReg assumes that BT was in fact referring to interventions applying to transit traffic (e.g., DNO, PN , Fixed and Mobile CLI Call Blocking) when using the term "Firewall", and not the dynamic "Voice Firewall" intervention.

flagged the adaptability of scammers. Furthermore, the adaptability of scammers informed the modelling of the benefits of different interventions, where evidence permitted. Europe Economics notes that this appears to be a first assessment of the benefit of interventions which does account for scammers switching. In particular, Europe Economics has explicitly modelled scammer switching through the use of:

- a "*decay*" rate which reduces the benefit over time, assuming that scammers improve over time in *side stepping* the interventions; and
- scenarios assessing the benefits in the event that scammers fully circumvent the static interventions for Voice and SMS (i.e., moving from spoofing to non-spoofing scam calls and text).

2.94 Europe Economics notes that its analysis supported the view that the dynamic interventions were beneficial for any level of switching by scammers within the same medium. Europe Economics observes that there is insufficient information available to estimate the potential switching between SMS and Voice and OTT and that there was reason to believe that switching between mediums may be lower, not least given that OTTs are end-to-end applications not interconnected networks, and therefore calls/messages are originated, transited and terminated by the operator. Europe Economics therefore refrained from estimating the level of switching between SMS/Voice and OTTs, which would not in line with taking an evidence-based approach.

Estimated cost of interventions

2.95 Europe Economics notes that its estimates were informed by engagement with industry, including Irish MNOs and international vendors, and that these costs were conservatively estimated. Europe Economics notes that no respondent has provided detailed explanation on how costs were underestimated, nor that cost were so greatly underestimated as to impact the analysis – noting the benefits to cost ratio of 55:1.

2.96 In relation to the Voice Firewall specifically, Europe Economics outlines that this was informed by discussion with domestic MNOs and international vendors. It should be noted that vendors have far more familiarity with implementing Voice Firewall and provided evidence to support their views, which no MNO did in their interview or submission.

ComReg's assessment

Identification of stakeholders

2.97 In relation to Twilio's concerns about the identification of Cloud Service

Providers as a stakeholder, it is important to note that different interventions apply to different types of traffic, and operators with similar business models may handle different traffic types (e.g., Tesco and Virgin are both MVNOs, but Virgin handles international Voice traffic and terminates fixed voice calls). Therefore, ComReg considered that the appropriate approach to assessing the impact of interventions in the draft RIAs was to group operators by traffic type and not business type (See Paragraph 5.42 of Consultation 23/52). For that reason, in its draft RIAs, ComReg identified stakeholder groups by the *types* of Voice and/or SMS traffic that they handled. ComReg considers that the impact of the regulatory options on Cloud Service Providers (CSPs) was broadly captured in the draft RIA – either under "Originating Operators" "small IGOs" or "large IGOs" depending on whether or not they transit international voice traffic.

2.98 Microsoft makes reference to CLI Call Blocking impacting CSPs in other markets but did not provide any specific evidence or examples. ComReg is not aware of any such issue emerging with Fixed CLI Call Blocking in the countries in which it has been applied, nor of such issues arising in Finland where Mobile CLI Call Blocking has been implemented.

Estimated harm from scams

2.99 In relation to Tesco's concern regarding the estimated cost of scams to the HSE, Europe Economics has confirmed that this assessment did not include the costs arising from the HSE's cyber-attack[70]. ComReg is of the view that the HSE case provides an important insight into the impact that scam calls and text can have on the delivery of important public services. The HSE is one of the most impersonated organisations and ignoring the impact on its operations and Ireland's healthcare appears imprudent.

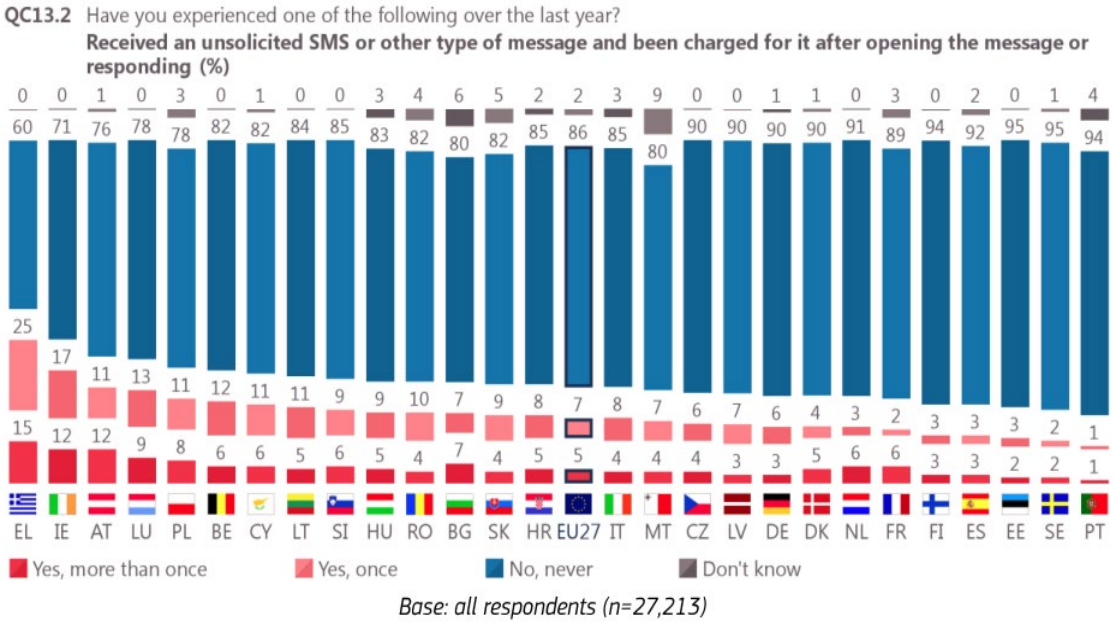
2.100 In relation to Eir's claim that Ireland was "*well down the league table*" in terms of scam and fraud call rates in Europe, ComReg notes that while Hiya's data shows a lower risk of scam calls compared to other countries, this is data that refers to Samsung Smart Call users only and is not a nationally represented survey of Irish consumers. ComReg previously relied on a Euro barometer survey of 27,213 people from the EU's 27[71], which found that Irish consumers were the second most likely to report having suffered an unwanted charge following an unsolicited text message (see Figure 3 below). That survey reveals that 29% of Irish consumers have received a call over the last year from an unknown number and been charged for it after answering the call or calling back, with 12% claiming it had happened more than once. The figure is more than double the EU average of 13%, with only Greece having a higher

[70] Europe Economics TBD
[71] Eurobarometer, "E-Communications in the Single Market" June 2021. Link

proportion of citizens experiencing the same problem (38%).

2.101 Regardless of the relative rates of scam calls across different jurisdictions, there is no question that there is a high prevalence of scam calls and texts in Ireland, as demonstrated by the detailed market research provided in Consultation 23/52. These findings are verified by other research published by external parties, such as the Irish Banking and Payments Federation and the European Commission. Indeed, it is noteworthy that neither Eir, nor any other respondent has disputed the harm estimates provided by ComReg. It remains the case that these calls and texts cause significant inconvenience and harm to consumers, and ComReg is obliged to act in line with its statutory objectives, functions and duties.

Figure 3: Eurobarometer survey "*E-Communications in the Single Market*" 2021



2.102 In relation to the comments of BT, Three, IBEC and Virgin regarding NIICs, ComReg notes that each of these respondents are all well aware that the scope of this work is limited to combatting scam calls and SMS made over public networks, and which represent a misuse of telephony numbers (as noted in Consultation 23/52). This project builds on the work of the NCIT which BT, Three and Virgin attend. Other platforms for scams such as emails or number independent communications platforms (e.g., emails or Over-the-Top applications) are outside the scope of this Response to Consultation.

2.103 ComReg highlighted the adaptability of scammers in multiple sections of the Consultation 23/52[72] and examined the impact of scammers switching between scams targeting different countries and types of traffic in its draft

[72] Consultation 23/52, Section 2.4

RIAs[73]. In that regard, ComReg agrees that some scammers may switch to using alternative communications platforms to contact consumers (e.g., WhatsApp) in response to better protection on Voice and SMS. However, ComReg considers that any concern that switching of scammers impacts the analysis of the Proposed Package to be misguided for a number of reasons.

2.104 First, ComReg notes Europe Economics' view that there is no evidence to inform the scale of switching by scammers from SMS and Voice to other platforms and the resulting harm. It is highly unlikely that the entire harm avoided/mitigated through SMS and Voice Calls will simply move to OTT alternatives such as WhatsApp. For example, the use of such applications is not universal across the population (e.g. older demographics make less use of alternative call and messaging services[74]) and this significantly reduces the hit rate and costs to scammers.

2.105 Second, there have been many recent reports of such providers implementing or upgrading anti-scam interventions to secure their applications in response to scammers. Recent reports indicate that a particular emphasis is being placed on both sender verification and content scanning, which are analogous to the proposal to regulate CLI and Sender ID as well as the dynamic interventions. For example:

- OTT messaging providers which typically operate encrypted end-to-end communication services, have taken the following actions:
  - Signal introduced usernames to enable account verification to combat scammers in 2024.[75]
  - WhatsApp has applied Machine Learning to identify and block suspect accounts based on consumer report since at least 2019.[76]
  - Meta introduced Meta Verified to protect paid users of Facebook, Instagram and WhatsApp from impersonation in 2023.[77]
- Large email providers, who like telecom providers operate interconnected networks, have taken the following actions:
  - Gmail upgraded its long-standing Gmail scam filter in 2023 that assesses the likelihood of inbound emails being a scam/spam[78]
  - Gmail introduced controls on bulk senders including verification to

[73] Consultation 23/52, Figure 33, Figure 36 and Table 18.
[74] B&A Consumer Survey.
[75] Signal >> Blog >> Keep your phone number private with Signal usernames
[76] WhatsApp "*Stopping Abuse: How WhatsApp Fights Bulk Messaging and Automated Behavior*" Link accessed on 21 February 2024
[77] Expanding Meta Verified to Businesses | Meta (fb.com)
[78] Google Online Security Blog: Improving Text Classification Resilience and Efficiency with RETVec (googleblog.com)

prevent spam and scam emails in 2024, stating *"To help fix that, we've focused on a crucial aspect of email security: the validation that a sender is who they claim to be. As basic as it sounds, it's still sometimes impossible to verify who an email is from given the web of antiquated and inconsistent systems on the internet,"*[79].

- Yahoo introduced controls on bulk senders including verification to prevent spam and scam emails in 2024 stating "*Sending properly authenticated messages helps us to better identify and block billions of malicious messages and declutter our users' inboxes,*"[80]
- Gmail introduced a "*checkmark*" to its branded emails (which were introduced in 2021), to further differentiate messages from verified senders from those trying to impersonate them[81].

2.106 In any event, the majority of scams appear at present to be made via SMS and voice calls which are services that telecom operators provide to their customers. ComReg has already identified over €300 million worth of harm which relates solely to voice and SMS services. Moreover, ComReg reiterates that voice calls and SMS are unique among calling and messaging services in that they are universally installed and activated on mobile devices by default, unlike alternatives which are reliant upon a consumer downloading the application to their device (e.g., WhatsApp etc). In that regard, it is particularly important to restore trust in these services given their universal availability and the reliance placed on them. To the extent that ComReg's proposed interventions cause some scammers to switch to WhatsApp or other OTT services, this is primarily a matter for such service providers and their users. ComReg will monitor this situation, and future measures may be required in that regard by appropriate agencies.

Estimated cost of interventions

2.107 ComReg notes that there is no consensus among respondents on whether the estimated costs of the proposed interventions are over or underestimated – some vendors contend that the estimated costs are too high while the operators view the costs as too low. ComReg agrees with Europe Economics that respondents' views did not consider the detailed methodology for cost estimation that Europe Economics applied and no respondent points to any error in assumption, figure or calculation. Therefore, ComReg remains of the view that the costs estimation provided by Europe Economics is justified and valid.

[79] https://blog.google/products/gmail/gmail-security-authentication-spam-protection/#:~:text=Focus%20on%20email%20validation&text=To%20help%20fix%20that%2C%20we,inconsistent%20systems%20on%20the%20internet
[80] https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam
[81] Google Workspace Updates: Expanding upon Gmail security with BIMI (googleblog.com)

Proportionality

2.108 In relation to Vodafone's contention that ComReg should examine the proportionality of the interventions in relation to profits and not revenues, ComReg notes, for the avoidance of doubt, that it does not determine the proportionality of the proposed interventions based solely on a comparison of implementation costs and revenues earned. While ComReg takes account of costs likely to arise from its proposed measures, it also recognises that any such impacts should be balanced against the benefits of achieving relevant statutory objectives, including promoting the interests of other users (i.e., consumers), protecting consumers more generally, promoting competition, and ensuring the efficient and effective use of numbers.

2.109 ComReg provided the comparison with revenue in order to illustrate the relatively low costs of protecting consumers compared to the revenues earned by operators from those same consumers. In that regard, revenue is the most appropriate metric because it reflects the overall value of services provided by operators to its consumers. Profitability on the other hand says little about the overall value of services and in many cases is simply reflective of overall efficiency, which typically varies across operators. A situation where the proportionality of an intervention(s) depended on operator efficiency or profitability, would lead to situations where regulatory measures are imposed more widely on the most efficient operators or even only those operators that make a profit. ComReg remains of the view that there is no real concern that these interventions are unaffordable to operators, noting that the sister companies of the Irish operators have deployed interventions in other jurisdictions (e.g., a "*SMS firewall*"[82] is deployed by Vodafone in the United Kingdom).

Impact on competition

2.110 IBEC's contention that ComReg did not consider the impacts of the proposed interventions on competition ignores that each of the draft RIAs has a dedicated 'Impact on Competition' assessment. IBEC has not pointed to any part of the assessments that it disagrees with or to any perceived error in any assumption, figure or calculation. It is also not clear what 'significant structural changes' alleged by IBEC are caused by which or any of the proposed interventions as IBEC has not provided any evidence to support its contentions. Therefore, ComReg does not propose to make any changes to its competition assessments in the final RIAs.

Coverage and enforcement

[82] https://www.vodafone.co.uk/newscentre/news/vodafone-hammers-christmas-fraudsters-with-spam-reduction-december-2021/

2.111 ComReg agrees with the views of BT and i3Forum that the effectiveness of each of the interventions is dependent on them being applied and enforced on all relevant operators. In Section 5.2.4 of Consultation 23/52, ComReg noted that the effectiveness of an intervention is a function of the operators that implement it – (i.e., if all operators implement each intervention, full coverage of effectiveness would be provided). In that regard, ComReg conducted a three-pronged assessment to determine which operators would be required to implement each of the interventions:

I. ComReg assessed which interventions require 100% coverage to achieve effectiveness, such that the intervention would apply to all relevant operators.

II. ComReg assessed what approach best provides the greatest coverage for all remaining interventions (i.e. interventions applied in a manner that achieves the greatest coverage while being proportionate in their implementation).

III. ComReg provided information on the number and type of operators that would be required to implement each intervention.

2.112 In summary, ComReg was of the view that interventions targeting call origination or international transit (i.e., DNO/PN, Fixed and Mobile CLI) should be applied to all operators that carry such traffic. The remaining interventions all concern terminating traffic (or combinations of originating and terminating traffic) and that such interventions, where technically feasible, should be implemented by the network operators. Separately, it would be appropriate to provide a threshold for the mandate of these interventions for virtual operators that do not rely upon their host network operators for core network services.

2.113 This approach best ensures that the effectiveness of the interventions is maximised whilst also being implemented in line with ComReg's statutory objectives and duties. It should be noted that ComReg has adjusted this assessment in the final RIA in light of views of respondents (See Section 6.2.1-6.2.4).

2.1.3 Do Not Originate, Protected Numbers and Fixed CLI Call Blocking Interventions

Summary views of ComReg in Consultation 23/52

2.114 In Chapter 4 of Consultation 23/52, ComReg outlined its reasons for finding that DNO, PN and Fixed CLI Call Blocking were technically feasible, effective and could be implemented within six months of any Decision.

2.115 In the draft 'CLI Call Blocking' RIA, ComReg set out its preliminary assessment on the impact of the DNO, PN, Fixed and Mobile CLI Call Blocking intervention on consumers, stakeholders, and competition. ComReg was of the preliminary view that implementing each of DNO, PN and Fixed CLI Call Blocking within six months of any final Decision best promotes the efficient use of numbers, competition, and efficient investment in ECS markets.

2.116 Chapter 7 of Consultation 23/52 contained the draft DIs for the DNO, PN and Fixed CLI Call Blocking interventions, outlined the types of operators that would have to apply these interventions, as well as the precise legal obligations which would apply to these operators. ComReg was of the preliminary view that it was proportionate to require all originating voice operators[83] to apply DNO and PN and all IGOs[84] to apply DNO, PN and Fixed CLI Call Blocking within six months of any Decision.

View of respondents to Consultation 23/52

2.117 The views of respondents on the DNO, PN and Fixed CLI Call Blocking are summarised and assessed by ComReg under the following headings:

- Support for the DNO, PN and Fixed CLI Call Blocking Interventions;
- Timelines for updating the DNO/PN List;
- Metrics on scam calls blocked;
- Proposed timelines for implementation;
- Exceptions for certain types of traffic; and
- Scope of Protected Numbers List.

Support for the DNO, PN and Fixed CLI Call Blocking Interventions

2.118 There was widespread support for these interventions, with ALTO, Bank of Ireland, BPFI, BT, Ericsson, Eir, HIYA, i3Forum, Magrathea, NetNumber, Twilio, Vodafone, Virgin, XConnect, Microsoft and Voxbone all expressing support.

Updating of the DNO, PN and MSRN lists

[83] Consultation 23/52 - Draft Decision Instrument for DNO, Draft Decision Instrument for Protected Numbers - "*"Originating Voice Operator" or "OVO" means an Irish Undertaking originating calls on the Irish PSTN capable of terminating on public networks;"*

[84] Consultation 23/52 - Draft Decision Instrument for DNO, Draft Decision Instrument for Protected Numbers, Draft Decision Instrument for Fixed CLI Call Blocking - *"International Gateway Operator" or "IGO" means an Irish Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN".*

2.119 Three contends that ComReg should increase the number of days that operators have to apply the updated DNO and PN List from two to [✂ ✂], to allow for '*network freezes*' that operators predominantly schedule in December.

2.120 In relation to Fixed CLI Call Blocking, Three contends that IGOs should be notified regarding updated Mobile Station Roaming Numbers ("MSRN") at least three months before they become effective.

Metrics on scam calls blocked

2.121 Three opines that operators should have 15 working days to report metrics for blocking based on DNO, PN and Fixed CLI Blocking, and that such reporting should be required only on a quarterly rather than monthly as proposed.

2.122 Eir seeks that blocking statistics be submitted at an aggregate level as it is "*unable to commit*" to gathering and submitting metrics for each individual static voice intervention because its Fixed Network "*do*[es] *not capture*" which of the three interventions (DNO, PN or Fixed CLI Call blocking) resulted in a block.

Proposed timelines for implementation

2.123 Eir considers that while six months may be an appropriate timeline for implementing each intervention in isolation, it does not allow sufficient time for operators that have yet to implement these interventions.

2.124 By contrast Voxbone agrees with the proposed timelines for these interventions.

Exceptions for certain types of traffic

2.125 Three highlights an issue with some of its customers using [✂ ✂]. Three submits that in the absence of an derogation [✂ ✂]

Scope of DNO and Protected Numbers list

2.126 NetNumber observes that the DNO and PN list would be more effective if it included assigned numbers that are not in use. XConnect urges ComReg to expand the DNO list to include [✂[redacted]✂].

Views of Consultants

Plum

Proposed timelines for implementation

2.127 Plum found that the timelines in the Decision Instrument for DNO, PN and Fixed CLI Call Blocking are appropriate, because the interventions[85];

- are already widely deployed by operators;
- use existing capabilities; and
- appear unlikely to be affected by other regulatory or commercial initiatives.

ComReg assessment

Support for the DNO, PN and Fixed CLI Call Blocking Interventions.

2.128 ComReg acknowledges the support of ALTO, Bank of Ireland, BPFI, BT, Ericsson, Eir, Hiya, i3Forum, Magrathea, NetNumber, Twilio, Vodafone, Virgin, XConnect, Microsoft and Voxbone for the DNO list, PN list and/or Fixed CLI Call Blocking interventions.

Updating to the DNO, PN and MSRN lists

2.129 Given Three's concern regarding the number of days that operators have to apply the updated DNO and PN List, ComReg proposes to extend this period for blocking calls from two to five working days. This should provide operators with more time for operators to implement the updates, to prevent from the updates interfering with network freezes and maintenance that operators typically conduct in December. Furthermore, this extension to five days should not impact the effectiveness of the DNO and PN interventions.

2.130 In relation to Fixed CLI Call Blocking, Three contends that IGOs should be notified regarding updated MSRNs at least three months before they become effective. ComReg notes that the Fixed CLI DI already specifies that relevant undertakings that are Mobile Service Providers shall inform ComReg three

[85] Readers are referred to the Plum Report for more information.

months in advance of any changes to their Irish MSRN number ranges. ComReg sees no issues with notifying IGOs once this information is received and it will action a process for the dissemination of this information as part of the relevant NCIT working group. ComReg also clarifies that the Mobile Service Providers shall provide the first iteration of Irish MSRN number ranges three months in advance of blocking. This clarification is reflected in the Final DIs.

Metrics on scam calls blocked

2.131 It should first be noted that blocked call statistics are an important tool to allow ComReg and other policymakers to identify emergent trends and to assess the effectiveness of the prevailing interventions. In order to be used effectively, blocked call statistics must be sufficiently detailed and granular, and submitted in a timely manner (i.e. on a monthly basis).

2.132 Three's suggestion of submitting quarterly data is not appropriate because monthly trends or patterns would be obscured in the quarterly aggregate. For example, how might one observe any see seasonal effects (e.g., if scammers are targeting specific periods such as certain holidays and whether blocking is increasing/decreasing during these periods)? If multiple different scams occur at different times in a quarter, it would be difficult to isolate the calls blocked from one scam to another.

2.133 Further, Three has not provided any reason why operators require fifteen rather than ten working days to submit their blocking data for the DNO, PN and Fixed CLI Call Blocking. ComReg is of the view that this would result in an unnecessary delay in the compilation and analysis of the blocking trends. Therefore, ComReg remains of the view that operators should submit data on calls blocked on a monthly basis, within 10 working days of the last day of the preceding month.

2.134 In relation to Eir's assertion that metrics would not be possible for each individual intervention, ComReg notes blocking data must be intervention-specific to enable ComReg and other policymakers to identify which scam types and traffic are targeting Irish consumers. Eir has not clearly articulated why metrics for each individual intervention cannot be reported to ComReg. ComReg also notes that other mobile and fixed operators are already providing metrics for individual interventions - it is therefore difficult to understand how Eir cannot also do so. ComReg also notes that absent a breakdown across individual interventions, it would be more difficult to conduct a review on the effectiveness of the technical interventions, a step that Eir itself has sought (See ComReg response below).

2.135 Further, ComReg notes that Eir will have to apply a Voice Firewall and that

this may provide Eir with an alternative means of recording blocking data. Several Voice Firewall vendors[86] have confirmed to ComReg that DNO, PN and Fixed CLI Call Blocking can be applied via the Voice Firewall and that the blocking for each list-based intervention can be collected separately.

Proposed timelines for implementation

2.136 ComReg agrees with Plum that the six-month deadline proposed in Consultation 23/52 is reasonable and proportionate, as these interventions are:

- Clearly defined and understood;
- Relatively straightforward to apply from a technical perspective; and
- Already applied by the operators which are at greater risk of "overburdening" i.e., having the greatest number of interventions to implement[87].

2.137 In light of this, ComReg remains of the view that a six-month deadline for implementation of DNO, PN and Fixed CLI Call Blocking is appropriate and proportionate.

Exceptions for certain types of traffic

2.138 In relation to Three's contention that certain existing traffic types to which DNO cannot be applied should be exempt from DNO and PN, ComReg is of the view that no such exceptions are required. Operators can and should make the necessary adjustments to the routing of their calls to accommodate these traffic types. ComReg reiterates that any uncontrolled, undefined exceptions to these measures (e.g., not a long line) would create a vulnerability which could expose consumers to scams and potentially undermine the efforts and investment of all compliant operators.

2.139 In relation to Three's contention that [✂ [redacted] ✂] as criminals have been known to takeover legitimate numbers or systems to perpetuate crime (e.g., PBX Hacking[88]). In February 2024, the UK's National Cyber Security Centre noted that PBX hacking may occur in order to "*so that the final called*

[86] See the comments of Ericsson and Cellusys in Section 2.1.1.
[87] As noted by Plum the only combinations of operators that could yet have to apply DNO, PN and Fixed CLI Call Blocking are smaller IGOs, and for DNO and PN it is smaller Voice Originators. As noted by Plum in both cases, 6 months appears more than sufficient amount of time to implement these interventions.
[88]. For further information please see PowerPoint Presentation (comreg.ie)

party sees the Customer Line Identifier (CLI) of the PBX rather than the scammer who is making the call."[89] Indeed, as network interventions are tightened, scammers may attempt to identify and exploit any such exemption. Furthermore, even if Three was correct that [✂[redacted]✂].

Scope of Protected Numbers List

2.140 In relation to NetNumber's suggestion that the PN list could include assigned numbers that are not in use, ComReg notes that this would require information on which phone numbers assigned by ComReg to a particular operator have not been provided by that operator to its end users.

2.141 Similarly, in relation to XConnects suggestion to expand DNO, ComReg notes that this would require information on active [✂[redacted]✂]. ComReg does not currently gather this information, which is only available to individual operators, who would be required to include such numbers on the PN list. However, it is likely that such numbers would be required by operators on a continuous basis to onboard new subscriptions that originate on their network. The process of including these numbers on the PN list only to be removed once an operator onboards a new customer would likely be unnecessarily complicated and could compromise the ability of operators to service customers in a timely fashion. By contrast, numbers not assigned by ComReg to operators cannot be used to onboard new customers until assigned by ComReg to an operator and can therefore be included on the PN list.

2.1.4 Mobile CLI Call Blocking

Summary views of ComReg in Consultation 23/52

2.142 In Chapter 4 of Consultation 23/52, ComReg outlined its reasons for finding that Mobile CLI Call Blocking was technically feasible, effective and could be implemented using a MAP (Mobile Application Part) protocol in a timely manner.

2.143 In Chapter 5 of Consultation 23/52, in the draft 'CLI Call Blocking' RIA,

[89] Private Branch Exchange (PBX) best practice - NCSC.GOV.UK

ComReg set out its preliminary assessment on the impact of Mobile CLI Call Blocking on consumers, stakeholders and competition. ComReg was of the preliminary view that implementing Mobile CLI Call Blocking best promotes the efficient use of numbers, competition, and efficient investment in ECS markets.

2.144 Chapter 7 of Consultation 23/52 contains the draft DIs for the Mobile CLI Call Blocking interventions which, among other things, outlined the types of operators that would have to apply these interventions. ComReg was of the preliminary view that it was proportionate to require all IGOs[90] to apply Mobile CLI Call Blocking under Phase 1 within six months of the Decision. Phase 1 was required on the assumption that at least some IGOs with the capability to use MAP would provide the roamer check facility as a service to smaller IGOs. For Phase 2, MSPs were required to implement a shared roamer database within 24 months of the Decision.

View of respondents to Consultation 23/52

2.145 The views of respondents on Mobile CLI Call Blocking are summarised and assessed by ComReg under the following headings:

- Support for Mobile CLI Blocking;
- Phase 1 of Mobile CLI Blocking – Access for Smaller IGOs;
- Phase 1 of Mobile CLI Blocking – Timelines;
- Phase 2 of Mobile CLI Blocking – Necessity and proportionality;
- Phase 2 of Mobile CLI Blocking - Cost;
- Draft DI; and
- Blocking Metrics.

Support for Mobile CLI Call blocking

2.146 Hiya, NetNumber, ALTO, BT, BPFI, Magrathea, Virgin, Bank of Ireland and Ericsson all expressed support for this intervention.

Phase 1 - Access for Smaller IGOs

2.147 Verizon contends that not all infrastructure can interface with MNOs roaming databases and in the absence of wholesale access, smaller IGOs would be

[90] Consultation 23/52 - Draft Decision Instrument for Mobile CLI Call Blocking - *"International Gateway Operator" or "IGO" means an Irish Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN"*

required to block all calls by IGOs to comply with the draft DI. Verizon notes that it is not aware of any large IGO offering wholesale access. Verizon further opines that even where large IGOs provide this service, a sufficiently high price could force one or more smaller IGOs to exit the market. For similar reasons, ALTO suggests that ComReg should set a wholesale access fee that an IGO can charge for this service.

2.148 Imagine and Magrathea both submit that ComReg should exempt 'smaller IGOs'[91] from Phase 1 of Mobile CLI Call Blocking. Imagine contends that exempt IGOs should be allowed to apply blocking as outlined in Phase 1 on a voluntary basis.

2.149 Sky maintains that Phase 1 could create particular difficulties for an entrant (such as itself) because it would need to negotiate with a large number of IGOs.

Phase 1 - Timelines

2.150 Vodafone opines that, in its view, the timelines for implementation are extremely challenging.

2.151 Eir states that MNOs cannot share their customer roaming status with IGOs until the Decision is formalised, for data protection reasons. Therefore, IGOs can only access the mobile Number Portability Database (NPD) once the Decision is published. For this reason, Eir contends that the deadline for blocking should be increased from 6 to 12 months, in light of the inter-operator work that can only be undertaken post-Decision.

2.152 Three states there [✂[redacted]✂]. Three agrees with the proposed deadline for IGOs to implement Phase 1, stating that the date for the obligation should be "*no earlier than six months after the Decision*" in the event of the Decision being published in Q1 2024[92]. Three maintains that any deadline for MNOs to provide access to other IGOs to their roaming data must precede the deadline for IGOs to implement blocking by at least three months.

2.153 Imagine contends that the timelines are unworkable for 'non-direct' IGOs, given the lack of readiness of larger IGOs to provide a wholesale service.

2.154 Virgin contends that the timeline for Phase 1 is disproportionate because, in its particular case, it is [✂[redacted]

[91] Imagine uses the phrase 'non-direct operators' and Magrathea uses the term 'VOIP based IGOs'.
[92] Three contends that this six-month period should be retained given uncertainty regarding vendors capabilities to implement the measure in a timely manner given its "newness", with ComReg only providing one example of this intervention having been implemented.

[redacted]✂].

Phase 2 – Necessity

2.155 Eir and Vodafone both contend that a roamer check may be unnecessary given the migration to VoLTE roaming which can use S8HR "*S8 home routing*"[93].

2.156 Eir and Vodafone both query whether there is a need for any roamer check to cover VoLTE roamers, in light of the home routing of VoLTE traffic.

2.157 Similarly, Three opines that a roamer check may not be required for MSPs that use ICS, for either VoLTE or non-VoLTE traffic, as with IMS Centralised Services' (ICS)[94] even non-VoLTE originating voice roaming traffic will be routed over the home network. Three is of the view that this is a simpler approach and should be examined alongside other alternatives by the NCIT before Q1 2024. Three contends that Phase 1 should be able to handle VoLTE because MSPs have their own roamers status and may correctly respond to a Roamer Check query based on MAP. Three also notes that VoLTE roamers are excluded from the Finnish Mobile CLI Call Blocking.

2.158 Eir questions the need for Phase 2 for large MSPs once the Voice Firewall is implemented.

Phase 2 – Cost and proportionality

2.159 Verizon and ALTO both contend that it is disproportionate for ComReg to require operators to implement both Phase 1 and Phase 2, as this incurs additional costs. Three questions the need for MSPs to partake in Phase 2 because it contends that MSPs would bear the cost of a service that benefits smaller IGOs.

2.160 BT opines that the roamer check[95] is not sufficiently scoped and that its cost to operators is therefore unknown. Consequently, BT questions whether mandating this intervention is in line with good regulatory practice and states that this may be challenged at the "*European Notification level*".

Draft Decision Instrument

[93] S8HR transports VoLTE traffic between visited and home networks as data traffic using the LTE S8 interface. IMS Roaming Architecture using S8HR- Paragraph 2.4.3 IR.65-v34.0-4.pdf (gsma.com)
[94] IMS Centralized Services provides communication services such that all services, and service control, are only based on IMS mechanisms and enablers. IMS Service Centralization and Continuity Guidelines IR.64_v8.0.pdf (gsma.com)
[95] This appears to be what BT is referencing, noting the timeline BT offers only matches with Phase 2 of Mobile CLI Call Blocking.

2.161 Eir seeks clarification that Decision 2[96] in the Draft DI is for MNOs and not IGOs as stated in the Draft DI.

Views of Consultants

Plum

Proposed timelines for implementation

2.162 Plum identified a number of preliminary concerns regarding certain enabling actions that are required to achieve the overall timeline. ComReg shared a number of updates to the timelines for these enabling actions, for Plum to consider. In light of these changes[97], Plum found that the timelines in the Decision Instrument for Mobile CLI Call Blocking:

- Phase 1 timelines are appropriate because;
    - only operators with MAP capability or the capability to acquire it will be required to implement Phase 1;
    - the complexity of testing has been reduced for the remaining Phase 1 IGOs and MSPs;
    - IGOs will be provided with the MSRNs in time to facilitate blocking.
- Phase 2 timelines are appropriate because;
    - the time permitted is greater than that typically required for such projects; and
    - the Finnish example indicates that development of a Proxy Server Database is achievable within 21 months.

ComReg assessment

Support for Mobile CLI Call Blocking

2.163 ComReg acknowledges the support of Hiya, NetNumber, ALTO, BT, BPFI, Magrathea, Virgin, Bank of Ireland and Ericsson for Mobile CLI Call Blocking.

Phase 1 - Access for Smaller IGOs

[96] ComReg 23/52, Draft Decision Instrument for Mobile CLI Call Blocking on page 269 "*Decision 2) Relevant undertakings that are MSPs shall: a. provide a Roamer Check facility based on use of MAP protocol to all requesting IGOs; and b. ensure that ComReg is informed three months in advance of any changes to their Irish MSRN number ranges.*"
[97] Readers are referred to the Plum Report for more information.

2.164 A number of respondents raised concerns in relation to the impact of Phase 1 on 'smaller' IGOs, which are unable to use MAP and would therefore need to rely upon a larger IGO to block illegitimate mobile traffic on their behalf (i.e. as part of a wholesale service). ComReg considered such concerns in Consultation 23/52 wherein it noted that the proposed implementation of Phase 1 was dependent on voluntary cooperation between industry players. In particular, at paragraph 5.112 ComReg noted that smaller IGOs could be exposed to higher costs if larger IGOs were unwilling to apply this blocking to international traffic on behalf of smaller IGOs. At that time, ComReg noted from NCIT discussions and bilateral discussions, that some larger IGOs were considering offering to apply this intervention to the traffic carried by smaller IGOs (subject to commercial agreements). ComReg also noted that larger IGOs should also have an interest in providing such a service given that any exceptions would create a 'gap' and potentially undermine their own investment.

2.165 ComReg notes that Phase 1, as proposed, could provide larger IGOs with significant bargaining power over smaller IGOs and potentially could result in excessive costs or harm to competition because the cost to a smaller IGO of not having its traffic scrubbed could potentially be very high (i.e., a smaller IGO would not be able to route international traffic). Furthermore, in circumstances where a smaller IGO decided not to carry the traffic, consumers would likely be harmed if that traffic from abroad was not carried or was blocked.

2.166 In light of the views of respondents, ComReg now includes a financial threshold to identify which operators must implement Phase 1, with implementation of Phase 1 only being required of IGOs with an annual revenue from the provision of ECS of over €50,000,000 in the State in 2023. The use of this financial threshold is based on the €50 million value already set out in Commission Recommendation (2003/361/EC) which is the instrument the European Commission currently uses to define small and medium-sized enterprises (i.e. firms below €50 million would be classified as a SME)[98].

2.167 The use of this financial threshold is appropriate because it identifies the larger IGOs that are able to implement Phase 1 from the smaller IGOs that are unable to utilise MAP or achieve this capability through investment in a short period of time (six months)[99]. The impact of this change is that ComReg

[98] ComReg notes that the results are not sensitive to the exact amount chosen, noting that the IGOs either side have revenues of c. €20 million and c. €300 million exactly,

[99] ComReg also notes that such an investment if it were made by smaller IGOs would likely be inefficient because Phase 1 only applies only for a 18-month period, beginning 6 months after the publication of the DIs. ComReg also notes that there is little benefit in adjusting this threshold to account for inflation etc (since 2003) because a higher threhold would not exclude any firms that would be included under the €50 million threshold.

will not now require Phase 1 to be implemented by smaller IGOs that are unable to handle MAP queries without the assistance of a larger IGO[100]. These changes have been reflected in the CLI Call Blocking RIA and Final Decision Instruments.

2.168 Importantly, this does not alter ComReg's view that complete coverage of mobile CLI is required for any intervention targeting call origination or international transit. Rather, this modification is time bound given that Phase 1 only applies for an 18-month period, beginning six months after the Decision. At the end of this period, Phase 2 will achieve 100% coverage across all relevant operators. Therefore, Phase 1 can be considered an intermediate measure which will ensure the majority of international voice traffic (c. [✂ ✂]%)[101] is screened for Mobile CLI spoofing before Phase 2 takes effect and achieves 100% coverage.

2.169 ComReg is of the view that this modification to the Phase 1 intervention addresses the concerns raised by respondents and importantly should result in improved outcomes for consumers without risking distortions to competition. Under ComReg's updated proposals, smaller IGOs can still arrange voluntary commercial agreements in order to protect consumers. In such cases, larger IGOs would have no perverse incentives to charge excessive prices and/or restrict competition because a smaller IGO could benefit from the exemption and still carry international traffic if the price was deemed excessive. That said, there would still be good incentives for larger IGOs to earn additional revenues by offering '*traffic scrubbing'* services to smaller IGOs at an efficient price, and there would be good incentives for small IGOs to seek such arrangements in order to protect the traffic originating on their network.

Phase 1 - Timelines

2.170 Given the financial threshold outlined above, only larger IGOs[102] will apply Phase 1 Mobile CLI Call Blocking. The timelines for the implementation of Phase 1 will now only apply to those IGOs above the financial threshold. Therefore, any IGOs below the threshold should have no concerns on the timelines for implementation of Phase 1. In effect, this reduces the number of IGOs which could be in this position from eleven to five.

2.171 In relation to BT, ComReg notes that [✂

[100] This exemption applies only to IGOs blocking traffic and not to MSPs, which are still required to provide the Phase 1 IGOs with access to the roaming status of their subscribers. ComReg is unaware of any reason to extend this exemption, noting that MSPs would have the required technical expertise and familiarity with MSPs processes to enable this. Moreover any such exemption would reduce the impact of the blocking undertaken by the Phase 1 IGOs.
[101] IGO RFI
[102] ComReg has confirmed that only larger IGOs meet this threshold. Consequently, there is no need to extend the deadline to facilitate smaller IGOs to secure terms with larger IGOs for a scrubbing service.

[redacted]. Furthermore, we note BT has not raised concerns regarding the timeline for Phase 1 in its submission.

2.172 In relation to Virgin, ComReg notes that it may consider the specific circumstances of the MSP/IGO including their effort and plans, or lack thereof, to implement the intervention. ComReg notes that Virgin [redacted]. By its own account, Virgin should then be [redacted] noting that even a slightly delayed implementation of Mobile CLI Call Blocking by [redacted]

2.173 In addition, the exemption of the smaller IGOs reduces the regulatory burden on the MSPs, which would now only have to provide access to fewer IGOs. Notably, these IGOs have [redacted].

2.174 For the reasons above, ComReg considers that the concerns of both MNOs and IGOs relating to the timeline for Phase 1 are largely ameliorated by the use of financial thresholds to identify the Phase 1 IGOs.

2.175 ComReg had inserted a requirement that Mobile CLI Phase 1 be implemented no later than six months from the date of Decision. It also stipulated that Mobile Service Providers should:

- ensure that ComReg is informed three months in advance of any changes to their Irish MSRN number ranges.
- provide a Roamer Check facility based on use of MAP protocol to all requesting IGOs;

2.176 The requirement to provide a roamer check facility was to allow for inter-operator works and testing to occur before the relevant IGOs can apply Phase 1. However, the 6-month deadline in the draft DI effectively bundled the blocking requirement with MSPs sending MSRNs to ComReg and providing roamer check to the IGOs. Logically, this timing makes little sense because it would not allow sufficient time for operator works and testing. ComReg now clarifies the timelines to require that MSPs provide information on any changes to their Irish MSRN number ranges 3 months after the decision (i.e., 3 months ahead of blocking). ComReg also makes clear that the Roamer Check facility based on use of MAP protocol should be provided to all Phase 1 IGOs one month in advance of blocking (i.e. 5 months after the Decision).

2.177 In that regard, ComReg agrees with Plum that the six-month deadline

proposed in Consultation 23/52 is reasonable and proportionate, as this intervention is:

- Clearly defined and understood;
- Relatively straightforward to apply from a technical perspective;
- Only being applied by larger operators, which are at lower risk of 'overburdening', given their greater organisational capacity[103]; and
- Already applied in full or in part by all of the relevant operators.

2.178 For these reasons, ComReg remains of the view that six months is an appropriate and proportionate deadline for implementing Phase 1 Mobile CLI Call Blocking. Furthermore, the IGOs in question are all members of NCIT and have been aware of the need for Mobile CLI Call Blocking using MAP for a considerable time.

Phase 2 – Necessity and proportionality

2.179 A number of MSPs challenged whether there is any need for MSPs specifically to implement a roamer check as outlined under Phase 2 given the migration to VoLTE roaming. While ComReg agrees that "*home routing*" can facilitate MNOs applying Mobile CLI Call Blocking to their own traffic, ComReg disagrees that this negates the need for Phase 2 for two main reasons:

I. First, the widespread adoption of VoLTE roaming does not appear imminent, and it remains uncertain when this will be achieved. Indeed, no operator provided any evidence or plans to migrate traffic to VoLTE roaming. ComReg cannot allow the substantial harm arising to consumers to continue for unknown periods. Rollout periods will likely vary across operators, and this would result in an asymmetric experience of scams for consumers.

II. Second, even as VoLTE roaming traffic grows as a share of all international voice traffic, some IGOs will continue to carry non-VoLTE roaming traffic into the State. As long as any IGO transits non-VoLTE traffic into Ireland, one or more scammers based abroad may potentially target Irish consumers while spoofing Irish Mobile numbers. This would occur even if larger IGOs such as the MNOs were to migrate fully to VoLTE roaming entirely. Therefore, even if VoLTE roaming migration is completed by one MNO this does not remove the need for this MNO to participate in the shared database, given the need for that MNO to

[103] As noted by Plum, the only combinations of operators that could yet have to apply DNO, PN and Fixed CLI Call Blocking are smaller IGOs and for DNO and PN it is smaller Voice Originators. As noted by Plum in both cases, six months appears a more than sufficient amount of time to implement this these interventions.

establish the roaming status of a call.

2.180 Consequently, the potential adoption of VoLTE roaming does not remove the need for Phase 2. ComReg also notes that the importance of successfully implementing Phase 2 is increased because not all IGOs are now required to implement Phase 1.

2.181 However, in relation to Eir and Three questioning whether VoLTE roaming traffic should feature as part of any roamer check, ComReg understands that the emerging solution for VoLTE roaming is the S8HR architecture, which would eliminate the need for such traffic to be included in a Roamer check. In this case roamer check would not need to be applied as part of normal call handling, since the home network verifies that the call is from a valid roamer and an IGO does not transit the call from a roamer into Ireland. Indeed, as Three has noted, TRAFICOM[104] did not include VoLTE roamers as part of the Finnish Mobile CLI Call Blocking solution. Therefore, on the assumption that S8HR will be uniformly adopted by all Irish MSPs as the solution for VoLTE roaming, ComReg agrees that no adaptation of the Mobile CLI blocking roamer check solution should be needed, and ComReg has removed this requirement from the Decision Instrument[105].

2.182 In relation to ICS and the origination of voice calls from roamers, ComReg notes that [✂ [redacted] ✂]. Widespread adoption of ICS for the origination of voice calls for roamers therefore does not appear imminent. Therefore, ICS is unlikely to remove the need for Phase 2 in any reasonable timeline.

2.183 With regard to Eir's view that Mobile CLI Call Blocking is not required because a Voice Firewall is also being introduced, ComReg notes that these interventions complement one another by ensuring that scam calls that are less likely to blocked by one intervention are covered by another intervention. Indeed a layered approach is considered best practice, when fighting crime of this nature. So, these interventions may overlap one another to some small degree but the overall effect is a more significant reduction in the rate of scam calls. While a Voice Firewall on its own could block some scam calls spoofing Irish mobile CLIs from abroad, it does not block all such calls reaching Irish consumers. The effectiveness of the Voice Firewall is greatly enhanced by having Mobile CLI Call Blocking already in place, such that the Voice Firewall would only be contending with any scam calls which would not be picked up

[104] The Finnish Transport and Communications Agency
[105] It should be noted that Europe Economics did include a VoLTE upgrade in its estimate of the cost for Phase 2, as a cost of €300,000-€500,000. Therefore, in the event that S8HR is adopted, and such an upgrade is unnecessary, the estimated cost of this intervention is likely to be significantly over-estimated, further improving its benefit-to-cost ratio.

by the Mobile CLI Call Blocking or other interventions (e.g., DNO/PN).

2.184 In terms of preventing scam calls spoofing Irish mobile CLIs, the Mobile CLI blocking interventions are by far the most effective approach. Absent same, some scam calls that would have been blocked by the Mobile CLI filter will be received by consumers. This arises because the Voice Firewall intervention will not be directly targeting spoofing in the same way as the Mobile CLI blocking intervention. Voice firewalls actively monitor network traffic and block malicious/scam calls depending on the rules configured within the firewalls. Such firewalls typically review calls with advanced real time call data analytics using machine learning to detect and act upon unusual patterns of call. This will without doubt include some CLI spoofing but it may not include all such calls – the blocking of these calls is best achieved through Mobile CLI Call Blocking.

2.185 Therefore, ComReg is of the view that Mobile CLI Call Blocking and Voice Firewalls are both required.

Phase 2 – Cost and proportionality

2.186 Neither Verizon or ALTO provide any evidence to support their assertions that mandating both Phase 1 and Phase 2 is disproportionate. In any event, ComReg disagrees with this view for a number of reasons.

- First, this argument could only now apply to larger IGOs, and not smaller IGOs (such as Verizon and many of ALTOs own members) which can now benefit from the Phase 1 financial threshold.

- Second, in relation to the larger IGOs, it is necessary to implement both Phase 1 and Phase 2 in order to achieve the full benefits of Mobile CLI Call Blocking. As outlined in both Chapter 2 and the CLI RIA:

    - Phase 1 requires all IGOs above the financial threshold to implement the Mobile CLI call blocking intervention. This is necessary to limit the misuse of numbers and CLI spoofing of Irish mobile numbers over the period preceding the implementation of Phase 2.

    - Phase 2 would require an industry roaming proxy server to include a non-MAP signalling protocol for IGOs to perform roamer check. This enables all IGOs (including smaller IGOs) to check the roaming status of mobile numbers on calls being transited into Ireland. This approach removes the need for smaller IGOs to invest in MAP.

2.187 More broadly, ComReg notes that neither the Verizon or ALTO submissions engage with the detailed consideration of costs outlined in both Consultation 23/52 and the Europe Economics Report which estimated the costs in respect

of Phase 1 and Phase 2.

2.188 Given that Phase 1 applies only to some IGOs and therefore not all transit traffic, Phase 2 is ever more important. Absent Phase 2, fraudsters would learn over time to circumvent Phase 1. This would reduce the effectiveness of Phase 1, and undermine the investment made by MSPs and IGOs in Phase 1 of Mobile CLI Call Blocking.

2.189 In relation to Three's contention that larger IGOs should not have to contribute to the cost of roamer check, ComReg restates that the participation of MNOs is essential to the efficient functioning of the roamer check and in turn combatting scam calls that utilise mobile CLI Spoofing. Therefore, the intended beneficiaries of Phase 2 are Irish consumers, business and society, who will enjoy greater protection from scams once smaller IGOs can access the shared database for roamer check. Furthermore, MNOs may also wish to move from MAP-based roamer check to the use of the shared solution to simplify their call routing protocols. ComReg has not specified how operators should attribute the shared costs for roamer check between themselves and will only examine this matter should issues arise.

2.190 BT questions the appropriateness of mandating roamer check because of alleged uncertainty over its cost. However, ComReg does not share those concerns and notes that some degree of uncertainty is unavoidable given that only one other country (Finland) has so far implemented this solution. Europe Economics has provided robust costs estimates based on the best available evidence. No respondent, including BT, has provided any evidence to suggest that the estimates provided by Europe Economics were incorrect.

2.191 ComReg has provided operators with information on the requirements in the draft Mobile CLI Call Blocking DI, the Functional Requirements and the Finnish example as a template. Therefore, operators have been given sufficient information to estimate their own costs of implementation. Furthermore, such issues can be further discussed at the relevant working groups. BT has simply asserted that there is some uncertainty with costs without providing any estimates of its own. It is therefore difficult for ComReg or Europe Economics to engage with BT's submission on this matter. Moreover, ComReg notes that this intervention would very likely still be proportionate even if costs were higher, such is the level of harm associated with call spoofing. In fact, Europe Economics has revised the estimate costs for Mobile CLI Blocking to reflect changes (made in response to submission from respondents) and the estimated costs have fallen from those consulted upon in Consultation 23/52[106]. Therefore, this finding appears robust to any

[106] Europe Economics Response, Annex.

credible margin of error in cost estimation.

Draft Decision Instrument

2.192 In relation to Eir's request for clarification on the role of MSPs, ComReg notes that Decision 2 in the Draft DI for Mobile CLI Call Blocking correctly refers to MSPs because it is the MSPs that must facilitate other IGOs to connect to their networks using MAP to assess the roaming status of a given number. However, the description in the "Part V – Effective Date" incorrectly refer to Decision (2) and this has been amended. Furthermore, the text in Parts IV and V has now been amended to reflect that only certain IGOs are participating in Phase 1, and that MSPs must grant such IGOs a connection within three months of the date of the decision.

2.1.5 Voice Firewall

Summary views of ComReg in Consultation 23/52

2.193 In Chapter 4 of Consultation 23/52, ComReg was of the preliminary view that the Voice Firewall was likely to be technically feasible and effective at reducing scam calls. ComReg was also of the preliminary view that the implementation of the Voice Firewall could be implemented within 18 months of any Decision.

2.194 In Chapter 5 of Consultation 23/52 and within the draft Voice Firewall RIA, ComReg set out its preliminary assessment of the Voice Firewalls impact on consumers, stakeholders, and competition. In summary, ComReg was of the preliminary view that the introduction of a Voice Firewall best promotes the efficient use of numbers, competition, and efficient investment in ECS markets.

2.195 Chapter 7 of Consultation 23/52 contained the draft DI for the Voice Firewall. Among other things, the DI outlined the types of operators that would have to apply this intervention, including the obligations which would apply to these relevant undertakings.

2.196 ComReg was of the preliminary view that it was proportionate to require only MSP or FSPs[107] with at least 330,000 voice capable subscribers[108] (i.e., 5%

[107] Consultation 23/52 - Draft Decision Instrument for Voice Firewall Specification – ""*Fixed Service Provider" or "FSP" means an Undertaking providing End-Users with publicly available voice telephony services using a Fixed Number at a fixed location, irrespective of the underlying technology over which such services are delivered; …..*"Mobile Service Provider" or "MSP" means an Undertaking providing End-Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network."

[108] Consultation 23/52 - Draft Decision Instrument for Voice Firewall Specification - "*Voice Capable Subscriber" means a mobile subscription or fixed line that is capable of originating and terminating a voice call on a public network".*

of mobile and fixed subscribers) to apply a Voice Firewall within 18 months. MSPs which were also Network operators would be required to apply a Voice Firewall on behalf of all virtual operators on their networks, where technically feasible[109].

View of respondents to Consultation 23/52

2.197 The views of respondents on the Voice Firewall are summarised and assessed by ComReg under the following headings:

- Support for the Voice Firewall;
- Effectiveness and proportionality;
- Draft DI and draft RIA;
- Legal Basis;
- Proposed Timelines;
- Scope; and
- Subscriber based Thresholds.

Support for the Voice Firewall

2.198 ALTO, Bank of Ireland, BPFI, Eir, Ericsson, Hiya, and NetNumber expressed support for this measure.

Effectiveness and proportionality

2.199 Hiya contends that a Voice Firewall is an important future-proofed intervention and that without it, scammers would inevitably circumvent any static measures. Hiya notes that Voice Firewalls can utilise AI systems to better identify scams, noting that its own products utilise AI.

2.200 Eir and Microsoft both submit that a voice firewall is potentially an effective means of combatting scams, if designed and implemented successfully.

2.201 ALTO states that a firewall[110] is "*useless*" in scenarios where it is not ubiquitous.

2.202 Virgin contends that ComReg did not provide sufficient evidence to support the three categories of scams that a Voice Firewall would combat compared

[109] Consultation 23/52 - Draft Decision Instrument for Voice Firewall Specification - "*Relevant Undertakings who are also a Network MSP and/or Network FSP shall satisfy the requirements below for other Undertakings who are MSPs and/or FSPs and for whom they provide a voice call origination and termination service, where technically feasible.*"

[110] ComReg understands that ALTO is referring a Voice Firewall when using the term "Nuisance Calls Firewall".

to the static interventions. Virgin states that it does not support a Voice Firewall "*at this stage*", as more evidence is needed, in its view, to justify its implementation. In relation to each category of scam identified by ComReg (highlighted in bold), Virgin asserts the following:

- **Scam calls originating in Ireland** – Virgin disputes that there is an increase in such scams and argues that the views of law enforcement, notably An Garda Síochána is not what it considers to be "*strong evidence*". Rather, Virgin contends that ComReg should suspend this work and focus instead on the production of empirical evidence that scams based in Ireland are increasing which it could then consider in turn.
- **Scam calls from abroad that do not spoof Irish numbers** - Virgin claims that its existing fraud management processes can identify suspect international traffic and that Virgin can address such issues by engaging with the relevant IGOs.
- **Future scams such as those driven by Artificial Intelligence (AI)** - Virgin concedes that AI may increase the risk of scams but notes that it is not clear whether a Voice Firewall would be effective in combatting AI-based scams.

Draft Decision Instrument and draft Regulatory Impact Assessment

2.203 Three and Virgin both argue that the draft DI for the Voice Firewall is too vague. Three further contends that the draft DI does not, in its view, provide legal certainty because it refers to "*highest probability*" or "*a high probability of being a scam call that is other than the highest probability*" but does not define a threshold for these classifications.

2.204 Three also maintains that neither the draft DI nor the draft RIA consider the impact of false positives (e.g., blocked legitimate calls) and false negatives (e.g., not-blocked scam calls) on originators and recipients.

Legal Basis

2.205 Three claims that the Voice Firewall raises issues with the ECHR because, in its view, it involves the profiling of individual data which is transmitted across borders.

Costs

2.206 Virgin and Vodafone both opine that the technical specifications are too vague to understand the potential cost impacts, and that there has been no engagement in relation to implementation and operational costs for a voice firewall. Vodafone submits that it would be more efficient for it to invest in

"*centralised solutions*" that will "*become available*" to it "*over the next year*".

Proposed Timelines

2.207 Hiya suggests bringing forward the deadline for the Voice Firewall, while Microsoft, which plans on providing voice firewall solutions in the future, claims that the implementation timeline of 18 months is too short.

Scope

2.208 Eir contends that there is no need for the Voice Firewall to apply to Fixed Voice traffic given the introduction of static measures.

Subscriber Thresholds

2.209 Eir contends that there should be no threshold for applying the Voice Firewall and that all operators should be required to apply this intervention.

2.210 Cellusys states that it has implemented signalling firewalls on several mobile networks with less than 100,000 subscribers including a start-up fixed network, as mandated by the Telecom Regulatory Authority of India (TRAI).

Views of Consultants

Plum

Proposed timelines for implementation

2.211 In summary, Plum found that the timelines in the Decision Instrument for Voice Firewall are appropriate, because the interventions[111];

- Are often deployed in less than 18 months in practice; and
- These same operators have already implemented DNO, PN and Fixed CLI Call Blocking.

ComReg assessment

Support for the Voice Firewall

2.212 ComReg acknowledges the support of ALTO, Bank of Ireland, BPFI, Eir, Ericsson, Hiya, and NetNumber for the Voice Firewall.

Effectiveness and proportionality

[111] Readers are referred to the Plum Report for more information.

2.213 ComReg acknowledges the support of Hiya and Eir regarding ComReg's view that the Voice Firewall is necessary to combat scams given its ability to adapt dynamically to scammers ever changing tactics. ComReg agrees that AI software appears to increase the effectiveness of such predicative models to identify scams, noting recent news that certain payment service providers such as Revolut are using AI for this purpose[112].

2.214 In relation to ALTO's views regarding the coverage required to ensure the effectiveness of a Voice Firewall, ComReg notes that a Voice Firewall applies to terminating calls and therefore cannot be circumvented by simply re-routing a network. For interventions that apply to terminating traffic, such as the Voice Firewall[113], the interventions effectiveness is proportionate to its coverage, a point which was raised and addressed in the draft RIAs.

2.215 In relation to Virgin's queries regarding the evidence supporting the Voice Firewall, ComReg addresses each of the points below.

1. Scam calls originating in Ireland.

2.216 An Garda Síochána is responsible for investigating fraud in the State and relevant staff of the Garda National Economic Crime Bureau (GNECB) previously informed ComReg that calls targeting consumers were originating in the State and that ongoing investigations into such scams were being conducted. ComReg has absolutely no reason to doubt that the information provided by An Garda Síochána is in any way incorrect. Indeed, it would have been negligent of ComReg to ignore information provided by the primary law enforcement agency of the State on matters that ComReg was actively consulting upon. Law enforcement agencies often have insights into the source of crime from crime reports for which there is no alternative source.[114]

2.217 ComReg also notes that in the intervening period since the publication of Consultation 23/52, An Garda Síochána intercepted a criminal enterprise based in Ireland that targeted Irish and international consumers. It was noted at the time that "*Officers attached to the Waterford Division Crime Hub say they have been conducting "a complex criminal investigation" focusing on organised transnational criminal activity involving the sending of a large amount of smishing texts, theft, deception and money-laundering,* ***both in Ireland and abroad*** "[115] [Emphasis added]. With that in mind, ComReg will

[112] Revolut launches AI feature to protect customers from card scams and break the scammers "spell" | Revolut United States
[113] ComReg assumes that ALTO was in fact referring a Voice Firewall and not CLI Call Blocking interventions in using the term "Nuisance Calls Firewall".
[114] Indeed in the UK public policymaking has taken into consideration the views of the London Metropolitan Police regarding the domestic and foreign origins of fraud. Link
[115] Waterford gardaí investigating scams seize €1.12m in 'first major seizure of cryptocurrency' (irishexaminer.com)

continue its engagements with An Garda Síochána.

2.218 In any event, the reduction in scams based abroad which spoof CLI due to the static interventions will inevitably increase the incentives for criminals to initiate national based scams. As previously noted, the package of interventions proposed by ComReg is designed to reduce scams calls and text through existing routes but also anticipate how scammers would react to the implementation of the interventions proposed by ComReg. As noted in the draft Voice Firewall RIA, "*the importance of the Voice Firewall grows as fraudsters adapt to the static interventions by either sidestepping (e.g., **scam calls without CLI spoofing**, **originating scams within Ireland**, bringing Irish SIM cards abroad) or overcoming them (e.g., impersonating businesses not on the DNO)*." [Emphasis added].

2. Scam calls from abroad that do not spoof Irish numbers.

2.219 It appears that Virgin may not fully appreciate the capabilities of the Voice Firewall. A Voice Firewall assesses all terminating traffic in real time for its likelihood of being a scam call and can therefore block likely scam calls. As noted in Consultation 23/52, scammers can circumvent the static interventions in a number of ways. First, scammers can continue to connect with Irish consumers simply by using international numbers or spoofing the trusted numbers of nearby countries (+44 for the UK). Indeed, international scammers can adapt to controls on CLI spoofing and continue to present Irish numbers by acquiring legitimate Irish numbers (e.g., acquiring an Irish SIM or illegitimately acquiring a Irish Geographic Number).

2.220 In the case of mobile numbers, this entails transporting or delivering Irish SIM cards to the country in which the scammer operates or downloading and activating an eSIM. Any scam calls from such SIMs would have a legitimate roamer status and connect with Irish subscribers while displaying an Irish CLI[116]. Only an intervention that applies to all terminating traffic and which is assessing factors other than the CLI could possibly identify and block such scam calls.

2.221 The alternative proposed by Virgin appears to involve allowing scam calls (and potential fraud) to occur so that it can be reported to Virgin, which would then engage with the relevant IGOs to disrupt the conduct (via an unspecific action) subsequently. It is unclear how Virgin proposes to block potentially scam calls without assessing individuals calls.

2.222 Virgin has not explained this process or how many calls it has blocked in this

[116] While operators may ultimately identify and block such SIMs from originating calls this can take time as consumers report call and operators investigate the issues.

manner to date. Moreover, this approach would require consumer reporting and inter-operator cooperation and would not prevent calls in real time compared to a Voice Firewall. Such a delay (possibly weeks) would permit potentially hundreds of thousands of scam calls to reach consumers before any action is taken. As previously noted, ComReg cannot allow a situation where consumers are harmed so egregiously to persist, particularly when there are viable solutions already available to reduce and mitigate that harm. ComReg is not considering ex-post interventions where follow up actions take place after the harm has occurred.

3. Future scams such as those driven by AI

2.223 ComReg remains of the view that a voice firewall is an effective intervention against AI based scams. Like existing scam calls, an AI based scam call may also have identifying characteristics that only a Voice Firewall could identify. Absent a Voice Firewall there would be no way of identifying and blocking such calls in real time. Therefore, while there is uncertainty regarding the risk posed by AI based scam calls, consumers are clearly more protected against AI based scam calls if operators apply a Voice Firewall, noting that additional actions might of course be required depending on the future development of AI.

2.224 In relation to the view that a consultation on the Voice Firewall should only occur after first assessing the impact of the static voice measures, ComReg notes that such an approach would inevitably result in consumer harm over an extended and undefined period for a number of reasons:

- First, as highlighted above, there are a number of existing scam call types that only a Voice Firewall can combat effectively (See Paragraph 5.152 of Consultation 23/52 as summarised in Paragraph 2.133 above.) These types of calls are not simply theoretical and have already been identified by ComReg as a source of scam calls. It would be remiss of ComReg to identify a source of scam calls in its consultation and then fail to put in place measures to protect consumers against same. Europe Economics estimated that €152 million in harm would be prevented by the Voice Firewall before 2030, based on the existing profile for scam calls. Therefore, even a delay of one to three years in implementing the Voice Firewall could permit a significant amount of consumer harm.

- Second, scammers are entrepreneurial and can be expected to switch to scams that circumvent the static voice measures once they are implemented. Europe Economics also estimates that the Voice Firewall could prevent €892 million in harm in the event that scammers fully switched to scam types that are not covered by the static voice

interventions (e.g., non-CLI Spoofing scam calls). The one-to-three-year delay created by a 'wait and see' approach would provide a considerable amount of time for scammers to learn and adapt to circumvent the static interventions. However, scammers would not be able to sidestep the Voice Firewall as readily because it applies to all traffic.

2.225 Evidence from Australia indicates that scammers quickly adapt to static interventions, at which point dynamic interventions such as the Voice Firewall become ever more important. Since the publication of Consultation 23/52, the ACMA has published a detailed breakdown of the number of scam calls blocked by each intervention which shows that between Q3 and Q4 of 2023 alone, blocking based on call characteristics (which is dynamic in nature) rose from 29% to 62%, while calls blocked on the basis of Protected Numbers fell from 54% to 21%.

Table 2: ACMA Blocking statistics per intervention.

	July-Sept 2023	Oct - Dec 2023	% change
PN	121,641,081	51,540,817	-58%
Invalid int'l CLI	3,162,376	3,745,189	18%
CLI Call Blocking	32,973,353	33,243,148	1%
Call characteristics	64,770,144	153,238,877	137%
Other	2,443,221	3,470,053	42%
Total	224,990,175	245,238,084	

Source: The ACMA's "*Phone Scams: Intelligence Report Q2 (Oct-Dec) 2023-24*"[117]

Draft Decision Instrument and draft Regulatory Impact Assessment

2.226 In relation to Three's and Virgin's views that the Voice Firewall DI is too vague, and that clarity around the "*highest probability*" terminology is required, ComReg makes the following observations.

2.227 ComReg's approach to the Voice Firewall DI is to mandate relevant undertakings to take certain actions but also provide flexibility to implement those actions in the most efficient manner possible. Broadly speaking, there are four operational requirements[118] in the Voice Firewall DI, within which relevant undertakings have flexibility over how those requirements are implemented in practice. In summary, relevant operators shall: (i) use a Voice Firewall which should (ii) identify and classify calls according to the probability

[117] For simplicity, ComReg has relabelled the ACMA interventions using the terminology contained throughout this report. *4.2.1-Invalid or unallocated Australian numbers – Protected Numbers, 4.2.3-Invalid international numbers (unallocated country code or digit length) – Invalid International CLI*
4.2.5-Australian Calling Line Identification (CLI) from international source – Fixed CLI Call Blocking
[118] The Decision Instrument also requires relevant undertakings to provide a number of fixed metrics.

of being a scam call, (iii) block calls with the highest probability of being a scam call, and (iv) modify calls with next highest probability classification.

2.228 Given these broad requirements, relevant undertakings have flexibility to determine how and what voice firewall should put in place and how that voice firewall classifies calls according to the highest probability. A voice firewall does not provide a guarantee that any particular call is a scam or not, rather it identifies calls which may be scams according to varying degrees of likelihood based on an assessment of the characteristics of the call. The Voice Firewall DI sets out that calls that have the highest likelihood of being a scam (however this is determined by the voice firewall) should be blocked. Scam calls that the voice firewall determines are highly likely to be a scam call (but not the highest likelihood) should have their CLI modified. All other calls should be treated as normal and forwarded to subscribers with the full unmodified CLI details.

2.229 It should be noted that the Voice Firewall DI does not seek to specify the levels of probability that a relevant undertaking should use to determine whether a call should be blocked or modified. This is a matter for the relevant undertaking based on the specification of the voice firewall and engagement with its vendor and/or other relevant parties[119]. It would not be appropriate for ComReg to specify the exact requirement of the firewall because operators may use different voice firewall solutions, and these may estimate the risk of scams differently and/or adopt different approaches. Indeed, ComReg has expanded the definition of “Modified” to provide even greater flexibility to operators when dealing with suspicious calls by allowing operators to take the most appropriate action to alert the consumer of the identified risk from a given suspicious call. These modifications allow operators to take action to inform and protect consumers even where a call is suspicious, but an operator deems the risk of inadvertent blocking of a legitimate call is high (i.e., a false positive).

2.230 ComReg envisages that, having been mandated to use a voice firewall and to block and modify calls, operators have strong incentives to ensure that the firewall is optimised correctly to block the maximum number of scams or warn consumers about potential scams through modification of the CLI. Furthermore, in order to ensure some consistency in the operation of firewalls across different operators, ComReg considers it appropriate to discuss any issues around the implementation of the voice firewall through the planned NCIT technical working groups. In this forum operators will have the opportunity to discuss issues and seek guidance on the use of a Voice

[119] The optimal probability to use would depend on balancing the risk of Type 1 (blocked legitimate calls) and Type 2 errors (not blocked scam calls), which will only be known once operators begin blocking and may change over time as the profile of legitimate and scam traffic changes.

Firewall to block suspicious voice traffic, including any guidance provided by ComReg.

2.231 ComReg has also considered whether the requirement to modify certain calls in the Voice Firewall DI is necessary. However, modification allows operators to categorise calls that the Voice Firewall determines may be scams but has less certainty compared to calls the Voice Firewall considers more likely to be scam. It is likely that consumers would prefer to be warned that there is a risk of being scammed by such calls. Modification should also reduce the false positives and false negatives associated with a voice firewall because consumers are still free to answer such calls and establish whether they are valid or not including accessing details on the call through their voicemail which may be used to leave a message by the caller.

2.232 In relation to Three's query regarding the impact of false positives and false negatives on originators and recipients, it should be noted that false negatives are scams which are not blocked, and these will be greatly reduced by the interventions. Therefore, this represents an improvement in the occurrence of false negatives, relative to the status quo. ComReg notes that it did analyse false negatives in the Draft RIA, and has provided further analysis of false positives (legitimate calls/SMS that are blocked) in paragraphs above.

Legal Basis

2.233 In relation to Three's claims in relation to various legal provisions, ComReg notes that it has not previously encountered the view that a Voice Firewall intervention raises concerns under any current EU law or relevant human rights law, including the ECHR. Three has not substantiated its point in relation to this. ComReg is unaware of any issues regarding the legality of the use of a number of Voice Firewall solutions, which are now used by operators in a number of EU countries, and notes that vendors contend that their solutions are compliant with EU law, namely GDPR and the ePrivacy Regulations. For completeness, ComReg notes that from a data protection perspective, even if "*personal data*" is involved, and the General Data Protection Regulation is engaged, then the "*legitimate interests*" basis for processing under Article 6(1)(f) is likely to be engaged. As Recital 47 of the GDPR states: "*The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned*."

2.234 ComReg notes that it is the responsibility of operators to ensure compliance of their systems with relevant EU law. ComReg is aware of a number of solutions which are in use across the EU, and also notes the submission from Hiya, which provides spam and fraud call protection and identity services to more than 450 million users around the globe.

Costs

2.235 In relation to Vodafone's contention that the Voice Firewall cannot yet be costed given the uncertainty and that there has been no engagement with operators, ComReg notes that Europe Economics produced detailed cost estimates based both on discussions with Irish operators[120] and discussion with vendors of Voice Firewall solutions[121]. ComReg notes that Vodafone makes no reference to either Europe Economics methodology or the calculations and estimates provided.

Proposed Timelines

2.236 Microsoft and Hiya, considered the proposed timeline of 18 months too short[122] and too long, respectively. ComReg agrees with Plum that the 18-month deadline given in Consultation 23/52 is in fact reasonable and proportionate, as these interventions are:

- Relatively straightforward to apply from a technical perspective with a wide variety of providers offering off-the-shelf solutions;
- Demonstrably possible, as vendors report that most of their international client operators have implemented this intervention within 18 months[123]; and
- Only being applied by larger operators, which are at lower risk of 'overburdening', given their greater organisational capacity[124].

2.237 In light of this, ComReg remains of the view that a 18-month deadline for implementation of the Voice Firewall is appropriate and proportionate.

Scope

[120] This included an interview in October 2022 between Europe Economics and Vodafone, attended by ComReg at which costs for interventions, including a Voice Firewall, were discussed.
[121] Including one vendor, [✂ ✂]. It should be noted that this informed the estimates of Europe Economics, which included further costs other than the "sticker price".
[122] ComReg notes that Microsoft made reference to "*Microsoft itself is currently developing products that will deploy AI as a powerful tool to combat illegitimate scam calls*.", which did not provide any specific information on the product pipeline. In February, Microsoft announced that it is conducting a trial of a new product called '*Azure Operator Call Protection*', which analyses the real-time audio of voice calls to detect scams, which can then be interrupted Link. ComReg does not consider this intervention as a potential regulatory option at this time given the uncertain timelines (e.g., it's currently in trial and testing) and that no respondent to Consultation 23/52 made reference to such products. ComReg considers the standard Voice Firewall which has achieved successful results in other markets is more appropriate for consideration at this time. ComReg will continue to monitor other potential interventions into the future.
[123] This information was provided by [✂ ✂].
[124][124] As noted by Plum the only combinations of operators that could yet have to apply DNO, PN and Fixed CLI Call Blocking are smaller IGOs (as this has been applied by most) and for DNO and PN it is smaller Voice Originators. As noted by Plum in both cases, six months appears more than sufficient amount of time to implement this these interventions.

2.238 In relation to Eir's view that the voice firewall should not apply to fixed voice connections (i.e. landlines), ComReg notes the following:

2.239 First, it should be noted that a large number of end-users are contactable by and make use of landlines, and are therefore at risk from scams targeting landlines, with roughly 1.2 million fixed voice subscriber lines in as of Q4 2023[125]. Over two in five Irish consumers report using a landline (41%)[126] rising to two thirds of consumers over the age of 65. Based on this, Europe Economics estimate that over 1.5 million consumers[127] may make some use of a landline. These consumers report receiving an average of 7 calls on their landline each week.

2.240 Second, ComReg established that landline users have experienced high levels of scam calls. In particular three in four (74%) landline users report to having received a scam call on their landline[128]. Landline users experience a wide variety of scam calls with approximately half of consumers reporting having received a Wangiri call (56%), a robocall (51%), or an impersonation scam call (47%). It is surprising that Eir dismisses this justification – indeed Eir has not provided any evidence whatsoever to contradict the fact that landline users suffer from scam calls. A considerable amount of preventable harm to landline users should be expected to persist absent the Voice Firewall given the likely millions of scam calls that were received by landline users. ComReg's rationale for the Voice Firewall applies to both mobile and fixed networks. Such scam calls would continue to occur over fixed networks if the Voice Firewall was applied to mobile calls but not to fixed (e.g., those based nationally, from foreign numbers, those spoofing foreign numbers etc.). This is exacerbated as many landline handsets do not have a display screen meaning many landline users may have no ability to screen calls (e.g., to not answer international calls).

2.241 Third, as previously noted, fraudsters can be expected to switch to scams that circumvent the static voice measures once they are implemented. In the event that a Voice Firewall is not applied to fixed traffic, fraudsters could easily target unprotected landline users, simply by targeting Irish Geographic Numbers instead of Mobile Numbers. Therefore, the number of scam calls being received by landline users would likely increase, disproportionately impacting older people who are more likely to use and be reliant on landline services.

2.242 Fourth, the B&A Consumer Survey established that where trust in a

[125] ComReg Quarterly data "Q4 2023 QKDR All Data" Link
[126] B&A Consumer Survey, slide 7.
[127] Europe Economics Report, page 103.
[128] B&A Consumer Survey, slide 14.

communication channel declined, use fell also. As older users rely far more on landlines, any loss of trust in landlines could reduce older users' likelihood to answer landlines calls which they may use to contact and be contacted by their friends and family or organisations (e.g., healthcare).

2.243 ComReg has taken care to ensure that the Voice Firewall is applied in a proportionate manner. Indeed, ComReg's decision to adopt a subscriber-based threshold for the Voice Firewall was based, in part, on the large number of smaller fixed networks that would otherwise have to apply the Voice Firewall to very low volumes of traffic. In relation to Fixed Voice traffic specifically, ComReg previously noted that there could be some flexibility in which operators are required to apply the Voice Firewall to Fixed Voice traffic in light of uncertainty regarding the data for Fixed Voice subscriptions at the wholesale level.[129] However, ComReg received no submissions from operators on this point. Therefore, there does not appear to be any reason to adjust how the number of subscribers are determined[130].

Subscriber based threshold.

2.244 As outlined in Section 5.2.4 of Consultation 23/52, ComReg was of the view that requiring all relevant networks to implement the Voice Firewall (including fixed voice[131]) at this time may be disproportionate and provide little additional benefit given the small number of subscribers held by some operators. In particular, it would potentially impose a large cost on smaller firms, possibly distorting competition, given that some fixed operators have fewer than 1,000 subscribers. More specifically, ComReg considered both a threshold of 66,000 subscribers (1% of total subscribers) and 330,000 subscribers (5% of total subscribers). ComReg was of the preliminary view that it would be appropriate to set the threshold at 330,000 subscribers, below which the implementation of the Voice Firewall is not required. This was to account for the smaller fixed networks providing Voice services that would otherwise be included[132].

[129] Footnote 209 in Consultation 23/52 "*Fixed Voice is measured using lines, both residential and non-residential, as a proxy for subscribers as this is the most appropriate data available. ComReg considers this a conservative estimate of end-users for landlines, noting that the true number of users may be higher in the case of non-residential lines. This data is the best data available to ComReg for attributing landlines at a wholesale level. ComReg will update this data where an operator can demonstrate with adequate evidence that a sufficient number of attributable Fixed Voice Lines on their network are either a) inactive or b) account for a negligible share of Fixed Voice* [subscribers]"

[130] Notwithstanding, ComReg notes Eir accounts for the majority of landline subscribers at a wholesale level, with several hundred thousand subscribers with a Fixed Voice capability. Realistically, a Voice Firewall that did not apply to Eir would not achieve a level of coverage that would protect most landline users and deter fraudsters.

[131] It should be noted that Eir suggest ComReg suggest that ComReg exclude Fixed Voice from the Voice Firewall **and** to remove the subscriber-based threshold for determining which operators must apply the Voice Firewall. ComReg understands that Eir wishes ComReg to do both simultaneously (i.e., have it applied by all MSP, to mobile traffic only). Nonetheless, despite its finding on the need to cover the Fixed Traffic, ComReg has still assessed the need for a subscriber based threshold.

[132] In practice, the number of operators benefiting from this threshold compared to the 1% threshold is very low.

2.245 In practice, the number of operators benefiting from this threshold compared to the 1% threshold is very low. Furthermore, because the threshold is stated as 'number of subscribers' (i.e. 330,000), rather than the '% of total subscribers' (i.e. 5%), it is likely that the % of the market not covered by the voice firewall will fall over time as number of total subscribers increases. ComReg noted that the proposed approach was proportionate as it only includes sufficiently large operators, while ensuring the majority of consumers benefit from the protection of a Voice Firewall. Indeed, the removal of the subscriber-based threshold would only increase coverage marginally.

2.246 Finally, it is not clear to ComReg what TRAI decision Cellusys refers to in its submission. ComReg notes Cellusys' view that it has implemented signalling firewalls for small operators (c.100,000) in the past. However, as noted above, there are a number of fixed line operators in Ireland that have less than 1,000 subscribers and the potential costs associated with the firewall (as referenced in Consultation 23/52) may be disproportionate if the threshold is removed altogether. ComReg will continue to monitor these thresholds and may review the requirement for a threshold, and if so its level, in the future.

2.1.6 SMS Sender ID registry

2.247 In Chapter 4 of Consultation 23/52, ComReg outlined its reasons for finding that a SMS Sender ID Registry was technically feasible, effective, and could be reasonably implemented within 18 months of any final Decision (12 months for modification and an additional six months for blocking).

2.248 The draft Sender ID RIA in Chapter 5 of Consultation 23/52 set out ComReg's preliminary assessment on the impact of the SMS Sender ID Registry on consumers, stakeholders and competition. ComReg was of the preliminary view that the SMS Sender ID Registry would provide protection to businesses/organisations that are most impersonated by fraudsters and best promote the efficient use of numbers, competition, and efficient investment in ECS markets.

2.249 Chapter 7 of Consultation 23/52 contained the Draft DI for the SMS Sender ID registry, which outlined the types of operators that would have to apply these interventions, as well as the precise legal obligations which would apply to these operators. In particular, the Sender ID Registry would apply to the following.

- Mobile Service Providers ("MSP")[133] with at least 270,000 mobile subscribers, excluding machine to machine ("M2M") and mobile broadband subscribers ("MBB")[134]. Such MSPs would also apply the intervention where technically feasible[135] to the subscribers of all virtual operators on their networks.

- Participating Aggregators ("PA")[136] to block any SMS making illegitimate use of Sender ID from 12 months after the Decision.

View of respondents to Consultation 23/52

2.250 The views of respondents on the SMS Sender ID Registry are summarised and assessed by ComReg under the following headings:

- Support for the full SMS Sender ID Registry;
- Operation;
- The competitive effect of ComReg's proposal;
- Draft Decision Instrument
- Proposed Timelines
- Legal Basis; and
- Analytics

Support for a full SMS Sender ID Registry

2.251 Bank of Ireland, BPFI, Ericsson, Hiya, NetNumber, Tanla, Three, Twilio, and Vodafone expressed support for this measure.

Operation

2.252 Twilio and Microsoft both contend that ComReg should operate the SMS

[133] Consultation 23/52 - Draft Decision Instrument for Voice Firewall Specification – ""*Fixed Service Provider" or "FSP" means an Undertaking providing End-Users with publicly available voice telephony services using a Fixed Number at a fixed location, irrespective of the underlying technology over which such services are delivered; …..*"Mobile Service Provider" or "MSP" means an Undertaking providing End-Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network."*

[134] Consultation 23/52 - Draft Decision Instrument for Voice Firewall Specification - "*Voice Capable Subscriber" means a mobile subscription or fixed line that is capable of originating and terminating a voice call on a public network".*

[135] Consultation 23/52 - Draft Decision Instrument for SMS Sender ID Registry Specification - "*Relevant Undertakings who are also a Network MSP and/or Network FSP shall satisfy the requirements below for other Undertakings who are MSPs and/or FSPs and for whom they provide a voice call origination and termination service, where technically feasible."*

[136] Consultation 23/52 - Draft Decision Instrument for SMS Sender ID Registry Specification - *"Participating Aggregator" or "PA" means a SMS Aggregator that is permitted to transit or forward a SMS carrying a Registered Sender ID from the SIDO to one or more MSPs within Ireland;"*

Sender ID Registry. Microsoft contends that if the registry was operated by industry it could function in a manner that it terms "*model-independent*".

2.253 MEF supports an administrator role, with separate streams for operational and technical matters, and for regulatory oversight and governance.

The competitive effect of ComReg's proposal

2.254 Twilio contends that Sender ID Operators (SIDOs) should be allowed to employ multiple PAs as this would promote the interests of SIDOs, promote competition, and remove the need for a SMS Sender ID portability system. Twilio observes that the Singaporean regulator, the IMDA, allows multiple PAs per SIDO. Twilio maintains that a PA-led registration could lead to one PA per SIDO in practice, and cause a distortionary land-rush for Sender IDs, as assignment is on a "*1st come 1st serve*" basis. Twilio further contends that any entity with an Irish business or operation should be eligible to become a SIDO and to register a Sender ID directly with ComReg.

2.255 Openmind contends that the SMS Sender ID registry would, as currently proposed, result in a concentration in SMS aggregators and that this can be avoided by only requiring MNOs to verify Sender ID.

2.256 Three contends that the proposed requirement for a single PA (Participating Aggregator) per SIDO is anti-competitive. Three states that this undermines MNOs ability to combat scams as it would prevent [✂[redacted]✂].

Draft Decision Instrument

2.257 Twilio does not agree that a direct connection to MNOs is required. However, Twilio submits that if this is required, MNOs should be obliged to provide access to PAs at least three months in advance to allow for testing.

2.258 Microsoft contends that ComReg should only modify Sender IDs and not block the SMS because consumers can simply ignore the scam SMS and block the numbers from which the SMS originated. Microsoft maintains that the IMDA only requires the modification of the Sender ID of SMS bearing unregistered Sender ID.

2.259 Virgin Media and Three both argue that ComReg should not implement this measure before further consultation with industry.

2.260 Eir contends that this intervention should not have a threshold and that all relevant operators should apply it.

Proposed Timelines

2.261 Three contends that the proposed timeline is unrealistic in its view. Similarly, Vodafone is concerned that a 12-month timeline for implementation is too short and could lead to an inferior design and solution. Virgin states that the [✂[redacted]✂].

Legal Basis

2.262 Vodafone questions whether filtering and the use of "*likely scam*" are permissible under the 1983 Act and the Intercept Act. Vodafone further opines that modification does not have a legal basis in Ireland.

Analytics

2.263 Revolut contends that SIDOs should be informed when illegitimate traffic using their Sender ID is blocked to enable organisations to take protective measures.

Views of Consultants

Plum

Proposed timelines for implementation

2.264 In summary, Plum found that the timelines in the Decision Instrument for SMS Sender ID Registry are appropriate, because;

- The bulk of the work lies with ComReg which has committed and prepared for the implementation of the Registry; and
- It no longer requires all aggregators to connect directly with MNOs.

2.265 Plum note that the timelines for ComReg are "*reasonable and achievable but challenging*".[137]

ComReg assessment

Support for a full SMS Sender ID Registry

2.266 ComReg acknowledges the support of Bank of Ireland, BPFI, Ericsson, Hiya, NetNumber, Tanla, Three, Twilio, and Vodafone for the SMS Sender ID Registry.

[137] Readers are referred to the Plum Report for more information.

Operation

2.267 ComReg agrees that it, rather than industry, is best placed to oversee the operation of the SMS Sender ID Registry.

The competitive effect of ComReg's proposal

2.268 Several operators have expressed concern that the proposed requirement of one PA per SIDO would reduce competition for the SMS transmission services required by SIDOs. ComReg is of the view that it needs to strike a balance between preventing/reducing scam SMS and allowing competition to take place in the selection of PAs per SIDO[138].

2.269 Promoting competition for SMS transmission services and reducing scams are both policy issues that should benefit consumers and SIDOs, but ComReg is of the view that consumers and SIDOs would prioritise the prevention/reduction in scams as a foremost requirement. However, there are also concerns about whether the requirement for a single PA would be effective in practice given the current SMS transmission processes which typically uses more than one PA to deliver a SMS with Sender ID to the end user.

2.270 Therefore, in order to provide additional flexibility, ComReg will now permit multiple PAs per SIDO, in a process that should also significantly reduce Sender ID Spoofing and at the same time, promote consumers' trust in the authenticity of Sender IDs[139] that they receive. This process of providing the safe routing of valid SMS with Sender ID will require various stakeholders to ensure that any SMS they receive is validated throughout the chain of transmission. More specifically, ComReg proposes to use an approach whereby a SMS bearing a Sender ID may only be originated or transmitted by SIDOs[140] and PAs[141] both of which need to register with ComReg to use and/or transmit an SMS with Sender ID.

2.271 In practice, any organisation that wishes to use a Sender ID will need to register with ComReg as a SIDO and also register the exclusive use of the Sender IDs that they wish to use, or empower a PA to undertake these actions on their behalf. The PA(s) originating SMS from the SIDO (the

[138] ComReg takes the potential for any detail of the SMS Sender ID Registry to have anti-competitive impacts very seriously. It may be the case that certain trade-offs between network security and maximal competition are unavoidable. Where these desirable policy goals are in conflict, ComReg may be required to make a decision with regard to which to prioritise, or what approach most appropriately balances the two desirable outcomes.
[139] This approach is conceptually more similar to that deployed in Australia and Singapore.
[140] 'Registered SIDOs' refer to SIDOs that have registered with ComReg and the Sender IDs that they are allowed to send.
[141] Participating Aggregators means a SMS Aggregator that is permitted by ComReg to transit or forward a SMS carrying a Registered Sender ID from the Register SIDO to one or more MSPs within Ireland. ComReg will retain a list of Registered Participating Aggregators and will monitor their compliance.

"Originating PA") would validate at the point of ingress that the SIDO is registered with ComReg and that the Sender ID(s) being used are registered against that SIDO. Any further transmitting of that SMS from the Originating PA to another PA (e.g. PA1) would require that each PA validates that the other is registered with ComReg and that the Sender ID is registered. This second step is repeated by each following hop between PAs, such that any further transmitting of the SMS from one PA to another (e.g. PA2) would require all PAs in a chain to mutually validate each other as being registered with ComReg as a PA. Finally, the MNO would validate that the SMS and Sender ID received by it is from a registered PA. If the validation checks fail, then the MNO would modify, and later block, messages with a Sender ID that come from any source other than a registered PA.

2.272 This is a relatively modest change in approach for operators compared to the proposal in Consultation 23/52, because a determination on whether to filter a SMS or not was already proposed as part of that consultation and is an integral part of any SMS Sender ID Registry. The burden of facilitating this revised approach falls primarily on ComReg who will need to build out a Sender ID Registry with validation capability to facilitate same. While some system changes and operating procedures may be required by operators and PAs, the process of validation is greatly simplified by just validating against the Sender ID Registry that ComReg will build. Importantly, this approach would operate on the basis of all stakeholders involved in the transmission of a SMS being obliged to follow certain rules, to ensure that trust is retained throughout the chain of transmission. Where such rules are breached, ComReg could take a variety of actions including removing offending parties from the registered list of PAs or SIDOs (e.g., losing their SIDOs).

2.273 ComReg considers that this approach provides greater flexibility in the use of SMS with Sender IDs relative to the approach outlined in Consultation 23/52, for two main reasons:

I. SIDOs may use multiple PAs to originate a SMS bearing their registered Sender IDs. This allows SIDOs to use multiple SMS aggregators, which increases a SIDO's range of choice for PAs and their ability to move SMS traffic between operators and aggregators to avail of lower prices where possible.

II. PAs would not have to carry the SMS for the entirety of the transmission path and could instead use multiple paths across different PAs in order to minimise costs in light of the location of the SIDO and their customers.

III. MNOs would have greater flexibility in their routing with PAs.

2.274 Importantly, ComReg considers that this approach should provide for more secure paths for a SMS bearing a Sender ID because, only a legitimate SMS

with a Sender ID should originate from a registered SIDO, as PAs should not originate any SMS with a Sender ID on behalf of a SIDO that is not registered with ComReg. Furthermore, no PA should forward any SMS with a Sender ID that is either received from an unregistered SIDO or an unregistered aggregator. MSPs will only forward an SMS bearing a registered Sender ID from a registered PA to other MSPs or their end-users.

2.275 Trust underpins this approach, and all participants will commit to validating a SMS received from other participants. It is expected that this approach should be secure and block scams messages with Sender IDs originating from unregistered sources, only if all participants act responsibly to protect consumers. Therefore, the security of this approach is dependent on all of the various entities in the chain of transmission (e.g., SIDOs, PAs and MSPs) playing their part in ensuring that any SMS received by them is appropriately validated.

2.276 Lax validation controls on the part of any participant could potentially expose all Irish consumers to scam texts using Sender ID spoofing. As noted previously, where the source of a scam SMS is traced to lax validation on the part of a PA or MSP, ComReg will take strong compliance action to ensure trust in the transmission of a SMS with a Sender ID is protected. ComReg may also re-consider the approach of one PA per SIDO, where it is evident that stakeholders involved in the transmission of a SMS with a Sender ID cannot implement relatively straightforward validation procedures across the chain of transmission. In such circumstances, ComReg will also consider whether Sender IDs should be banned altogether.

2.277 For this reason, ComReg will include a requirement in the DI that all participating MSPs and PAs will provide, upon request from ComReg, certain information relating to any SMS(s) that ComReg suspects to have been relayed or delivered in breach of the blocking requirements in this intervention. This would include the name of the sending party, the date and time of delivery and a record of what checks the operators performed on the incoming message before relaying or delivering it. This will enable ComReg to trace the source of the SMS breach more effectively, through the chain of PAs to the PA that originated it.

2.278 In the event of any such breach, ComReg can and will determine the cause of the breach and consider what action will be taken. This could include initiating enforcement which could result in either the exclusion of an aggregator or MSP from the register or the use of administrative fining powers under the the Communications Regulation and Digital Hub Development Agency

(Amendment) Act 2023[142] ("Act of 2023") (which could involve a fine of up to €5 million or 10% annual turnover of the undertaking concerned).

2.279 The RIA and the DI have been updated to reflect the changes as outlined above. ComReg will aim to increase the responsibility of SIDOs through the terms of the contracts that SIDOs must enter into with ComReg in order to be assigned a given Sender ID. This ensures that all parties have a role in ensuring the secure transmission of a SMS with Sender IDs.

Draft Decision Instrument

2.280 In relation to Twilio's contention that ComReg needs to require MNOs to allow access to enable testing, ComReg notes that the direct connections have been removed from the DI for the reasons outlined above and such a requirement is therefore not required.

2.281 Microsoft's contention that a SMS should only ever be modified and not blocked is misguided. It should be noted that the modification period (i.e., three months) is only intended to provide businesses/organisations using a SMS with a Sender ID time to register themselves and their Sender IDs[143]. Absent same, business/organisations who have not registered with ComReg would have their SMS with Sender IDs blocked. By providing for modification, consumers would still receive their SMS and provide businesses/organisations with strong incentives to get registered on the Sender ID Registry. ComReg also wants to avoid a scenario where large numbers of potentially valid SMS are blocked because business/organisations have yet to be registered.

2.282 While Microsoft cites the Singaporean regulator, the IMDA, as an example of a regulator using Sender ID modification, the IMDA has planned on the registry ultimately being used by operators to block a SMS and Sender ID modification was only intended to provide additional time for organisations to have their Sender IDs registered. Indeed, ComReg's inclusion of modification arose from taking learnings from the IMDA on its approach to the Sender ID Registry. It noted that:

> "*As some organisations may need more time to prepare and register, their SMS cannot be clearly differentiated from other SMS that come from unknown sources and may be scam messages. Therefore, as a transition measure, all non-registered SMS Sender-IDs after 31 January 2023 will be channelled to a Sender ID with the header* "Likely-

[142] Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 https://www.irishstatutebook.ie/eli/2023/act/4/enacted/en/html
[143] A SMS with Sender IDs that have not been registered will appear on end users CLI as "Likely Scam" for a period of three months.

> SCAM". *This is akin to a "spam filter and spam bin" and will be in place for around 6 months. Consumers are advised to exercise caution upon receiving such SMS as these are non-registered Sender IDs. Merchants are also urged to have their Sender IDs registered as early as possible with the SSIR*."[144]

2.283 Microsoft's proposed approach would permit scam SMS to reach Irish consumers on an ongoing basis, albeit with a warning, and although such texts are less likely to be engaged with, they will serve as a nuisance to some and potentially confuse others leading to unnecessary anxiety and stress. It should be noted that ComReg has included a modification period for Sender ID intervention to give organisations time to register their Sender IDs. It should also be noted that ComReg may decide to extend the period of modification depending on the effectiveness of the Sender ID registry during the modification period.

2.284 In relation to Virgin and Three's contentions that ComReg should not implement this measure without further consultation, ComReg notes that it has already consulted on the SMS Sender ID registry in Consultation 23/52 and provided an extended consultation period at the request of IBEC. ComReg also provided interested parties with an additional opportunity to ask questions and receive answers within the consultation period[145]. ComReg has now made modifications to its original proposal in response to submissions made to Consultation 23/52. Therefore, ComReg is satisfied that it has sufficiently consulted on this intervention[146].

2.285 In relation to Eir's view that this intervention should not have a threshold, ComReg notes that it is necessary to have a threshold because, if the Decision Instrument is applied to all MSPs (without any threshold), there may be a category of MSP who would be unable to reasonably comply with its requirements[147]. Requiring such MSPs to implement the measures in the Decision Instrument may be disproportionate, provide little additional benefit while imposing a large cost on smaller firms and potentially distorting competition as an unintended consequence. Such an operator can therefore choose whether or not to participate in the SMS Sender ID Registry and avoid the cost of the intervention if it was overly burdensome.

---

[144] Full SMS Sender ID Registration Is To Be Required | IMDA - Infocomm Media Development Authority

[145] ComReg Document 23/67, "*Clarification Questions and Answers on Consultation 23/52*", 10 August 2023. Link

[147] ComReg is placing the responsibility primarily on the network operators to ensure that all relevant traffic (including third party traffic e.g., MVNOs) terminating on its network has been subject to the Sender ID Registry, where technically feasible. However, there may be some MSP not captured by this provision and the threshold primarily targets such operators. For example, a potential entrant, either a MNO or a MVNO which is not covered by their network MSP (noting that the requirement in the DI is subject to this being provided "where technically feasible").

2.286 However, in order to protect consumers, such an operator would not be permitted to transmit or deliver any SMS bearing a Sender ID destined for an Irish number or customer. ComReg is not aware of any existing MSP that would fall into this category and the impacts should be minor if they occur at all. Notwithstanding, in the interests of clarity, ComReg has added text to the Decision Instrument to make it explicit that any operator below the threshold that does not implement the SMS Sender ID intervention would not be permitted to transmit or deliver any SMS bearing a Sender ID destined for a Irish number or customer. It should be noted that any MSP that does not either apply the blocking, or have the blocking applied for it by a host MNO, cannot deliver a SMS bearing a Sender ID – ComReg has added text to the Decision Instrument to clarify this point.

Proposed Timelines

2.287 Plum is of the view that the 18-month deadline for blocking of unregistered SMS with a Sender ID is reasonable and proportionate[148] for the following reasons:

- Allows sufficient time for SIDOs, whose required actions are relatively straightforward;
- While more complex for PAs and MNOs, this is demonstrably possible, as a number of international operators appear to have implemented this intervention within the 9 months;
- It is the only SMS intervention which operators are required to work on at present;
- It is only being applied by larger operators, which are at lower risk of 'overburdening', given their greater organisational capacity; and
- The most pressing timeline lies with ComReg.

2.288 However, Plum is of the view that additional time should be provided to allow for the set-up of the registry, such that modification would only begin 15 months after the Decision. The modification period would then last for three months with full blocking beginning 18 months after the Decision.

2.289 In light of this, ComReg is of the view that the overall 18-month period (15 months plus 3-month modification period) for implementation of the SMS Sender ID Registry is appropriate and proportionate.

2.290 In relation to Virgin, ComReg notes that it may take into account the specifics circumstances of the MSP/IGO, including their efforts and plans, or lack

[148] Readers are referred to the Plum Report for more information.

thereof, to implement the intervention. ComReg notes that Virgin [✂[redacted]✂].

Legal Basis

2.291 In relation to Vodafone's claim that Sender ID modification has no legal basis under interception law, ComReg would note that the modification requirement in Part IV (1) of the Sender ID DI (i.e., that when delivering an SMS with a Sender ID, relevant undertakings that are Participating MSPs shall modify the Sender ID where that Sender ID: (a) is not registered; or (b) is registered, but sent by a source other than the Registered PA or a participating MSP) does not properly fall within the definition of "interception" in for example the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. Participating MSPs are checking against a set, contained list of Sender IDs, and these checks do not constitute general and indiscriminate interception. This analysis applies mutatis mutandis to all other relevant "interception" legislation, e.g., s.98 of the Postal and Telecommunications Services Act, 1983, and Regulation 5(1) of the E-Privacy Regulations, S.I. 336 of 2011.

Analytics

2.292 ComReg supports all efforts to inform businesses that wish to gather information to assist in their efforts to reduce and prevent scams texts. However, there is little to be gained in reporting when illegitimate traffic using their Sender ID is blocked to SIDOs; indeed, the fact that such communications have been blocked means that no additional preventative measures should be necessary. Moreover, it is likely that providing such information could be burdensome and require operators to put in place parallel processes to report blocking statistics to potentially thousands of businesses and organisations that use the Sender ID Registry. This would likely require additional investment that could not be justified given the lack of obvious benefits. Therefore, ComReg will not require operators to provide such information to ComReg and/or third parties.

2.293 ComReg will separately gather – on a monthly basis, blocking statistics from operators to determine an aggregate figure of the number of calls or SMS blocked by a specific intervention. This should be sufficient to monitor the effectiveness of the Sender ID Registry.

2.1.7 Other Interventions

Summary views of ComReg in Consultation 23/52

2.294 In Chapter 4 of Consultation 23/52 ComReg examined a long list of

interventions to determine which were appropriate for assessment in light of their technical feasibility, effectiveness, and timeline for implementation. A number of interventions were deemed unsuitable and not assessed in the draft RIAs, such as STIR/SHAKEN[149], "shortening the chain"[150], and SMS Origin-Destination verification ("O-D Verification")[151].

2.295 In the draft Sender ID draft RIA in Chapter 5 of Consultation 23/52 ComReg assessed a number of options for regulating Sender ID, before determining that a full Sender ID registry was preferable to the identified alternatives which included banning Sender IDs altogether or implementing a partial Sender ID registry.

View of respondents to Consultation 23/52

2.296 The views of respondents on other potential interventions are summarised and assessed by ComReg under the following headings:

- STIR/Shaken;
- Other voice interventions;
- Alternative forms of Sender ID Regulation; and
- Other SMS interventions.

STIR/Shaken

2.297 A number of operators agree with ComReg's position on STIR/SHAKEN, namely: BT, Eir, Hiya, i3Forum, Magrathea, Twilio, Verizon, Virgin and Voxbone.

2.298 Microsoft considers that ComReg should promote STIR/SHAKEN to Irish operators capable of reading STIR/SHAKEN tokens. Although agreeing with ComReg's position on STIR/SHAKEN, Voxbone contends that ComReg should promote voluntary engagement by industry with STIR/SHAKEN.

2.299 Both MEF and I3forum submit that data from Youmail[152] indicates that Stir/Shaken has not reduced the prevalence of scam calls in the United

[149] The STIR/SHAKEN framework, an industry-standard caller ID authentication technology, is a set of technical standards and protocols that allow for the authentication and verification of caller ID information for calls carried over Internet Protocol (IP) networks.
[150] The STIR/SHAKEN framework, an industry-standard caller ID authentication technology, is a set of technical standards and protocols that allow for the authentication and verification of caller ID information for calls carried over Internet Protocol (IP) networks.
[151] This entails securing Sender ID would be through use of message verification Codes.
[152] https://robocallindex.com/

States[153].

Other Voice interventions

2.300 i3Forum and XConnect both contend that ComReg should consider requiring operators to validate CLI on international calls, which could use international DNO and PN lists.

Alternative forms of Sender ID regulation

2.301 MEF agrees that the use of SMS Sender IDs should not be banned. MEF contends that ComReg should adopt a partial SMS Sender ID Registry, which should include the most-smished brands as a sufficiently expansive list of Sender IDs would achieve most of the benefit, and that a full registry forecloses more than one organisation from using any registered Sender ID. MEF opines that both the Irish and UK telecom industry has made significant progress in combatting scam texts, using MEFs "Sender ID Protection Registry".

2.302 MEF maintains that businesses do not understand SMS routing and are therefore unable to participate in the "Shorten-the-chain" option. Virgin also agrees with ComReg's decision not to pursue a "Shorten-the-chain" option. By contrast, Eir disagrees with ComReg's decision to not consider the "Shorten-the-chain" option, noting that operators alone cannot be expected to bear the burden of implementing interventions.

Other SMS Interventions

2.303 Tanla suggests the use of a co-regulatory regime based on distributed ledger technology and operated by the telecom service providers. Eir and Virgin agree with ComReg that O-D verification should not be pursued at this time.

2.304 Cellusys opines that ComReg should subscribe to a shared number database and/or URL reputation database on behalf of operators and allow operators' firewall solutions to access it in order to block SMS containing suspicious URLs.

2.305 MEF submits that ComReg should set up the common numbering database (CNDB), similar to that used in the USA.

ComReg assessment

STIR/SHAKEN

[153] I3forum notes however that alternative "verified CLI systems" could enable greater verification of callers CLI, improve trust and enable services such as branded calling.

2.306 ComReg acknowledges the support of BT, Eir, i3Forum, Magrathea, Twilio, Verizon, Virgin and Voxbone.

2.307 In relation to the views of Voxbone and Microsoft that ComReg should promote STIR/SHAKEN to Irish operators, ComReg notes that Section 4.2 of Consultation 23/52 assessed STIR/SHAKEN as a potential voice intervention. Therein ComReg noted that STIR/SHAKEN was not a valid regulatory option at present because, among other things, its success depends on effective deployment across multiple different jurisdictions and only a few countries have implemented it to date. Furthermore, there is no coordinated plan for its broad implementation.

2.308 Nevertheless, ComReg considered that the introduction of STIR/SHAKEN in Ireland may have some merit as a potential solution to reduce consumer harm from spoofed CLIs in the future. ComReg noted that it intends to monitor developments of this technology, including international deployments of STIR/SHAKEN in future. Finally, ComReg remarked that it may need to revisit the use of STIR/SHAKEN, particularly if the other proposed interventions fail to deliver in a timely and effective fashion.

2.309 ComReg sees no reason to deviate from this approach at this time. There has not been any substantial change in the evolution of STIR/SHAKEN in the period since the publication of Consultation 23/52. Therefore, ComReg will continue to monitor developments in STIR/SHAKEN along with the effectiveness of the interventions discussed in this consultation.

Other Voice interventions

2.310 In relation to i3Forum's suggestion that ComReg should consider requiring operators to validate CLI on international calls, ComReg notes that the work to combat scams is first and foremost aimed at preventing the misuse of Irish telephony numbers. In the case of CLI-Analysis of incoming calls, this relates more specifically to the misuse of Irish numbers by international scammers to deceive Irish consumers. This has been the priority given the trust placed in Irish numbers by Irish consumers, which scammers have exploited. Therefore, ComReg did not consider the use of checks by Irish operators of incoming calls bearing international numbers. However, although ComReg has focussed on the spoofing of Irish numbers as presentation CLI on international calls to Irish consumers, the minimum requirements and options for international CLI have also been addressed in ComReg's update to its Numbering Conditions in Chapter 4.

2.311 ComReg will continue to monitor the potential for improvement in CLI-Analysis to combat scams. ComReg may revisit this issue once more information is available on the completeness of international DNO and PN lists, and their

potential use by IGOs to block illegitimate traffic. ComReg continues to monitor the progress of the i3Forum in this area.

Response to alternative forms of Sender ID regulation

2.312 ComReg agrees with MEF that a partial SMS Sender ID registry could achieve much of the benefit of the full SMS Sender ID Registry. Indeed, ComReg noted this in the Draft RIA, which assessed the benefits and costs of both a partial and full Sender ID Registry. However, ComReg also noted a number of issues with a partial SMS Sender ID Registry, including that it would, by definition, not serve the needs of all businesses[154] without compromising the security of Sender ID. MEF has not disputed this trade off and indeed made reference to a "*sufficiently expansive*" partial registry. Indeed, a key benefit of the SMS Sender ID registry is that it could result in greater use of Sender IDs by organisations of all types and sizes - noting that any partial Sender ID registry needs to incorporate a blocking rule for all use of unregistered Sender IDs or use of registered Sender IDs by other parties. Otherwise, the partial registry will have limited impact on reducing SMS Sender ID spoofing[155]. Furthermore, ComReg considers that the avoidance of multiple users of Sender IDs is beneficial given the potential for consumer confusion[156].

2.313 ComReg acknowledges the support of MEF and Virgin for ComReg's decision not to further pursue the "*shorten-the-chain*" approach to securing SMS Sender ID. While Eir may disagree with ComReg's decision and reasoning regarding "*shortening-the-chain*", it should be noted that ComReg determined that, as evidenced by the attempts at shortening the chain, businesses struggled with the complexity of attempting to oversee and coordinate the design of SMS Sender ID paths that would be used by their SMS aggregators. Indeed, Eir does not provide examples of any businesses that it managed to help "*shorten-the-chain*". ComReg's views are corroborated by MEF's opinion that that many businesses do not understand SMS routing which inhibits their ability to "*shorten-the-chain*". It appears unrealistic therefore, based on the experience to date that "*shorten-the-chain*" can effectively prevent Sender ID spoofing. A key advantage SMS Sender ID registry is the ease of use for businesses, being achievable by more than the few companies with the resources to (in theory) successfully engage with their SMS aggregators. In any event, for the purpose of this consultation

Other SMS Interventions

[154] See in particular pages 158-161 of Consultation 23/52.
[155] Where the Sender ID has been faked by a fraudster and the text appears to be from a genuine number or business.
[156] To reduce consumer confusion in relation to Sender IDs, ComReg intends on using a sunrise period for the Sender IDs of key SIDOs..

2.314 ComReg notes the suggestion of Tanla of a co-regulatory regime based on distributed ledger technology and operated by the telecom service providers to be an interesting approach. ComReg acknowledges the support of Eir and Virgin Media that ComReg should not examine O-D verification at this time.

2.315 ComReg understands that individual operators applying SMS Scam Filters can and often do access URLs reputation databases to improve the effectiveness of a SMS Scam Filter, through subscribing directly or via their solution providers. It is a matter for operators to assess whether joint purchasing of shared number database and/or URL reputation database, brings benefits, and is in compliance with the relevant law.

2.316 In relation to MEF's suggestion to adopt a common numbering database, ComReg notes that, based on MEF's limited explanation[157], this appears similar to the Protected Numbers list, but for SMS Sender ID. It is unclear how this would improve upon a Sender ID registry, as this does not involve any verification of the SIDO, or process for ensuring the provenance of the SMS as it is transmitted from aggregator to aggregator.

2.1.8 Other Matters

View of respondents to ComReg 23/52

2.317 The views of respondents on other matters relating to the Proposed Package are summarised and assessed by ComReg under the following headings:

- Consumer awareness campaigns;
- Handsets;
- International traceback;
- Consumer Reporting; and
- SIM farms.

Awareness campaign

2.318 ALTO states there is no substitute for ComReg engaging in information campaigns concerning "messaging frauds". ALTO also notes that the Verizon Data Breach Incident Report identifies users being "responsible" for fraud and various data breaches.

2.319 BPFI suggests that ComReg joins it in an annual campaign on Nuisance

[157] The text was somewhat unclear, noting that MEF state that this intervention should be "managed by Ofcom directly".

Communications.

Handsets

2.320 Eir submits that ComReg should establish a separate taskforce with handset manufacturers and application developers to promote handset-based interventions.

International Traceback

2.321 i3Forum and Twilio both contend that ComReg should consider international traceback which would act as a further deterrent to scams, noting the role for law enforcement.

Consumer reporting

2.322 Revolut, MEF and Mr. Bugler all suggest that Irish customers be offered a mechanism to report scams.

SIM Farms

2.323 MEF submits that the sale of "*SIM farms*" equipment should be banned.

ComReg assessment

Awareness campaigns

2.324 ComReg notes that raising consumer awareness alone is no substitute for network-based interventions in prevent harm from scams. Consumer awareness campaigns aim at increasing the likelihood that a consumer recognises a received scam and that the consumer remembers the cautionary message during a scam, likely long after hearing or seeing the advertising campaign. Scammers have proven themselves adept at deceiving consumers, constantly evolving to exploit the latest consumer behaviour and opportune events. Moreover, consumer awareness campaigns are only effective where they *decrease* trust in ECS and ECN. Consumer awareness campaigns can only ever be a complementary action to a robust, preventative solutions, such as ComReg's Proposed Package.

2.325 Notwithstanding, ComReg agrees that it is important consumer awareness has a role to play. Indeed, ComReg has raised awareness of scams both through press releases[158], and through coverage of its work to combat scams[159]. ComReg is not acting alone in this regard, as An Garda Síochána,

158

159

the Central Bank of Ireland, BPFI and NCSC as well as government departments regularly warn consumers regarding the incidence of scams. ComReg plans to continue to raise consumer awareness of scams in the future.

Handsets

2.326 ComReg has no specific role in relation to handset functionality or security, at least in terms of ComReg's numbering duties and related powers, and it is unclear how ComReg could enforce any action on handset manufacturers. Notably Eir does not provide details on what specific interventions handset manufacturers could implement in a timely manner that would approach the effectiveness of network-based interventions. ComReg notes the view of Hiya, which supplied handset-based interventions to Samsung, that network-based interventions are key to combatting scam calls.

International Traceback

2.327 International call traceback is typically used to gather evidence to identify fraudsters and uncover evidence of fraud. ComReg has no investigative powers for fraud, which is a criminal offence. International call traceback typically involves collaboration between international telecommunication providers and law enforcement agencies.

Consumer reporting

2.328 As previously explained, blocking metrics are critical to monitoring the effectiveness of any network-based interventions to combat scams, both for individual interventions and collectively. ComReg has committed to considering what further information and data can be used to inform its work to combat scams. However, this is outside of the scope of Consultation 23/52. ComReg may return to further consider this issue at a later time.

SIM Farms

2.329 ComReg notes that the misuse of any telephony equipment, including "*SIM farms*", to perpetuate scams constitutes a misuse of numbers and can constitute a civil/criminal offence.

Chapter 3

3 Response to comments on the Specification Documents

Introductory Remarks

3.1 In its draft Technical and Functional requirements (the "Specification Documents"), ComReg set out its preliminary guidance to operators on how they should implement and operate each intervention from a technical perspective. In this chapter, ComReg considers the views of interested parties on the draft Technical and Functional specifications.

3.2 The aim of the draft Technical and Functional specification documents is to provide operators with guidance as to the approach that operators should take to fulfil the requirements of the Decision Instruments. Therefore, the Specification Documents are living documents and will be adapted and revised as required to benefit from lessons learned in their implementation and from feedback provided in the associated working groups. The technical working groups of the NCIT will facilitate more detailed discussion of matters by the relevant technical experts such as developing the Specification Documents for each intervention.

3.3 ComReg shared the draft Specification Documents with relevant operators upon request (for security reasons) with the aim of initiating a process whereby ComReg and operators share experiences and information in order to facilitate more effective and consistent blocking of scam calls and texts across industry.

3.4 While ComReg has assessed the submissions on the Technical Specifications herein[160], all views expressed by ComReg in this Chapter are preliminary and should not be treated as final. These issues will be discussed and addressed by the relevant NCIT working groups.

3.5 ComReg did not publish the technical specifications to avoid making public information that could be utilised by scammers. Instead, ComReg shared the Specification Documents upon request, with relevant operators, namely those that will be involved in the implementation of the interventions. Similarly, such information is redacted from the published version of this Chapter, as this

information:

- if published, would inform scammers as to workings of the interventions, improving their ability to circumvent the proposed interventions; and
- relates to activities of the NCIT and participation in the NCIT is expressly on the basis that its activities are confidential.

3.6 ComReg will share a version of this document that includes the information above, as well as revised Technical Specifications, with the relevant operators upon request (the "NCIT Version")[161]. The NCIT Version will still redact information submitted by interested parties which is confidential to them[162].

3.1 Assessment of the submissions

Summary views of ComReg in Consultation 23/52

3.7 ComReg shared the draft technical specifications with relevant operators upon request, which contained ComReg's preliminary views as to the detailed implementation and operation of the Proposed Interventions.

View of respondents to Consultation 23/52

3.8 The views of respondents and ComReg's assessment of same are grouped under the following headings:

- Overarching views;
- DNO, PN, Fixed CLI Call Blocking;
- Mobile CLI Call Blocking;
- Voice Firewall; and
- SMS Sender ID Registry.

3.9 Interested parties will appreciate that ComReg does not outline the details of each of the individual interventions given the need to avoid such information being improperly used.

3.10 ComReg discusses key matters raised by operators below, noting that all

[161] A week after publication of the Decisions.
[162] ComReg has removed only the most sensitive information from the published version of the submissions to 23/52. ComReg will provide a version to NCIT members with such information included, except where such information is confidential to the respondent (as per ComReg's procedure on confidential information).

relevant issues, including those raised in the submissions, will be discussed within the relevant technical working groups.

Overall views on the Functional Requirements

3.11 [redacted]

Do Not Originate, Protected Numbers and Fixed CLI Call Blocking

3.12 [redacted]

3.13 [redacted] [✂ [redacted] ✂].

3.14 [redacted]

Mobile CLI Call Blocking

3.15 [redacted]

3.16 [redacted]

3.17 [redacted]

3.18 [redacted]

Voice Firewall

3.19 [redacted]

3.20 [redacted]

SMS Sender ID registry

3.21 [redacted]:

i. [redacted];

ii. [redacted]; and

iii. [redacted].

3.22 [redacted] [✂ [redacted] ✂].

3.23 [redacted]

3.24 [redacted] [✂ [redacted] ✂].

3.25 [redacted]

[redacted]

3.26 [redacted]

3.27 [redacted]

3.28 [redacted]

3.29 [redacted]

ComReg Assessment

Overarching views

3.30 [redacted]

Do Not Originate, Protected Numbers and Fixed CLI Call Blocking

3.31 [redacted]

Mobile CLI Call Blocking

3.32 [redacted]

[redacted].

3.33 [redacted]

3.34 [redacted]

3.35 [redacted].

Voice Firewall

3.36 [redacted]

SMS Sender ID registry

3.37 [redacted].

3.38 [redacted]

[redacted], [redacted]

3.39 [redacted]

3.40 [redacted]

3.41 [redacted]

3.42 [redacted]

3.43 [redacted]

3.44 [redacted]

3.45 [redacted]

[redacted].

Chapter 4

4 Response to comments on Draft Updates to the Numbering Conditions

Introductory Remarks

4.1 In this chapter, ComReg considers submissions on the draft updates to the Numbering Conditions of Use and Application Process document[163][164] as described in Chapter 6 of Consultation 23/52. These draft updates were required to align the numbering conditions, particularly in relation to the CLI conditions of use ("CLI Conditions"), with the nuisance communications interventions.

4.2 In light of these, the views of respondents to Consultation 23/52 on the draft updates and other relevant material, ComReg sets out its final position on each of these draft updates in this chapter.

4.3 The views of respondents are grouped under the following headings, with the relevant section from Consultation 23/52 in brackets for reference:

1. *Updates in light of Voice Interventions (Chapter 6.1 of Consultation 23/52)*

   - CLI Conditions – Assigned Numbers;
   - DNO;
   - PN;
   - Fixed CLI Call Blocking;
   - Mobile CLI Call Blocking;
   - CLI-Analysis

2. *General Updates to CLI Conditions (Chapter 6.3 of Consultation 23/52)*

   - Geographic Numbers (GN);
   - Non-Geographic Numbers ("NGNs");

[163] ComReg 15/136R3
[164] ComReg 23/52d "Draft Numbering Conditions of Use and Applications Process", published together with Consultation 23/52.

- 1800 Freephone;
- Emergency Numbers 999/112

3. General Updates to provide CLI Guidance (Chapter 6.4 of Consultation 23/52)

- CLI Principles and associated Usage Cases;
- CLI Conditions – Calls that Ingress into the Irish PSTN from International PSTNs;
- Sub-assignment of numbers;
- Future Number Management – Needs and Developments

4. Updates in light of the SMS interventions (Chapter 6.2 of Consultation 23/52)

- SMS Interventions – Sender ID.

1. Updates in light of Voice Interventions (Chapter 6.1 of Consultation 23/52)

CLI Conditions - Assigned Numbers

Views of ComReg in Consultation 23/52

4.4 In Consultation 23/52, ComReg noted that Section 3.1 (5) (a) (i) of the Numbering Conditions required the originator of a call to ensure that the CLI is the assigned number for the calling party and is from a set of permitted classes of number. However, to provide more clarity, ComReg proposed to break-out the assigned number requirement as a stand-alone condition. To that end, ComReg proposed to add the following underlined text as a new paragraph "i" in Section 3.1 (5) (a) and to delete the text as indicated;

> *(a) "the undertaking which originates a call shall ensure:*
>
> *i that the CLI for the call shall be the assigned number for the calling party;*
>
> *~~i~~ ii that the presentation CLI for the call shall be ~~the assigned~~ a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number ~~for the calling party~~;*

Views of respondents to Consultation 23/52

4.5 There were no submissions objecting to ComReg's proposal.

ComReg's Assessment

4.6 In the absence of any objections from respondents, ComReg has decided to adopt the proposed wording as set out in Consultation 23/52 and will amend Section 3.1 (5) (a)i of the Numbering Conditions accordingly.

DNO

Views of ComReg in Consultation 23/52

4.7 In Consultation 23/52, ComReg proposed the DNO intervention. This intervention required a list of DNO numbers to be generated and managed. ComReg noted that, by submitting its assigned numbers to the DNO list, an organisation confirms that it does not and will not use those numbers as CLIs. Furthermore, if originating operators comply with Section 3.1 (5) (a) (i) of the Numbering Conditions by ensuring that only the assigned numbers for the calling party are used as CLI, then no numbers on the DNO list can legitimately appear as CLI on calls originating on the Irish PSTN.

4.8 ComReg proposed that it would manage the DNO list and, to that end, proposed the following text as part of new paragraph 4 of Section 1 "Introduction" of the Numbering Conditions;

> *(4) As set out in its Response to Consultation 24/24 and Decision 24/24 on Nuisance Communications, ComReg supports industry by managing the following;*
>
> *Do Not Originate ("DNO") List*

Views of respondents to Consultation 23/52

4.9 ALTO, BT, Eir, Twilio and Viatel each confirmed their agreement with the proposed change to the Numbering Conditions. There were no objections to the proposed change from other respondents.

4.10 With regard to the proposed paragraph 4 of Section 1, ALTO and BT queried whether the omission of Fixed Lines is an error.

ComReg's Assessment on DNO

4.11 In considering its preliminary proposal in the light of respondents' views, ComReg has decided to adopt this proposal and will insert the said text, with the updated references, in new paragraph 4 of Section 1.

4.12 In response to ALTO and BT queried as to why Fixed Numbers are omitted from proposed Section 1.4, ComReg notes that Section 1.4 provides details of ComReg's proposed management of the DNO/PN/MSRN lists and SMS Sender ID registry. These are new management functions that support the DNO/PN/Fixed and Mobile CLI Call Blocking and SMS Sender ID interventions. ComReg assumes that ALTO and BT's question is in relation to a management function associated with the Fixed CLI Call Blocking intervention. However, Fixed Numbers are already defined in Consultation 23/52 as all Geographic and Non-Geographic numbers and perhaps this is an oversight on the part of the respondents. In any event, there is no new management function related to fixed number lists.

PN

Views of ComReg in Consultation 23/52

4.13 In Consultation 23/52 ComReg noted that the proposed PN blocking intervention is in accordance with Regulation 79(4) of the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444/2022)[165]. This states that it is an offence to use numbers that have not been assigned by ComReg. In support of this intervention, ComReg proposed that it would manage a list of unallocated numbers, or PN list. Furthermore, ComReg proposed to update the Numbering Conditions by inserting the following text as part of new paragraph 4 of Section 1 "Introduction";

> *(4) As set out in its Response to Consultation 24/24 and Decision 24/24 on Nuisance Communications, ComReg supports industry by managing the following;*
>
> *Protected Numbers ("PN") List*

Views of respondents to Consultation 23/52

4.14 ALTO, BT, Eir, Twilio and Viatel each confirmed their agreement with the proposed change. There were no objections to the proposed change from other respondents.

ComReg's Assessment on Protected Numbers

4.15 In considering its preliminary proposal in the light of respondents' views, ComReg has decided to adopt this proposal and will insert the said text, with the updated references, in new paragraph 4 of Section 1.

Fixed CLI Call Blocking

[165] S.I. No. 444 of 2022

Views of ComReg in Consultation 23/52

4.16 Chapter 4.2 of Consultation 23/52 provides details of the proposed Fixed CLI Call Blocking intervention. To align the Numbering Conditions with this intervention, ComReg proposed updates to the Numbering Conditions as follows:

i. For the avoidance of doubt on the CLI Conditions that apply in the case of long-lining, ComReg proposed to insert the following underlined text in Section 3.1 paragraph 5(a) of the Numbering Conditions;

> *(a)The undertaking which originates a call <u>on the Irish PSTN</u>, shall ensure:*
>
> *(i) that the CLI for the call shall be the assigned number for the calling party;*

ii. Furthermore, to provide for the intended use of long-lining as described in Section 4.2 of Consultation 23/52, ComReg proposed to add a new paragraph 9 in Section 3.2 of the Numbering Conditions as follows;

> *<u>(9) Long-lining – Undertakings shall only implement long-lining for their own end-users.</u>*

iii. Furthermore, ComReg proposed a definition for long-lining in the proposed Appendix 12 "Definitions" as follows:

> *<u>"**Long-lining**" means the implementation by an undertaking of a dedicated SIP or alternative trunk type to serve an end-user to ensure that calls from that end-user originate on the Irish PSTN;</u>*

Views of respondents to Consultation 23/52

4.17 ALTO, BT and Twilio each confirmed their support for the long-lining proposal with some qualifications. BT opines that ComReg's long-lining proposal enables wider competition of services (not just telecoms) in the Irish market. However, BT also contends that long-lining should apply to NGNs only and additionally should be distinguished from occasional nomadic use outside Ireland.

4.18 Twilio referred to the condition in Section 4.1 (2) of the Numbering Conditions which sets out that "*A Geographic Number shall only be assigned to an end-user whose residential/business premises is physically located within the designated minimum numbering area (MNA) for that Geographic Number*". In relation to this condition, which ComReg refers to as the "physical location condition", Twilio contends that long-lining should provide for other legitimate use cases. In this respect, Twilio refers to Question 12 in Section 2.7 of

ComReg's Document 23/75 which asked if calls from overseas branch offices or call centres can be interpreted as including remote/home workers of the companies and call centres concerned. ComReg responded in ComReg Document 23/75 that Irish fixed CLIs include those of remote/home workers of the companies and call centres concerned. ComReg added that calls from such remote/home workers would be blocked under the Fixed CLI call blocking intervention.

4.19 Eir states that it has no objection to the proposed changes in the Numbering Conditions.

4.20 Viatel highlights a scenario where long-lining was not setup directly to an end user abroad but involved a SIP Trunk Long Lined from the end user to a Reseller who then routes traffic to the operator over standard National Interconnect. Viatel contends that ComReg had previously confirmed that this scenario was a correct use of long-lining and consequently it is of the view that ComReg's proposed numbering condition should reflect this.

4.21 Viatel, contends that the use of NGNs as CLI is, in its view, unreliable in nature and provides inconsistent results. Furthermore, Viatel contends that the use of "1" as the leading digit in 1800 and "0" in 0818 further compounds the problem.

4.22 Vodafone opines that the Irish operations of a company may use its wider group organisation to complete its long-line requirement for the customer. Vodafone maintains that this is an important clarification as centralised infrastructure often forms part of modern networks across group organisations and certain elements of the network may not be physically located in Ireland.

ComReg's Assessment on Fixed CLI Call Blocking

4.23 Regarding concerns expressed by both Viatel and Vodafone regarding the ability to use another operator to provide long-lining, ComReg notes that the proposed condition is not intended to place restrictions on the use by other parties in the delivery of a long-line solution. Rather, it is intended to ensure that the operator seeking to long-line its end-users can authenticate the CLI of those end-users as required by the CLI conditions.

4.24 In response to BT's suggestion that long-lining be restricted to NGNs only, ComReg notes paragraph 6.20 of Consultation 23/52, which indicated that ComReg considered the use of NGNs by Irish overseas branch offices or call centres as a possible alternative to the use of Geographic numbers. ComReg noted that such use of NGNs would require long-lining to prevent call blocking by IGOs but might better meet consumer expectations concerning the origin of a call when compared with long-lined geographic numbers. ComReg stated

that it will carry out a review within the next two years of the options that would balance the needs of business while maintaining consumer confidence in the use of numbers. ComReg further indicated in Consultation 23/52 that it would monitor the use of long-lining to ensure that it is being used as intended.

4.25 In response to BT's comment that long-lining should be distinguished from occasional nomadic use outside Ireland, ComReg notes paragraph 6.79 of Consultation 23/52 which defines a nomadic service as one provided by an operator to an individual customer whereby that individual may use the SIP capabilities of their communications equipment (device) to make and receive calls on that device using their assigned Irish fixed phone number while travelling. This distinguishes the long-lining of, for example, a call-centre from a person being provided with a nomadic service while travelling.

4.26 In light of ComReg's preliminary position and respondents' comments, particularly Viatel and Vodafone's concerns regarding ComReg's proposed condition that undertakings only implement long-lining for their own end-users, ComReg has decided that the proposed paragraph 9 in Section 3.2 of the Numbering Conditions should be amended as follows:

> ~~*(9) Long-lining – Undertakings shall only implement long-lining for their own end-users.*~~
>
> *(9) Long-lining – For clarity, undertakings implementing long-lining must ensure that CLI-Analysis is carried out on calls originating on the Irish PSTN.*

4.27 ComReg will also include the definition of long-lining in Appendix 12 of the Numbering Conditions.

Mobile CLI Call Blocking

Views of ComReg in Consultation 23/52

4.28 Chapter 4.2 of Consultation 23/52 provides details of the proposed Mobile CLI Call Blocking intervention.

4.29 To support the Mobile CLI Call Blocking intervention, ComReg proposed to manage the Mobile Station Roaming Number (MSRN) list. To that end, ComReg proposed the following text as part of a new paragraph 4 of Section 1 "Introduction";

> *(4) As set out in its Response to Consultation 24/24 and Decision 24/24 on Nuisance Communications, ComReg supports industry by managing the following:*
>
> *(iii) Mobile Station Roaming Number ("MSRN") List*

Views of respondents to Consultation 23/52 on Mobile CLI Call Blocking

4.30 Eir contends that the proposed maintenance of an MSRN list is premature as the matter is, in its view, still under discussion at the NCIT.

4.31 There were no other objections to ComReg's proposed amendment.

ComReg's Assessment on Mobile CLI Call Blocking

4.32 In response to Eir's objection to the maintenance of an MSRN list at this time, ComReg notes paragraph 6.21 of Consultation 23/52 which highlights that such a list is important for both the Fixed and Mobile CLI call blocking interventions. ComReg also notes that the Fixed CLI call blocking intervention has been agreed by the NCIT.

4.33 To enable the ongoing implementation of the intervention by IGOs, ComReg, in agreement with the NCIT, has already compiled and issued an MSRN list to IGOs. The use of an MSRN list for the Fixed CLI Call Blocking intervention is now mandated in the Fixed CLI Call Blocking Decision Instrument in this Response to Consultation 23/52. Furthermore, in relation to the Mobile CLI Call Blocking intervention, the use of an MSRN list is now mandated in the Mobile CLI Call Blocking Decision Instrument of this Response to Consultation 23/52.

4.34 In light of ComReg's preliminary position and respondents' comments, ComReg confirms its position and will include the said text, with the updated references, in the Numbering Conditions.

CLI-Analysis

Views of ComReg in Consultation 23/52

4.35 In Consultation 23/52, ComReg noted that originating operators must comply with the numbering condition that only the calling party's assigned number, from within a certain set of number classes, is permitted as CLI and, to that end, originating operators must carry out CLI-Analysis. ComReg proposed to insert the following clarification as a new paragraph "e" in Section 3.1 (5) in the Numbering Conditions:

> *(e) "For the avoidance of doubt, Undertakings shall carry out CLI- analysis on all calls originating on the Irish PSTN. This is to ensure that such undertakings can comply with the CLI conditions of use."*

Views of respondents to Consultation 23/52 on CLI-Analysis

4.36 Eir stated that it has no objection to the proposed changes to the Numbering

Conditions.

4.37 Three highlights an issue with some of its customers using [✂ ✂] More generally, Three notes that more time is required to implement these changes to the Numbering Conditions of use.

4.38 Three references the [✂ ✂]. Three contends that one form of validation could be a copy of a bill, which details the number assignment from the Service Provider that assigned the number to the customer.

4.39 Furthermore, in relation to CLI validation, Three opines that a letter of authorisation from the call centre customer, authorising the origination of the CLI in question, should be sufficient in its view. Three suggests that this letter of authorisation would be in addition to the validation carried out in respect of the assignment of the number to the customer.

4.40 Viatel queries what operators should do if the CLI-Analysis finds that the CLI is invalid. In this regard, Viatel queries what would happen in the case of ECAS calls with invalid CLIs.

4.41 Virgin Media maintains that it can only authenticate its directly connected customers and is unable to authenticate numbers from other providers or wholesale operators. Given its circumstances, Virgin Media contends that consideration needs to be given to how comprehensive authentication will be achieved.

ComReg's Assessment on CLI-Analysis

4.1 In response to Three's contentions that it is not possible for it to analyse the CLI on [✂ ✂]. Therefore, any operator with such customers will have to enable CLI checking for the DNO and PN list (as all originators of voice traffic will apply to these interventions).

ComReg notes that for the same reasons no exception can be made for CLI-Analysis. A "*derogation*" for such services, as suggested by Three, would undermine the principle that the CLI needs to be checked to ensure full compliance with the CLI conditions. ComReg does not agree with Three's suggestion of inserting the words "*where practical*" into ComReg's proposed text as this is open to interpretation in an area that is clearly critical for consumer protection. Nevertheless, having considered the matter, ComReg has decided to provide a period of 6 months for undertakings to comply with the CLI condition. In relation to the more general comment, ComReg considers that this is addressed by the updates to its proposals (e.g., permitting sub-assignment and formalisation of number hosting) as well as the introduction of timelines for implementing certain Decisions in the Numbering Conditions DI.

4.2 In response to Three's [✂ ✂], ComReg notes that paragraph 3 of Section 6.71 of Consultation 23/52 also sets out a use case where a customer is served by many operators. ComReg recognises the need for operators to be aware of their customer's assignments from other operators in order to comply with the CLI conditions. Three's suggestion that a letter of authorisation from the customer authorising the origination of all its assigned numbers as CLI is useful. ComReg also considers that this letter of authorisation would be in addition to the validation of the customer numbers by the (originating) operator.

4.3 In response to Viatel, ComReg notes that originating voice operators have a business relationship with their customers and so it is not unreasonable for operators to seek the list of valid numbers from these customers. If, through CLI-Analysis, operators find invalid numbers are being sent then it should rectify the situation with these customers directly. Regarding calls made to the emergency services with invalid CLI, ComReg understands that operators do not at present block such calls, irrespective of the use of CLI.

4.4 In response to Virgin Media's submission that it can only authenticate the CLI on calls by its directly connected customers and that it cannot authenticate numbers from other providers or wholesale operators, ComReg confirms that it is the operator originating a call for its end-user that must carry out CLI-analysis and thereby authenticate the caller.

4.5 ComReg reiterates that CLI-Analysis is a critical means of preventing calls using illegitimate CLI spoofing from originating within Ireland. In this way, CLI-Analysis complements the Fixed and Mobile CLI Call blocking measures which aim at preventing calls with illegitimate CLI spoofing from transiting into the State.

4.6 In light of ComReg's preliminary position and respondents' comments,

ComReg confirms its position that it will enter the said text in the Numbering Conditions as follows;

> *(e) "For the avoidance of doubt, Undertakings shall carry out CLI-analysis on all calls originating on the Irish PSTN. This is to ensure that such undertakings can comply with the CLI conditions of use.*

The Effective Date for this condition is set out in Section 7.7, entitled "*Decision Instrument for Numbering Conditions of Use and Application Process* ", of this Response to Consultation 23/52.

2. General Updates to CLI Conditions (Chapter 6.3 of Consultation 23/52)

Geographic Numbers

Views of ComReg in Consultation 23/52

4.7 In Consultation 23/52, ComReg highlighted the condition attached to geographic numbers which is set out in Section 4.1 (2) of the Numbering Conditions as follows:

> *"A Geographic Number shall only be assigned to an end-user whose residential/business premises is physically located within the designated minimum numbering area (MNA) for that Geographic Number".*

4.8 ComReg noted that this condition, which it referred to as the "physical location" condition for the purposes of Consultation 23/52, is an important tool in maintaining trust in numbers. However, as an end-user may be assigned geographic numbers in more than one MNA and to maintain clarity on the use of Geographic numbers as CLI, ComReg proposed the following underlined amendment to Section 3.1(5)(a) of the Numbering Conditions;

> *(a) The undertaking which originates a call on the Irish PSTN shall ensure:*
>
> *(ii) that the presentation CLI for the call shall be a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number appropriate to the designated MNA for that number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number;*

4.9 ComReg asked the following question:

> *Q2; Do you agree with ComReg's general updates to the CLI Conditions as set out above? Please explain the basis for your response in full and provide supporting information*

Views of respondents to Consultation 23/52 on Geographic Numbers

4.10 Eir stated that it has no objection to the proposed changes to the Numbering Conditions to preserve MNAs.

4.11 Three contends that, for several reasons that are set out in its submission, some customers of certain services may not have geographic numbers appropriate to the MNA for those numbers. Three suggests that ComReg add the phrase “where practical” in relation to the geographic location obligation where such services are concerned and for existing number assignments.

4.12 Twilio disagrees with the proposed amendment and maintains that, in its view, ComReg has not sufficiently justified the physical location condition. Twilio contends that many business end-users express legitimate demand for more flexibility in the use of geographic numbers.

4.13 Twilio also contends that Cloud Services and Cloud Service Providers are barely recognised in the Consultation 23/52 and that, apart from the reference in paragraph 6.62 of that consultation, any references to Cloud have a negative connotation.

4.14 Viatel contends that ComReg’s proposed wording refers to MNAs but the consumer survey, to which ComReg refers, is in its view about area codes rather than MNAs. Viatel contends that consumers do not have any knowledge of MNAs and, in any event, it disagrees with the concept of MNA.

ComReg’s Assessment on Geographic Numbers

4.15 In response to Eir’s comment on maintaining MNAs, ComReg notes that it did not consult on maintaining the MNA concept. Rather, ComReg proposed amending text in the Numbering Conditions to clarify the use of CLI with reference to the existing physical location condition that is based on that MNA concept.

4.16 In response to Three’s note that some end-users may not have geographic numbers appropriate to the MNA for those numbers, ComReg emphasises that the physical location condition is a key requirement to ensure trust in numbers and exceptions cannot be made for this condition. It is therefore disappointing that end-users may have inadvertently been provided with a number that does not meet the condition and any further breaches of this fundamental condition will be examined.

4.17 Noting the above, ComReg considers that it would be disproportionate for these end-users to have to change their number at this time but future transgressions will not be tolerated. To this end, ComReg notes that its draft KYC Guidance document (ComReg 24/24c) includes address validation as a

means of ensuring that the physical location condition is met. If operators adhere to the KYC Guidance, then this problem of incorrectly provided geographic numbers should not arise in the future. ComReg may return to this issue in the future.

4.18 In response to Twilio's objection to the physical location condition, ComReg points out that, as referenced in Consultation 23/52, ComReg consulted on this condition in 2021[166] and decided, for the reasons set out in its Response to Consultation[167], to retain the condition.

4.19 In response to Twilio's contention that ComReg generally refers to Cloud services in a negative way in Consultation 23/52, ComReg notes that Twilio has not indicated the relevant text where negative comments are made. Furthermore, Twilio contends that ComReg's current poor view of cloud services is in contrast with its view in previous consultations, which, Twilio maintains, have been largely positive towards Cloud Services. In response, ComReg notes that Consultation 23/52 focussed on nuisance communications and did not seek to analyse such services except where they directly related to nuisance communications. Moreover, ComReg maintains a technology-neutral stance but has a duty to ensure that the Numbering Conditions are upheld by all operators, including, so far as relevant, cloud service providers.

4.20 In response to Viatel's objection to the MNA concept and its submission that consumers understand area codes rather than the MNA concept, ComReg notes that, as referenced in Consultation 23/52, it consulted on the retention of MNAs as recently as 2021[168]. ComReg further notes that Viatel did not respond to that consultation. In its Response to Consultation, and for the reasons set out in that document, ComReg decided to retain the MNA concept. Therefore MNAs, rather than area codes, are the appropriate geographic units for the Numbering Conditions.

4.21 In light of ComReg's preliminary position and respondents' comments, ComReg confirms that it will insert the proposed text as consulted upon into the Numbering Conditions.

Non-Geographic Numbers

Views of ComReg in Consultation 23/52

4.22 In Consultation 23/52, ComReg considered it timely to review the criteria for

[166] Consultation 21/28 - Review of the Numbering Conditions of Use and Application Process - Consultation
[167] ComReg 21/75 and D06/21 – Review of the Numbering Conditions of Use and Application Process – Response to Consultation, Decision and Further Consultation – Section 4.2
[168] Consultation 21/28- Review of the Numbering Conditions of Use and Application Process - Consultation

the assignment of NGNs to end-users, particularly with the current surge in nuisance communications. ComReg highlighted that a requirement for an end-user to, for example, demonstrate that it is carrying out business in Ireland, would reduce the risk of the misuse of NGNs.

4.23 Sections 4.3 and 4.4 of the Numbering Conditions set out that an authorised undertaking shall only be granted the Rights of Use of (1800 Freephone or 0818 Standard Rate) Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for, together with the end-user's unique identifier. The end-user identifier is required for assignment of an NGN on ComReg's Individual Number Assignment ("INA")[169] system which leverages the existing industry Fixed Number Portability ("FNP")[170] System provided by PortingXS[171].

4.24 To ensure that businesses seeking NGNs are carrying out business in Ireland, ComReg proposed to amend Sections 4.3 and 4.4 Rights of Use conditions as follows:

> Add the following underlined text to paragraph 2 of Section 4.3;
>
> *Furthermore, as 1800 Freephone numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 1800 Freephone number, a business end-user shall be required to provide the following:*
>
> *i. A company's Irish CRO number, Revenue VAT or business number, [and/or]*
>
> *ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration.*
>
> And add the following underlined text to proposed paragraph 2 of Section 4.4;
>
> *Furthermore, as 0818 Standard Rate numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 0818 Standard Rate number, a business end-user shall be required to provide the following:*
>
> *i. A company's Irish CRO number, Revenue VAT or business number, [and/or]*
>
> *ii. A partnership/sole trader's Irish VAT number in their*

[169] The INA is the ComReg system that assigns individual 1800 and 0818 NGNs
[170] The FNP process is the mechanism by which Subscribers are able to retain their telephone number when changing to a new service provider
[171] PortingXS website

name(s) or proof of their business or Irish income tax registration.

4.25 With regard to the retrospective application of this proposed condition, ComReg noted that there is a relatively large number of individual NGNs, approximately 66,000 (1800 Freephone) and 55,000 (0818 Standard Rate), assigned and in use. ComReg considered that requiring operators to apply the proposal to existing NGN customers was not proportionate and therefore proposed that the condition be applied in the case of new applications only.

Views of respondents to Consultation 23/52 on NGNs

4.26 Viatel agrees with ComReg's proposal.

4.27 Eir contends that organisations such as charities and voluntary organisations etc. would be excluded by the proposed eligibility criteria.

4.28 Twilio queries whether European Union-based businesses, governments, agencies and NGOs will be able to continue to use Irish Non-Geographic Numbers. Twilio contends that, in its view, eligibility should also extend to others who can demonstrate what it terms "a relevant link to Ireland" whilst not being actually present in Ireland. Twilio provides examples such as those selling products and services in Ireland from abroad, providing warranty, technical support etc.

4.29 Twilio also refers to the differences in eligibility criteria for NGNs and Sender IDs, noting in particular the Sender ID requirement relating to trademark.

ComReg's Assessment on NGNs

4.30 In relation to Eir's contentions in relation to charities and voluntary organisations, ComReg confirms that the aim of the proposed criteria is to ensure that organisations with a connection to Ireland may be provided with NGNs. Therefore ComReg agrees that the organisations identified by Eir should indeed be included and ComReg will amend the eligibility criteria accordingly.

4.31 Regarding Twilio's views regarding access to NGNs, ComReg emphasises that the proposed criteria do not prevent entities that are not physically present in Ireland from being eligible for NGNs but that they must adequately demonstrate their need for such an Irish numbering resource.

4.32 In light of ComReg's preliminary position and respondents' comments, ComReg will amend its eligibility criteria for NGNs with the insertion of the following text in paragraph 2 of Section 4.3 for 1800 Freephone numbers. The text that is deleted, underlined /bold is in response to submissions to

Consultation 23/52;

> *Furthermore, as 1800 Freephone numbers are only provided to ~~businesses~~* ***organisations****, to demonstrate its eligibility to be assigned an 1800 Freephone number, an ~~business~~* ***organisation*** *end-user shall be required to provide* ***at least one*** *of the following:*
>
> *i. A company's Irish CRO number, Revenue VAT or business number~~, [and/or]~~;*
>
> *ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration;*
>
> ***iii. For a trademark holder that holds a trademark that is enforceable in the state, the trademark number or a digital copy of the trademark certificate;***
>
> ***iv. Registered charity number from the Charities Regulator or evidence of registration as a voluntary non-profit making organisation in the State; or***
>
> ***v. Evidence that the organisation's premises is in the State, e.g. organisations such as schools, clubs etc;***
>
> ***For clarity, any organisation that does not meet the above criteria but wishes to submit other evidence of its need for an Irish 1800 Freephone number may do so. ComReg reserves the right to refuse any application that does not meet the above criteria.***

4.33 In light of ComReg's preliminary position and respondents' comments, ComReg will amend its eligibility criteria for NGNs with the insertion of the following text in paragraph 2 of Section 4.4 for 0818 Standard Rate numbers. The text that is deleted, underlined /bold is in response to submissions to Consultation 23/52;

> *Furthermore, as 0818 Standard Rate numbers are only provided to ~~businesses~~* ***organisations****, to demonstrate its eligibility to be assigned an 0818 Standard Rate number, an ~~business~~* ***organisation*** *end-user shall be required to provide* ***at least one of*** *the following:*
>
> *i. A company's Irish CRO number, Revenue VAT or business number~~, [and/or]~~;*
>
> *ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration;*

iii. For a trademark holder that holds a trademark that is enforceable in the State, the trademark number or a digital copy of the trademark certificate;

iv. Registered charity number from the Charities Regulator or evidence of registration as a voluntary non-profit making organisation in the State; or

v. Evidence that the organisation's premises is in the State, e.g. organisations such as schools, clubs etc;

For clarity, any organisation that does not meet the above criteria but wishes to submit other evidence of its need for an Irish 0818 Standard Rate Number may do so. ComReg reserves the right to refuse any application that does not meet the above criteria.

1800 Freephone

Views of ComReg in Consultation 23/52

4.34 In Consultation 23/52, and in response to requests from some operators for clarity on the use of 1800 as CLI, ComReg highlighted that Section A.8.1 of the revised Annex A of ITU Recommendation E.164[172] states that "Any number within the responsibility of an Administration, which does not conform to the structure, length and uniqueness as defined in the main body of this Recommendation, is not an international E.164-number, and is termed a National-Only Number". Thus, ComReg noted, 1800 Freephone is a national-only number as it is dialable on Irish networks but not generally dialable from abroad.

4.35 ComReg highlighted that Section 3.1 paragraph (5)(a)(i) of the Numbering Conditions permits use of 1800 Freephone as presentation CLI as follows:

> *"that the presentation CLI for the call shall be the assigned Customer Support Short Code (for on-network calls),* ***a Freephone Number****, a Geographic Number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number for the calling party"*

Views of respondents to Consultation 23/52

4.36 There were no submissions in respect of ComReg's views on the use of 1800

[172] ITU Rec E.164 - SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS International operation – Numbering plan of the international telephone service

Freephone as CLI.

ComReg's Assessment

4.37 In Consultation 23/52, ComReg indicated that it did not propose to change the condition permitting the use of 1800 Freephone as CLI and notes that it has not received any submissions to that consultation seeking such a change.

Emergency Numbers - 999/112

Views of ComReg in Consultation 23/52

4.38 In Consultation 23/52, ComReg outlined that it had received a request from the Emergency Call Answering Services (ECAS)[173] to permit ECAS to originate calls with 112 and 999 as presentation CLI. The 112 number is the single European emergency number. The national emergency number 999 is a national-only number. Dialling 112 or 999 will contact ECAS when dialled on the Irish network. The 112 and 999 numbers were collectively known as the "emergency numbers" in the consultation.

4.39 ComReg noted that the use-case outlined by ECAS arises in circumstances where an emergency call to ECAS breaks down and ECAS may make a call-back to the emergency caller using one of the emergency numbers as CLI. This, ECAS maintained, may encourage the emergency caller to answer the call-back.

4.40 In its preliminary assessment, ComReg considered that using the emergency number as CLI on a call-back would indeed encourage an answer by the emergency caller. Therefore, ComReg proposed to permit the use of emergency numbers as presentation CLI. To that end, ComReg proposed to add the following underlined text to Section 3.1 paragraph (5)(a)(ii) of the Numbering Conditions:

> *(a) The undertaking which originates a call on the Irish PSTN shall ensure:*
>
> *ii that the presentation CLI for the call shall be a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number appropriate to the designated MNA for that number, a Harmonised Code of Social Value, a Mobile Number, ~~or~~ a Standard Rate Number, the single European emergency number 112 or the national emergency number 999;*

[173] ECAS website

4.41 However, while ComReg proposed to permit emergency numbers to be used as presentation CLI, it also recommended that this use case be considered further by ECAS and industry to ensure there are no unintended consequences of such use.

Views of respondents to Consultation 23/52 on Emergency Numbers

4.42 Eir agrees with ComReg's recommendation that the use of 999/112 as CLI should be considered further by ECAS and industry to ensure there are no unintended consequences of such use. Eir contends that permission to use 999/112 should not be included in the Numbering Conditions before an assessment of such use is carried out.

4.43 Twilio contends that including emergency numbers with other numbers that are permitted to be used as CLI could generate problems of misuse where the 999 is presented by another entity that is not an emergency service. Twilio opines that ComReg introduce a separate paragraph dedicated to CLI for emergency services.

4.44 Viatel agrees with the use of the emergency numbers as CLI but highlights possible technical difficulties which will require considerable interoperability testing by operators.

4.45 Vodafone contends that ComReg should consider clarification on the treatment of 999/112 (or international equivalent) for long-line circuits and connection to the local emergency service in the originating country.

ComReg's Assessment on Emergency Numbers

4.46 In response to Eir, and as recognised in Consultation 23/52, there is a requirement for an assessment by industry of this use case. In particular industry needs to ensure that there is no unintended consequences or misuse of emergency numbers as presentation CLI. ComReg notes that only ECAS, as the holder of the emergency numbers, may originate calls on the Irish PSTN using 112/999 as presentation CLI. However, it is not clear to what extent emergency numbers, that are used by PSAPs[174] in other countries, might transit onto the Irish network. This would cause difficulty in distinguishing legitimate and potential scam calls using emergency numbers as presentation CLI.

4.47 In response to Twilio, ComReg sees merit in setting out a separate paragraph for such numbers to highlight this particularly important use case.

[174] Public Safety Answering Points ("PSAP") - The PSAP answers all emergency calls and text messages and connects the caller to the required emergency service. This service is currently provided by ECAS in Ireland

4.48 ComReg notes Viatel's view that considerable interoperability testing by operators will be required to ensure the correct working of emergency numbers as CLI.

4.49 Vodafone seeks clarification on the working of emergency calls for long-lined organisations. In response, ComReg notes that operators providing long-line services to their end-users should ensure the correct routing of emergency calls to the local PSAP.

4.50 ComReg notes that respondents to its proposal on permitting 999/112 emergency numbers as CLI recognised the importance of this use-case but had concerns around its implementation.. Therefore, in light of ComReg's preliminary position and respondents' comments, ComReg will permit 999/112 emergency numbers as CLI on the understanding that ECAS will liaise with industry at an appropriate forum, such as the ECAS forum, to ensure that any technical and operational concerns are addressed before implementing such numbers as CLI on networks. Therefore ComReg will enter the following underlined text as paragraph iii of Section 3.1(5)(a);

(a)The undertaking which originates a call on the Irish PSTN shall ensure:

i that the CLI for the call shall be the assigned number for the calling party;

ii *that the presentation CLI for the call shall be ~~the assigned~~ a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number appropriate to the designated MNA for that number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number.*

iii that the presentation CLI for the call may be the single European emergency number 112 or the national emergency number 999 when the call originates from the national PSAP, but not otherwise;

Furthermore, ComReg will insert the following definition for PSAP in Appendix 12;

Public Safety Answering Points ("PSAP") means the entity that answers all emergency calls and text messages and connects the caller to the required emergency service. This service is currently provided by ECAS in Ireland

3. General Updates to provide CLI Guidance (Chapter 6.4 of Consultation 23/52)

CLI Principles and associated Use Cases

Views of ComReg in Consultation 23/52

4.51 In response to requests from operators, in Section 6.4 of Consultation 23/52 "general updates to provide CLI Guidance", ComReg proposed a number of principles to guide operators on the general use of CLI and provide the clarity necessary to ensure compliance with the CLI conditions. In paragraphs 6.75 to 6.83, ComReg provided some example use cases of how the CLI conditions would apply in practice.

4.52 As part of its analysis, in Section 6.4 paragraphs 6.72 to 6.74 of Consultation 23/52, ComReg assessed the current CLI conditions associated with calls that enter into the Irish PSTN from International PSTNs.

4.53 In respect of the definitions used for CLI in the Numbering Conditions, ComReg noted in Consultation 23/52 that the current definitions of presentation and network CLI in the Numbering Conditions are technology neutral and are sufficiently clear for operators to ensure their compliance irrespective of the technologies used.

4.54 ComReg posed the following question;

> *Q3; Do you agree with ComReg's general updates to provide CLI Guidance as set out above? Please explain the basis for your response in full and provide supporting information.*

Views of respondents to Consultation 23/52 on CLI Principles and associated Usage Cases

4.55 While some respondents commented on ComReg's use cases, others sought clarity on additional use cases they identified. ComReg addresses all submissions in this respect in its response.

4.56 Eir agrees with ComReg's assessment.

4.57 ALTO supports ComReg's assessment but maintains that some existing operators will be impacted by the high cost of, what it refers to as, the proposals in the ComReg CLI Guidance. ALTO opines that this is a strategic matter that must be properly considered by ComReg.

4.58 BT contends that it was unusual for ComReg to address private network solutions within the consultation as these are, in its view and for the most part, no longer in use. BT is of the view that such legacy type networks are self-

built networks usually based on leased lines. BT maintains that these legacy networks have been replaced because of the availability of more advanced and efficient cloud-based solutions with integrated security and that truly private networks, as described, no longer exist.

4.59 In relation to what it refers to as Virtual Private Networking, BT maintains that such networking should not be exempted from the obligations of an IGO.

4.60 BT generally agrees with ComReg's view that the definitions of CLI in the Numbering Conditions are sufficiently technology neutral.

4.61 BT and Twilio both identify examples of, what ComReg refers to as, the doctor's surgery/hospital use case. This is where a doctor who is using his / her mobile phone on their patient rounds, wishes to present the surgery/hospital number rather than their own private handset CLI. BT contends that the surgery and the doctor are related so that the doctor has a right to both assigned numbers and accordingly this is a valid use of CLI, albeit, BT considers that the non-geographic condition should apply. Twilio contends that a doctor should be able to set the number of the hospital, rather than their personal mobile number as the CLI, so that the patient is able to call back even when the doctor is not available.

4.62 Both Imagine and Three contend that the CLI Conditions should permit, for example, a contracted party, such as a call centre, to display its end-user customer's number as CLI.

4.63 Twilio suggests a number of examples where, in its view, flexible CLI use should be permitted, such as a delivery person or driver exchanging messages about an impending delivery or cab ride but where neither party wants to be called or texted subsequently.

4.64 Viatel contends that the presence of Resellers makes it difficult to ensure that the principle of authenticating the presentation and network CLI is met. This, Viatel maintains, is because Resellers may not be directly connected to and servicing the end-user. Viatel maintains that such Resellers must therefore take more responsibility, in its view, in ensuring the correct use of CLI.

4.65 Viatel also comments on section 6.71 of the Consultation 23/52 which notes that the originator of the call must ensure that the CLI is the calling party's assigned number. Viatel contends that it does not adequately detail the obligation in what it calls the Operator – Reseller – End User relationship.

4.66 Vodafone opines that ComReg needs to ensure that important customer use cases are not unintentionally restricted. As an example, Vodafone highlights the case where a customer, in this case a large company, might often be assigned multiple numbers across several operators. The operator originating

the call will need to satisfy itself that the numbers are validly assigned.

4.67 In relation to the physical location and CLI conditions, Vodafone outlines a general use case whereby a caller may wish to originate a call from a location that is not within the MNA of the number they wish to use as CLI. Vodafone provides the example of a remote worker for a company in Dublin, residing in Meath who will make a call on the company network and present the company 01 number as opposed to an 041 number when originating calls. In this example, the CLI presented by the remote worker is appropriate to the physical location/MNA of the company. Vodafone maintains that, as more companies start to look at breakout using unified comms such as Microsoft Teams and other solutions, key workers will need to present their company DDI while working remotely.

ComReg's Assessment on CLI Principles and associated Usage Cases

4.68 ALTO comments on what it maintains is the high cost impact to some operators of complying with the CLI conditions. However, ALTO does not identify specific CLI requirements that would have such an additional costly impact. ComReg notes that, apart from its proposal to amend the conditions associated with international CLI, the CLI guidance simply highlights and clarifies, where needed, the existing CLI conditions.

4.69 In response to BT's views on the inclusion of Private Networks in the consultation, ComReg notes that this was one of the few specific examples raised by operators with ComReg in relation to CLI. Furthermore, ComReg did not refer to a Private Network as being built on any technology but noted that it provided fixed telephony services to an organisation with a pre-determined set of end-users across various locations. The example of the call routing across public and private networks was simply to clarify permitted CLI under the current CLI conditions, nothing more.

4.70 Regarding BT's contention regarding "Virtual Private Networking", for the record, ComReg did not indicate in the consultation that such operators are exempt from any conditions that apply to originators of calls on the Irish PSTN.

4.71 In response to both the BT and Twilio's examples, ComReg notes that the doctor may be considered an employee of their surgery/hospital and may use the surgery/hospital number rather than their own private number as CLI. Indeed, in carrying out their professional duties, the doctor should not be forced to use his / her own private mobile number.

4.72 Imagine and Three both provided examples of CLI use by Call Centres that provide services to their end-user customers. ComReg notes that, in this

example, there is a contract between the Call Centre and the end-user organisation. ComReg expects that, as part of the call centre's service offering, the organisation permits the call centre to use its assigned number to contact its end-users. ComReg recognises that an organisation may wish to use its assigned number itself or allow its contractor, such as a call centre, to use the number as CLI as part of the service offered by the call centre.

4.73 Twilio set out examples of a delivery person or taxi driver exchanging messages with the users of the service but where neither party wishes to be called or texted after the service is complete. In response, ComReg notes that Twilio has not provided full details of this CLI use, such as how it might or might not meet the CLI conditions. Nevertheless, this example appears to involve the use of temporary CLIs. On that assumption, ComReg notes that CEPT WG NaN is currently engaged in work[175] in this area and ComReg will consider its findings in due course.

4.74 In response to Viatel's concern regarding the perceived difficulty with validating the CLI where Resellers are concerned, ComReg notes that it made a proposal in Consultation 23/52 that would ensure that end-users are only served by the holder of the numbers being used. In this case the number holder, such as a Reseller in Viatel's example, must ensure compliance with the CLI conditions when originating the end-user's call.

ComReg's Final Position

4.75 Improving trust in numbers is crucial given the upsurge in nuisance communications. Scammers use CLI spoofing to carry out their activities and anything less than a strict application of the CLI conditions increases the risk of undermining trust in numbering. That said, ComReg also recognises that organisations often use CLI for carrying out business, and so ComReg will seek to accommodate legitimate use-cases where possible.

4.76 Although respondents to Consultation 23/52 sought certain assurances that their various use cases can all be accommodated within the CLI conditions, in some instances the same respondents have not shown how such cases might not meet the CLI conditions or how use of an alternative number to meet those conditions is not possible. This lack of information impedes ComReg's ability to act even if ComReg sees merit in certain use cases. ComReg is minded to permit certain CLI use cases as follows.

4.77 ComReg will insert the following text as new paragraphs "f" and "g" in Section 3.1(5) as follows:

[175] CEPT NaN1 work programme

(f) An end-user organisation may give permission to its call centre contractor to use the organisation's assigned number as CLI while providing the service.

(g)An employer may give permission to its remote working employees to use the employer's assigned number as CLI while carrying out their employment duties.

CLI Conditions - Calls that ingress into the Irish PSTN from International PSTNs

Views of ComReg in Consultation 23/52

4.78 In Consultation 23/52 ComReg indicated that, due to the current upsurge in nuisance communications, particularly from international sources, it would review the conditions of use associated with calls entering the Irish PSTN with international numbers as CLI. In that regard it made reference to the following in the Numbering Conditions:

i. Section 3.1(5)(d) provides for the modification of an international CLI as follows;

> *"for international calls originating from outside the State, the CLI may be modified with appropriate prefixes including "00", "+" and the relevant country code"*

ii. Section 3.1 (5)(e) of the Numbering Conditions provides for the insertion of "Caller ID unknown", or equivalent for an invalid CLI as follows:

> *"a presentation CLI may shall be marked as "Caller ID unknown" or equivalent if an operator cannot ensure that the presentation CLI information is valid"*

4.79 In Consultation 23/52 ComReg highlighted that the option to modify the CLI facilitated an operator who has received a trusted international call but for which the correct CLI has not been provided. There is no numbering condition at present that requires, for example, that the CLI is in E.164 format. ComReg noted that such a requirement would provide a minimum, although insufficient, indication that the CLI is dialable.

4.80 In the case of the condition relating to invalid CLI and marking the CLI as "Caller ID unknown", ComReg noted that this condition implicitly applies only to international calls. This is because originating operators on the Irish PSTN must ensure that the CLI is the assigned number for the calling party so that the CLI must always be valid.

4.81 Given the above analysis, ComReg proposed that the current Section 3.1(5)(d) and Section 3.1(5)(e) be replaced with a new Section 3.1 (5)(d) as follows:

> *"That the CLI on inbound international calls shall be in international E.164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code". If the international call is untrusted and the CLI not in E164 format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".*

4.82 Furthermore, ComReg recommended that operators enter into an understanding with their international operator partners that all reasonable efforts are made by that partner to ensure that only calls that are authenticated and dialable are transmitted.

4.83 ComReg posed the following question:

> *Q3; Do you agree with ComReg's general updates to provide CLI Guidance as set out above? Please explain the basis for your response in full and provide supporting information*

Views of respondents to Consultation 23/52 on CLI Guidance

4.84 BT and Eir both support the proposal.

4.85 Three contends that while the CLI Guidance is a useful consolidation of ComReg's views on the issues relating to CLI, it should be issued as a standalone document. In relation to CLI in general, and in particular CLIP and CLIR, ALTO proposes that a bulletin style standalone CLI guide on these topics should be prepared at a later time when, what it refers to as, deliberations and the resulting decisions on these topics are complete.

4.86 Verizon proposes inserting the underlined text in the proposed text as follows:

> *That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code, or setting the correct ISUP "Nature Of Address" flag". If the international call is untrusted and the CLI not in E164 a correct format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".*

4.87 For its part, Viatel refers to paragraph 5e in Section 3.1 "General Authorisation Conditions" of the Numbering Conditions where it is specified CLI "may" be marked as unknown if the operator "cannot ensure" the CLI info is "valid." Viatel contends that ComReg should remove the ambiguity that arises with

the use of "may" and should confirm specific consequences where such a case arises.

ComReg's Assessment on CLI Guidance

4.88 ComReg notes BT and Eir's support for the proposal.

4.89 In response to Three and ALTO's suggestion of a bulletin style standalone guide on CLI, ComReg has identified the CLI principles in the consultation and has provided use-cases to highlight their application. ComReg also notes that submissions to the consultation have generally been supportive or have not disagreed with any of these principles. Therefore, ComReg does not see the need for such a guide at this point but would be willing to re-visit this should the need arise in the future.

4.90 With regard to Viatel's views, ComReg highlights that the consultation proposed replacement text to that referred to by Viatel. In ComReg's proposed text, the option to suppress CLI applies to international CLIs which must be treated differently to national CLIs. This is because operators, for the most part, have no capability to authenticate international CLIs.

4.91 In response to Verizon, ComReg understands that the suggested additional text relates specifically to the technical standard for interconnections using Signalling System Number 7 "SS7" signalling with ISUP. ComReg understands that the number of international connections using SS7 have been in decline as IP voice interconnections using Session Interconnection Protocol "SIP" signalling replace them. Nevertheless ComReg sees merit in making reference to the relevant technical standard[176] as Verizon proposes as it relates to the handling in networks of the nature of address indicators where ISUP is used either with SS7 or SIP encapsulated with ISUP "SIP-I" signalling.

4.92 In light of ComReg's preliminary position and respondents' comments, ComReg confirms its position and will insert the said text, with the underlined amendment, as new Section 3.1 (5)(d) of the Numbering Conditions, as follows;

> *That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code, or setting the correct ISUP "Nature Of Address" flag". If the international call is untrusted and the CLI not in E164 a correct format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".*

[176] Q.763: Signalling System No. 7 - ISDN User Part formats and codes (itu.int)

Sub-Assignment of Numbers

Views of ComReg in Consultation 23/52

4.93 In Section 6.5 of Consultation 23/52, ComReg proposed a KYC guide for operators that would assist them in reducing the risk of scammers being assigned numbers. Furthermore, ComReg identified the current arrangements for operators to provide numbers to end-users. In response to the surge in scam communications, ComReg proposed to amend the permitted types of number arrangements to enable better management of number use. This amendment would ensure that the operator providing service to the end-user is responsible for the obligations attached to the use of those numbers as set out in the Numbering Conditions.

4.94 In Consultation 23/52 ComReg sets out a typical number provision scenario whereby ComReg assigns phone numbers to an authorised operator and that operator in turn provides its customer with those numbers as part of its service. If an issue arises with an assigned phone number, ComReg will contact the operator to whom the number was assigned (the "number holder").

4.95 In Consultation 23/52, ComReg also clarified the use of the Transfer facility. Section 8 paragraph 3 of the draft Numbering Conditions[177] sets out that a transfer occurs when two undertakings agree that one will transfer rights of use of its numbers to the other.

4.96 In paragraph 6.101 of Consultation 23/52, ComReg also referred to the definition of Sub-Allocation/Sub-Assignment, as set out in ECC report 311[178], as: "the assignment of numbering resources by an assignee to another entity that is not an end user".

4.97 Therefore, to ensure the better management of numbers, ComReg proposed that the operator serving an end-user should hold the rights of use of its numbers. To that end, ComReg proposed the following amendment to Section 7.1 of the Numbering Conditions;

> *(2) Undertakings are obliged to only use their assigned numbers for their own end-users. Sub-assignment to other undertakings is not permitted.*

4.98 In its clarification document ComReg 23/75, ComReg responded to the operator question "*Is secondary or tertiary assignment (sub-allocation or sub-suballocation) of numbers allocated from the national numbering plan*

[177] ComReg 23/52d

[178] ECC Report 311 - Sub-assignment and number hosting - Implementation models, rights of use and obligations for E.164 numbers across the electronic communications supply chain

prohibited under your communications law?", by highlighting that it has set out its current position on sub-assignment/sub-allocation in paragraph 6.101 of its Consultation 23/52. ComReg noted in Consultation 23/52 that sub-assignment is not permitted in Ireland. In paragraph 6.100 of that consultation ComReg described a scenario of what it termed "irregular number provision" which, ComReg indicated, appeared to be similar to the examples the same operator provided as illustration of its question. Furthermore, ComReg indicated that, for clarity in the case of irregular number provision, there is no sub-assignment of the rights of use as the number holder involved, i.e. the operator to whom ComReg has assigned the rights of use, remains responsible for the conditions of use of the number.

Views of respondents to Consultation 23/52

Provision of Numbers – Existing Business Practices

4.99 ALTO maintains that the sub-allocation of numbers has been a feature of the Irish market for many years and opines that some operators, perhaps providing or facilitating Over The Top ("OTT") services, may be using sub-allocated numbering to facilitate communications services. ALTO refers to, what it terms, as ComReg's removal of sub-allocation "*in or around*" 2015 despite, as ALTO contends, what the industry might have understood the regulatory position to have been. ALTO maintains that ComReg should take such existing services into account when setting out its regulation in this area.

4.100 ALTO identifies various operators that would use sub-assignment, for example White-Label Network Operators; and Switchless Resellers; Virtual Access Operators (FVNO and MVNO). With this in mind, ALTO seeks what it calls" *a regulated and sub-allocation permissive with certain criteria*", in respect of sub-assignment, referencing Poland and at least two (unnamed) other European countries that, according to ALTO, permit sub-assignment.

4.101 BT contends that ComReg's proposed sub-assignment rules appear to undermine what it considers to be a key segment of the Electronic Communications Provider market and a significant area of competition, particularly with regard to international competition into Ireland. To illustrate its concern, BT provides details of what it sees as the stakeholders in the provision of numbers, from the assignment of numbers by ComReg to the use of those numbers by end-users. In its submission BT relies on a scenario whereby a network operator, to whom numbers have been assigned, is providing a white label service to a retailer who manages the provision of the numbers to its end-users. BT contends that ComReg's proposal is breaking this existing model.

4.102 BT claims confusion with ComReg's clarification concerning the services

provided by, what it refers to as, "*Switchless Resellers*". BT appears to equate such Switchless Resellers to the retail operation of an incumbent which generally does not own or control a network whether physical or virtual. BT maintains that such Switchless Resellers have largely been provided with White Label products by Network Operators through products such as Regulated Wholesale Line Rental WLR and more recently VoIP Voice products over Broadband Next Generation Access (NGA) and Fibre Broadband Access. BT assumes that ComReg's intention is not to prohibit the market for such products.

4.103 BT contends that ComReg's Know Your Customer (KYC) proposal would appear sufficient to meet the objective of knowing the end customers in this case and therefore ComReg's proposal concerning the holder of the rights of use of numbers is not required.

4.104 Magrathea contends that, as part of its fraud control, its clients go through a comprehensive KYC process, and in turn they are required to do the same for their customer or end user. Magrathea contends that ComReg's proposal is therefore unnecessary and is a significant change that will not have the desired effect in its view.

4.105 In the context of the reselling of services by multiple operators. Magrathea comments on the mainly negative impact of what it describes as ComReg's wish to remove such a "*multi-level*" number allocation model. Magrathea contends that withdrawing this model, either retrospectively or in the future, would be deeply detrimental to the Irish telecoms market. Furthermore, Magrathea opines that withdrawing this model would prevent ComReg carrying out its tasks or meeting its objectives as set out in Part 2 of SI.I 444. In that respect, Magrathea quotes extracts from Part 2 of SI.I 444 as follows; "*any conditions must be necessary and proportionate; promote access and take up of networks; promote competition, develop internal markets by removing obstacles, ensure widespread connectivity, promote investment and innovation and must not discriminate in the treatment of ECN and ECS."*

4.106 Three contends that ComReg's proposed condition is incompatible with the supply of wholesale voice services where the supplier of such services has numbers allocated to it but enjoys no relationship with the end user.

4.107 Twilio contends that ComReg recognises sub-assignment through what ComReg calls "*irregular use*" but now proposes to prohibit sub-assignment going forward by its proposed amendment. Twilio makes reference to other NRAs, such as ANACOM in Portugal and CNMC in Spain, that have identified the benefits of sub-assignment.

4.108 Twilio maintains that ComReg could provide an enabling framework for at

least, what it refers to as, a 1-stage number sub-assignment. Twilio contends that such sub-assignment could, as it claims is implemented in Portugal and Spain, include a simple notification process to ComReg. Twilio is of the view that this process would provide clarity on the identity of both the assignee and the sub-assignee, and details of the number ranges involved.

Number Hosting

4.109 With regard to Virtual Network Operators ("VNO"), BT opines that by using the internet and IP cloud connectivity, it provides connectivity to customers but would purchase a number hosting facility from a network operator rather than establish itself as an interconnecting network operator. BT maintains that, as a consequence of ComReg's proposal, whereby the VNO would have numbers assigned to it, other operators would have to be informed as to which Network Operator is hosting the VNO's directly assigned numbers.

4.110 In paragraph 2.77 of ComReg Document 23/75, ComReg noted BT's request for clarity on how it would treat VNOs as, BT maintains, just allocating numbers to VNOs creates the problem of how others route calls to them. BT sought clarity as to whether ComReg will formalise network hosting so that industry network operators can host and route calls to the VNOs given that they will have their own allocation of numbers.

4.111 Magrathea contends that the proposals would impact negatively on number hosting which, it maintains, relies on larger network operators sub-assigning numbers to smaller operators to enable smaller operators to have numbers opened on networks. Furthermore, Magrathea opines that number hosting is an extremely cost effective, efficient and technically prudent way for smaller networks to establish themselves in the market.

Resellers

4.112 BT contends that, in the absence of Switchless Resellers, every number would become a direct retail number and would need to be registered / re-registered with ComReg. BT also maintains that any refresh of end user information will be the same for Network Operators, Virtual Network Operators and Switchless Resellers with an appropriate period required to review end user data.

4.113 Magrathea makes a number of comments in relation to the recognition of Resellers as set out in the Numbering Conditions, maintaining that the references to Regulation 79(4) and Regulation 79(5) of SI444 of 2022 conflict, in its view, with the understanding of such Resellers, as set out by ComReg, and also the "*reselling*" of numbers, as prohibited by ComReg.

4.114 Magrathea opines that ComReg wishes to remove the Reseller model to

enable it to have greater visibility of the user to help reduce scam calls and to protect the numbering resource.

4.115 Viatel states that it does not agree with ComReg's proposal. ComReg understands that Viatel's objection concerns the difficulties that such a condition might have for the use of Resellers in the market. Viatel contends that ComReg had confirmed during Nuisance Communications bilateral meetings that it would only address, what it referred to as, Operator to Operator sub-assignments and would not hinder the existing Operator to Reseller relationships.

4.116 Viatel also maintains that the consultation uses the terms Reseller and Cloud Provider interchangeably and therefore it is seeking clarifications on the responsibilities of these and other such entities that would enable all to operators to comply with the Numbering Conditions.

4.117 Vodafone does not agree with ComReg's proposal and requests clarification of circumstances where an operator resells other operator services or where virtual operators exist on a network using a sub-range of the network operator's allocation.

Call Routing

4.118 Magrathea make a number of observations in relation to its perceived impact of ComReg's proposed change to, what it refers to as, Call Routing Efficiency. Magrathea contends that calls are mainly routed at a network level to the range holder of the number and that changing the holder to an individual number level would require additional number lookups. Furthermore, Magrathea contends that such a step would increase the size of the numbering database as individual numbers would need to be added to that database. Magrathea further maintains that the additional costs of these changes would act as a major barrier to entry for many smaller telecommunication providers.

Number Transfer

4.119 Twilio contends that while number transfers are relevant and need to be maintained, they are not a substitute for sub-assignment, as in its view, this would result in an undue burden on smaller operators.

Numbering Forum

4.120 ALTO, BT and Vodafone suggest that, in the light of the many numbering issues raised in the consultation, ComReg establish a forum, such as the Numbering Advisory Panel, for policy discussions.

ComReg's Assessment

Provision of Numbers – Existing Business Practices

4.121 ALTO opines that the sub-allocation of numbers existed before 2015 but has not been allowed since then. In response, ComReg notes that its Numbering Conventions[179], recognised the sub-assignment of numbers which, for clarity, did not mean the sub-assignment of the rights of use of numbers. ComReg's Numbering Conditions[180] which was adopted as a result of its Consultation 15/60[181] in 2015, did not recognise Sub-Assignment for the reasons set out in that Consultation. However given the confusion on this issue, ComReg will, in the light of comments from Respondents, address Sub-Assignment in its final position.

4.122 In support of its view that sub-assignment should be permitted in Ireland, ALTO references other countries where sub-assignment is permitted, such as Poland, albeit with different levels of permission. In response, ComReg wishes to clarify that it is aware of the different models of sub-assignment in countries that permit sub-assignment, and will take account of these models in its analysis.

4.123 As a general note, BT's classification of stakeholders in the delivery of services, as comprising Network Operators, Virtual Network Operators and Switchless Resellers, is welcome and provides clarity to its submission. ComReg notes, for example, that BT includes KYC as a service requirement or responsibility that applies to all stakeholders and ComReg sees this as a key service in combatting scam communications. However, both BT and Magrathea contend that KYC might be sufficient or would significantly reduce the risk of scammers being provided with real numbers. In response, ComReg views its draft KYC Guidance as necessary but not sufficient of itself in addressing scam communications and its objective, of requiring the end-user service provider to hold the numbers used, is necessary in combatting scam communications.

4.124 Magrathea and Three both contend that ComReg's proposal will, respectively, remove "*multi-level*" number allocations and is not compatible with the supply of wholesale voice services. In response, ComReg notes that it previously clarified in its response to Question 28 in Section 2.12 of ComReg Document

[179] ComReg 11/17 - National Numbering Conventions v7.0
[180] ComReg 15/136 - Numbering Conditions of Use and Application Process
[181] ComReg 15/60 "Numbering Conditions of Use and Application Process". Consultation document – Section 3.12 "Transfer of numbers between operators".

23/75[182] that its proposal does not seek to remove white label services, which includes wholesale services, or what Magrathea refers to as "*multi-level*" number allocations.

4.125 Twilio contends that ComReg currently recognises sub-assignment by making reference to "*irregular use*" in Consultation 23/52. In response, and as set out in paragraph 6.101 of Consultation 23/52, ComReg viewed such irregular use as inappropriate as it creates unnecessary complexity for the number holder in ensuring compliance with the Numbering Conditions. Furthermore, the irregular use scenario does not meet ComReg's objective of ensuring that the provider of services to end-users is the holder of the rights of use of the numbers.

4.126 Notwithstanding this objective, ComReg will set out its final position on sub-assignment in this Response to Consultation 23/52 while taking all submissions into account.

Numbering Forum

4.127 In response to comments regarding the re-establishment of the Numbering Advisory Panel (NAP), ComReg does not see a need for this particular Panel at present. Rather, ComReg will, as a suitable alternative for discussion of any issues concerning voice-based nuisance communications, establish a relevant NCIT working group.

Number Hosting

4.128 In relation to ComReg's proposal, BT highlights the issue of how to route calls to VNOs that will now have their own number assignments. To address this issue, BT requests that number hosting is formalised, by which ComReg takes to mean that the permission for number hosting is included in the Numbering Conditions. In response ComReg notes that, while the Numbering Conditions does not prevent number hosting, ComReg will insert clarification text to this effect in the Numbering Conditions.

4.129 Margathea opines that the prevention of sub-assignment has a negative impact on number hosting. In response, ComReg does not consider sub-assignment to be necessary for number hosting. Nevertheless, in the light of all comments from respondents, ComReg will review and set out its final position on sub-assignment in this Response to Consultation 23/52.

Resellers

[182] ComReg 23/75 – Nuisance Communications - Clarification Questions and Answers on Consultation 23/52

4.130 BT refers to the resulting absence of Switchless Resellers as a consequence of ComReg's proposal that obliges undertakings to only use their assigned numbers for their own end-users. In response, ComReg notes that its proposal is not intended to prohibit Switchless Resellers in the market and would consider its proposed clarity on number hosting as allaying any concerns in this respect. Furthermore, in the light of comments from respondents, ComReg will review and set out its final position on sub-assignment in this Response to Consultation 23/52.

4.131 Magrathea appears to conflate Regulation 79(4) of SI 444 of 2022 and, what Magrathea refers to as, the reselling of numbers. Regulation 79(4) provides that: "*any person who assigns to locations, terminals, other persons or functions on public communications networks numbers from the national numbering plan that the regulator* has *not specifically allocated to the person in connection with the provision of publicly available electronic communications services commits a hybrid offence*". Therefore this regulation is concerned with the prohibition on the use of unassigned numbers and is not concerned with the trading of numbers, nor is Regulation 79(4) of SI 444 of 2022 referenced by ComReg in that respect.

4.132 Magrathea also refers to Regulation 79(5) of SI 444 of 2022, in the context of the resale of numbers. This regulation provides an option for ComReg to assign numbers to a person who is not a provider of electronic communications networks or services. For clarity, this provision is not related to ComReg's recognition of Resellers that, as set out in the Numbering Conditions, are authorised undertakings.

4.133 Magrathea opines that ComReg wishes to eradicate the Reseller model to enable it to have greater visibility of the user to help reduce scam calls but also to protect the Irish number resource. In response, ComReg notes paragraph 2.72 of its clarification Document 23/75 which set out clearly the objective of its proposal as follows; "*The objective of ComReg's current proposal is to ensure that the provider of the service to the end-user has responsibility for the conditions attached to the numbers being used. It is not intended to prevent the resale of white-label voice services*".

4.134 With regard to Viatel's and Vodafone's Reseller-related comments, ComReg continues to recognise Resellers but it has proposed that the operator providing service to the end-user, whether a Reseller or not, must hold the rights of use of those numbers. However, in the light of comments by respondents, ComReg will set out its final position on sub-assignment in this Response to Consultation 23/52.

4.135 Regarding Viatel's comments that there is a need for some clarification with regard to the obligations on various entities, ComReg notes that the

numbering conditions are in the main set out at a principle level and apply to all authorised undertakings that use Irish phone numbers.

Call Routing

4.136 Magrathea maintains that ComReg's proposed changes would mean that operators would have an additional workload leading to increased costs. This, it contends, would add a major barrier to entry for smaller telecommunication providers. In response, ComReg recognises that some changes may be required on networks to accommodate its proposal. Nevertheless, in the light of comments by Respondents on this and other matters that relate to sub-assignment, ComReg will set out its final position on sub-assignment in this Response to Consultation 23/52.

4.137 While largely submitted in the context of what was mistakenly perceived by some respondents as a prohibition on existing sub-assignment scenarios, ComReg noted that many respondents raised certain operational issues concerning ComReg's proposal. In response, ComReg sees these as implementation details that could be discussed within the relevant NCIT working group if required.

Number Transfer

4.138 In response to Twilio's comments on the importance of Transfer and Sub-Assignment processes, ComReg will address both in its final position.

ComReg's Final Position

4.139 Scam communications are undermining trust in the telecommunications industry. ComReg is aware of numbers being misused by end-users whose operator does not hold the rights of use of those numbers. To combat scams and to improve the overall management of the use of numbers for the good of consumers and the industry which serves them, ComReg must have oversight of the operator providing service to the end-user. Therefore, ComReg's objective is to amend the permitted types of number arrangements to enable such effective oversight.

4.140 ALTO, BT, Magrathea, Three, Twilio and Vodafone all contend that, in summary, sub-assignment has been a feature of the telecoms market to date and that ComReg should not seek to change this market by preventing sub-assignment. In response, ComReg notes that its aim is to combat scam communications by amending the permitted types of number arrangements so that ComReg would have better oversight of number use. ComReg has already set out the definition of Sub-Assignment as "*the assignment of numbering resources by an assignee to another entity that is not an end user*". However, to ensure a common understanding going forward, ComReg will

clarify sub-assignment in terms of the entity or entities holding the rights of use of sub-assigned numbers.

4.141 Therefore in light of respondents' comments, ComReg will permit sub-assignment as an option for an operator providing services to another operator. This will be in addition to the transfer of numbers and direct assignment of numbers by ComReg. The sub-assignee will be jointly responsible with the primary assignee for the rights of use of the numbers.

4.142 Furthermore, in recognition of ComReg's aim of having oversight of the operator providing services to the end-user, ComReg will include a notification process for operators who wish to sub-assign numbers.

4.143 In response to BT and Magrathea's views on the importance of number hosting in the market, ComReg will clarify such hosting in the Numbering Conditions.

4.144 Therefore, in light of ComReg's preliminary position and respondents' comments, ComReg will carry out the following;

i. Insert the following text as new paragraph 2 of Section 7.1;

(2) Undertakings are not encouraged to engage in sub-assignment of numbering resources, where sub-assignment means the assignment of numbering resources by an assignee to another entity that is not an end user. Transfer of numbers between undertakings is to be preferred. Where sub-assignment is necessary, it is subject to the prior notification of ComReg, and the consent of the Primary Assignee. The responsibilities regarding the compliance with the Numbering Conditions in relation to the assigned number(s) shall be shared between the Primary Assignee and the Sub-Assignee."

ii. The replacement of proposed paragraph 2 of Section 7.1 of the Numbering Conditions, which was as follows:

"*Undertakings are obliged to only use their assigned numbers for their own end- users. Sub-assignment to other undertakings is not permitted."*

with the following text inserted as new paragraph 3 of Section 7.1:

(3) "In providing services to its end-users, an undertaking shall only use numbers for which it solely, or jointly in the case of sub-assignment, holds the rights of use."

iii. Add the following definitions to Appendix 12;

*"**Primary Assignee**" means, in the context of the sub-assignment of numbers, an undertaking which has been granted a right of use for any class or description of number by ComReg.*

*"**Sub-Assignee**" means an undertaking which has been sub-assigned a number by a Primary Assignee.*

*"**Sub-Assignment**" means, the assignment of numbering resources by a Primary-Assignee to a Sub-Assignee.*

iv. insert the following underlined text in Section 3.2, paragraph 8, as follows;

(8)For the purposes of ComReg making any information requirement under regulation 99 of the 2022 Regulations , holders shall maintain accurate and current records in respect of rights of use for all classes of numbers granted to them, to include the following:

(j)rights of use for numbers sub-assigned to them;

(m)rights of use for numbers sub-assigned by them;

v. insert the following underlined text as a new paragraph 13 in Section 3.1 "General Authorisation Conditions" as follows;

"(13)For the avoidance of doubt, number hosting is permitted in Ireland.

vi. insert a definition of Number Hosting in Appendix 12 "Definitions" of the Numbering Conditions as follows;

"Number Hosting" means the implementation of numbers, which are held by an undertaking, on another undertaking's network; this is to enable connectivity for the number holders' end users.

vii. Where "transfer" is indicated in Sections 3.2(1), 3.2(3), 3.2(4), 3.2(5) and 3.2(6) add "or sub-assign"

Future Number Management – Needs and Developments

ComReg Proposal in Consultation 23/52

4.145 In Consultation 23/52, ComReg noted that one of its functions is to manage the national numbering resource by, among other things, encouraging efficient and effective use of these resources. Furthermore, ComReg recognised the need for it to address the misuse of phone numbers as part of that management function, particularly in light of the ongoing problem of nuisance

communications and the need to protect consumers.

4.146 In its Consultation, ComReg considered possible topics for further discussion with industry:

i. Automated rather than manual number assignment;

ii. Dynamic rather than static voice interventions;

iii. Call routing based on authenticated individual numbers;

iv. Stir/Shaken - monitoring developments of this technology; and

v. Call Authentication Framework that incorporates dynamic and evolving interventions to address the ever-evolving threat of nuisance communications, including the possibility of outsourcing the role of blocking scam calls and SMS to specialist firewall providers who have the expertise to keep up with fraudsters.

4.147 In relation to these topics, ComReg asked the following question;

> *Q5 Do you have any views on ComReg's assessment of future number management as described? Please explain the basis for your response in full and provide supporting information.*

Views of respondents to Consultation 23/52

4.148 BT welcomes ComReg's assessment of future number management and, noting that the INA automated system has worked well, supports an automated number assignment process for efficiency purposes. Viatel also supports such an automatic process for geographic numbers.

4.149 ALTO suggests that ComReg consider re-establishing the Numbering Advisory Panel ("NAP"), or a new form of NAP, to discuss numbering issues. BT also suggests the re-establishment of the NAP, to discuss numbering issues in a changing industry. BT maintains that the NCIT is less suitable for such a discussion as it is more focused on the delivery of specific targets. Vodafone contends that there is a need, in its view, for ongoing collaboration within the industry to enable protection of consumers from scam traffic and that such a broader collaboration, which it believes goes beyond that afforded by the NCIT, will be required as scam communications become more sophisticated.

4.150 ALTO opines that ComReg should avoid measures that appear to impact any particular form of call flow or attempt to implement measures that could impact the wider EU market, whether inadvertently or not.

4.151 BT contends that future interventions should address how to protect or facilitate genuine calls as much as preventing fraudulent calls.

4.152 Eir and Three disagree with, what appears to them as, a suggestion that the NCIT should move towards developing an industry firewall solution provided by third parties. Viatel maintains that the outsourcing of future interventions would make existing investment by operators in this area redundant.

4.153 Magrathea expresses its disappointment that future number management matters are only discussed towards the end of ComReg's consultation which is focussed on scam calls and texts. Magrathea contends that this is a significant topic that requires its own consultation.

4.154 Twilio maintains that, in addition to the aims identified by ComReg, the future of numbering should also reflect, what Twilio refers to as, the evolving technology landscape, including innovative services which meet users' needs, and are welfare-enhancing. Against that, Twilio suggests caution against the risk of what it terms over reach in relation to the adoption of new technologies and, in particular, the risk of false positives when blocking traffic and the need to roll-back on any inadvertent blocking of legitimate traffic.

4.155 Twilio also contends that the ability to perform traceback on harmful calls will be an essential part of any future nuisance communications measures.

4.156 The MEF supports the suggestion of creating a common numbering database which could play a role in CLI authentication among other services.

4.157 Respondents' comments in relation to Stir/Shaken, are dealt with in Section 2.1.7 of this Response to Consultation.

ComReg's Assessment

4.158 For clarity, in Consultation 23/52, ComReg saw an opportunity to set out several topics concerning the future of numbering. These topics were detailed to a sufficient level to allow stakeholders to provide an initial view on the future management of the numbering resource.

4.159 ComReg acknowledges Magrathea's comments on the need to emphasise discussion of these issues with industry. However, ComReg would also point out that nuisance communications is now a major matter of global importance that will shape number management. Consequently, the inclusion of what is an initial, high-level, discussion on numbering within this consultation is clearly appropriate.

4.160 In light of ComReg's preliminary views and comments from respondents on the future of numbering;

i. Respondents that indicated a preference supported an automated, as opposed to a manual process, for number assignment;

ii. Respondents that indicated a preference supported dynamic rather than static nuisance communications interventions; and

iii. Respondents, that commented on the Call Authentication Framework did not express a preference for the outsourcing of the role of blocking scam calls and SMS to third parties.

4. *Updates in light of the SMS interventions (Chapter 6.2 of Consultation 23/52)*

SMS Intervention – Sender ID

Views of ComReg in Consultation 23/52

4.161 Consultation 23/52 proposed two interventions to combat SMS spoofing. One of these interventions was entitled "Sender ID Registry" and consisted of the registration of permitted SMS Sender IDs (" Sender IDs"), and the concept of participating aggregators (PA) in the forwarding of SMS to Irish mobile operators.

4.162 ComReg proposed to include the Sender ID as a class of number in the Numbering Conditions by adding the following table to Appendix 10 "Classes of Numbers" as follows;

Code	Designation	Notes
Alpha-numeric	SMS Sender ID ("Sender ID")	Recognised Sender IDs are included in the SMS Sender ID Registry intervention. The Registry shall include information such as the Sender ID, Sender ID Owner (SIDO) and Participating Aggregator (PA).

4.163 ComReg set out its proposed conditions of use and application process for Sender IDs and the establishment of the Sender ID Registry in accordance with the proposed one-to-one model of Sender ID owner ("SIDO") to Participating Aggregator ("PA"). The proposed text in the Numbering Conditions is related to the following;

i. Management of the Sender ID Registry; ComReg proposed that it would manage this Registry.

ii. Timelines for activation of Sender IDs; ComReg proposed a three month timeline for the activation by the holder of a registered

Sender ID.

iii. Switching PAs; To promote competition, ComReg proposed a means by which a SIDO could switch its serving PA.

iv. Rights of Use Conditions; ComReg set out the format, including the set of permitted characters, for a Sender ID.

v. General Application criteria; ComReg proposed a "first come, first served" basis and set out a Sender ID application form for manual registration of Sender IDs. ComReg also highlighted the possibility of an automated registration process.

vi. Eligibility Criteria; ComReg proposed that the SIDO must have a connection with Ireland and set out the criteria and the information that must be supplied to ComReg to demonstrate this connection.

vii. Administrative changes to reflect the addition of Sender ID as a number.

4.164 In relation to the Sender ID, ComReg asked the following question:

> *Q.1 Do you agree with ComReg's proposal to amend the text in the Numbering Conditions as set out above? Please explain the basis for your response in full and provide supporting information.*

Views of respondents to Consultation 23/52

4.165 There were no objections to ComReg's proposal that it would manage the Sender ID Registry.

4.166 Eir expresses concern that it appeared that the Irish Language Sender IDs would not be supported by the proposed Sender ID format. It also notes that the proposed Sender ID registration eligibility requirements seemed to exclude charities, voluntary organisations, schools etc. Eir points out that such a step could effectively leave those organisations more vulnerable to being impersonated by an Irish mobile number.

4.167 Three supports, in principle, the SMS Sender ID Registry proposal but notes that this intervention results, in its view, in a new commercial situation whereby SIDOs must contract with one aggregator rather than continuing to have the option of contracting with multiple aggregators.

4.168 Three maintains that it is not necessary or proportionate for ComReg to impose what Three terms an access obligation on MSPs by requiring them to accept new direct connection requests from PAs.

4.169 Three contends that the proposal will, in its view, need to clarify the IT systems needed to accommodate the type and throughput of data between stakeholders.

4.170 Three maintains that there is a need for a mechanism to prevent what it refers to as “Sender ID Squatting”. It also maintains that a process is needed to allow trademark holders to register their trademarks in order to protect them for future use and, in this respect, refer to the 3 month timeline[183] to activate a Sender ID.

4.171 Twilio considers that a Sender ID Registry, managed by the independent regulatory authority, is a relevant and sensible way forward for Ireland. However, Twilio outlines a number of issues regarding ComReg’s proposed approach to Sender ID and what it terms the proposed responsibilities between SIDOs, PAs, and ComReg. Twilio contends that the proposed one-to-one relationship between SIDOs and PAs would be an obstacle for many businesses and organisations that see benefit in using more than one SMS aggregator. Twilio also expresses concerns with regard to the first-come-first-served system which, Twilio contends, will lead to a rush to register by PAs.

4.172 Twilio contends that, in addition to individual businesses and organisations being eligible for the assignment of an Irish Sender ID, aggregators should also be entitled to register a Sender-ID in their own name.

4.173 Twilio also seeks clarification that European Union-based businesses, governments, agencies and NGOs will be permitted to use SMS Sender IDs.

4.174 Virgin Media contends that the Sender ID Registry seems like a potentially promising intervention but maintains that the specification of the Registry lacks detail. Virgin Media therefore considers that it would be useful to discuss the matter further at the NCIT and postpone any ComReg decision. Virgin Media further opines that appropriate promotion will be key.

4.175 BPFI and Bank of Ireland support the Sender ID Registry intervention although both maintain that the Registry has certain limitations which they highlight in their submissions.

4.176 Openmind opines on the 1 to 1 (SIDO to PA) configuration in the proposal and outlines what it terms in its view some disadvantages such as the prominence given to certain aggregators and the perceived complexity of switching PA.

4.177 Tanla supports the idea of establishing a full Sender ID Registry. However it comments on several aspects of the Registry that it believes would need to be

[183] ComReg 23/52d - draft Numbering Conditions - Section 3.2 (1)

considered for the Numbering Conditions. Tanla contends that;

i. Unnecessary registrations can be avoided by ComReg charging a fee for each one;

ii. The building and operation of the Registry is not trivial and suggests an approach where operators are responsible for certain activities which Tanla outlines in its submission;

iii. An auction of Sender IDs that are likely to be in demand by several applicants should be considered; and

iv. SIDOs should be able to engage with multiple PAs without the need to port.

ComReg's Assessment

4.178 In response to Eir's comment, ComReg will make provision for Irish Language Sender IDs.

4.179 In response to Virgin Media's contention that the Registry specification lacks detail, and that further discussion on this topic at the NCIT is required, ComReg notes that the Registry is urgently needed to combat the impact that scam texts using Sender IDs are having on Irish consumers. Respondents will be aware that implementation of the registry will take 18 months, further compounding the harm experienced by consumers. As outlined below, and in light of the valuable submissions received, ComReg has made a number of amendments to its proposal. ComReg also plans to engage with Industry on the implementation of the Sender ID Registry following its decision, where matters such as set up phase can be teased out.

4.180 In response to Three, Twilio, Openmind and Tanla's dissatisfaction with the proposed one to one (SIDO to PA) configuration, ComReg has revised the intervention so that SIDOs can contract with multiple PAs, as outlined in Chapter 2.

4.181 In response to Three's comment on the 3 month timeline to activate a Sender ID, ComReg will extend the Sender ID activation timeline to 6 months.

4.182 In response to Three's request for details concerning the initial registering of Sender IDs, ComReg will discuss the set-up of the Registry with Industry at the relevant NCIT working group.

4.183 In response to both Eir and Twilio's views on the Sender ID eligibility criteria, ComReg will provide appropriate amendments to criteria in the Numbering Conditions to remedy, including ensuring that valid international companies

may apply for a Sender ID . Furthermore, as previously indicated in Section 3 of this Response to Consultation 23/52, ComReg is minded to accede to Twilio's suggestion that PAs be permitted to register a Sender ID to be used by the PA's customers who do not wish to register their own Sender ID. While this arrangement will be referred to as a "shared" Sender ID, the Sender ID will be assigned to the PA who will be responsible for the attached conditions of use. Please note that the assignment of shared Sender IDs will be kept under review by ComReg.

4.184 ComReg acknowledges Tanla's comments and suggestions. ComReg does not currently charge for numbers and has not considered whether to charge for Sender IDs numbers, or indeed auction them in this Consultation.

4.185 In light of ComReg's preliminary position and the responses received, ComReg will adopt its proposed amendments to the Numbering Conditions, subject to the following amendments:

i. ComReg will include the Sender ID as a class of number in Appendix 10 of the Numbering Conditions.

ii. ComReg has amended its preliminary proposal for a one to one (SIDO to PA) model to a multi-PA (SIDO to multi-PA) one. In the multi-PA model, ComReg will only accept applications for Sender IDs from SIDOs or PAs in the case of shared Sender ID. While SIDOs are not providers of electronic communications networks or services, and are therefore non-authorised entities, ComReg notes Article 79(5)(a) of SI No 444 of 2022 which provides for the following;

(a) The Regulator may also grant rights of use for numbering resources from the national numbering plan for the provision of specific services to a person who is not the provider of electronic communications networks or services, provided that adequate numbering resources are made available to satisfy current and foreseeable future demand.

Therefore ComReg will carry out the following amendments to Section 2(2)(a) RoU[184] Conditions:

Insert the following underlined text;

(a)"RoU Conditions" are attached to rights of use for numbers

[184] Rights of Use ("RoU")

granted by ComReg to individual undertakings, pursuant to Regulations 10 and 79 and Part E of Schedule 1 to the 2022 Regulations.

Insert the following text at the end of paragraph “a”;

(a)In the case of Sender IDs, end-users, which are non-ECS/ECN and are therefore non-authorised entities, may be assigned such numbering resources based on Article 79(5)(a) of SI No 444 of 2022

iii. Management of the Sender ID Registry; ComReg will manage the Sender ID Registry and, to that end, will insert the following underlined text in new paragraph 4 of Section 1;

As set out in its Response to Consultation 24/24 and Decision 24/24 on Nuisance Communications, ComReg supports industry by managing the following:

(iv)SMS Sender ID Registry

iv. Timelines for activation of Sender IDs; ComReg will amend its proposed text at the end of Section 3.2 paragraph 1 of the Numbering Conditions by inserting the underlined text as follows;

In the case of Sender ID, and unless ComReg otherwise consents, a Sender ID shall be activated by its holder (a) within ~~3~~ 6 months of the date on which the right of use for the Sender ID was first granted to the holder; or (b) within one month of the date on which the right of use for the Sender ID was transferred or sub-assigned, as applicable.

v. Switching PAs; ComReg has amended its preliminary proposal for a one to one (SIDO to PA) model to a multi-PA one. In the latter model, SIDOs will apply and hold the rights of use of Sender IDs. As the holder is free to choose its PA(s), there is no requirement to allow for Sender ID portability in the Numbering Conditions. Consequently, ComReg will remove its preliminary proposal to include text on Sender ID portability as paragraph 8 of Section 3.1. For clarity, processes will be developed in due course to allow the SIDO to change its registered PAs and for PAs and MNOs to take account of the changes on their networks.

vi. RoU Conditions; ComReg will make provision for Irish language characters by amending its preliminary proposal with addition of the

following underlined text:

For example: Not permitted are all characters with accents (E.g. è Ç), Greek letters (E.g. Ω Ψ) and the following: £ $ " ' ¡ €, <u>with the exception of the Irish Fada which is permitted.</u>

vii. Eligibility Criteria; Amend the proposed eligibility criteria for Sender IDs in the Numbering Conditions; the text that is deleted, underlined/bold is in response to submissions to consultation (note that ComReg has also changed, where relevant, "Ireland" to "the State");

The ~~SIDO~~ applicant must be a legitimate organisation and have a need to register a Sender ID in the State ~~Ireland have a connection with Ireland~~ . ~~The connection with Ireland~~ The ~~SIDO~~ organisation shall ~~be demonstrated by the SIDO~~ <u>demonstrate that it meets these criteria by</u> submitting at least one of the following;

i. A company's Irish (<u>or international equivalent</u>) CRO number, Revenue VAT or business number ~~[and/or]~~;

ii. A partnership/sole trader's Irish (<u>or international equivalent)</u> VAT number in their name(s) or proof of their business or Irish income tax registration;

<u>iii. For a trademark holder that holds a trademark that is enforceable in the State ~~Ireland~~, the trademark number or a digital copy of the trademark certificate;</u>

<u>iv. Registered charity number from the Charities Regulator or evidence of registration as a voluntary non-profit making organisation in the State ~~Ireland~~; or</u>

<u>v. Evidence that the organisation's premises is in the State ~~Ireland~~, e,g. organisations such as schools, clubs etc;</u>

<u>For clarity, any organisation that does not meet the above criteria but wishes to submit other evidence that it is a legitimate organisation and has a need to register a Sender ID in the State ~~Ireland~~ may do so. ComReg reserves the right to refuse any application that does not meet the above criteria.</u>

viii. Sender ID application process; ComReg does not envisage a manual process. Therefore the pdf type application form that was proposed in Consultation 23/52 to be included as Appendix 9 in the Numbering Conditions, will not now be included in that document.

ix. Include for Shared Sender IDs carrying out the following:

a. Insert the following text as a definition in Appendix 12

"Shared Sender ID" means a Sender ID which is assigned to a Registered PA for use by its customers who do not wish to register their own Sender ID.

b. Add the following text as paragraph "c" to Section 7.2(8)

(c)The applicant for a Shared Sender ID shall be a Registered PA.

Chapter 5

5 Response to comments on KYC

Introductory Remarks

5.1 In ComReg 23/52, ComReg set out its preliminary views in relation to how operators should apply Know Your Customer (KYC) processes to prevent the misuse of telephone numbers. ComReg also included draft KYC Guidance in Consultation 23/52 and sought comments. In this chapter, ComReg considers the views of interested parties on these matters.

5.2 ComReg has published an accompanying document, the "*Draft Guidance on Know Your Customer" (*ComReg 24/24c*)* which is informed by this Chapter. This document aims to outline what ComReg considers to constitute best practice in terms of KYC.

5.3 To ensure that the KYC Guidance is as useful and complete as possible, ComReg has decided to provide a short period for comments on its *Draft Guidance on KYC.* Comments should be sent by email to kyc@comreg.ie by 5.30pm on Wednesday 1 May 2024. ComReg will consider the comments received and will revise its KYC Guidance as needed.

5.1 Assessment of the submissions

Summary of ComReg's views in Consultation 23/52

5.4 In Consultation 23/52, ComReg outlined how "*a key factor in preventing phone scams is ensuring that numbers are only assigned to customers who plan to use them lawfully*". KYC involves maintaining a certain level of information on customers before and during the delivery of a service or product, allowing for timely tracing and resolution of issues as needed. Electronic KYC ("eKYC") includes the electronic identification of customers by document verification, biometrics, and facial recognition etc.

5.5 In Consultation 23/52, ComReg stated that Ireland is one of only a very small number of countries without mandatory SIM registration for prepay mobile phones. ComReg noted, in Consultation 23/52, that it does not currently plan to require SIM registration for prepaid SIMs and that alternative measures, such as voice and SMS firewalls along with SMS Scam Filters, should be explored in the first instance.

5.6 ComReg proposed that operators should implement eKYC for new eSIM subscriptions. ComReg also noted that, over time, this would result in many

customers being registered as they upgrade to new eSIM devices.

5.7 ComReg urged all operators, including cloud service providers, to implement a robust KYC process without delay.

5.8 ComReg further proposed a KYC guidance document ("KYC Guidance") to assist operators in developing and implementing KYC processes. This outlined the minimum KYC checks that operators should carry out before providing numbers to individual and business customers, as well as the steps operators should take to monitor number use and to report potential number misuse. ComReg also outlined that it may contact operators, as part of any investigation into number misuse, and request information on or "*audit*" operators' KYC processes.

5.9 ComReg asked the following question in Consultation 23/52:

> *Q. 4 Do you agree with ComReg's views on KYC and the proposed draft Know Your Customer Guidance document? Please explain the basis for your response in full and provide supporting information.*

Views of respondents to Consultation 23/52

5.10 The views of respondents and ComReg's assessment of same are grouped under the following headings:

- Prepay Mobile SIM Registration and eSIMs;
- Guidance on KYC;
- KYC requirements for 1800 and 0818 numbers;
- Audit of KYC processes; and
- Reporting number misuse.

Prepay Mobile SIM Registration and eSIMs

5.11 Two respondents (Three and Vodafone) agree with ComReg's approach not to introduce mandatory SIM registration for prepaid SIMs at this time.

5.12 Vodafone contends that the impact of the current NCIT work programme should be assessed before imposing further process or systems change that could mean an overhaul of the Pay As You Go customer journey. Vodafone further contends that unintended consequences should also be considered e.g., Pay As You Go phones are sometimes purchased as gifts where the purchaser will not be the end-user.

5.13 Eir notes ComReg's views in relation to implementing eKYC policies for eSIM so that all customers are registered and known to them. However, Eir does not believe that the introduction of eSIM of itself will lead to the registration of all prepay users.

Guidance on KYC

5.14 Several respondents commented on the proposed KYC Guidance (Vodafone, ALTO, Verizon, Three, Eir, Viatel, Tesco Mobile, Twilio, Tanla).

5.15 Vodafone believes that requesting some of the proposed customer details is appropriate (e.g., customer details and company information such as Irish CRO number, Revenue, VAT or business number) but contends that other details may be considered disproportionate, intrusive or impose an unnecessary obstacle to commercial engagement (e.g., nature of business, existing phone numbers, business websites, contact details for senior manager with responsibility for numbering, business customer's network and services provided, volume of number request versus intended use of numbers).

5.16 Vodafone is of the view that further details can be obtained from customers after the event if substantial amounts of numbers are requested but that seeking this data from all customers directly would not be appropriate. Vodafone contends that certain details are not practical to require in its view and contends that customers would consider them unnecessary.

5.17 Vodafone further submits that it collects what it terms considerable and necessary data when allocating services/numbers to business customers and to bill pay customers. Vodafone also maintains that it has checks in place to prevent fraudulent activity for new service applications, as well as ongoing processes to manage potentially fraudulent use.

5.18 In relation to providing support and information to affected customers, cooperating with ComReg, other regulators, law enforcement and other relevant organisations, Vodafone asserts that it will always cooperate fully to resolve incidents affecting its customers.

5.19 Both ALTO and Verizon agree that the proposed KYC Guidance includes helpful suggestions for communications providers that have yet to implement processes to ensure they know their business customers. Verizon opines that the guide can be used to help plan and focus the development of suitable processes. Both also agree that KYC is important to ensure communications providers are confident in how their customers use valid numbers, but both contend that communications providers that have already implemented what they describe as robust and efficient processes should not be required to

implement new processes.

5.20 ALTO opines that a third-party risk management vendor could be engaged to ensure a high level of consistency in the KYC approach taken by providers and encourages ComReg to consider this further.

5.21 ALTO and Verizon both opine that the risk profile of business customers should be considered when applying KYC but that it is not proportionate, in its view, to require new and prescriptive processes for corporate and enterprise customers that have a low number misuse risk profile.

5.22 Both ALTO and Verizon contend that ComReg should avoid being prescriptive on measures that communications providers are expected to implement to ensure compliance with their regulatory obligations. Each suggests that ComReg should focus its guidance on encouraging communications providers to support the principle of assigning numbers to low risk and/or reputable customers, while allowing providers the flexibility to individually define the relevant measures for their customer base and service offerings.

5.23 Three contends that what it describes as the binary distinction between KYC checks for individual customers and those for organisation/business customers is overly simplistic in its view. Three maintains that applying ComReg's proposed "*minimum KYC checks*" to all business customers regardless of size is disproportionate, given that, in its view, different services have different levels of risk and that there may be technical features (unspecified) inherent to the service that either lends itself to or mitigate against their use for fraud. Three contends that KYC should be explored more fully at the NCIT before being advanced.

5.24 Eir contends that it is important for KYC to operate effectively where it is required. In relation to the proposed KYC Guidance for business customers, Eir opines that "*Nature of business*" and "*Information about the business customer's network and services provided*" appear to it to be the same requirement. Eir is unsure about what an operator should do with such information and would welcome further guidance from ComReg about the forms of business, trades and professions that should be prohibited and also with regard to what it terms the implications of an access seeker providing limited information about the nature of their business.

5.25 In relation to ComReg's proposal to seek information on "*Existing phone numbers and business websites*", Eir contends that the provision of a website is a matter for the business customer and queries whether operators will be expected to perform an audit of business websites.

5.26 Eir also seeks clarification on how number volume requests and intended use

of numbers should be considered by operators ("*Volume of the request for numbers does not match the intended use of numbers*").

5.27 Viatel maintains that KYC is not mandated but rather is an outline of future suggested improvements.

5.28 Tesco Mobile contends that ComReg has contradicted itself by proposing standalone KYC guidance but expecting all operators to adopt a KYC process without delay and indicating that it may audit operators' KYC processes.

5.29 Tesco Mobile welcomes the publication of KYC guidance as long as it does not impose what it describes as unnecessary additional burdens on operators. Tesco Mobile contends that while ComReg has referenced increased fraudulent activity using prepay SIMs, the proposed KYC requirements relate to bill-pay SIMs. Tesco Mobile contends that operators are already invested in completing risk assessments when registering a bill-pay customer on their network and that prepay is the matter for attention as registration is not currently mandatory.

5.30 Tesco Mobile further maintains that where a contract requires explicit reference to the numbering conditions as proposed, any such change should be permitted without invoking any right of exit right.

5.31 Twilio welcomes the proposed KYC guidance which it believes is closely aligned with established practice in the UK. Twilio also welcomes clarity and alignment as it claims to face challenges due to the application of different regulatory obligations in different jurisdictions. Twilio opines that ComReg should work with its counterparts e.g., in BEREC and CEPT ECC, to aim for and maintain maximum harmonisation of KYC requirements for telecoms operators with specific attention to the challenges faced by multi-country providers of cloud-based communications services.

5.32 Tanla appreciates that ComReg recognises the significance of KYC verification and the importance of validating a business's official documents (e.g., physical address). In its view, such measures have been instrumental in enhancing the KYC verification process for small and medium businesses in India.

KYC requirements for 1800 and 0818 numbers

5.33 Three contends that the proposed additional KYC requirements for 1800 Freephone and 0818 Standard Rate numbers will impose some operational overhead at point of sale. However, Three is of the view that [✂[redacted]✂].

Audit of KYC processes

5.34 Vodafone contends that ComReg's proposal to audit KYC processes appears quite interventionist in terms of a ComReg "*guideline*" and seeks clarification on ComReg's basis for such proposed audits.

Reporting number misuse

5.35 In relation to the points raised in ComReg 23/52 on "*Previous complaints about numbers provided to the business customer*" and "*Consumers and organisations should be able to notify operators quickly and easily of suspected number misuse incidents*", Eir opines that previous complaints may not be known to the current operator providing service to the business. Eir also contends that consumers and organisations suspecting number misuse incidents may not be aware of the identity of the operator providing services to the business under suspicion.

5.36 Eir suggests that it would be more effective if complaints were recorded at a central level and a list of suspected businesses maintained and circulated to operators. Eir has no objection working with a central body to assist in investigating complaints and asks if ComReg would assume this central coordinating role.

5.37 Vodafone contends that, with regard to paragraph 6.128 of Consultation 23/52, the proposed reporting "*obligation*" / expectation requires definitive reporting thresholds such as those provided for network security and integrity reporting. Vodafone opines that use of the terms "*significant*", "*timely or appropriate*" are also important as well as the manner in which an operator would submit a report.

ComReg's Assessment

5.38 Firstly, ComReg believes that KYC is vitally important to building trust with customers and maintaining a good business reputation. It has been implemented extensively in some sectors, e.g. financial services, for many years, and its application in other sectors such as telecoms is long overdue. For KYC to be both successful and impactful in the telecoms sector, it must be understood and supported at all levels in the operator's organisation. It should be factored into and implemented at all relevant stages in a customer's journey.

5.39 In order to combat nuisance communications, telecoms operators and cloud service providers should implement KYC measures before assigning phone numbers to customers. This will reduce the likelihood of fraudsters getting

hold of phone numbers in the first instance and then using them to scam or deceive consumers.

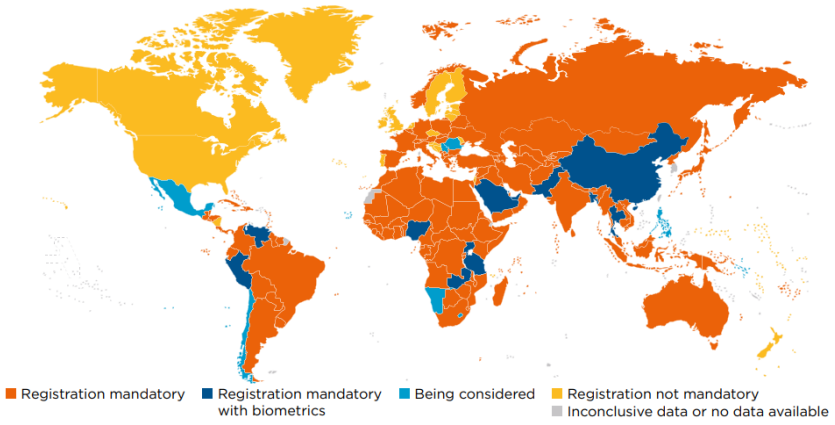
Prepay Mobile SIM Registration and eSIMs

5.40 Prepay SIMs are now being widely used to perpetrate scams as these are easily acquired absent any registration. Fraudsters can then conduct their scams almost without impunity and may even have discarded a SIM before the fraud is even detected. ComReg recognises this as a significant and rapidly growing problem.

5.41 Some operators seem animated with regard to the possibility of unintended consequences. ComReg agrees there is a need to be mindful of unintended consequences if changes are introduced for prepay SIMs but the avoidance of unintended consequences is a matter that ComReg is always conscious of given its regulatory role. That said, one way to mitigate the risk of prepay SIM fraud is to register all users of these SIMs. SIM registration would require that Mobile Service Providers (MNOs and MVNOs) collect or verify a customer's identification credentials and other personal information before registering or activating a prepaid mobile SIM card in their name.

5.42 As illustrated in Figure 4 below, Ireland is one of only a few countries worldwide that does not currently require prepay SIM registration. Other countries are stricter in controlling access to these SIMs. Registering existing prepay SIMs would however not be without its challenges as there are already millions of these SIMs in circulation and used in phones around Ireland. Consequently, ComReg considers, at this stage, that mandatory registration for existing prepay SIM users should not be introduced for the moment pending an assessment of the effectiveness of voice and text firewalls.

Figure 4: SIM Registration Globally



Source: GSMA as of 2021. Note – Denmark, Lithuania and Sweden have introduced mandatory SIM registration since 2021.

5.43 It is in the interest of operators to ensure that the interventions are implemented in the most effective and efficient manner possible (e.g. firewall solutions which target national based fraud and are becoming increasingly prevalent). To the extent that nuisance communications continue to cause significant harm or where harm can be attributed to prepay phones in the future, ComReg may decide to revisit the issue of prepay SIM registration.

5.44 In the prevailing absence of requiring prepay registration, ComReg expects operators to take proactive KYC measures to prevent prepay SIMs falling into the wrong hands. ComReg therefore strongly recommends that mobile operators introduce KYC measures for all new prepay SIMs, including eSIMs.

5.45 Lax KYC policies may fuel scams not just in Ireland, but abroad as scammers seek out SIMs from more permissive MNOs. Absent stronger KYC, Ireland risks becoming a hotbed for the supply of SIMs for fraud not just at home, but internationally.

5.46 ComReg agrees with Eir that the introduction of eSIM alone will not lead to the registration of all prepay users. However, the introduction of eSIM nonetheless represents a timely opportunity for operators to implement KYC/eKYC properly in this nascent sector of the market.

5.47 Indeed, as ComReg noted in Consultation 23/52, the migration to eSIM, although slow, presents a great opportunity for operators to improve KYC, but only if the utility of eSIM is properly stewarded from the outset; anything less and this market opportunity will be damaged or even perished.

5.48 Absent strong eKYC, the rollout of eSIM could in fact exacerbate the misuse of prepaid SIMs, as eSIM enables the download of a mobile subscription within minutes.

5.49 Gathering sufficient information to securely verify customers at the point of sale and across all channels will enable prompt tracing and resolution of any issues that arise. Rigorous KYC processes themselves will also deter fraudsters from acquiring eSIMs.

Guidance on KYC

5.50 Some respondents welcomed the draft KYC guidance (Tesco Mobile, Twilio) while some contended that KYC should not be mandated (Viatel).

5.51 In relation to Twilio's comment on the alignment of the proposed KYC Guidance with the UK's KYC approach and suggestion that ComReg liaise with its counterparts, ComReg continues to discuss and track KYC matters at a European level, for example through the offices of BEREC and CEPT ECC. Indeed, in Consultation 23/52, ComReg examined recent international

developments in KYC to inform its views, which highlighted that Ireland is an outlier at present, in particular by not requiring the mandatory registration of prepaid SIMs.

5.52 Both ALTO and Verizon contend that some communications providers have already implemented robust and efficient processes. That is to be welcomed, but ComReg considers that all operators should review their existing KYC processes, and where necessary increase the level of KYC checks to meet the KYC Guidance. Operators should also ensure that all staff are informed of the importance of proper KYC and embedding and implementing appropriate KYC processes at every stage of the customer journey.

5.53 ComReg notes the views of some respondents that some customers may warrant more checks than others and that a balance should be struck between the level of customer checks and the scale of the potential risk posed. ComReg has taken these views into account in the draft KYC Guidance (ComReg 24/24c, published alongside this document).

5.54 In relation to Vodafone's contention that some proposed customer details, (e.g., nature of business, existing phone numbers and business websites) may be disproportionate, intrusive or impose an unnecessary obstacle to commercial engagement, ComReg responds that the 'nature of business' is key to understanding a customer and their risks. ComReg believes it essential for operators to know and understand the customers to whom they are providing numbers. Only then can they be assured that their customers are legitimate and unlikely to misuse numbers which is of course what all operators want. In relation to Eir's enquiry as to what operators should do with this information ComReg notes that it should be used by operators to assure themselves that prospective customers have a valid use for telephone numbers, thereby better ensuring the efficient use of the national numbering resource.

5.55 In relation to Eir's contention that the provision of a website is a matter for the business customer, ComReg notes that most businesses now have websites to promote their business and to advertise services. While ComReg does not currently expect operators to carry out an "*audit of business websites*", ComReg stresses that it is critical that operators know who they are providing services to and gathering such rudimentary details hardly seems an onerous task. Of course, and as Eir will be aware, most businesses are typically contactable by phone so ComReg would not consider it disproportionate or intrusive to seek existing phone numbers and websites from customers. It is essential that operators have a way to contact business customers in the event of any issue that arises, so ComReg does not consider gathering and retaining this information laborious or disproportionate.

5.56 ComReg notes ALTO's suggestion that a third-party risk management vendor could be engaged to ensure a high level of consistency in the KYC approach taken by providers. At present, KYC is a matter for individual operators and operators have implemented KYC policies unilaterally. ComReg intends that the KYC Guidance will set a clear and consistent level of KYC for operators to achieve. As noted in Consultation 23/52, ComReg may consider how to check the KYC policies of operators in the future, if needed. For now, it is a matter for operators to determine how best to ensure the fitness of their own KYC procedures, and operators may engage with such vendors in that regard.

5.57 In response to Tesco's comment on contract right of exit, ComReg clarifies the recommended inclusion of Numbering Conditions compliance in customer contracts does not relate to consumer contracts but rather to wholesale and reseller contracts. ComReg has reflected this in the *Draft Guidance on KYC*.

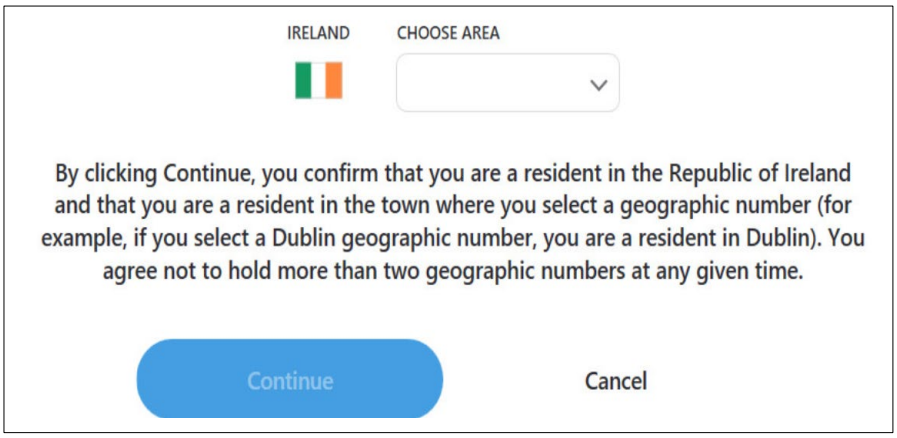
5.58 In response to Three's suggestion that KYC be further considered at the NCIT, ComReg has now decided to publish the KYC Guidance in draft form, with a short period for comments.

5.59 Eir also raises the matter of volume requests and what should be considered by operators with regard to the intended use of numbers. Of course, operators will naturally be very interested in volume requests given the very nature of their business but of course operators cannot be neglectful of reasonable responsibilities regardless of the size of the prospective account. It follows therefore that operators should check that customer requests for numbers are appropriate for the services those customers plan to offer. Excessive number requests or discrepancies between the services provided by the customer and quantity of numbers requested should raise the curiosity of operators to ensure matters are as they should be. Vigilance by operators is required and expected. It is not sufficient for operators to hand out numbers without an appropriate justification for the numbers requested, given that numbers are a finite national resource. Such an approach would inevitably lead to inefficient resource allocation and misuse of numbers, something that the industry will of course wish to avoid.

5.60 Turning more specifically to cloud services where some specific problem areas have been identified, fraudsters are spoofing Irish geographic phone numbers on cloud platforms. The Fixed CLI blocking intervention is designed to prevent calls with spoofed Irish CLIs. However, a further problem highlighted to ComReg is that fraudsters have been assigned <u>real</u> Irish phone numbers through cloud platforms. This is a very concerning development and one that must be addressed without delay. Given the distant nature of their business, cloud providers must be particularly vigilant when assigning numbers. Geographic numbers must only be provided to customers whose location has been verified. For example, a simple self-declaration that an

applicant for an Irish geographic number is a resident in the Republic of Ireland and a resident in the town for which a geographic number is sought is open to widespread misuse (see Figure 5).

Figure 5: Example of self-declaration for a geographic phone number application.



5.61 If there is no proper address verification, fraudsters would be able to easily access Irish numbers and use them to perpetrate fraud on Irish consumers from abroad. Such a situation would be wholly unacceptable and is a matter which ComReg will be monitoring and engaging with relevant parties in due course. It should be noted that this is required even if the Irish CLI is suppressed on calls using that number, as scammers may still use these numbers to contact consumers or to be contacted by them (e.g., for in-bound calls). Indeed, ComReg has been made aware of scam texts which include Irish geographic numbers for customers to call.

5.62 For the avoidance of any doubt, ComReg confirms that, as per the Numbering Conditions of Use (ComReg 15/136R4), customers provided with Irish geographic numbers must be located in the relevant Minimum Numbering Area (MNA) for those numbers. Self-declarations of location by the customer are insufficient and ineffective. Evidence of customer location must be sought and retained by operators providing geographic numbers to customers. This matter is addressed in more detail in the draft KYC Guidance.

5.63 Finally, and with regard to Viatel's observation that KYC is not mandated, this is correct and ComReg hopes that the voluntary approach will ensure a high level of KYC, with widespread compliance. However, if this approach does not demonstrably improve KYC, ComReg will have to revisit its position.

KYC requirements for 1800 and 0818 numbers

5.64 Three contends that the proposed additional KYC requirements for 1800 Freephone and 0818 Standard Rate numbers will impose some operational

overhead at point of sale but noted [✂[redacted]✂]. Of course, this is essential information and should be collected from the customer before an 1800 or 0818 number is provided.[185] The introduction of KYC Guidance is just a codification of existing arrangements that should have been collected in any event. This is therefore, merely, a marginal cost of doing business.

Audit of KYC processes

5.65 In Consultation 23/52 ComReg outlined that it may carry out KYC audits of some operators' KYC processes. For the avoidance of doubt, ComReg clarifies that this means it may check operators' KYC processes for compliance with the Numbering Conditions e.g., to ensure evidence of customer location is recorded for geographic number provision. In relation to aspects of the KYC Guidance which are not presently required by the Numbering Conditions, ComReg notes that it will consider the comments provided on the draft KYC Guidance before publishing final KYC Guidance.

Reporting number misuse

5.66 ComReg notes Eir's observation that previous complaints about a business may not be known to the current operator, along with its suggestion that complaints could be recorded at a central level by ComReg. ComReg expects that operators' KYC checks and procedures should be sufficiently stringent to query prospective new customers and identify problematic customers in advance of providing services. ComReg considers that operators are best placed to design and develop any industry required solutions for handling complaints.

5.67 Finally, ComReg notes Vodafone's comments in relation to number misuse reporting which it addresses in its draft KYC Guidance.

[185] Section 4.3(2) of the Numbering Conditions sets out that "*An authorised undertaking shall only be granted the Rights of Use of 1800 Freephone Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for together with the end-user's unique identifier*". Section 4.4(2) of the Numbering Conditions sets out a similar condition in respect of 0818 phone numbers. In addition, the order shall include certain customer business information as also set out in sections 4.3 and 4.4 of the Numbering Conditions.

Chapter 6

6 Regulatory Impact Assessments

6.1 This Chapter provides ComReg's three Final RIAs which are the 'Sender ID' RIA, the 'CLI Call Blocking' RIA and the 'Voice Firewall' RIA[186]. These RIAs assess each of the relevant interventions and also provide an assessment of the combined effect of the preferred interventions across all RIAs. In preparing these Final RIAs, ComReg has also had regard to the following:

- views received in response to the draft RIAs and other related chapters as set out in Consultation 23/52;
- the Europe Economics Report and Europe Economics response to issues raised in relation to its analysis and findings; and
- the Plum Report which assesses the timelines associated with the implementation of each of the interventions.

6.2 The remainder of this Chapter is structured as follows:

- First, ComReg describes the RIA framework which ComReg uses to assess the likely effect of a proposed new regulation or regulatory change. (See Section 6.1)
- Second, ComReg assesses the main policy issues relevant to all RIAs noting that each individual RIA will have additional and distinct policy issues. (See Section 6.2.1 and 6.2.3)
- Third, within each individual RIA, ComReg then assesses the various regulatory options available having regard to the impact on stakeholders, competition, and consumers. (See Section 6.3, Section 6.4 and Section 6.5)
- Finally, ComReg assesses the preferred options from each of the RIAs (the "Overall Preferred Option") against ComReg's statutory remit, including relevant functions, objectives, duties and principles. (See Section 6.6)

[186] This excludes the 'SMS Scam Filter RIA ' which was included in Consultation 23/52 as this is not a regulatory option and therefore this document does not contain a Decision Instrument for this intervention. Reference is only made to the SMS Scam Filter where relevant to the assessment of the Interventions (e.g., the potential cumulative impact on operators).

6.3 Each RIA has regard to ComReg's statutory objectives which are summarised in Annex 3, including that ComReg is required to take all reasonable measures which are aimed at achieving its prescribed statutory objectives while such measures must also be proportionate to those objectives.

6.1 RIA Framework

6.4 In general terms, a RIA is an analysis of the likely effect of a proposed new regulation or regulatory change, and, indeed, of whether regulation is necessary at all.

6.5 A RIA should help identify the most effective and least burdensome regulatory option and should seek to establish whether a proposed regulation or regulatory change is likely to achieve the desired objectives, having considered relevant alternatives and the impacts on stakeholders. In conducting a RIA, the aim is to ensure that all proposed measures are appropriate, effective, proportionate and justified.

6.1.1 Structure of the RIAs

6.6 As set out in ComReg's RIA Guidelines[187], there are five steps in a RIA. These are:

a) Step 1: Describe the policy issue and identify the objectives;
b) Step 2: Identify and describe the regulatory options;
c) Step 3: Determine the likely impacts on stakeholders;
d) Step 4: Determine the likely impacts on competition; and
e) Step 5: Assess the likely impacts and choose the best option.

6.7 A RIA typically assesses each of the five analytical steps consecutively before concluding on its preferred option. The RIAs in this consultation follow a similar structure, however, the inclusion of many potential interventions across both voice and SMS poses a challenge because many of the possible interventions are not mutually exclusive, are complementary or target the same overarching policy issues. Further, as these interventions apply in many cases to the same operators, any combination of interventions could potentially result in cumulative or complementary effects. Therefore, a number of steps will be conducted jointly across all RIAs.

[187] See Document 07/56a – Guidelines on ComReg's approach to Regulatory Impact Assessment – August 2007.

6.8 Considering the above and to allow for the appropriate assessment of the interventions, while avoiding any duplication of analysis in the following sections, ComReg first identifies the overarching policy issues and objectives to be addressed across all RIAs, noting each of the individual RIAs may have separate policy issues and objectives. (i.e., Step 1). Then ComReg determines the RIAs that will be required and the associated regulatory Options (i.e., Step 2 of the RIA process) and identifies the industry stakeholders (i.e., Step 3 of the RIA process).

6.9 ComReg has adopted the following structure in relation to Step 3 and Step 4 – the impact on consumers is considered first, followed by the impact on stakeholders, competition and consumers. This order does not reflect any assessment of the relative importance of these issues – however much of the impact on industry stakeholders (e.g., use of voice calls) and competition (e.g., distortions to competition) derive from consumers' likely reaction to scam calls and texts.

6.10 Of themselves, the RIA Guidelines and the RIA Ministerial Policy Direction provide little guidance on how much weight should be given to the positions and views of each stakeholder group (i.e., Step 3 of the RIA process), or the impact on competition (i.e., Step 4 of the RIA process). Accordingly, ComReg has been guided by its statutory objectives which it is obliged to seek to achieve when exercising its functions.

6.11 Finally, ComReg assesses the extent to which the Overall Preferred Option would, if implemented, be likely to achieve one or more of ComReg's statutory objectives in the exercise of its related statutory function or functions (Step 5) across all Interventions from the individual RIAs. In doing so, ComReg assesses any cumulative effects of interventions on their proportionality, competition, and consumers.

Competition and consumers

6.12 The focus of Step 4 is to assess the impact on competition of the various regulatory options available to ComReg. In that regard, ComReg notes that it has various statutory functions, objectives and duties which are relevant to the issue of competition. These are set out at Annex 3. The 'Impact on Competition' assessment, arising from each of the regulatory options, is assessed within each RIA under the headings provided in (i) to (iv) below.

6.13 As outlined below, there are different elements to competition that are relevant in determining the impact of any of the preferred options. These include:

i. ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality[188] ("Impact on consumers").

ii. Encouraging efficient use and ensuring the effective management of numbering resources[189] ("Efficient use of numbers");

iii. ensuring that there is no distortion or restriction of competition in the electronic communications sector[190] ("Promoting competition"); and

iv. Promoting efficient investment and innovation in new and enhanced infrastructures[191] ("Efficient Investment").

6.14 Telephone numbers are a finite resource with many different services and users, and the management of these numbers involves the careful consideration of a broad range of factors (e.g., administrative, regulatory, social, economic, and technical) with a view to ensuring that telephone numbers are optimally and efficiently used. Broadly speaking, the efficient use of numbers cannot be consistent with widespread harm to consumers and business arising from their use.

6.15 Further, it can be generally assumed that what is good for competition is good for consumers. This is because increased competition between operators brings benefits to their customers in terms of price, choice and quality of services. In that regard, options that are good for competition are likely to be good for consumers.

6.2 The RIAs (Joint steps 1-3)

6.2.1 The policy issues & the objectives (Joint Step 1)

Policy issues

6.16 The distinct policy issues for each of the three RIAs are discussed at the outset of those assessments. However, ComReg has identified two broad policy issues that are relevant to all RIAs and these are considered here first. These are:

I. To reduce the harm to consumers and businesses from Nuisance Communications ("Economical and Societal Harm"); and

[188] Section 12(2)(a)(i) of the Communications Regulation Act 2002, as amended, and see too Regulation 4(3)(d) of S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022.
[189] Section 12(2)(a)(iv) of the Communications Regulation Act 2002, as amended.
[190] Section 12(2)(a)(ii) of the Communications Regulation Act 2002, as amended.
[191] Regulation 4(5)(d) of S.I. No. 444 of 2022. See too Regulation 4(3)(b) of S.I. No. 444 of 2022.

II. To restore and protect trust in ECS Networks and telephone numbers ("Loss of trust in ECS Networks and numbers").

6.17 The overarching policy issues for all RIAs is to implement those technical interventions that best achieve these two objectives, having regard to ComReg's statutory framework and associated objectives and the particular facts and circumstances of the technical interventions.

6.18 This Section also serves as a repository of key findings of ComReg's research which should be of use to a wide array of policymakers, enforcement agencies and businesses and notably in relation to raising awareness of scams among most at-risk consumers[192], implementing measures to catch fraudsters[193] or legislating to enable the full benefit of certain technical interventions[194].

I. Economic and societal harm

6.19 In order to propose suitable interventions, it is first necessary to understand the multifaceted effects of scam calls and texts on our society. In particular, estimates of harm assist ComReg in determining whether the proposed interventions are proportionate and effective in reducing and mitigating the harms to consumers and businesses. This section is therefore a necessary precursor to the policy issues in each of the RIAs that follow.

6.20 There have been various international estimates of the harm caused by nuisance communications. However, these are of a very general nature[195] and neither ComReg nor Europe Economics are aware of any estimates which are based on seeking direct insight and evidence from consumers and businesses about how they have been harmed. The estimates of Europe Economics therefore broke new ground by providing novel and robust estimates of harm that were informed by a wide variety of sources including:

1. **Consumer Survey:** B&A conducted a survey of over 1,200 consumers to understand the prevalence and harm caused by scam calls and texts.
2. **Business Survey:** B&A also conducted a survey of over 800 representative businesses in Ireland to understand the harm from scams to their operations.

[192] ComReg's econometric research on scam victimhood and payments can enable consumer awareness campaigns to target at-risk consumers.
[193] This includes for example the use of call tracing to aid in the prosecution of international fraudsters.
[194] For example, legislation is required to fully enable the SMS Scam Filter.
[195] For example, the FCC estimated benefits of at least $3 billion from eliminating illegal scam robocalls. That estimate assumed a benefit of ten cents per call and multiplied it across an estimated figure of 30 billion illegal scam robocalls per year, derived from third-party data. https://docs.fcc.gov/public/attachments/DOC-362932A1.pdf

3. **Interviews with relevant stakeholders:** ComReg and Europe Economics conducted interviews with businesses and public sector bodies that had particular insight into the harm caused by nuisance communications and to the provision of critical services (e.g., Ireland's key retail banks, An Post, the HSE, and An Garda Síochána).
4. **Europe Economics estimates of the harms:** Europe Economics designed a bespoke empirical model to estimate all quantifiable harms. This model used as inputs data from both the consumer and business surveys, key stakeholder interviews, and desk-based research.
5. **Econometric research on scam victims:** ComReg has conducted research into the demographic determinants of scam victimhood and payments using the consumer survey data, contained in Annex 2.
6. **Analysis of media reports of scam calls and texts:** ComReg monitors print and online media to identify the scams targeting Irish consumers.

6.21 The remainder of this Section is laid out as follows:

A) Provides an overview of the key findings in relation to the different types of scams in Ireland, the consumers targeted, and businesses impersonated by scammers, and the risk posed by AI powered scams.

B) Provides a summary of the approach used by Europe Economics to estimate the various harms, including some updated information since the publication of Consultation 23/52.

C) Estimates the harm to consumers, businesses and other bodies (e.g., public bodies and operators etc) respectively, including some updated information since the publication of Consultation 23/52.

D) Summaries the overall estimated harm to Irish society.

A) Overview of key findings on scam texts and fraud in Ireland

6.22 The key findings are grouped as follows:

i. The prevalence of scam calls and texts.
ii. The increase in scam calls and texts.
iii. The organisations being impersonated by scammers.

iv. The impact of scams on recorded fraud

v. The consumers most susceptible to scams.

vi. The future of scams - AI powered scams

i. The prevalence of scam calls and texts.

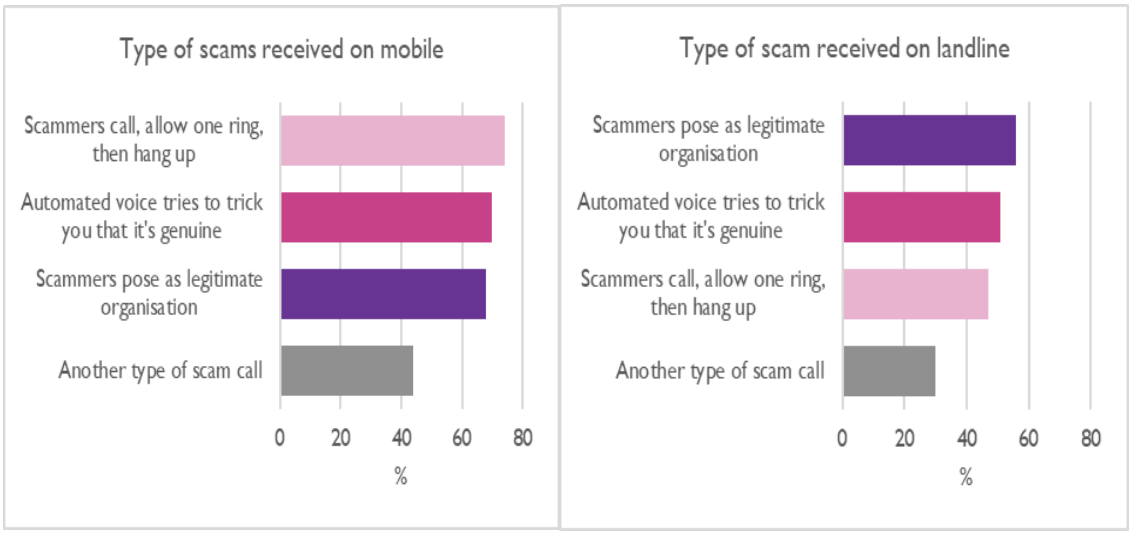
Scam calls.

6.23 The B&A Consumer Survey investigated the prevalence and type of scams that consumers have encountered. There is a high prevalence of scam calls in Ireland with approximately 91% and 74% of Irish mobile and landline consumers having received scam calls in 2022[196]. This implies that 3.5 million Irish consumers[197] have received 59 million scam calls[198] (18 scam calls per subscriber a year). This points to an average of approximately **161,000 scam calls being received each and every day.**

6.24 The B&A Consumer Survey shows a variety of different scams across mobile and landline platforms. The most prevalent types of scams are Wangiri calls (one ring and hang up), automated voice calls, and calls posing as a legitimate organisation. While Wangiri calls appear most often, there is a high prevalence of other types of scams across both mobile and fixed platforms, demonstrating that fraudsters rely on multiple scam types in parallel rather than any one particular scam type at any one time; indeed a scam can involve the interplay of different approaches (for example a mixture of vishing and smishing) in order to dupe the unsuspecting consumer.

[196] B&A Consumer Survey, Slide 14.
[197] Europe Economics Report, page 103.
[198] Europe Economics Report, page 37.

Figure 6: Types of scam calls received by mobile and landline users

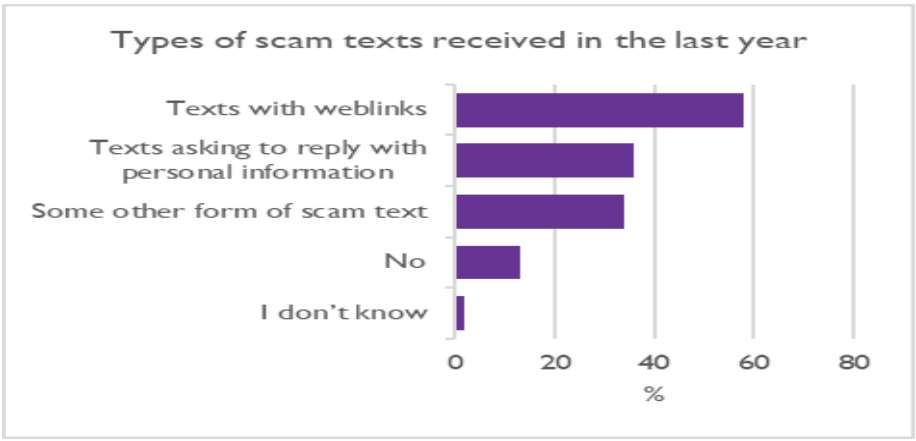


Source: Europe Economics analysis of consumer survey data

Scam texts.

6.25 Approximately 84% of Irish consumers report having received any type of scam text in 2022[199]. On average, Irish consumers received at least 15 scam texts a year. This implies that 3.2 million Irish consumers[200] received over 47 million scam SMS messages in 2022 alone[201]. As shown in Figure 7 below, most scam texts include a hyperlink and are the most prevalent means of scamming customers. This equates to an average of **approximately 129,000 scam texts being received each and every day.**

Figure 7: Types of scam texts received by mobile users



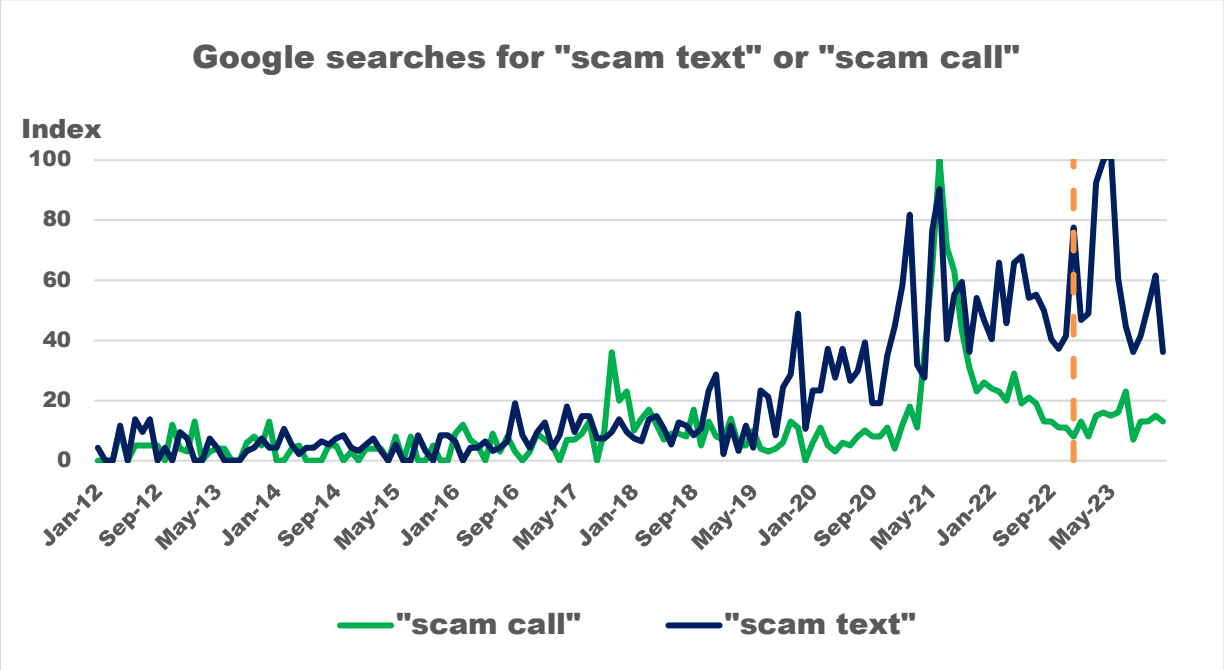
Source: Europe Economics analysis of consumer survey data.

[199] B&A Consumer Survey, Slide 21.
[200] Europe Economics Report, page 103.
[201] Europe Economics Report, page 38.

ii. increased concern in relation to scam calls and texts.

6.26 In Consultation 23/52 ComReg noted that while there was limited data on the number of scams, over time, consumers' online behaviour indicated an increased concern with scam calls and texts since 2021. It appears that this concern has not abated since then as the relative frequency of searches for "scam texts" or "scam calls" indicates that the number of SMS and Voice scams experienced by Irish consumers remains elevated, as shown by Figure 8 below. This highlights the need for constant vigilance given the inherent fluctuations of scam waves – any lull in scams may be followed by a spike.

Figure 8: Relative frequency of Google searches for scam calls or texts in Ireland, 2012-2023



Source: ComReg analysis of data from Google Trends[202]. Vertical dashed line indicates the end of the period examined in Consultation 23/52.

iii. The organisations being impersonated by scammers.

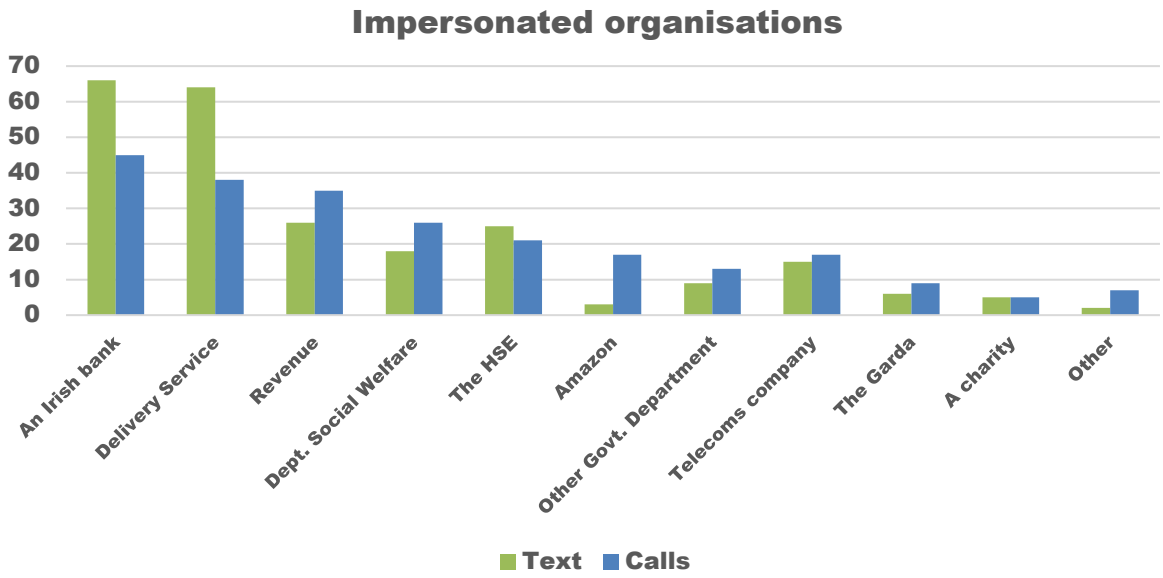
6.27 Scams involve impersonation of a trusted organisation or individual, with the majority of recipients of scam calls (74%) and texts (89%) having received scams impersonating a legitimate organisation[203].

6.28 Recipients of scams involving impersonation most commonly report having received scams from Irish banks, delivery service providers and government agencies (Revenue, Dept. of Social Welfare, HSE) as shown in Figure 9.

[202] Google Trends is a website by Google that provides data on the popularity of top search queries in Google Search across various regions and languages.
[203] ComReg analysis of B&A Consumer Survey data.

While there is a considerable overlap between the types of business and organisations impersonated by scam calls and texts, fraudsters are more likely to impersonate government agencies using calls, and banks and delivery service companies using SMS.

Figure 9: Reporting of different organisations by recipients of scams involving impersonation.



Source: Consumer Survey Q.27b (n=911) & Q.10b

6.29 Overall, over half of Irish consumers report receiving a scam call or text impersonating a government department, with this rising to up to seven in ten if the government owned An Post is included. This indicates that as many as 2.5 million Irish people may have received a scam call or SMS impersonating a government agency. This is of particular concern because voice and SMS provides ubiquitous reach for State agencies contacting consumers about important public services (i.e., voice and SMS are included as a default service on each and every mobile phone in the country).

6.30 ComReg staff have also been actively monitoring print, broadcast, online and social media to remain informed of to the latest scams in Ireland. ComReg includes a list of scams[204] identified in Table 3 below. Again, this demonstrates that fraudsters rely on multiple different types of scams, many operating in parallel. Moreover, fraudsters have developed new scams over time. In particular:

[204] This is not intended as an exhaustive list of media mentions, merely a list of mentions of distinct waves of scams that appear to use SMS or Voice. It should be noted that no scam forwarding service (e.g., texting 7726" Is in use in the UK and Canada) exists at present in Ireland.

- Delivery services, Revenue and the Department of social welfare were the most impersonated in-early 2020 at the beginning of the Covid-19 lockdown;
- The HSE and retail banks were impersonated throughout 2020 and 2021, with more agencies being targeted in 2022 (an Garda Síochána, Credit unions); and
- Fraudsters have now moved onto targeting users of other number-based platforms (e.g., Revolut, WhatsApp) and smaller companies (e.g., eFlow, Credit Unions, recruitment agencies, household waste companies) in 2022 and 2023.
- Additionally, and perhaps contrary to popular belief, many scams originate in Ireland. For example, in 2023 alone:
    - In Waterford, Gardaí arrested 9 men as part of an investigation involving Money Laundering and Smishing (Fraudulent SMS/WhatsApp Messages) nationally and internationally.[205]
    - In Kildare, Gardaí arrested a man accused of taking part in a smishing scam.[206]

Table 3: Selection of scam waves, January 2020 - February 2024

[205] Nine men arrested in Waterford involving Money Laundering and Smishing scams | WLRFM.com
[206] https://www.leinsterleader.ie/news/home/1424195/kildare-over-8-000-taken-from-two-accounts-in-text-smishing-scam-claim.html

Year	Month	Body Impersonated	Scam
2020	January	Amazon	Prime Scam (Wave 1)
	March	DSP	PUP SMS scam
		An Post	Delivery scam
	April	Netflix	Netflix Scam
	May	Revenue	Revenue Tax Refund
	July	DSP	PUP SMS scam
	June	DSP	Welfare SMS (Wave 1)
		Revenue	Revenue SMS (Wave 1)
	July	HSE	Contact Tracing SMS
		Revenue	Revenue Tax Refund
		AIB	AIB Smishing (ATM card)
	August	BOI	BOI Smishing
		DSP	Welfare SMS (Wave 2)
	December	Customs	Customs SMS
		An Post	Delivery SMS
		Revenue	Revenue SMS (Wave 2)
2021	January	Customs	Customs SMS
		HSE	Vaccine appt. SMS scam
		DSP	PUP SMS scam
		KBC	KBC Fraud services scam
	March	Gardaí	Gardai Confidential Line Spoofing
	April	DSP	DSP Hotline
			Welfare SMS (Wave 3)
		FluBot	FluBot (Delivery Scam)
		Amazon	Prime Scam (Wave 2)
		Gardaí	Imminent Arrest Scam
		Customs	Customs SMS
		HSE	Covid Test SMS
	May	HSE	HSE Cyber Attack
			Medical appt. scam
	June	FluBot	FluBot (Delivery Scam)
	July	Gardaí/DSP	Imminent arrest SMS
			Compromised PPS SMS
		PTSB	PTSB Smishing
		DSP	"Neighbour spoofing" Calls
		HSE	Vaccine appt. SMS scam
	August	Eir	Eir broadband fix
		KBC/Ulster	KBC/Ulster Bank exit
	October	HSE	HSE Cyber Attack
		The Courts of Justice	Taxes owed, call from Courts
2022	March	Banks	Crypto scam
		P2P via WhatsApp	"Hi Mam" WhatsApp scam
	April	AIB	Taxi scam (ATM card)
		Revolut & AIB	Smishing scam
	May	Various	Money laundering
	July	BOI	BOI Smishing and Phishing
	August	BPFI	Bank Smishing
		P2P via WhatsApp	Irish language romance scam
		An Post	Delivery SMS
	September	P2P via WhatsApp	Investment scams
	October	Banks/Gardaí	Money mules
	November	BOI	Combined call and text scam
		P2P via WhatsApp	"Wrong number" scam
	December	P2P via WhatsApp	'Hi Mum' WhatsApp scam (Wave 2)
		Amazon	Amazon Phishing
2023	January	P2P via WhatsApp	Blackmail (intimate photos)
		Revolut	Revolut phishing scam
		Revolut & AIB	Revolut vishing
		Revolut	Revolut Smishing
	February	Various credit unions	Credit Union Phishing Scam
		eFlow	M50 toll payment
		DECC & ESB	Electricity benefit
		PTSB	PTSB Smishing (Wave 2)
	March	P2P	Grandparent Scam
		Recruitment agencies	Hays Recruitment scam
		P2P via WhatsApp	Family emergency
		Garda (GNECB)	Garda calling in relation to fraud
		P2P via WhatsApp	Account takeover via 2FA SMS to target users contacts
		Criminal Court of Justice	Tax owed to courts
		Department of Justice	Call from Immigration Service Delivery
	April	eFlow	Motorway Toll Payment SMS
		Sky	Sky Account Scam Text
		Department of Justice	Immigration Services Call
		Santander	Santander Fraud Department Scam Call
		Eir	"Quick Support" App Download Scam Call
		P2P	"Hi Mam" Scam Text
		Gardaí (GNECB and FIU)	Calls
		Bank	Personal Details Confirmation SMS Scam

	May	P2P	"Hi Dad" SMS
	June	P2P	"Wrong Number" SMS scam
		HSE	SMS Scam
		Electric Ireland & Revolut	Fraudulent Activity Scam Call
		Family Member	Voice Cloning Call
		Irish Life Investment Managers	Investment Opportunities Scam Call
	July	Revenue	Tax Credits SMS Scam
		Missed Caller	One Ring Call
	August	DPD	As Gaeilge SMS
		DHL	Delivery Charge SMS
		P2P	Grandparent SMS Scam
		Irish Phone Number	Compromised PPS Number Scam Call
		Credit Union	SMS scam
	September	Bank of Ireland	"Live Chat" Scam Call
		County Council	Rent In Arrears Scam Call
		CFO	Smishing Scam
	October	Gov.ie	Energy Support Scheme Credit Scam
		An Post	Delivery Charge SMS
	November	Amazon	Scam Call
		An Post	Scam Call
		Irish Phone Number	Caller ID Spoofing- Cryptocurrency Scam Call
		Phone Providers	SMS Scam
	December	DPD	SMS Scam
		Bank of Ireland	Cloning Scam Call
2024	January	Bank of Ireland	Compromised Account Scam Call & SMS
		An Post	Account Details Scam Call
		Department of Justice	Call from Immigration Service Delivery
	February	Gardai	Fine Scam SMS
		P2P	Romance Scams
		Department of Justice	Call from the "Immigration Bureau"
	March	Revolut	Suspicious Transaction Scam Call
		Panda	Smishing
		Delivery service	Delivery scam text
		AIB	Call & SMS scams

6.31 ComReg staff also track international reporting on scams because many scams that originate abroad, particularly in the Anglosphere, will inevitably be copied by fraudsters targeting or operating in Ireland. For example, the recent wave of road tolling scams via text message first began in Australia in the summer of 2022 and had moved to Ireland by the Spring of 2023. Similarly, the Hays recruitment scam was initially focussed on Hays Australian branch in January 2023 before spreading to both the UK and Ireland in March.[207]

6.32 This should not be surprising given that many scam calls and texts require the scammers to be able to create conversation in real time. There has also been a number of cases recently where scam operations were raided, and information on their operations were made public. As recently as February, there were reports that police raids[208] in the Indian cities of Patna, Kharagpur and Kolkata on scam call centres, the consequence of an initial complaint from Dungarvan, Co. Waterford. Importantly, these scammers targeted both the UK and Ireland.

6.33 Scammers continue to emerge abroad and ComReg expects that variants of scams emerging abroad will eventually target Ireland or be copied by Irish scammers (e.g., the latest scam text in Australia which began in February 2024, involves scammers posing as a bank to issue a fake "security alert",

[207] Recruitment Scam Alert | Hays
[208] ED busts cyber scam in India on Irish complaint | India News - Times of India (indiatimes.com)

which includes a link which asks customers to secure their account[209]).

iv. The impact of scams on recorded fraud

6.34 The continued prevalence of scam calls and texts has unsurprisingly fuelled a rise in the rate of fraud, as illustrated by annual data on fraud published by the CSO. While the data does not solely relate to fraud conducted via scam calls or texts, the CSO noted that the 90% year-on-year increase in 2021 was "*largely driven by unauthorised transactions and attempts to obtain personal or banking information online or by phone*."[210]

6.35 While reported annual fraud has declined in 2023, An Garda Síochána report that reported offences of "*Phishing/Vishing/Smishing Fraud*" have in fact increased by 20% in the same period (see Figure 10 below)[211]. In January 2024, An Garda Síochána reported that the increase in scam texts specifically was even greater: "*Our Garda National Economic Crime Bureau … recorded an over 30% increase in the number of reports received by Gardaí from victims of fraudulent texts in 2023.*[212]" As noted by Detective Chief Supt. Pat Lordan of the GNECB: *"If we can shut down the text messaging and the voice messaging… it really is the lifeblood, the embryo, that sows the seeds for all these types of crime.""*[213]

Figure 10: An Garda Síochána press release, December 2023

Source: An Garda Síochána

[209] Scams in Australia in pictures: CBA warns of new 'security alert' con (9news.com.au)
[210] Please see the CSO's statistical release on crime in Ireland "Recorded Crime Q1 2022" accessible here
[211] An Garda Síochána press release An Garda Síochána remind the public to be suspicious of texts/calls asking for personal data - Garda
[212] An Garda Síochána post on Linkedin, 24 January 2024. ComReg notes that the absolute figures reported to An Garda Síochána comprise only a share of total scam victims and losses, given that many victims do not report scams.
[213] Independent.ie, 18 June 2023 "*War against phone fraud: Top garda warns mobile networks to tackle pandemic of scam texts and calls*" Link

v. The consumers most susceptible to scams

6.36 ComReg has conducted an econometric analysis of the B&A Consumer Survey data[214] in order to better understand the people most susceptible to financial fraud. ComReg has found that younger consumers, in particular those under 25, are much more likely to report having been scammed in 2022.[215] In particular, respondents between the ages of 16-25 and 26-35, were far more likely (14 and 3 times respectively) to report having lost money as a result of a scam call or text, relative to older users.

6.37 This aligns with other recent research that shows that while all age groups suffer financial losses, it is younger people who are disproportionately impacted by these losses. For example:

a) Recent Research by Permanent TSB found that victims are more likely to be young (under 45, particularly Millennials) living in Dublin or urban areas.[216]

b) In the UK, younger people were significantly more likely to be victims of fraud with those aged 20 to 39 accounting for 39% of all reports to Action Fraud.

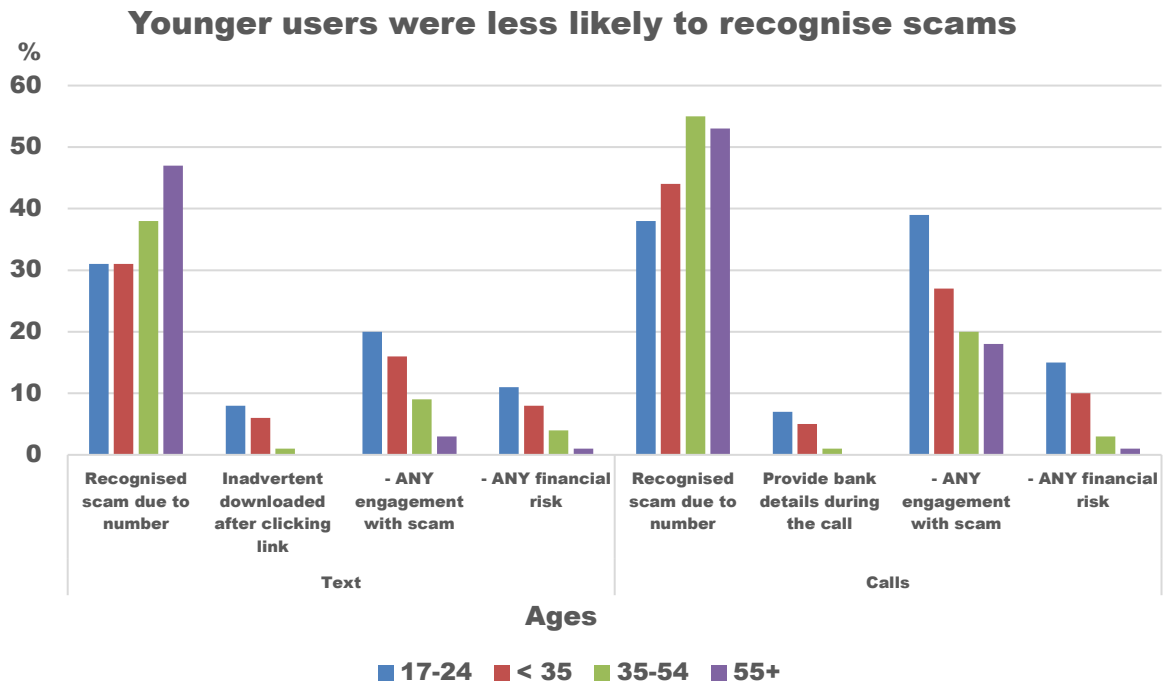
c) Recent research by Barclays bank found that 21–30-year-olds being fifteen times more likely to be a victim compared with those aged over 70.[217]

6.38 This does not appear to result from fraudsters specifically targeting younger consumers. Rather, that this cohort is more likely to fall for a scam, potentially as younger consumers make greater use of mobile payments and online purchases. Indeed, the Barclays research provides some insight into the reasons that make young people more susceptible to scams. Around 40% of this cohort reveal they rarely read Terms & Conditions, and a third admit to shopping with a brand they have not heard of if they appear to be offering a good deal. This finding is supported by evidence regarding consumer behaviour following receipt of a scam, shown in Figure 11 below, which shows that younger consumers were less likely to recognise scams.

[214] Econometrics is an application of statistical methods to economic data in order to give empirical content to economic relationships. In short, econometric techniques can be used to examine the correlation between two variables, controlling for other variables.
[215] In particular respondents between the ages of 16-25 and 26-35, were 14 and 3 times more likely to report having lost money as a result of a scam call or text, relative to older users.
[216] PermanentTSB.ie 23 November 2023 "*Reflecting Ireland: An insight into consumer behavioural change in Ireland – Fraud*" Link
[217] Barclays 14 June 2022 "*Young people warned to be vigilant this summer as Barclays data reveals 21-30 year olds are most at risk of scams*" Link

6.39 However, as noted below, older people are more likely to be concerned or very concerned about scam texts (81%)[218] and therefore are more likely to be victims of emotional and mental distress even if they do not suffer a direct financial loss.

Figure 11: Scam recipients' reactions to scam calls and texts, by age



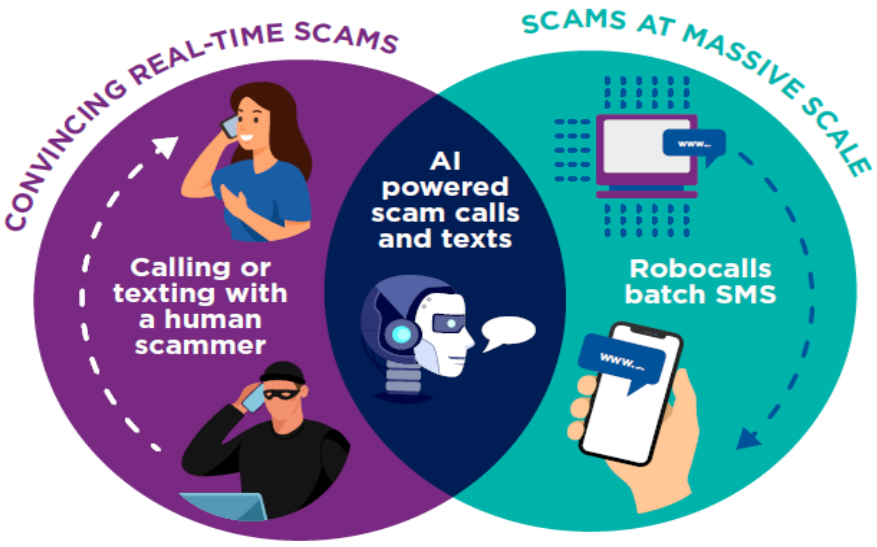
Source: B&A Consumer survey, Questions 28 & 11[219]. The percentages above are for users that received a scam call or text (applies to t160 of the total sample of 176 (c.90%)).

vi. The future of scams: AI powered scams

6.40 Concerningly, emerging evidence indicates that some fraudsters are using advanced AI based software to perpetuate scams. AI based scams could combine the relative strengths of human and automated scams (e.g., robocalls); being able to both generate convincing speech or text in real time and perpetuate such scams at a massive scale (given the reduced need for personnel)[220]. Alternatively, such scams could be highly targeted (given their increased effectiveness) and thereby avoid the usual suspicious patterns of call origination, making detection even more difficult.

[218] B&A Consumer Survey, slide 13.
[219] Q.28 When you received scam texts on your mobile phone in the past year, did you do any of the following? Q6a/Q6b Yes
[220] For example, robocalls can reach many consumers but rely on recorded messages, whereas scam callers are more convincing but can only make one call at a time.

Figure 12: The unique harm from AI based scams.



6.41 In that light, we note that there are growing reports of the following:

a) AI based voice-mimicry software is being used to imitate the voice of business associates or even family members in distress[221] as well as to commit identity fraud[222]. Recent cases in Australia, the USA, and Canada would suggest that similar scam calls may soon arrive in Ireland. A large share of Irish consumers could be targets for impersonation by voice-mimicry software, given the ubiquity of video content publicly available on social media.

b) AI based chatbots, such as ChatGPT, enabling fraudsters to automate instant messaging apps that conduct convincing conversations in real-time via text or email, at massive scale[223]. Indeed, this risk was recently highlighted by Europol in a report titled "*ChatGPT: The impact of Large Language Models on Law Enforcement*"" published in in March 2023:

"ChatGPT's ability to draft highly authentic texts on the basis of a user prompt makes it an extremely useful tool for phishing purposes. Where many basic phishing scams were previously more easily detectable due to

[221] For example, see Business Insider 6th March 2023 "A couple in Canada were reportedly scammed out of $21,000 after getting a call from an AI-generated voice pretending to be their son" Link and Dailymail.co.uk 31 March 2023 "Scammers cloned VOICE of Houston man with AI and conned his parents out of $5K by claiming he'd been in car accident - mom forced to postpone cancer treatment as a result" Link

[222] For example, the Guardian "AI can fool voice recognition used to verify identity by Centrelink and Australian tax office" 16th March 2023 Link

[223] See for example The Strait Times online 12th March 2023 "*Broken English no longer a sign of scams as crooks tap AI bots like ChatGPT: Experts*" and 14th March 2023 ABC7 news online "*Thieves can use ChatGPT to write convincing scam messages with human-like language, experts warn*".

> *obvious grammatical and spelling mistakes, it is now possible to impersonate an organisation or individual in a highly realistic manner even with only a basic grasp of the English language…..ChatGPT may therefore offer criminals new opportunities, especially for crimes involving social engineering, given its abilities to respond to messages in context and adopt a specific writing style…*
>
> *To date, these types of deceptive communications have been something criminals would have to produce on their own. In the case of mass-produced campaigns, targets of these types of crime would often be able to identify the inauthentic nature of a message due to obvious spelling or grammar mistakes or its vague or inaccurate content.* ***With the help of LLMs, these types of phishing and online fraud can be created faster, much more authentically, and at significantly increased scale***."[224]

6.42 Next-generation AI-based scam calls and texts should be expected to reach Ireland and increase with time as the underlying technology becomes more widely available (e.g., software like ChatGPT from OpenAI for text generation, or like VoiceLab from Elevenlabs for voice cloning). Regulating or even banning[225] AI-based software and applications alone cannot be expected to mitigate the risk of AI-based software being used to scam Irish or indeed European consumers while the cost of developing such software has declined rapidly in recent years[226]. In the face of barriers to development in certain jurisdictions, development of AI-based software will likely shift to more permissive jurisdictions. Fraudsters should be expected to deploy such software in the EU regardless of the legality and even train their own models on datasets of past scams and illustrative scripts.

6.43 Scammers have quickly integrated AI into their operations, with 'deepfakes', being used to perpetuate scams, which rely on both image and voice cloning. These typically use well known politicians, businesspeople or celebrities to convince potential victims of the authenticity of their offers and are often broadcast via online or social media channels[227]. Such figures are prime targets for impersonation being well known to many and having a significant volume of video content to train text, voice and image models to produce compelling voice clones or deepfakes. Impersonating such figures has proven useful to scammers attempting to present the same scam to a large number of people, typically via broadcast such as adverts on online channels (e.g., YouTube).

[224] Europol (2023) "ChatGPT - The impact of Large Language Models on Law Enforcement" Link
[225] BBC News 1 April 2023 "ChatGPT banned in Italy over privacy concerns" Link
[226] ARK Investment Management LLC, 2023 "BIG IDEAS 2023" Link
[227] NBC News "*Deepfake scams have arrived: Fake videos spread on Facebook, TikTok and Youtube*" Link

6.44 Next generation, AI based scams seem likely to rely on content gathered from social media to fuel scams. As the power of AI-based generative models improve and scammers learn and adapt to them, scammers may be able to generate compelling voice or video cloning with less and less data. Fraudsters may then use video content or posts from social media to imitate the voice, speech and/or image of an individual in real time[228]. Once scammers are able to impersonate and clone the voice and image of more typical people, who may have limited video content online, this will pose a real risk to normal telephony users.

6.45 In Europe alone, tens of millions of users could be targets for impersonation, given the widespread use of social media – exposing a far higher number of friends and family to being potential victims. This could enable a wave of personalised scams, especially if combined with personal information and/or contacts from data leaks[229]. Indeed, since ComReg first flagged this in Consultation 23/52 reports have already begun emerging of scammers cloning the voice of figures of authority in relatively small organisations[230] or impersonating a family member in distress [231] to demand payment.

6.46 ComReg also observed that such scams could be even more convincing when combined with CLI Spoofing (e.g., using a company's number and mimicking the voice of staff) and reports have emerged of voice cloning being combined with CLI Spoofing, to make spam calls where the target not only hears the voice of the impersonated caller, but also sees their number displayed on their device[232].

6.47 This aligns with recent research from PWC (December 2023) which highlighted six ways that AI could be used to perpetrate fraud and scams.

- Generating text and Image Content;
- AI enabled chatbots;
- Deep fake videos;
- Voice cloning scams and voice ID;
- Sophisticated targeting of victims; and

[228] CBC News "*How scammers likely used artificial intelligence to con Newfoundland seniors out of $200K*" Link
[229] Business Insider 03.04.2024 "*533 million Facebook users' phone numbers and personal data have been leaked online*" Link
[230] Irish Mirror Online 25.02.2024 "*Nuns scammed out of thousands of euros by AI bishops*", Link South China Morning Post 04.02.2024 "'*Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting*" Link
[231] Financial Times 19.01.2024 "*AI heralds the next generation of financial scam*" Link
[232] Business Insider, 22 January 2024 "A robocall impersonating Joe Biden telling voters to stay home is the dawn of a devastating new era for phone spam: 'We knew this day would happen, and now it's here'" Link

- Pressure testing.

6.48 While there is evidence of AI already being use for scams, the extent of its reach was currently limited to certain areas and sectors. However, the PWC research observed that it was only a matter of time before fraudsters adopt AI for fraud and scams at scale. Importantly, this research also clearly identified the role of AI in combatting these same scams. In particular, it highlighted the role of telecom operators in making use of machine learning as part of network filtering to identify and remove malicious content.[233]

B) Identifying and estimating the harm from scam calls and texts

6.49 Europe Economics' approach to estimating the harms from scam calls and texts combines evidence from public data sources, stakeholder interviews and results from the B&A Consumer and Business Surveys with extrapolation to the relevant Irish population and business demographics. Europe Economics has deployed three approaches to estimating harms.

I. **Bottom-up cost modelling** which involves estimating the harm to a stakeholder group by summing up all individually estimated harms, derived from the surveys including losses from fraud, the monetary value of time spent resolving scams; or the monetary value of time spent engaging with scam calls or texts.

II. **Willingness-to-Pay (WTP)** calculations which estimate the harm to a stakeholder group (in the Consumer or Business survey) by asking the group how much they would be willing to pay to avoid all scams. Three complementary categories of WTP questions were asked in order to provide added robustness to the estimates and avoid the double counting of harms. The WTP values are then extrapolated to the business and consumer population using CSO consumer and business demographic data.

III. **Case studies** provide examples of harm that were not captured above given their bespoke nature. Europe Economics presents several case studies of harms caused to public bodies, particularly those that rely on calls and texts to deliver important public services.

6.50 For the purpose of this section, ComReg presents the final estimates or range of estimates provided by Europe Economics with the more detailed analyses contained within the Europe Economics Report. Although Europe Economics has endeavoured to gather as much information as possible, it will be apparent to the reader that some harms are inescapably difficult to estimate

[233] Impact of Artificial Intelligence on Fraud and Scams (pwc.co.uk)

with any reasonable margin of certainty, given the data available or lack of certainty regarding future market trends. Therefore, Europe Economics estimates of harm are necessarily conservative estimates because many harms are not quantifiable (but may still occur).

6.51 For further information on the methodologies deployed by Europe Economics, please see the Appendices to the Europe Economics Report.

6.52 Respondents to Consultation 23/52 raised no issues in relation to the methodology used by Europe Economics.

C) Harm to stakeholders.

6.53 ComReg first assesses the harm to consumers before assessing harm to businesses (including public services) and the operators themselves.

Harm to Irish consumers.

6.54 ComReg assesses the impact of scams on Irish consumers under the following headings.

i. Financial losses from fraud; and

ii. Emotional harm and wasted time (which could have been used more productively).

i. Financial losses from fraud

6.55 The majority of scams do not succeed, and the vast majority of recipients of scam calls or texts will not be defrauded. Rather the approach taken by scammers is to spread the net wide with the objective of catching a few, because even a few is sufficiently lucrative to make the effort worthwhile. Consequently, and although borne by only a small share of consumers[234], financial losses are the largest and most evident harm suffered by consumers. It is estimated that there were approximately 365,000 cases of direct financial losses in Ireland in the 12 months to June 2023, with 175,000 people defrauded after receiving scam calls and 190,000 people defrauded after receiving a scam text[235]. This equates to an average of approximately 1,000 cases of fraud each day because of scam calls and SMS texts.

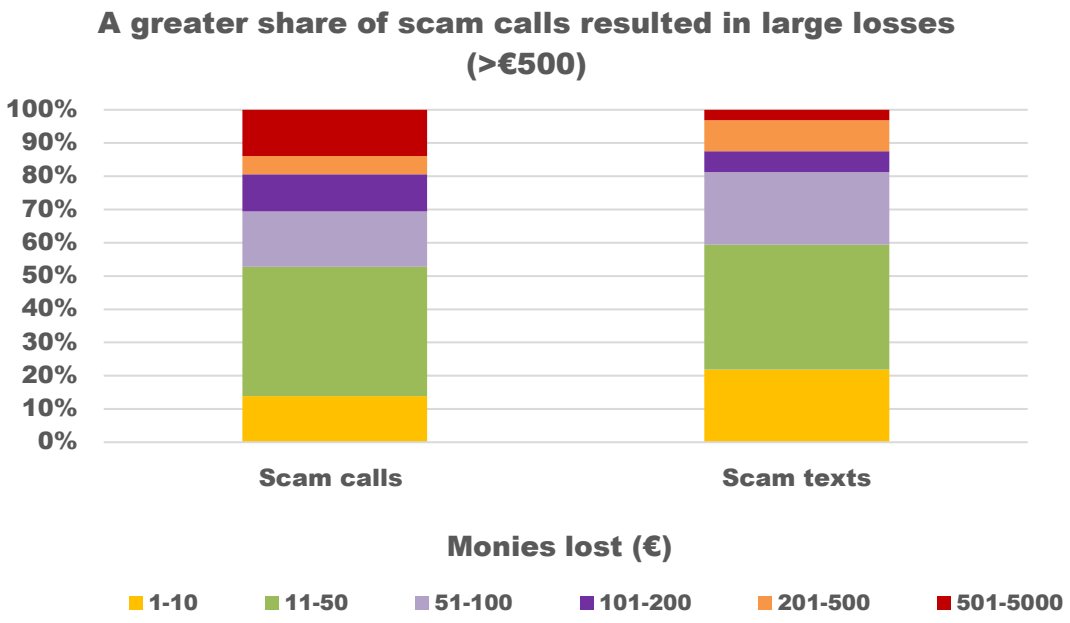
6.56 The losses observed in the consumer survey range from €5 to €5,000 with scam calls accounting for a higher share of large scams (e.g., >€500). This broad range is to be expected given how the amount defrauded varies

[234] However, scams also affect other groups, with young consumers under 25 years of age more likely to experience financial loss as a result of a scam call or text.
[235] Europe Economics Report, Page 5

significantly across individual instances of fraud (e.g., subscription scams, one-off payment, emptying a current account[236]). Notably, the median loss is around €50 for both scam calls and texts, while the average is somewhat higher for scam calls than texts, from €230 to €490 respectively. This aligns with other research which shows that most (but not all) fraud attempts typically involve amounts in the low to mid hundreds of euros, for example:

- Permanent TSB found that people are more likely to experience fraud attempts seeking to take less than €500.[237]
- European Commission research also shows that the magnitude of financial losses varied markedly and depending on the type of fraud experienced, with 46% for amounts less than €50 and around 85% for amounts less than €500.[238]

Figure 13: Shares of scam calls and texts, by monies lost.



Source: ComReg analysis of B&A Consumer Survey data. This excludes the approximately one in three victims that could not recall the amount lost.

6.57 Of course, the financial status of the victims varies greatly, and for some, even these smaller sums of money can have devastating impacts. For example, CSO data shows that 20% of households are now short of money to cover

[236] Numerous media accounts indicate a high prevalence of direct payments or account takeover. Although less well covered by media reports, there is evidence that many fraudsters attempt to sign consumers up to subscription payments. This may be desirable from the perspective of a fraudster as such payments are less likely to arouse suspicion and accrue over time.
[237] Permanent TSB "Under 45s more likely than older people to fall victim to financial fraud, according to Permanent TSB's latest Reflecting Ireland consumer research" Published on 23 November 2022 Link
[238] European Commission, 2020, Survey on "Scams and Fraud experienced by Consumers" Link

their expenses every month.[239] Amounts of €100 or less could be highly detrimental in such cases. Further, younger people (15 – 29) who are most impacted by fraud have the lowest average incomes.[240] This aligns with recent European Commission research[241] which showed that the financially vulnerable might be particularly at risk. The survey illustrates that the probability of experiencing a financial loss due to a scam or fraud (amongst those who experienced such a fraud) is 12 percentage points higher for someone in a financially difficult situation compared to someone whose financial situation is more straightforward. Recent research by Ofcom regarding online scams found that while one in five suffered a loss of greater than €1,000, losses below €100 were more frequent (42%)[242].

6.58 However, large financial losses also occur, with thousands of people likely to have been defrauded for amounts of over €1,000 through scam calls and texts. These are significant amounts regardless of individual income levels and can wipe out life savings in some cases.

Quantified financial loss.

6.59 In total, Europe Economics estimates that Irish consumers suffered financial losses of €109 million to scam calls and texts (with €75 million from calls and €35 million from texts).[243]

Table 4: Europe Economics estimates of consumer harm from fraud (€ million)

Scam type	Gross Loss	Net loss	Cost of resolution	Total
Scam Calls	86	75	0.8	76
Scam Texts	44	35	0.2	35
Total	130	109	1	111

Source: Europe Economics analysis. Numbers may not sum due to rounding.

Comparison to previous estimates of fraud

6.60 The estimate of approximately 365,000 victims of fraud significantly exceeds other estimates of reported fraudulent crime by a considerable amount. For example, the CSO Recorded Crime shows that there were approximately 12,000 Fraud, Deception & Related offences recorded on An Garda

[239] CSO "Pulse Survey: Our Lives, Our Money - October to November 2022" Link
[240] CSO "Earnings Analysis using Administrative Data Sources 2020" Link
[241] European Commission,2020,Survey on "Scams and Fraud experienced by Consumers", page 45.
[242] Yonder "Online Scams & Fraud Research 2022 Executive Summary Report" page 19.
[243] The total amount lost by consumers is lower because victims recover some of the monies lost. This depends on the specific circumstances of the scam and the actions taken by the consumer. Once this and the value of time lost to such actions is included the total financial loss is €109m.

Síochána's PULSE database in the year 2022[244]. However, this is to be expected as the B&A Consumer Survey is the first attempt to survey a representative sample of the Irish population to estimate the prevalence of scam calls and texts. Long standing evidence suggests that scams of this type are severely underreported to police authorities.[245]

6.61 We can see this ably demonstrated in the UK where Office of National Statistics ("ONS") measures the prevalence of crime based on a survey (not dissimilar to ComReg's) and can be compared to actual reported offences. Indeed, the ONS note that the survey is the most reliable indicator for the more common types of crime experienced by the general population. The ONS report around 3.2 million instances of fraud[246] - by contrast, Action Fraud (the UK public-facing national fraud and cybercrime reporting centre) reported 297,980 offences – i.e., 94% of such fraud are not reported.

6.62 This occurs for a multitude of reasons, including that consumers feel too embarrassed to report the crime, amounts taken are relatively small, or simply those defrauded do not know who to contact. As we have observed, the majority of cases are for amounts of less than €100 and victims may decide it is simply not worth reporting such cases.

ii. Wasted time and emotional harm.

6.63 The majority of recipients of scam calls or texts do not suffer any financial loss. However, the surveys show that there are other impacts that cause harm to consumers while also distorting the efficient and effective functioning of the numbering platform. Europe Economics estimates that between approximately 3.2 and 3.5 million consumers are at the very least inconvenienced by scam calls or texts (but do not suffer a direct financial loss).

6.64 Consumers have reported a variety of different non-financial harms. Prior to estimating the harm associated with this category, ComReg first describes the harm associated with wasted time and emotional harm.

Wasted time.

6.65 Scams waste time which otherwise could have been spent on activities that consumers value. As described by Europe Economics, consumers incur an

[244] An Garda Síochána records details of crime incidents on a central database (PULSE). This facilitates the categorisation of crime into various Incident Categories and Types. Crime figures generated from PULSE are used within An Garda Síochána as management information and play an important part in operational and strategic decision-making. The data recorded are also used by a wide variety of organisations that have an interest in specific or general aspects of crime. See Crime Reporting Document (garda.ie)

[245] The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable; Routledge, December 2020

[246] Crime in England and Wales - Office for National Statistics (ons.gov.uk)

opportunity cost when they receive and engage with scam calls and texts as these actions consume time and resources that could otherwise be allocated to other things. Scam calls and texts received during working hours take time out of a productive activity that, in aggregate, could be costly to the economy; while those received out of work hours takes away valuable leisure time. Europe Economics estimates indicate that consumers spent around 2 million[247] hours dealing with scam calls in 2022.

Emotional harm.

6.66 Falling victim to scams and fraud can have significant negative impacts on mental health and wellbeing, with victims typically reporting significantly higher levels of anxiety and lower levels of happiness as a consequence. Long standing research[248] shows the additional hidden harms that victims of financial fraud face and these can have a steep emotional toll. Successful scams can be traumatic for their victims, in particular following the loss of a substantial sum of their monies. This can be seen in the experience of one Irish man after losing an unspecified amount:

> "*Just sat there staring at my life savings account which had been absolutely drained…. Went home. Sat down on the couch. Looked at my account again. Called the family. Fighting back the tears*"[249].

6.67 Furthermore, research[250] [251] [252] shows that scams can impact the health and well-being of individuals, irrespective of whether they have experienced a financial loss or not. Constant scam attempts can increase stress levels and harmfully impact people's mental health which is even more insidious when the fraudsters target those most vulnerable who are often older, lonely and/or managing an illness. It is therefore unsurprising that 70% of Irish consumers reported being concerned about either texts or calls[253]. Given the large volume of such calls and texts, and their negative toll on consumers, the overall emotional burden is likely to be high.

---

[247] Europe Economics Report page 106 – 3.49 million users, receiving 17 scam calls on average, which last 2 minutes on average.
[248] For full discussion, See Chapter 4, Button, M and Cassandra, C,' The impact of fraud upon victims, 2017, Routledge.
[249] Irishmirror.ie 30 August 2023 "*Irishman 'fighting back tears' warns others after latest AIB scam 'raided' life savings*" Link
[250] After reviewing 16 research papers and datasets from across the world and from UK police, Which? UK found victims suffer personal harm from fraud regardless of whether they lost money or were reimbursed.
Devastating emotional impact of online scams must force government action - Which? News
[251] Bailey, J (2021) et al showed that scams impact individuals in terms of health and well-being, irrespective of whether they have experienced financial loss, and trigger implementation of strategies intended to avoid being defrauded. Older adults and "scams": evidence from the Mass Observation Archive Bailey, Jan; Taylor, Louise; Kingston, Paul; Watts, Geoffrey. The Journal of Adult Protection; Brighton Vol. 23, Iss. 1, (2021): 57-69
[252] Gordon and Buchannan (2013) observed that anxiety could be triggered independently of actually being defrauded; simply being aware scams exist may incite fear of being defrauded.
[253] B&A Consumer Survey, Slide 12

6.68 The B&A Consumer Survey demonstrates how harmful even unsuccessful scams can be to consumers. The majority of consumers that received a scam call (85%) or a scam text (81%) found such communications were an annoying inconvenience. More troublingly, nearly one in three (29%) found such communications were distressing. Europe Economics estimate that that there was a total of 89 million calls or texts that were annoying/irritating and 31 million scam calls or texts that were distressing in the last 12 months[254].

Quantified harm

6.69 Europe Economics estimates that the total inconvenience of scams (which would include both the value of time lost to calls and the emotional distress caused by scam texts)[255] at €62 million. The full methodology is outlined in Appendices of the Europe Economics Report.

Total consumer harm from scam calls and texts

6.70 The total estimated impacts[256] on consumer harm are summarised in Table 5 below – this consists of the sum of the financial loss and the costs of wasted time and emotional harm.

Table 5: Europe Economics estimates of consumer harm (€ million)[257]

Quantified Harm	Scam Calls	Scam Texts	Total
Financial Losses from fraud	75	35	109
Wasted time and emotional harm	41[258]	22	63
Total Harm	116	57	172

Figures may not sum due to rounding

Harm to Irish businesses.

6.71 Businesses may also suffer losses from a reduction in sales because of a degradation of consumer trust in SMS and Voice. The B&A Business Survey highlights the high degree to which businesses rely upon SMS and Voice for business to consumer ("B2C")[259] communications. This includes advertising and sales, and ComReg notes that:

[254] Europe Economics Report page 46.
[255] Using a bespoke backward-looking WTP model. See the Annex of the Europe Economics Report for further details.
[256] Other impacts not estimated include increased phone bills etc.
[257] Europe Economics Report page 49.
[258] As a robustness check Europe Economics separately estimated the value of lost time. Europe Economics estimated the cost of lost time to scam calls as €40 million using the estimated value of an hour produced by the Department of Transport combined with the time lost to scam calls. See Europe Economics Report page 106.
[259] B2C refers to communications between businesses or organisations and their actual or potential customers.

a) More than half of businesses (56 per cent) use mobile calls or texts for one part of their communication strategy;[260] and

b) Among these firms, on average 10 per cent of revenue was supported by telecommunications (e.g., calls or texts for reminders) in the past year.

6.72 Combining these statistics with the CSO data available on Irish business profiles, Europe Economics estimates that €48bn in revenue is supported by calls and texts, which is exposed to the impact of nuisance communications.[261]

6.73 The B&A Business Survey also found a small share of businesses believed they had lost some revenues as a result of scam calls and texts reducing consumers' confidence in their B2C communications, with over a third of businesses reporting having lost between 2.5%-5%. Based on this and CSO data on average business, Europe Economics note that business perceive a potential loss in revenue of €2.4 billion annually due to scam calls and texts.

6.74 ComReg assesses the impact of nuisance communications on Irish businesses under the following headings.

i. Financial losses from fraud.

ii. Wasted time dealing with nuisance communications; and

iii. Increased operating costs due to mitigating harm from fraud attempts.

i. Financial losses from fraud

6.75 Fraudsters regularly impersonate Irish businesses (e.g., banks and delivery services) in order to establish trust with the caller before attempting to obtain personal, banking or security information with the intention to commit fraud. This has consequences for the businesses being imitated which are discussed below (e.g., communicating with customers, mitigation measures etc.).

6.76 Approximately 10% of businesses (or around 30,000 firms) have been the victim of fraud through calls/texts in 2022, accounting for circa 15% of total business fraud. Europe Economics estimate that around 5,000 businesses suffered a financial loss in 2022, losing around €1,707 on average (which is

[260] B&A Business Survey. Q.19(a) Does your business use mobile calls (text) for any of the following parts of its telecommunication strategy?
[261] CSO, Enterprises in 'total business economy', 2020, Average turnover, uplifted to 2021 prices.

broadly in line with the average loss of €1,400 reported by FraudSMART).[262] Furthermore, where a business is the victim of financial fraud, time is spent engaging with scams and dealing with the fallout of same. Dealing with attempts to defraud a business is a costly use of valuable staff time, imposing a high opportunity cost on affected businesses.

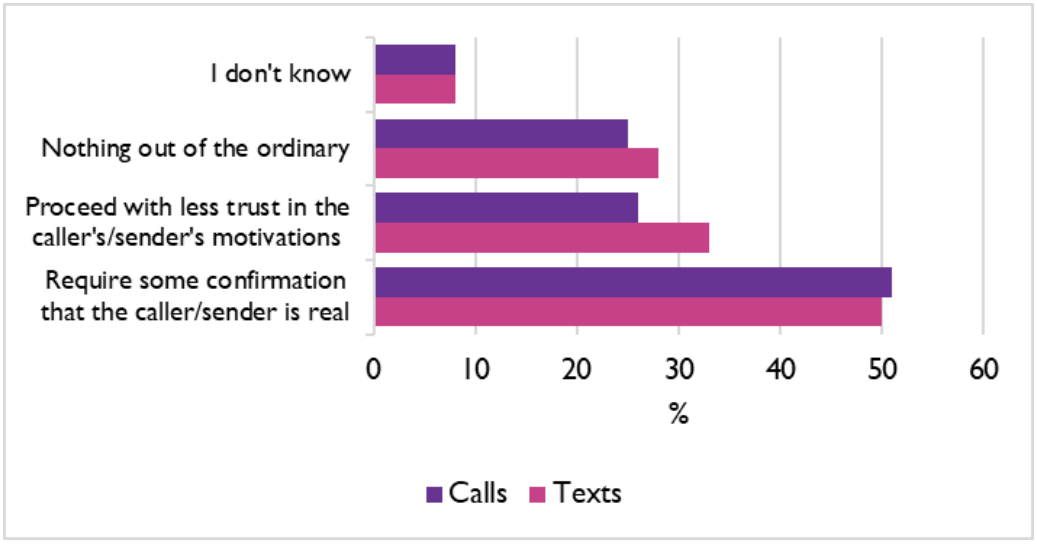
6.77 Europe Economics estimate the total financial loss to businesses in Ireland to be circa €10.5 million in the last 12 months (€8.8m from direct financial loss and €1.7m spent by businesses engaging directly with scams).

ii. Cost of wasted time dealing with scams

6.78 Businesses spend time and resources dealing with consumer queries and complaints where their customers are the target or victims of the scam. Consumers reach out to businesses to report potential scams and or seek resolution where losses have been incurred.

6.79 Businesses also spend a significant amount of time and resources convincing consumers their communications are in fact genuine given the reduced trust in SMS and Voice calls. Half of consumers now require additional information to authenticate the caller or sender (e.g., what is the call about, is it a follow up call or is the issue something I am aware of etc) (See Figure 14). This is unsurprising given the prevalence of scams impersonating legitimate organisations and severely decreases the utility and efficiency of answered calls and texts.

Figure 14: Impact of scam texts on trust in communications from organisations.



Source: Europe Economics analysis of B&A consumer survey data

[262] FraudSMART (2022). 'Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud'

6.80 Europe Economics estimates the value of this time lost to be approximately €21m in the last year alone (based on the mean time spent on resolving customer problems caused by impersonation attempts).

iii. Increased operating costs.

6.81 Scam calls and SMS can raise the operating costs of affected businesses in a number of ways.

- First, businesses reported incurring costs through a failure to communicate with consumers as a result of scam calls or texts, which may inhibit business's ability to schedule appointments or receive payments. Europe Economics estimates the harm from this additional expenditure at €28m in the last year, using the average cost reported by businesses that experienced this cost (€1,997). This harm may increase over time given that the need to reassure consumers of the veracity of a business's communications may intensify the longer scams persist at such high levels.

- Second, businesses reported incurring costs to mitigate the harm from scam calls and texts. Europe Economics estimates the harm from this additional expenditure at €50 million in the last year, using the average cost reported by businesses as having been incurred to implement scam-prevention measures.

- Third, organisations such as banks may incur costs from dealing with fraudulent payments. Consumers may recover some of the monies lost through fraud through scam calls and texts. In some cases, this may be the result of a successfully cancelling a payment[263], in other cases, it may be because of organisations (e.g. banks) themselves refunding affected parties. Europe Economics estimates that this harm could be as high as €23 million in the past year, based on the monies reported as having been recovered by respondents to the B&A Consumer Survey.

Conclusion on the harms to businesses from scam calls and texts.

6.82 Europe Economics estimates **a total harm to business of €132.5 million** from scam calls and texts over the last 12 months as shown in Table 6.

Table 6: Summary of quantified harms to businesses (€m)

Quantified Harm	Total (€m)

[263] For example, consumers cancelling a cheque after sending by post.

Financial Losses from fraud	10.5
Time and resource spent dealing customer experience of scams	21
Cost of scam prevention measures	50
Cost of not engaging with customers	28
Cost of refunding customers	21
Total Harm	130.5

iii) Harm to other organisations.

Public Bodies

6.83 Government departments (e.g., Dept. of Social Welfare), public agencies (e.g., HSE, An Garda Síochána) suffer many harms as a direct consequence of scams. To understand these harms, Europe Economics conducted interviews with a number of bodies, to understand and where possible estimate the cost of the harms. The purpose of this section is to provide a snapshot of the potential harm to public facing bodies – but because it only estimates harm for selected agencies the overall harm estimate is conservative.

6.84 Scam calls and texts reduce consumers trust in SMS and Voice calls, which are used by many public bodies to provide information, schedule appointments or otherwise communicate with Irish citizens. Scam calls and texts may therefore raise the operating cost of public bodies which may invest in alternative communication channels and/or anti-cyber security measures or software. This arises given the key role SMS and Voice as means of near universal B2C communications.

6.85 For example, consumers may simply ignore texts purporting to be sent by public bodies, which may result in missed appointments or information regarding critical services. This harm is likely to be most acute precisely when such communications are most vital, as fraudsters often target notable events (e.g., Covid-19 scams, An Post Christmas scams). In this way, fraudsters may exacerbate the impact of negative events on consumers, frustrating the effort of public bodies to ameliorate the effect of various events or crises.

6.86 Europe Economics interviewed a select number of agencies, which are considered especially likely to suffer harm as a result of scam calls. Based on information provided in the stakeholder interviews, Europe Economics has estimated that the harm suffered by these few agencies alone amounts to

around €7 million[264].

a) **HSE –** Europe Economics have estimated the cost to the HSE of scams calls and texts from a greater number of missed appointments and the cost of certain cyber security measures[265].

b) **An Garda Síochána –**the additional cost of staff to handle scam calls and texts, based on discussions with An Garda Síochána.

c) **An Post –** As an example of the measures undertaken by An Post, a direct-to-consumer campaign.

6.87 It should be noted that each body suffers further harms which were not readily quantifiable given data availability or inherent uncertainty, and the interviews covered only a fraction of potentially affected public bodies. Accordingly, the likely cost of the total harm to public bodies is probably many multiples of this identified cost. Unlike for consumers and businesses, it is not possible to estimate total harm by extrapolating the harm experienced by surveying a representative sample, given the uniqueness of the harms suffered by different public bodies (which are themselves unique).

6.88 An Garda Síochána has been impersonated by scammers who target consumers and request important personal and financial information. For example, scams aim to obtain personal information such as bank account details and/or PPS number[266]. This has included:

- A phone call from a number similar to the Garda Confidential Line contacts a person stating they are investigating fraud activity or investigating a crime and require your details to progress the investigation. The phone call comes from 0-1800-666-111. The actual Garda Confidential Line number is 1800-666-111 and does not make outgoing calls.

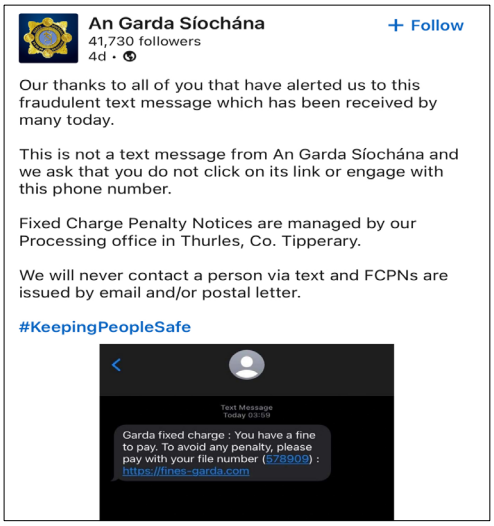
- A person or automated message tells you there is a warrant out for your arrest or a fine. To prevent further action you are asked to make a payment.

[264] This is non-exhaustive, and merely represents the harms which were quantifiable given the available information.
[265] This relates only to a specific share of the HSE's total expenditure to tackle cybersecurity.
[266] https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2021/april/fraud-warning-impersonating-members-of-an-garda-sochna.html

- Other similar scams include scams that pretend to be from the Financial Intelligence Unit (FIU Ireland) of the Garda National Economic Crime Bureau (GNECB) and from the government's Immigration Service Delivery.[267]

- More recently, there has been an uptick in scams requesting consumers to pay a fixed penalty charge (claims that the recipient has an outstanding Garda fine to pay). [268]

Figure 15: Garda Síochána SMS Scam



Harm to operators.

6.89 Operators may also suffer a range of harms[269], including but not limited to:

- Potential revenue reductions from a reduced use of SMS and/or Voice;
- Cost of carrying fraudsters' traffic which may be unpaid;
- Opportunity cost of time spent handling complaints; and
- Cost of configuring network to handle peaks associated with waves of scam calls or texts.

[267] https://www.donegaldaily.com/2023/04/01/garda-warning-over-two-sophisticated-phone-scams/
[268] Donegal Gardaí warn of new text message scam asking recipients to pay fine | Independent.ie

[269] This section covers harms from scam calls and texts to operators. Notably the cost of interventions are borne by operators and this is handled separately in the RIAs.

6.90 However, unlike other stakeholders, operators may potentially benefit from scams by earning revenues, sometimes known as "*toxic revenues*"[270] arising from scam calls or texts. Given the data available, Europe Economics has not estimated the direct harms to operators.

6.91 ComReg considers that an operator's business case for investment in the proposed interventions should be made given the harm arising to operators' consumers and long-term commercial interests. In the long-run, scam calls and texts could negatively impact the revenues generated by operators from providing Voice and SMS services, and from the networks over which such services are transmitted. As noted by Europe Economics[271]:

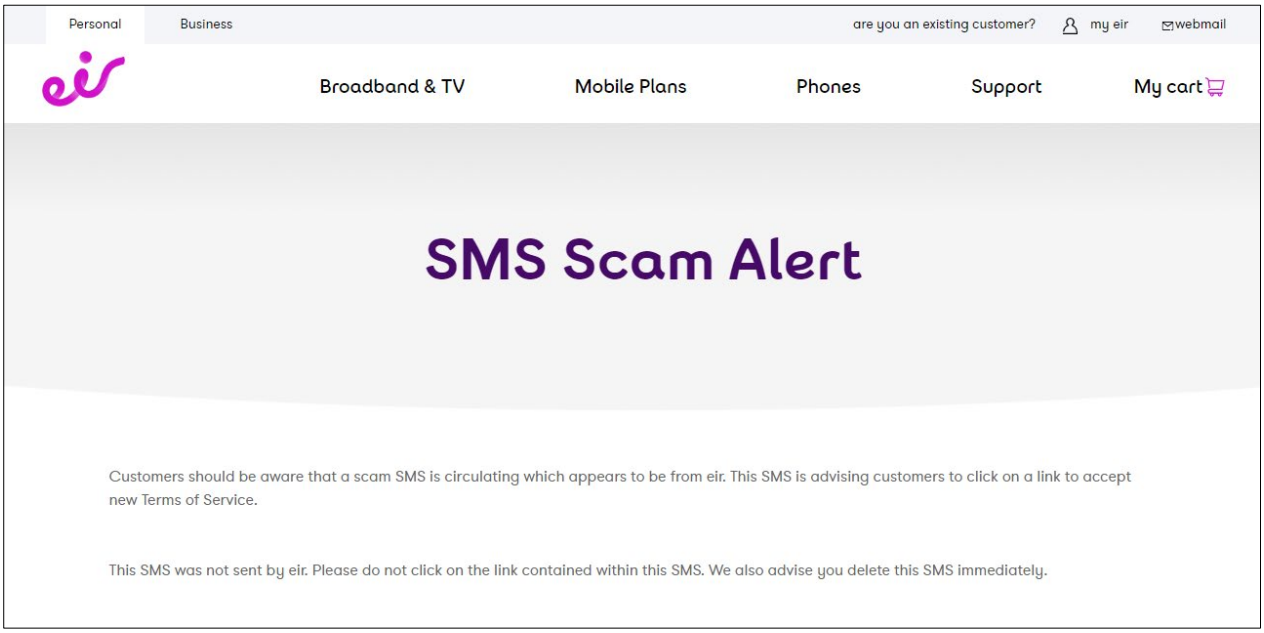
> "*Operators were clearly aware of the potential impacts of scam calls and texts on the communications they facilitate. One MNO, in particular, noted that interventions to curtail fraudulent communications could increase trust in mobile numbers, and suggested that there was scope for operators to benefit commercially from being able to offer networks of trust. The operators were also clearly aware of damage scam calls and texts can do to organisations' reputations, and hence also the trust consumers have in the communications they send*."[272]

6.92 Notably, the key harm suffered by operators relates to second order effects of scams (e.g., reduced use by consumers of Voice/SMS) and not direct harms, such as financial loss. This highlights an asymmetry in the incidence of harm; while consumers and businesses are suffering today, operators may not suffer for a time and bear only a fraction of the total social cost of harms for now. In essence, while operators suffer harm, the cost of unprotected networks is primarily being borne by Irish consumers and businesses.

6.93 Finally, ComReg notes that operators themselves are being impersonated by fraudsters advising customers to click on a link accepting new terms of service.[273]

[270] https://www.upstreamsystems.com/press/press-releases/passive-reliance-on-toxic-revenues-no-longer-acceptable-for-mnos-upstream-says-at-global-carrier-billing-summit-2020/
[271] Europe Economics Report, page 31.
[272] Operators are clearly concerned with how consumer perceptions can damage reputation and revenue growth. For example, Eir in its latest set of published accounts observed in relation to Risks Related to Our Business and Industry that "*If we are unable to maintain a favourable brand image or maintain a positive customer experience, we may be unable to retain existing and/or attract new customers, leading to loss of market share and revenue*." eir_Q4-22_results_report.pdf – p20.
[273] Scam SMS alert (eir.ie)

Figure 16 Eir SMS Scam Alert



D) Overall economic and societal harm from scam calls and texts

6.94 Unsurprisingly, and given the diversity of harms and the large number of impacted parties, the overall harm from scam calls and texts is substantial. Europe Economics conservatively estimates that scam calls and texts resulted in harm of over **€300 million in the 12 months to November 2022** as shown in Table 7. As noted earlier, **this a conservative estimate,** being limited to only those harms that were quantifiable given the data available**.**

Table 7: Summary of all harms quantified by Europe Economics (€m)

Quantified Harm	Total (€m)
Harm to consumers	172
Harm to business	130.5
Public Body (Case Studies)	7
Total Harm	**309**

Figures may not sum due to rounding.

6.95 ComReg discusses the implications arising from this harm in each of its RIAs that follow.

II. Loss of trust

6.96 The second main policy issue that applies to all RIAs is the loss of trust caused by nuisance communications. Scam calls and texts may cause

consumers to lose trust in numbers through attempts to commit fraud thereby undermining the benefits of ECS services to Irish consumers, businesses and wider society. ComReg sets out below how Nuisance Communications can damage trust and reduce the effectiveness of the numbering platform in the delivery services to consumers.

6.97 Nuisance communications create a number of distinct effects that threaten the efficient and effective functioning of the Numbering platform, including:

- uncertainty caused by a previous scam call experience may infect a consumers' beliefs across all calls regardless of who is calling (Contagion effect);
- such problems may reduce the volume of calls made and received over the numbering platform (Call reduction);
- a reduction in the use of services through numbers by consumers would eventually reduce the incentives for Service Providers ("SPs") to continue to provide services over the numbering platform (Feedback effect); and
- there may be additional issues of equity for some services used by vulnerable groups (i.e., some services that would normally be provided over voice or SMS may move to alternative platforms not readily available to all social groups) (Social effect).

6.98 ComReg considers these issues below in assessing consumer harm.

Contagion effect

6.99 ECS networks are public platforms enabling any user in the world with a signal or a line to connect with any other user almost instantaneously. The openness and convenience of such global networks has underpinned their rise and there has been a transformational impact on society. This underpins the benefits of Voice and SMS as a means or two-way communications for consumers and businesses, and SMS as a means of broadcasting information for businesses.

6.100 However, consumers may not wish to receive calls given the problems associated with fraud and scams. Indeed, the B&A Consumer Survey reveals that many consumers use their devices primarily to communicate with people and businesses that are local or known to them. A single bad experience of nuisance communications may lead a consumer to expect that other calls unknown to them may also be scam related.

Call/SMS Reduction effect

6.101 ComReg considers that the high incidence of nuisance communications reduces the usefulness of the numbering platform to consumers and suppresses the volume of calls and texts, leading to a loss of consumer surplus. Where consumers lose trust in numbers, and in Irish ECS more broadly, this can cause consumers to not answer calls or read SMS messages, inevitably leading to a greater non-response rate. A greater non-response rate in turn could undermine the usefulness of Voice and SMS as a means of communication to consumers, ultimately leading to a greatly reduced utility as a means of communication. Indeed, the B&A Business Survey found that nuisance communications are leading to missed appointments and lost business for Irish businesses. In short, trust is being lost in electronic communications services, and this is in turn impacting consumers and the economy at large.

Feedback effect

6.102 Scam calls and texts and the ensuing reluctance of many consumers to properly engage with voice calls and texts acts as a disincentive for businesses offering services through these means and this, in turn, leads to a reduced and/or lower quality range of telephony/text services which callers may require (e.g., fewer consumer help lines, fewer businesses using SMS to remind consumers of appointments). If the value of providing these services through calls and texts to service providers is diminished, then this may affect the quality of service provided over the platforms.

Social effects

6.103 There may be additional issues with regard to accessing some services over the numbering platform in that nuisance communications could have a particularly negative impact on some more vulnerable consumers for whom voice calls and/or texts provide important access to essential services (e.g., paying bills) or social services (e.g., healthcare, social security). For certain classes of more vulnerable consumers, including some elderly persons or persons with disabilities, voice-based telephony services are essential when travelling to a physical location is difficult; often these are the groups that are most vulnerable to nuisance communications.

6.104 Given the frequency of nuisance communications and the damaging effects on public confidence in the integrity and trustworthiness of electronic communications, it is apparent that absent interventions to combat nuisance communications and restore consumers trust in networks, trust in Voice and SMS services and consequently ECS networks could be harmed irreparably.

Loss of economic and social benefits from the use of ECS

6.105 People need to trust that people contacting them are genuine, otherwise call avoidance would result in legitimate calls and texts going unanswered. Consumers want to answer calls and read text messages in the anticipation that the caller or sender is someone they know or with a reason to contact them, or a business providing services of value to them (e.g., banking and parcel delivery). This trust underpins the use of Voice calls and SMS, and the benefits Irish consumers and businesses derive from these networks[274]. Any such loss of trust could result in significant consumer harm, were it to undermine the benefits of SMS and Voice set out above. This will lead to precipitous decline in use of the numbering platform over time if measures are not implemented to address lack of trust.

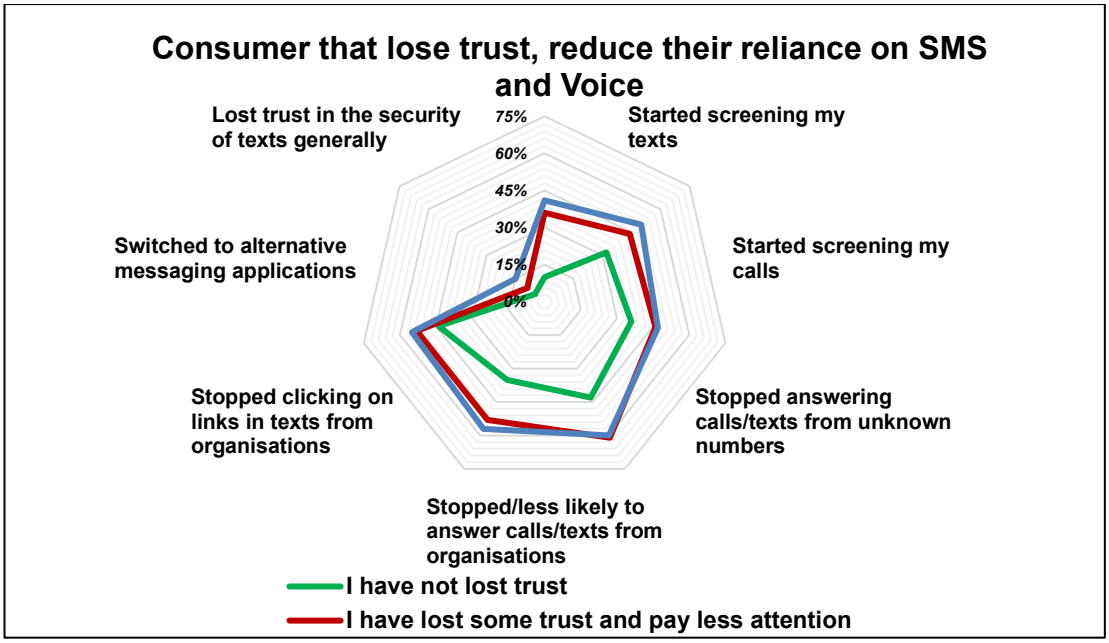
6.106 The B&A Consumer Survey found concerning signs of scams reducing consumers' trust in voice and text communications. For example:

- Around half of consumers now require some confirmation of the legitimacy of the caller/sender.
- Over 40% of consumers that use SMS services[275] are losing trust in these communications and pay less attention to them[276].

6.107 The B&A Consumer survey reveals that consumers have become increasingly distrusting of the calls and texts they receive. As illustrated in Figure 17, consumers that have already lost trust due to scam calls and texts are more likely to show reduced use or reliance on SMS or Voice subsequently (i.e., screening calls/texts, stop answering unknown calls/texts etc).

Figure 17: Reduction in trust in and use of Voice and SMS

[274] See the CLI Blocking RIA and Sender ID RIA for more information on the trust in numbers and Sender IDs.
[275] Such services include information/reminders about health appointments, banking and utility bills.
[276] One in four consumers claim to pay no attention to SMS as a result of their unpleasant experiences with scam texts.



Source: ComReg analysis of B&A consumer survey data.[277]

6.108 This all points to a reduced utility of Voice calls and SMS for senders and users alike as many legitimate calls/texts now go unanswered/unread. Indeed, a sizable minority of survey respondents reported a loss of trust in texts and have switched to alternative messaging applications (e.g., WhatsApp) because in their experience calls and texts over the telephone numbering platform have become untrustworthy.

6.109 The evidence suggests that this usually occurs not because consumers prefer alternative applications or because it views these alternatives as being essentially equivalent to one another. Instead, such migration usually occurs because the consumer decides that the harms and nuisance associated with using calls and/or texts are so high that they avoid using voice and SMS altogether or insofar as possible. It stands to reason that if the telephone numbering platform operated more effectively then consumers would have no need to migrate to alternative means.

6.110 Europe Economics estimates that the lost benefit to consumers due to lack of trust could be as high as **€230 million per annum**[278]. This is not included in the total quantified harm above given these are second order impacts and difficult to estimate with certainty. Nevertheless, this is considered further under the "Impacts on consumers" within each of the RIAs.

[277] This uses data gathered in response to Q.38 "*In relation to your awareness of scam call and texts, has any of the following happened?*" and Q.40c "*If so, has your experience of scam calls and texts affected your trust in communications from the organisations that provide the aforementioned services?*" where Q.40c was asked only to consumers that reported using SMS or Voice calls.
[278] Europe Economics Report, page 44

6.2.2 Identifying Regulatory Options (Joint Step 2)

6.111 This section identifies and describes the potential interventions that are available to ComReg in combatting Nuisance Communications (and that have been consulted upon in Consultation 23/52). The main output from this Section is to identify a list of interventions to be assessed in one or more RIAs that follow. In that regard, this Section forms the basis of Step 2 of ComReg's RIA Guidelines.

6.112 In order to ensure that all potential interventions are appropriately considered, ComReg provides a full list and description of all technical interventions that are available to ComReg and have been considered in other jurisdictions and/or proposed by stakeholders in the NCIT and/or over the course of stakeholder interviews. Table 8 provides a high-level summary of the interventions available to ComReg, the source of the interventions and the intended impacts.

Table 8: Long list of interventions and their intended impact

	Interventions	Source	Intended Impact
Voice (6)	1. Do Not Originate	NCIT	Prevents Voice calls from certain assigned numbers, from originating in, or being carried into the State.
	2. Protected Numbers	NCIT	Prevents Voice calls from all unassigned numbers, from originating in, or being carried into the State.
	3. Fixed CLI call Blocking	NCIT	Prevents Voice calls from abroad using Irish fixed numbers, from being carried into the State.
	4. Mobile CLI call Blocking	NCIT	Prevents Voice calls from abroad using Irish mobile numbers (except for roamers), from being carried into the State.
	5. Voice Firewall	Discussion with other NRAs	Screens and blocks Voice calls from terminating on public ECS networks.
	6. Stir/Shaken	Discussion with NRAs	Authenticates Voice calls at the point of origination and termination.
SMS (5)	1. Shortening the Chain	NCIT	Limit the number of "hops" in SMS journey to a known, limited number of trusted 'hops' and blocks SMS for those Sender IDs coming other sources.
	2. ID Ban	Discussion with NRAs	Blocks SMS with SMS Sender ID from terminating on public Mobile networks in the State.
	3. ID Registry – Full or partial	Discussion with NRAs	Permits only SMS from registered Sender IDs using verified paths to terminate on public mobile networks.
	4. O-D verification	Discussion with industrial stakeholders	Terminates only SMS with Sender ID, when authenticated by the recipient network via a passcode database.
	5. SMS Scam Filter	NCIT	Blocks or labels SMS containing suspect content from any source including mobile phones, terminating on public Mobile Networks.

6.113 Not all interventions listed in Table 8 are necessarily appropriate for consideration in the RIAs. ComReg notes that any intervention that is not technically feasible, effective and/or cannot be implemented in a timely manner could not be considered a valid regulatory option in a RIA because it would not be able to reduce or mitigate the harms. Further, even where an intervention is technically feasible and effective, its implementation over an extended period could result in the harms to society continuing over that period (where other interventions could have been more effective in reducing the harm in the short term).

6.114 Any interventions that are technically feasible/effective and implementable over a timely period can be assessed in the RIAs as regulatory options against ComReg's broader statutory objectives and duties including the obligation to promote competition. ComReg also notes that the impact on stakeholders arising from each intervention is assessed separately in the 'Impact on Stakeholders' for each RIA below.

6.115 With that in mind, ComReg assesses each of the interventions as follows.

I. **First**, ComReg provides a description and illustration of each intervention including how it could reduce the harm caused by Nuisance Communications ("Description");

II. **Second**, ComReg assesses whether the proposed intervention is technically feasible and effective in relation its intended purpose ("Technical feasibility and effectiveness"); and

III. **Third**, ComReg assesses whether the intervention is implementable over a reasonable period[279] ("Timelines")

Potential Voice Interventions

1. Do Not Originate & 2. Protected Numbers

I. Description

1. Do Not Originate

6.116 Many organisations have telephone numbers that are never used for making outgoing calls to customers. These are usually phone numbers that consumers call for service information such as a customer care line (e.g., banking, credit cards etc.). Using CLI spoofing, fraudsters can make calls that

[279] ComReg notes that these timelines are associated with a greenfield deployment and some interventions may have already been implemented voluntarily by some operators. It is in part due to the slow implementation of these interventions by some operators (through the auspices of the NCIT) that ComReg is now mandating these measures over the proposed timelines.

appear to originate from these “inbound-only” numbers to trick consumers into answering the calls. Operators may block calls from these numbers to prevent fraudsters impersonating legitimate businesses. This creates no difficulty for the business concerned as the numbers in question are not used for making outbound calls. A list of such “inbound-only” numbers is called a DNO list.

2. Protected Numbers

6.117 PN numbers are numbers that have not been assigned by ComReg to operators, and which should therefore not originate calls. Using CLI spoofing, fraudsters may make calls that appear to originate from these Irish numbers to trick consumers into answering the calls. To combat such scam calls, operators can block any calls supposedly originating from these numbers. This creates no difficulties in the delivery of services because there are no services currently being provided via these numbers.

II. Technical feasibility and effectiveness

6.118 The DNO and PN lists and their feasibility are assessed together because both aim to address spoofing of numbers which should not originate calls. The general feedback from operators is that these interventions are not overly complex to implement.

6.119 In relation to technical feasibility, a DNO trial[280] was conducted by ComReg and a small number of telecoms[281] operators (September 2022) demonstrated the technical feasibility and effectiveness of the DNO and PN lists with operators successful in blocking calls that are provided on both the DNO and PN lists. The trial also tested ComReg’s administration of the DNO list by preparing the application process and encouraging organisations to apply for the addition of suitable numbers to that list[282].

6.120 Several of the trial operators had also implemented blocking of numbers on the PN list during this time. The trial tested the capability of operators to block calls on the lists and this was effective in demonstrating the technical feasibility of the interventions. ComReg and industry agreed to a wider implementation of DNO, which has already been successfully launched and no issues with technical feasibility have arisen. Currently 15 telecoms operator members of ComReg’s NCIT, have implemented DNO and PN and report that the interventions are working well with calls already being blocked from such sources.

[280] ComReg notes that a trial is possible to as this intervention does not require upfront investment costs from operators.
[281] The five operators who took part implemented the initial DNO list of 17 numbers.
[282] This initial list, which comprised numbers from several organisations, was prepared with the assistance of the Banking and Payments Federation of Ireland.

6.121 In relation to effectiveness, all NCIT members agree that the interventions based on the DNO and PN lists should be effective in tackling nuisance communications. Indeed, these interventions have already proved very useful, with thousands of calls presenting as coming from numbers on the trial DNO List blocked. ComReg notes that this intervention is already in use and proving effective in Belgium, Australia[283], UK[284] & USA[285] as a means by which to reduce nuisance communications.

6.122 ComReg published an Information Notice regarding DNO (ComReg 22/86)[286], a Guidance Note and Application Form (ComReg 22/86a)[287], and a dedicated webpage[288] where further information is available. The implementation of the PN list is analogous to the DNO list and many of the trial operators have also implemented blocking of numbers on the PN list.

6.123 Therefore, ComReg is of the view that the DNO/PN intervention is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

6.124 ComReg is of the view that the DNO and PN intervention can be implemented within 6 months of any final Decision. This view is informed by:

- Discussions with industry stakeholders in the NCIT which indicate that this requires a simple manual update to operators' systems.
- It is currently implemented by the majority of NCIT members, with remaining NCIT members expected to complete in due course.
- The successful trial of this intervention was completed within a 6-month period;
- A number of NCIT members have implemented this intervention in less than 3 months; and
- The Plum Report[289] concludes that the timeframe of 6 months from a final decision for implementation of DNO List and PN is reasonable and achievable.

[283] https://www.acma.gov.au/sites/default/files/2019-11/Combating-Scams-summary-report.DOCX
[284] Tackling scam calls and texts: Ofcom's role and approach
[285] FCC Acts to Stop International Robocall Scams | Federal Communications Commission
[286] https://www.comreg.ie/publication-download/nuisance-communications-launch-of-do-not-originate-protocol
[287] https://www.comreg.ie/publication-download/do-not-originate-list-guidance-note-for-organisations-and-application-form
[288] http://www.comreg.ie/dno
[289] See Section 4.1 of Document 24/24b.

6.125 Therefore, ComReg is of the view that the implementation of the DNO and PN intervention within six months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow.

3. Fixed CLI Call Blocking

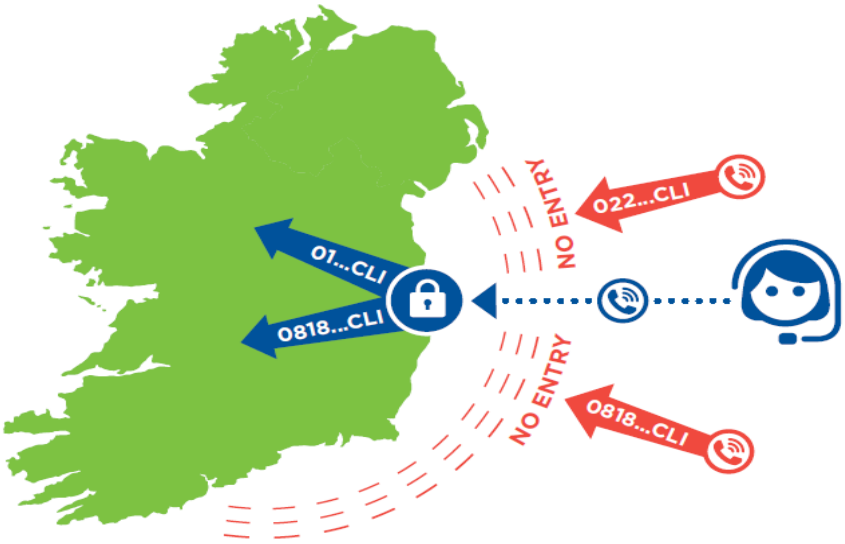
I. Description

6.126 Currently, IGOs allow Voice calls with Irish Fixed CLIs[290] into the State from abroad. Using CLI spoofing to disguise their identity and exploit the trust Irish consumers place in Irish Geographic Numbers and Non-Geographic Numbers, fraudsters based overseas can make calls appear to originate from Ireland. Operators could block calls presenting these numbers as CLIs (i.e., spoofed CLIs) to prevent fraudsters impersonating legitimate Irish organisations. This is known as Fixed CLI Call Blocking.

6.127 There are a small number of legitimate use cases for an Irish Fixed CLI originating outside the State (for example an overseas call centre). This however can be facilitated by use of a dedicated and secure connection, known as a "*long line*".[291] The 'long line' PSTN call origination measure was agreed by NCIT members as part of its Fixed CLI specification and is an intervention that is to be implemented as soon as possible in anticipation of the implementation of the call blocking measure being discussed here. Any lack of progress on this intervention will put Irish telephone users at serious risk from fraudsters while undermining the integrity of the PSTN voice service.

[290] Irish Fixed CLIs refers to CLI presenting all Irish numbers except mobile (e.g., Geographic numbers and Non-Geographic Numbers).
[291] Long-line means the implementation by an undertaking of a dedicated SIP or alternative trunk type to serve an end-user to ensure that calls from that end-user originate on the Irish PSTN.

Figure 18: Fixed CLI Call Blocking and long-lining



II. Technical feasibility and effectiveness

6.128 In relation to the technical feasibility, the specifications for this intervention have been operator led and determined in collaboration with other NCIT members. The specifications have been completed and the network designs required for the Fixed CLI call blocking intervention commenced in Q3 2022. The testing and deployment of the intervention in the individual operator networks followed by 'go-live' commenced in Q1 2023[292]. Six operators[293] have so far activated the measure in their networks. ComReg published an Information Notice regarding DNO (ComReg 23/47)[294], where further information is available. ComReg's functional requirements specification for the intervention is available upon request to relevant operators.

6.129 In relation to effectiveness, NCIT members have agreed that this intervention should prove effective in reducing nuisance communications by identifying and blocking nuisance calls stemming from international networks and presenting with Irish fixed CLIs. Calls originating from overseas which are using an Irish fixed Calling Line Identification as a Presentation Number shall always be blocked by IGOs. Calls from overseas platforms such as call centres that use Irish fixed CLIs may continue to so with a direct private

[292] This assumes that each involved operator continues to give very high priority to the implementation of the intervention in their networks.
[293] Nine NCIT members are in scope for that intervention, 6 have it fully deployed, BT are expected to have it deployed in Q2 alongside their Mobile CLI solution, Vodafone's solution based on presentation CLI is also due in Q2.
[294] https://www.comreg.ie/publication/tackling-nuisance-communications-cli-call-blocking-update

customer connection from such platforms to the Irish telephone network (*longline*). This intervention is likely to be effective by preventing fraudsters from spoofing Irish Fixed CLIs and allowing such calls to be made to Irish consumers and businesses who may perceive that a call is from a legitimate source and are thus more likely to answer it. Feedback from operators that have already implemented this intervention is that the intervention is effective at blocking spoofed calls originating from abroad with an Irish Fixed CLI.

6.130 Therefore, ComReg is of the view that the Fixed CLI call blocking intervention is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

6.131 ComReg is of the view that the Fixed CLI intervention can be implemented within 6 months of any final decision. This view is informed by the following:

- Based on information provided at the NCIT, ComReg understands that the blocking requires a simple manual updated to operators' systems. Operators have suggested that it would take six months to have this intervention fully operational in their networks (subject to organisation prioritisation).

- Discussions with industry stakeholders in the NCIT who indicated that that this intervention can be based on existing technologies deployed by network operators (e.g., Session Border Controllers).

- Operators have already been making progress on implementing this intervention through the auspices of the NCIT and 7 operators have already implemented the Fixed CLI intervention. This also accounts for the time operators may need to implement the "long-lining" solution for extraterritorial use of Irish fixed numbers, such as by call centres.

- The Plum Report[295] concludes that the timeframe of 6 months from a final decision for implementation of DNO List and PN is reasonable and achievable.

6.132 Therefore, ComReg is of the view that the implementation of the Fixed CLI intervention within six months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow this section.

[295] See Section 4.1 of Document 24/24b.

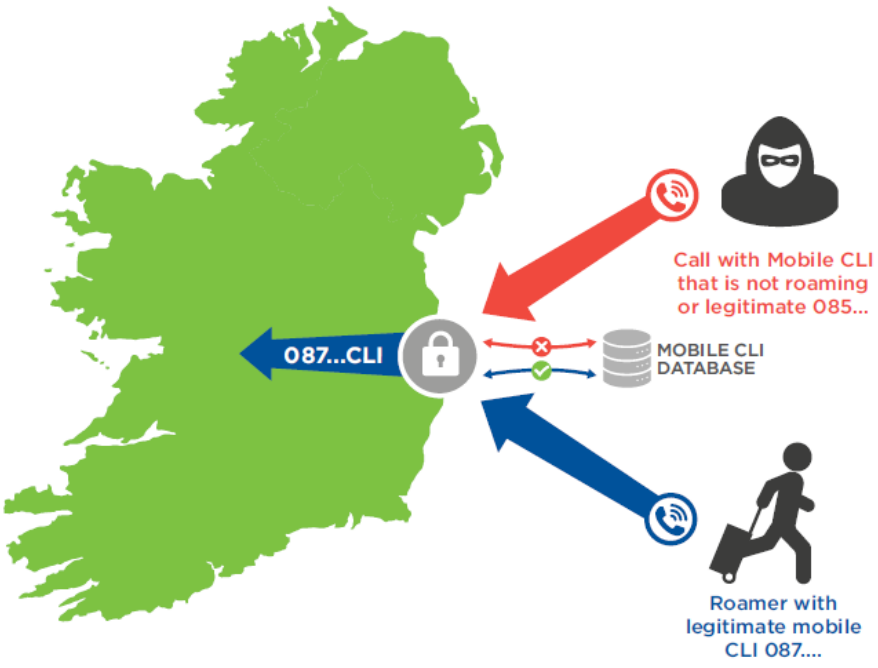
4. Mobile CLI Call Blocking

I. Description

6.133 Currently, IGOs allow any Voice calls with Irish Mobile CLIs[296] into the State. Using CLI spoofing, fraudsters based abroad can make calls that appear to originate from Irish mobile numbers. IGOs may block calls presenting these numbers as CLIs, to prevent fraudsters impersonating legitimate Irish mobile numbers. This is known as Mobile CLI Call Blocking.

6.134 There are limited legitimate use cases for a call originating abroad to present an Irish Mobile CLI. For example, in the case of calls from Irish mobile users abroad ("outbound roaming") or for calls from Irish mobile or fixed line users to non-Irish mobile users who are in Ireland ("inbound roaming"). Such calls are routed via the inbound roamers home network into the state using an Irish Mobile Number assigned ("Mobile Station Roaming Number") by Irish MNOs to those roamers on a temporary basis.

Figure 19: Mobile CLI Call Blocking



II. Technical feasibility and effectiveness

6.135 In relation to technical feasibility, the 'roamer check' aspect of the intervention is based on the 'MAP' signalling protocol which is part of the SS7 protocol stack and widely in use in mobile networks. For this intervention, it is used to

[296] Irish Mobile CLIs refers to CLI presenting all Irish mobile number (e.g., 087, 083 ranges).

implement the 'roamer check' capability from the Irish IGO to the serving Irish mobile network operator (as per the telephone number indicated in the CLI of the call). The 'MAP' signalling protocol approach for the roamer check is part of Phase 1.

6.136 However, based on NCIT and associated discussions with operators, it is understood that the MAP signalling protocol is not available on all the Irish networks, particularly in the case of some of the smaller IGOs.

6.137 The intervention will in the future include an industry 'proxy server' approach accessible by a protocol other than MAP. This server would also contain Mobile Number Portability ('MNP') data which would be needed to determine the serving network for the mobile CLI which being checked for its roaming status. This approach, if availed of by smaller IGOs, would remove the need for such operators to use the services of another operator in the manner described above. Rather, incoming calls could be validated by using the 'proxy server' once the IGO receiving the call sends a validation request to the proxy server in respect of such calls. ComReg notes that this approach has been implemented in Finland for the same purpose[297].

6.138 In order to address the issues raised above – this intervention would be implemented in two phases:

- Phase 1 would require larger IGOs ("Phase 1 IGOs") to implement the Mobile CLI call blocking intervention. Each IGO would undertake the roamer check from its own international ingress point[298] and therefore avoid blocking calls from legitimate roamers.
- Phase 2 would require an industry roaming proxy server to include a non-MAP signalling protocol for IGOs to perform roamer check. A technical specification for Phase 1 of this intervention was developed by the NCIT member operators. ComReg is satisfied that this intervention is technically feasible.

6.139 Mobile CLI call Blocking covering Phase 1 has an agreed technical specification developed by the NCIT members. ComReg's functional requirements specification for the intervention, covering both Phase 1 and Phase 2, is available upon request to relevant operators. This specification includes the proposed network architecture for the Phase 2 roaming proxy server.

[297] EN Recommendation to Telecommunications Operators on Detecting and Preventing Caller ID Spoofing.pdf (kyberturvallisuuskeskus.fi)
[298] Failure to apply screening for one operator will impact Nuisance calls for all fixed and mobile users in the Irish network. Fraudsters will learn this vulnerability quickly and will move to exploit it.

6.140 In relation to effectiveness, NCIT members agree that this intervention should be effective in tackling nuisance communications by identifying and blocking nuisance calls stemming from international networks and presenting with Irish mobile CLIs. Fixed and mobile operators in Ireland would implement a roaming status check for all calls they receive that present with mobile CLIs. Those calls with CLIs which are not actually roaming would be blocked. This intervention would be effective because Irish Mobile CLIs would not be received on calls from abroad unless the call is from a legitimate Irish roamer. Similar measures have already been introduced in other EU countries.[299] In November 2023, Traficom reported that Mobile CLI Call Blocking was resulting in 200,000 blocked scam calls every day[300].

III. Timelines

6.141 Mobile CLI Intervention is divided into two phases and the timelines are assessed across these phases.

6.142 ComReg is of the view that Phase 1 of the Mobile CLI Call Blocking intervention can be implemented within 6 months of any final decision for the following reasons:

- The current technical specification (v1) was agreed by NCIT at the beginning of August 2022 at which point relevant operators indicated that it would take one year to have this intervention fully operational in their networks (subject to prioritisation within each operator organisation).
- Relevant operators have been making some progress on their preparations to activate this intervention and ComReg has continually urged these operators to ensure priority is given within their organisations in meeting this timeline.
- The Plum Report[301] concludes that the timeframe of 6 months from a final decision for implementation of Phase 1 of the Mobile CLI Call Blocking remedy is reasonable and achievable[302].

6.143 ComReg is also of the view that Phase 2 of the Mobile CLI Intervention can be implemented within 2 years of any final decision for the following reasons.

[299] Notably, in Germany (link) and in Finland (link).
[300] Obligations of the Regulation come into effect - up to 200,000 scam calls are prevented per day | Traficom
[301] See Section 4.2 of Document 24/24b.
[302] This view was provided in light of changes ameliorating concerns about the implementation of Phase 1 by non-MAP enabled IGOs,

- Phase 2 would require the setup of an industry roaming proxy server to include a non-MAP signalling protocol for IGOs to perform the roamer check. This requires some time, given the inevitable complexity of implementing a new platform and the related inter-operator process.
- ComReg observes that VoLTE still accounts for a small minority of voice calls made and that VoLTE roaming is likely to be based on the S8HR architecture.
- Based on the Finnish example 24 months appears an appropriate amount of time for implementation.
- The Plum Report[303] concludes that the timeframe proposed by ComReg of 24 months from a final decision for implementation of Phase 2 of the Mobile CLI Call Blocking remedy is reasonable and achievable.

6.144 Therefore, ComReg is of the view that the implementation of the Mobile CLI intervention within six months (Phase 1) and within two years (Phase 2) of a ComReg Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow this section.

5. Voice Firewall

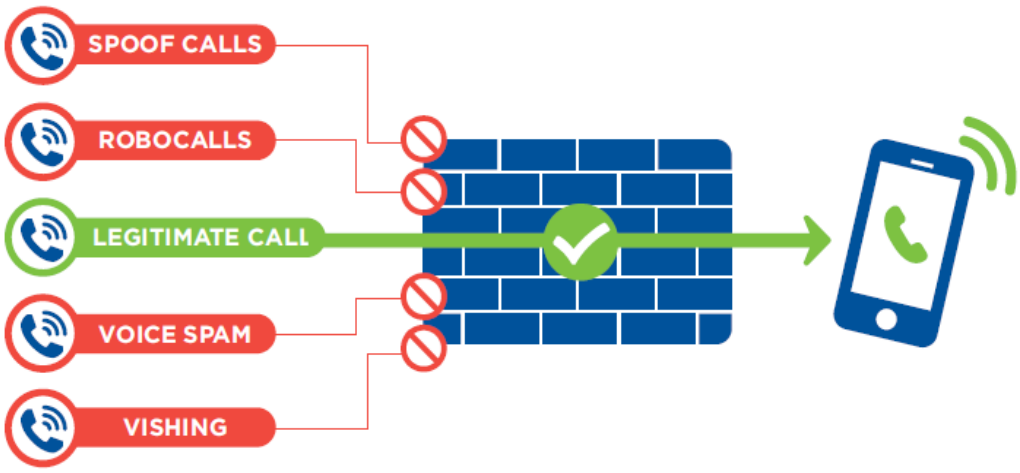
I. Description

6.145 Voice firewalls are designed with advanced real time call data analytics using Machine Learning and Artificial Intelligent techniques to detect and act upon unusual patterns of call signalling data, traffic volumes etc. The deployment of Voice Firewalls by Irish operators can be expected to significantly enhance and extend the range of protections afforded to Irish telephone users beyond what is provided for by the current 'static' CLI spoofing focussed interventions.

6.146 As part of the NCIT process, ComReg and the NCIT identified voice firewalls as a potential means of dynamically combatting scam calls, noting that fraudsters would over time find new means to execute scams and new pathways to contact Irish consumers.

[303] See Section 4.3 of Document 24/24b.

Figure 20: A Voice Firewall



II. Technical feasibility and effectiveness

6.147 Voice firewalls are technically feasible with various different types having already been introduced by MNOs abroad (e.g., Norway[304], Spain[305] and UK[306]). Voice firewalls are also readily implementable noting that multiple security solutions providers provide not only Voice Firewall software, but also installation and training. ComReg notes that this work stream is not as advanced as other proposals discussed in NCIT as part of the NCIT layered approach to implementing interventions[307]. In that regard, ComReg proposes to provide extended timelines (see below) to allow for the intervention implemented.

6.148 In relation to effectiveness, voice firewalls actively monitor network traffic and block malicious/scam calls depending on the rules configured within the firewall[308]. Voice firewall solutions use different sets of protocol information and therefore differ between providers depending on their vendors approach – for example some use consumer reporting of whether a call was a scam. However, firewalls typically use a form of AI to review calls with advanced real time call data analytics using machine learning to detect and act upon unusual

[304] Hiya News: Telenor Norway Deploys Hiya to Stop New Wave of Fraud Calls Targeting Norwegians
[305] https://blog.hiya.com/masmovil-pepephone-hiya-in-the-spanish-market
[306] https://newsroom.ee.co.uk/ee-takes-a-stand-against-scammers-with-latest-international-call-blocking-technology/
[307] It was decided to park the voice firewall intervention work for 12 months to focus on developing the DNO, LTPN, Fixed and mobile CLI interventions.
[308] In the context of a Voice firewall, a type 1 error (sometimes referred to as a 'false positive') occurs when the firewall mistakenly blocks a legitimate call, while a type 2 error (sometimes referred to as a 'false negative') occurs when the firewall fails to block a scam call. To minimize both false positives and false negatives, Voice firewalls often use a combination of filtering techniques, which analyse various aspects of the call, such as the sender, content, and behaviour, to determine whether it is legitimate or scam/fraudulent. By continuously updating their filtering rules and algorithms, Voice firewalls can improve their accuracy and reduce the occurrence of both false positives and false negatives.

patterns of call signalling data, traffic volumes etc. ComReg notes the recent experience of:

- T-Mobile reported that it blocked, or labelled as "Scam Likely", over 41 billion scam calls in 2022.[309]
- In Australia, operators have blocked 153,238,877 calls based on call characteristics between October and December 2023[310].
- EE in the UK which blocked as many as 11 million scam calls in a little over a month, following the introduction of an artificial intelligence-based Voice Firewall in July 2022[311].

6.149 Therefore, ComReg is of the view that the Voice Firewall is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

6.150 ComReg is of the view that Voice Firewalls can be implemented within one year of any final decision, for the following reasons:

- The timeline from Vendors suggests that, once procured, the installation takes no more than 6-9 months; and
- Voice firewalls appear readily implementable noting that multiple security solutions providers provide not only Voice Firewall software, but also installation and training.

6.151 However, consistent with its layered approach to interventions as specified at the NCIT an additional 6 months would be provided such that Voice Firewalls should be implemented within 18 months of any final decision. This is also in recognition of the fact that overlapping resources will be required to implement both the static interventions (as outlined above) and the Voice Firewall (a point raised by respondents to Consultation 23/52 and which ComReg had already considered).

6.152 In that regard, the Plum Report[312] concludes that the timeframe of 18 months from a final decision for implementation of the Voice Firewall remedy is reasonable and achievable.

[309] T-Mobile "Scam and Robocall Report" Link
[310] The ACMA's "*Phone Scams: Intelligence Report Q2 (Oct-Dec) 2023-24"*
[311] EE Press release *"EE TAKES A STAND AGAINST SCAMMERS WITH LATEST INTERNATIONAL CALL-BLOCKING TECHNOLOGY*" Link.
[312] See Section 4.4 of Document 24/24b.

6.153 Therefore, ComReg is of the view that the implementation of the Voice Firewall within 18 months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow.

6. Stir/Shaken

I. Description

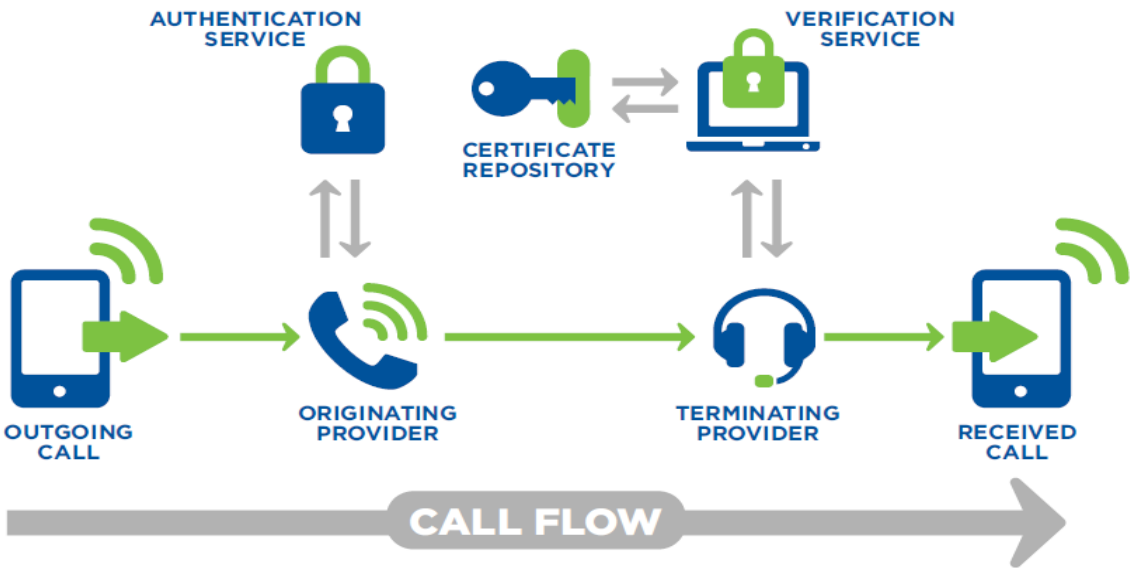
6.154 Currently, Voice calls are not authenticated as legitimate at origination. Therefore, fraudsters can originate calls which may terminate on Irish networks, ultimately reaching Irish consumers. Without a process of verification at source, operators cannot block Voice calls based on the source of origination alone given its unreliability.

6.155 In recognition of the CLI spoofing problem and the absence of end-to-end validation of the CLI, the Internet Engineering Task Force ("IETF") [313] has defined a technology architecture based on extensions to the Session Initiation Protocol[314] ("SIP") for call validation, called Secure Telephone Identity Revisited ("STIR"). This is implemented with the Signature-based Handling of Asserted information using toKENs ("SHAKEN") to form the STIR/SHAKEN scheme. STIR/SHAKEN could be a potential long term global solution for CLI validation. In summary, under STIR, phone numbers are 'attested' and 'signed' at call origination and 'verified' at call termination. The terminating network can then block or label the call as suspicious.

[313] https://datatracker.ietf.org/doc/html/rfc7340

[314] Session Initiation Protocol (SIP) is a signalling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. SIP is used for signalling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol (IP) networks as well as mobile phone calling over LTE (VoLTE).

Figure 21: STIR/SHAKEN



II. Technical feasibility and effectiveness

6.156 STIR/SHAKEN has been in place in the US and has since evolved and been adopted in both Canada and France. Indeed, the efficacy of the technologies used for call authentication" in the STIR/SHAKEN framework was assessed by the United States Federal Communications Commission ("FCC") (December 2022) which concluded that the framework is "*effective at authenticating caller ID information and identifying illegally spoofed calls, and we anticipate its effectiveness would increase as STIR/SHAKEN implementation becomes more widespread*". [315] Furthermore, it was noted that while there was concern that providers may be applying its technical requirements inconsistently. "*There is general agreement in the record, however, that when applied as designed, the technology used in the STIR/SHAKEN framework effectively allows providers to identify calls with illegally spoofed caller ID information.* Therefore, if implemented correctly and on a widespread basis, STIRSHAKEN would be technically feasible in Ireland.

6.157 However, due to the underlying technology, STIR/SHAKEN's caller ID authentication standards can only work on IP-based phone networks[316]. Because a non-IP approach has yet to be determined the above evaluation could not include feasibility of STIR/SHAKEN for non-IP networks. ComReg notes that the FCC has launched an inquiry to examine potential call authentication solutions for non-IP networks, including the nexus between

[315] Triennial Report on the Efficacy of STIR/SHAKEN | Federal Communications Commission (fcc.gov)
[316] Non-IP networks do not have the capability to maintain this type of digital information on calls, therefore the STIR/SHAKEN verification information, including who generated the call, is not available on those networks.

non-IP caller ID authentication and the IP transition generally.[317] Given the substantial use of non-IP networks in Ireland currently – the use of STIRSHAKEN absent a solution for non-IP based networks would mean that STIRSHAKEN may be technically feasible but it is not viable at this point given the extent of legacy non-IP technologies in Irish networks. However, ComReg would continue to monitor progress on a solution for non-IP based networks and update its view in line with last available information.

6.158 In relation to effectiveness, implementation of caller ID authentication technology using the STIR/SHAKEN standards should reduce illegal spoofing and help operators identify calls with illegally spoofed caller ID information before those calls reach their subscribers. STIR/SHAKEN allows voice service providers to verify that the caller ID information transmitted with a call matches the caller's number.[318] Its widespread implementation aims to reduce the effectiveness of illegal spoofing and allow operators to identify calls with illegally spoofed caller ID information before those calls reach their subscribers.

6.159 However, its effectiveness is dependent on widespread rollout across all operators and over an appropriate period which is discussed further below. For example, in the US where it has been implemented since 2021[319] consumers received an extraordinary 34.9 billion unwanted robocalls over the first half of 2022, but only 8% of this volume originated from the top-seven US carriers (AT&T, Lumen, Charter, Comcast, T-Mobile, US cellular and Verizon), each of which have implemented the STIR/SHAKEN framework. [320]The framework has yet to be implemented by smaller operators who account for much of the remaining unwanted calls originating in the US, but all are required to do so by June 30, 2023.

6.160 Furthermore, given that many of the nuisance calls in Ireland are generated offshore, there would be little value currently in implementing these standards in Ireland on its own unless it became a globally adopted approach or the balance of nuisance communications swung heavily toward onshore generation. Consequently, its effectiveness will depend on its use globally. Given that many of the nuisance calls in Ireland are generated offshore, there would be little value currently in implementing these standards in Ireland on its

[317] See Call Authentication Trust Anchor, WC Docket No. 17-97, Notice of Inquiry, FCC 22-81, at 17-21, paras. 37-42 (rel. Oct. 28, 2022) (Non-IP Authentication Notice of Inquiry).
FCC Seeks to Fill Challenging Gap in STIR/SHAKEN Robocall Defenses | Federal Communications Commission
[318] In summary, under STIR, phone numbers are 'attested' and 'signed' at call origination and 'verified' at call termination. STIR/SHAKEN allows voice service providers to verify that the caller ID information transmitted with a particular call matches the caller's number. If a call fails verification, there is high likelihood it is maliciously spoofed, and such information can be shared with the caller, or the call can be blocked.
[319] Both the CRTC and the FCC required operator use of the protocols by June 30, 2021 Combating Spoofed Robocalls with Caller ID Authentication | Federal Communications Commission (fcc.gov)
[320]

own unless it became a globally adopted approach or the balance of nuisance communications swung heavily toward onshore generation.

6.161 In order to tackle the large number of nuisance calls originating and terminating outside North America, the FCC issued an order in May[321] that requires each gateway provider to submit a certification and mitigation plan to the Robocall Mitigation Database[322]. The order also requires gateway providers to authenticate calls with US NANP numbers in the caller ID field by June 30, 2023[323]. Non-gateway intermediate providers not subject to an extension must use STIR/SHAKEN to authenticate caller ID information for all unauthenticated SIP calls received directly from an originating provider no later than 31 December 2023. However, it remains to be seen how effective such an approach will be in practice.

6.162 The latest TNS' Robocall Report 'October 2023' (published after Consultation 23/52) highlighted the continuing disparity between the top-7 carriers and all others in fully implementing the new standards. It further notes that IP interconnectivity, peering and termination complexities can negatively impact signed call traffic from top carriers to smaller providers – undermining the full potential that STIR/SHAKEN and robocall mitigation efforts can deliver to consumers. Again, ComReg will monitor developments in this regard but would need to be satisfied as to this interventions effectiveness prior to considering further.

6.163 Implementing a STIR/SHAKEN type intervention would require the input and cooperation of other countries at least on a quasi-global scale. Such input and cooperation would need to be carried out at least at a European level, most likely by the Conference of Postal and Telecommunications Administrations ("CEPT"), so as to encompass all of Europe and would thus require the commitment of many nation states[324], European and beyond, and far more than the two that have done so in North America[325]. Bearing in mind the immaturity of implementation of any of these standards globally and the

[321] https://docs.fcc.gov/public/attachments/DOC-383499A1.pdf
[322] The FCC maintains a Robocall Mitigation Database in which voice providers are required to "certify whether and to what extent they have implemented the STIR/SHAKEN caller ID authentication framework." Phone companies must reject any calls from voice service providers that are not listed in the database, and the FCC can issue fines to providers that don't file certifications.
[323] In effect, the FCC expands the prohibition to include calls from not only foreign originating voice service providers but also foreign intermediate providers. Therefore, once effective, domestic providers may only accept calls carrying U.S. NANP numbers sent directly from foreign-originating or intermediate providers that are listed in the Database.
[324] The French decision of 2019 [15] also evokes STIR/SHAKEN as a long-term solution. In order to test it, ARCEP has already introduced specific ranges (for geographic, mobile and non-geographic numbers) which are dedicated to authenticated numbers. In July 2020, France adopted legislation requiring French service providers to implement a call authentication solution protecting their customers from various types of telephony-based fraud by July 2023
[325] In 2021, Canada's telecommunication regulator, the CRTC, mandated the use of caller ID authentication (IP voice calls only) using the STIR/SHAKEN protocol that the FCC already applies in the US to block robocalls .

uncertainty surrounding which approach is likely to win out, ComReg considers this potential intervention can only be considered a longer term one at this point, notwithstanding its indubitable potential to be a long-term global solution for CLI validation[326] and the rapidly evolving macroenvironment. ComReg may need to revisit the use of STIRSHAKEN, particularly if the other proposed interventions referenced in this consultation fail to deliver in a timely and effective fashion.

III. Timelines

6.164 The proposed implementation timelines are not considered further given the technical feasibility/effectiveness issues highlighted above.

6.165 In light of the above assessment, ComReg is of the view that STIR/SHAKEN is not a valid regulatory option for the purpose of this consultation and consequently is not considered further at this time.

Potential SMS Interventions

7. Shortening the chain

I. Description

6.166 Currently, many organisations that contact their customers via SMS, use a Sender ID to enhance the recognition and credibility of their SMS messages. Using Sender ID spoofing, fraudsters can send messages that appear to originate from legitimate businesses to deceive consumers into following the instruction contained within the message and providing financial or personal information.

6.167 SMS are not authenticated as legitimate at origination and are often rerouted internationally through one or more cloud/aggregator networks before arriving at the terminating network. Terminating networks therefore cannot block or screen Sender ID, without further information on their origination or pathway. Therefore, fraudsters can originate SMS using misleading Sender ID which may terminate on Irish networks, ultimately reaching Irish consumers.

[326] It is likely that all European operators wishing to terminate calls, where both the called party number and the calling party number are US numbers would have to implement STIR/SHAKEN at some point.

6.168 From initial responses garnered from relevant companies, the banks (and it appears, other SMS clients such as delivery companies) appear to rely on a number of business communication providers, who in turn depend on an unknown (and potentially varying) number of aggregators 'hops' to deliver an SMS message to the end user. SMS messages which traverse several providers have an increased exposure to potential interception by threat actors, thereby compromising the privacy of the message.

6.169 ComReg and the NCIT initially proposed to reduce such risk by limiting the use of particularly sensitive Sender IDs to certain paths, an approach known as "shortening the chain". This amounts to ensuring that the pathways for key Sender IDs are secure and would not carry SMS with false or misleading Sender ID. Further, limiting these messages to defined routes would enable the MNOs to filter spoofed messages arriving on other routes. ComReg and the NCIT agreed to progress this measure for key companies with Sender IDs most susceptible to impersonation by fraudsters. While the members of the NCIT (all ECS providers) agreed this was technically feasible, the success of this measure ultimately depends on engagement and action by the relevant businesses.

II. Technical feasibility and effectiveness

6.170 This intervention would require businesses (e.g., financial institutions) to work with their messaging providers to 'shorten the chain', ensuring messages are delivered over a short, fixed route. MNOs can then block messages bearing these Sender IDs over other routes (i.e., distinguishing the scam messages from the genuine). This initial filtering has the potential to be very effective in blocking many of the most harmful scam messages and should notably address scams based on spoofed Sender IDs, at least in the case of the particularly sensitive Sender IDs (e.g., Banks).

6.171 While technically feasible and achievable with a bank's existing messaging provider, or it might involve a change of messaging provider, or even a direct connection from a banks' systems to one or more MNO networks, its success depends on engagement and action by the relevant businesses (e.g., banks/delivery companies). To help achieve this, and at the request of MNO NCIT members, ComReg has contacted the financial institutions, via the BPFI, seeking information on the routes that their SMS messages might take and suggesting that they could look to 'shorten the chain' to enable the MNOs to block scam messages from other sources.

6.172 However, progress on this intervention can be best described as underwhelming, with delays in the confirmation of key Sender IDs by target companies. Based on the responses received from the target companies to its letter of 1 June 2022 and subsequent meetings, ComReg has formed the view

that the companies were not prepared or willing to undertake the work necessary to "shorten the chain"[327]. It might be the case that such companies do not fully understand the SMS services they have come to rely upon for their critical business operations and therefore assume little to no responsibility for the integrity of the end-to-end delivery path; to their mind the matter has been outsourced. ComReg has not received any further engagement from these businesses since Consultation 23/52.

6.173 In light of the disappointing level of engagement, it is unlikely that this intervention would be effective as ComReg cannot mandate business to 'shorten the chain' and the effectiveness of this intervention cannot be achieved without the committed voluntary assistance of Sender ID users.

6.174 In light of the above assessment, ComReg is of the view that the 'shortening the chain' intervention is not a valid regulatory option for the purpose of this consultation and is not considered further in this consultation.

Interventions 8 - 10 – The regulation of Sender ID

6.175 The following three proposed interventions (i.e., 8, 9 and 10) all concern regulating the use of SMS originating addresses including Sender ID, which is one means of tackling Sender ID spoofing.[328] In summary, a regulator can require operators to block all SMS carrying Sender IDs, or only those that are unregistered or do not conform to certain rules. This is not a novel approach and has been implemented to various degrees in other jurisdictions.

6.176 In total, it appears that over one in three countries regulate Sender ID to some extent, with data from Twilio[329] covering over 200 countries indicating that while Sender ID is permitted in the majority of countries (62%), a significant minority of countries require pre-registration (24%) or do not permit Sender IDs (14%) such as the USA and Canada. Twilio report that this number is increasing over time as "*In many countries, regulatory bodies are increasingly filtering illegitimate A2P SMS use cases to curb unwanted messaging*."[330] Indeed, ComReg is aware that both AGCOM and the ACMA are currently

[327] In ComReg's view these responses did not fully address the questions asked and did not constitute a willingness to 'shorten the chain' as requested. One response claimed that the chain has already been shortened according to its messaging provider which ComReg considered to not be credible given that provider's position regarding the approach of shortening the chain in the NCIT and in bilateral meetings. ComReg continued to apply pressure via engagement with the Central Bank of Ireland which resulted in a round of meetings with the three largest (remaining) retail banks – BOI, AIB and Permanent TSB. During the meetings with the banks, ComReg put forward the case that it is impossible to secure the bank's Sender IDs with the current A2P messaging market structure; that the MNOs stood ready to block messages from unapproved sources; and that ComReg are available to advise on the dialog between the banks and their messaging providers if desired.

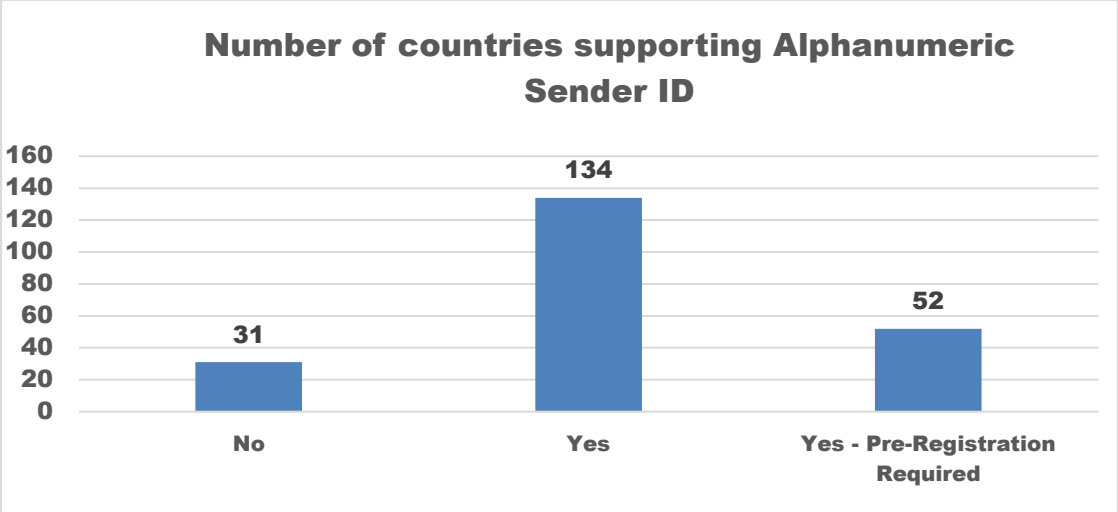
[328] SMS using a Sender ID are not necessarily authenticated in any way (neither at point of origination in spoofing cases nor along its "route"), facilitating fraud using Sender ID Spoofing.

[329] Twilio website "I*nternational support for Alphanumeric Sender ID*" https://support.twilio.com/hc/en-us/articles/223133767-International-support-for-Alphanumeric-Sender-ID

[330] Ibid

consulting on similar measures.

Figure 22: International regulation of Alphanumeric Sender ID



Source: Twilio[331]

6.177 ComReg now examines a number of different interventions which work by requiring MSPs ("Mobile Service Providers") to block SMS spoofing Irish mobile numbers or carrying Sender ID deemed invalid, which are to block all:

- SMS with Sender ID ("Sender ID Ban")
- SMS with Sender IDs which are not pre-registered ("Sender ID Registry")
- SMS with ID which cannot be verified by code verification ("SMS OD Verification")

8. Sender ID Ban

I. Description of interventions

6.178 The most straightforward means of preventing Sender ID spoofing is to require mobile operators to block SMS messages containing any alphanumeric Sender ID.

II. Technical feasibility and effectiveness

6.179 This approach involves blocking all SMS messages bearing any Sender ID. This is technically feasible because operators would block all Sender IDs in the same way as it would block Sender IDs not on a SMS Registry.

[331] ComReg assumes this information is accurate, and accepts the information as described by Twilio on its website – Link "*Alphanumeric-Sender-ID-for-Twilio-Programmable-SMS*". Twilio link to the data underlying the Table stating "*Which Countries Support Alphanumeric Sender IDs? You can find out which countries support Alphanumeric Sender IDs on this page*."

6.180 This approach would be effective because it would block all SMS communications using Sender IDs (only the originating numbers would be displayed). In this way, fraudsters would be unable to pose as legitimate businesses by contacting consumers using Sender IDs.

III. Timelines

6.181 ComReg is of the view that a Sender ID Ban could be implemented within 3 months of any final Decision. This view is informed by:

- Discussions with industry stakeholders in the NCIT indicates that blocking SMS with Sender IDs could be implemented relatively straightforwardly with time mainly required to provide businesses notice that Sender IDs would no longer be available as a means to communicate; and
- The need for some amount of time to allow for the usual change management processes/practices within an operator environment.

6.182 Therefore, ComReg is of the view that the Sender ID Registry is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow this section.

9. Sender ID Registry – Full or partial

I. Description

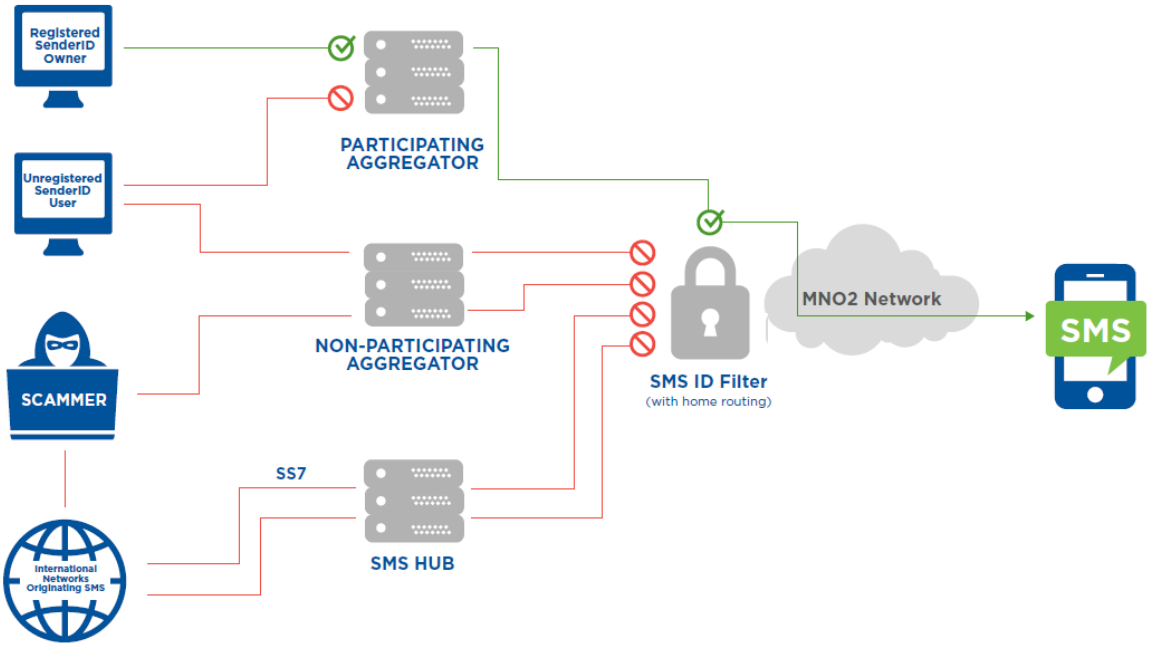
6.183 Sender ID may also be protected by securing the pathways by which SMS are transmitted. This would involve requiring senders and aggregators that send or carry messages containing any alphanumeric Sender ID ("Participating Aggregators") to follow a set of rules or a code of practice which requires that they register their Sender ID with ComReg or a registry operator and thereby authenticate the source of such messages. The MSPs[332] are then responsible for blocking any message bearing that Sender ID or potentially any unregistered Sender ID from any other source. To clarify, this would include blocking SMS that are spoofing Irish mobile numbers instead of using invalid Sender ID. This blocking is required to ensure the effectiveness of the Sender ID Registry and reduce the avenues for scammers for impersonating businesses/organisations or individuals. Absent such blocking scammers would move scams based on Sender ID to scams based on spoofing of Irish mobile numbers using SMS, significantly reducing the effectiveness of the Sender ID Registry.

6.184 A registry may be "full", encompassing all potential Sender IDs or "partial"

[332] For the avoidance of doubt, all participating MSPs are responsible for blocking all SMS containing a Sender ID that are not compliant with the technical specification.

whereby only the most important Sender IDs are covered. A key design parameter for any partial registry is whether SMS messages with unregistered Sender IDs are permitted or blocked automatically. Alternatively, such messages could be labelled, so as to inform consumers of the unverified source[333].

Figure 23: Full Sender ID Registry



II. Technical feasibility and effectiveness

6.185 The technical feasibility of this intervention concerns (i) the setting up and running of the registry by ComReg including the secure authentication of Sender ID owners (ii) the implementation of filtering functionality and relevant MNO connections by the Participating Aggregators and (iii) the technical requirement for operators to block any message spoofing Irish mobile numbers or bearing a Sender ID from any source other than approved Participating Aggregators connections according to the registry.

- In relation to (i), while the set-up and running costs associated with the SMS Registry are non-trivial (discussed below), there are no technical barriers preventing its implementation. Both full and partial SMS are technically feasible and have already been implemented in other

[333] The IMDA adopted this approach for its implementation period of its full registry to facilitate the transition.

jurisdictions. For example, ComReg notes that a SMS registry has been introduced in Italy[334], Singapore[335] and the Czech Republic.

- In relation to (ii), most aggregators operate in the global market and have implemented similar or identical functionality in other jurisdictions.
- In relation to (iii), blocking any message spoofing Irish mobile numbers or not on an authenticated list is straightforward for operators to implement and no technical issues should arise in its implementation.

6.186 In relation to its effectiveness, this intervention would be effective at reducing nuisance communications by requiring aggregators to register their Sender IDs to ensure that only legitimate businesses or organisations can use Sender IDs to send SMS to mobile users. For example, since the establishment of the Singapore Sender ID Registry ("SSIR") in March 2022:

- There has been a 64% reduction in scams through SMS from Q4 2021 to Q2 2022.
- Scam cases perpetrated via SMS now account for around 8% of scam reports in Q2 2022, down from 10% in 2021.[336]

6.187 It is no longer a voluntary regime, where organisations that wish to protect their Sender IDs ("Protected Sender IDs") could register with the SSIR. The full registration requirement took effect in Singapore on 31 January 2023 which will further increase its effectiveness by including all organisations that use Sender IDs.

6.188 Therefore, ComReg is of the view that the SMS Registry is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

6.189 While introducing a Sender ID registry takes considerable work on the part of the regulator (full or partial), ComReg is of the view that a partial or full Sender ID registry could be implemented within 12 months and 24 months of any final Decision. This view is informed by:

- Discussions with industry stakeholders and the IMDA that indicate that while introducing a Sender ID registry takes considerable work

[334] The rule requires that the senders of bulk SMS messages register their Sender ID with AGCOM, the Italian Communications Authority, as per AGCOM Resolution No. 42/13/CIR NRA entitled: Rules for Testing of Indicators for Alphanumeric identification of the Subject in the caller SMS/MMS used for Messaging Services. A Sender ID cannot be used if it has not been registered on AGCOM's database. https://alias.agcom.it/docs/guida_registrazione_alias.pdf
[335] https://www.sgnic.sg/smsregistry/overview
[336] Full Sender ID Registration to be required by January 2023 - Infocomm Media Development Authority (imda.gov.sg)

on the part of the regulator (full or partial) it is implementable within a reasonable timeframe, from 6 months in the case of a partial registry to 18-24 months in the case of a full registry.

- In relation to the full registry, 15-18 months accounts for the need for time to allow for are a number of parallel workstreams required to make SMS ID registry which are for:
    - ComReg – 6-12 months approvals, before implementation which could take another 12 months.
    - MNOs & participating aggregators - 6-12 months to set up system and conduct testing etc.
- The only benchmark for a full registry is Singapore, which suggests that 18 months is possible.
- The Plum Report[337] concludes that, subject to the dependencies[338] identified being delivered on schedule, the timeframe proposed by ComReg of 18 months from a final decision for implementation of the SMS Sender ID Registry is reasonable and achievable.

6.190 Therefore, ComReg is of the view that the Sender ID Registry is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow this section.

10. SMS Origin-Destination verification

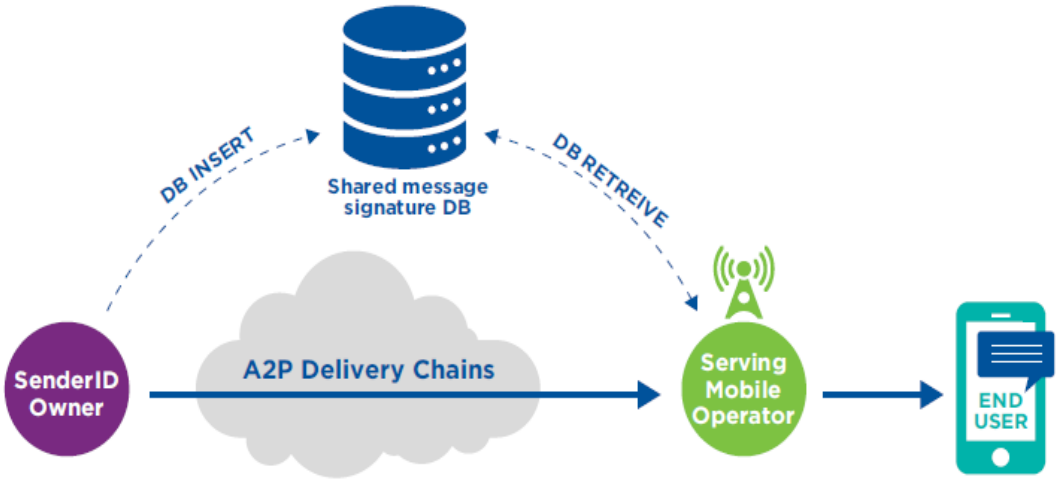
I. Description

6.191 One means of securing Sender ID would be through use of message verification codes. This solution would involve requiring aggregators, (the originator of an SMS bearing a protected Sender ID) to publish to a shared cloud-based database with a unique signature of the message, using a unique identifier known as a "hash value", before sending it down an unmodified, un-shortened delivery chain. A hash value is a very large number that's calculated through an algorithm, and that is associated with a particular piece of data (in this case some combination of the Originating Address, Destination Address and text message content). If the data is altered in any way, and the hash is recalculated, the resulting hash will be completely different. The concept of hashing is a cornerstone of IT security and is often used in digital forensic investigations to verify the authenticity of digital evidence for example.

[337] See Section 4.5 of Document 24/24b.
[338] Firstly, it will require the establishment of the Registry by ComReg. It also requires collaboration of SIDOs and aggregators, and integration of their systems.

6.192 Once the message arrives at the MNO for delivery, its signature would be freshly re-calculated and checked against the shared database. Only unmodified messages from sources with write-access to the shared database would pass this check, thereby allowing other messages to be discarded by the MNO before delivery.

Figure 24: SMS Origination-Destination verification



II. Technical feasibility and effectiveness

6.193 Several solution providers, and Italian NRA AGCOM, have posited this concept which is sometimes informally (and very loosely) referred to as "STIR/SHAKEN for SMS". However, this solution appears solely theoretical at present, as ComReg is unaware of any network applying this in a real-world setting. Therefore, it requires further studies to confirm its practicality and process design, and no existing implementations based on this approach exist today. ComReg is therefore of the view that it is prudent not to consider SMS Origin-Destination verification at this juncture but will continue to monitor its development.

6.194 In light of the above assessment, ComReg is of the view that SMS Origination-Destination verification is not a valid regulatory option for the purpose of this consultation and consequently is not considered further at this time.

11. SMS Scam Filter

I. Description

6.195 A SMS Scam Filter involves the use of advanced real time data analytics using Machine Learning and Artificial Intelligent techniques to detect and act

upon unusual patterns of content or hyperlinks in SMS messages. The deployment of SMS Scam Filter by Irish operators can be expected to significantly enhance and extend the range of protections afforded to Irish mobile telephone users beyond what is provided for by any other interventions focussed on 'static' Sender ID Spoofing[339]. As part of the NCIT process, ComReg and the NCIT identified SMS Scam Filters as a potential means of dynamically combatting scam texts, noting that fraudsters would over time find new means to execute scams and new pathways to contact Irish consumers.

6.196 The SMS Scam Filter scans the contents of the SMS by automatically scanning all text messages and filters those that are likely to contain malicious content. Absent this approach only a rudimentary evaluation of SMS is possible, and any such evaluation is inherently limited (e.g., the metadata). This data provides a far more limited indication of the nature of message content, being unable to identify let alone examine URLs and other signs of a scam.

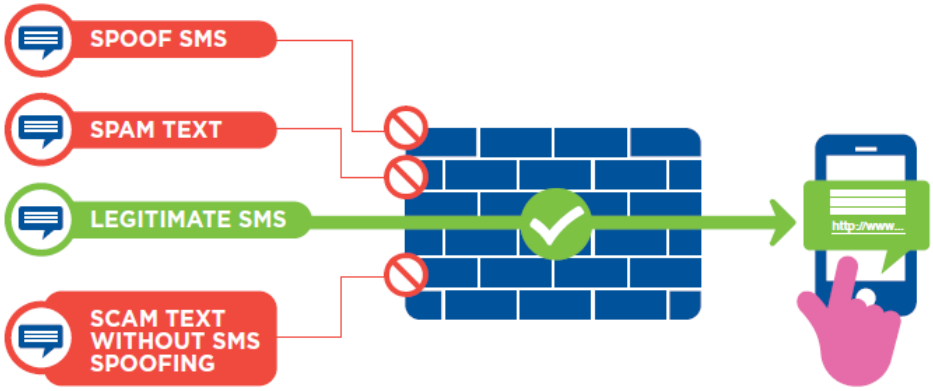
6.197 Any attempt to filter scams without content filtering is unlikely to be accurate and therefore ineffective in combatting scam texts. Indeed, numerous scam texts present in Ireland today may be far less likely to be identified and blocked absent content scanning (e.g., P2P scams such as the "Hi Mum" scam). Moreover, any filtering which excluded content would be easily overcome by fraudsters, as it would not identify suspicious contents and URLs that are highly indicative of a scam.

6.198 For these reasons, content filtering is pivotal to enabling the eventual deployment of a what could be termed a "SMS firewall", whereby all SMS messages routed to Irish consumers are analysed, classified and blocked where deemed likely to be scam. Therefore, throughout this Consultation, where ComReg refers to a SMS Scam Filter, this involves the use of content scanning.

6.199 ComReg notes that the SMS Scam Filter can be implemented in a number of ways as discussed in Paragraph 4.93 of Consultation 23/52. The form of Scam Filter considered in this Section and Consultation 23/52 is the '**All in' approach** whereby all mobile consumers are included by default. This is also the approach modelled by Europe Economics.

[339] In the context of SMS Scam Filter, a type 1 error (sometimes referred to as a 'false positive') occurs when the firewall mistakenly blocks a legitimate text, while a type 2 error (sometimes referred to as a 'false negative') occurs when the SMS Scam Filter fails to block a scam text. To minimize both false positives and false negatives, SMS Scam Filters use a combination of filtering techniques, which analyse various aspects of the message, such as the sender, content, behaviour, and most importantly the message content to determine whether it is legitimate or scam/fraudulent. However, by continuously updating their filtering rules and algorithms, a SMS Scam Filter can improve their accuracy and reduce the occurrence of both false positives and false negatives.

Figure 25: Graphical representation of SMS Scam Filter



II. Technical feasibility and effectiveness

6.200 SMS Scam Filters have been implemented by numerous operators and are readily available noting that multiple security solutions providers provide relevant software, installation, and training services. Under this intervention, the mobile operators would deploy an anti-scam filtering capability to scan for indicators of SMS scam and harmful content in real time on new or pre-existing SMS Scam Filters. The overall aim of this approach is to prevent the spread of malware via SMS by adding advanced SMS Scam Filter capabilities to the messaging domain.

6.201 Discussions with market players indicate that SMS Scam Filters are effective in blocking scam texts. SMS Scam Filters have been highly effective in other countries also which have seen a significant decline in the rates of scam texts. For example:

- Vodafone UK reported that daily average volumes of scam texts fell by 76% in December compared to May, with over 45 million phishing messages blocked since the end of August 2021.[340]
- Everything EveryWhere (EE) in the UK, blocking as many as two hundred million scam texts in a year, following the introduction of an artificial intelligence based "anti-scam filter" in 2021[341].
- In April 2022, Telstra in Australia[342] introduced the technology and had blocked over 185 million scam text messages in the three months to

[340] https://www.vodafone.co.uk/newscentre/news/vodafone-hammers-christmas-fraudsters-with-spam-reduction-december-2021
[341] https://newsroom.ee.co.uk/ee-takes-a-stand-against-scammers-with-latest-international-call-blocking-technology/
[342] Australian operators must "make best efforts to identify, trace, block and otherwise disrupt scam calls and scam SMS" messages, the new rules mandate, noting tell-tale signs of scams including blocked or invalid caller

July[343] and 225 million to December – around 775 malicious texts blocked every minute[344].

- In 2019, Optus deployed an SMS Scam Filter to combat the rise of SMS scams. Between 1 December 2020 and 31 March 2022, Optus blocked more than 232 million scam calls and now block an average of ten million texts every month.[345]
- Singtel, Starhub, and M1 in Singapore have implemented anti-scam filtering solutions in their networks from end-October 2022.

6.202 Therefore, ComReg is of the view that an 'All In SMS Scam Filter is likely to be technically feasible and effective at reducing nuisance communications.

6.203 However, the imposition of the SMS Scam Filter with content scanning as an "All-In" or an "Opt-Out" introduces potential legal issues on the protections of end user rights in relation to interception and data protection as provided in the ePrivacy directive and the GDPR. It is ComReg's understanding that a change to the current legislation to allow for this SMS Scam Filter is necessary.

6.204 Consequently, ComReg has engaged with its parent department, the DECC[346] with a view to providing such a legislative amendment in line with laws passed in other EU member states to enable such a SMS Scam Filter (e.g., Belgium and Poland). This would enable ComReg to meaningfully consult on implementing a SMS Scam Filter via an "All-In" approach, to maximise the benefits to consumers. At the time of publication, and notwithstanding continuing engagement with the DECC[347], there is as yet no confirmation that legislation will be introduced to support this SMS Scam.

6.205 In light of the above, ComReg is unable to proceed with this SMS Scam Filter intervention based on legislation at this time. Therefore, this SMS Scam Filter is not a regulatory option for the purpose of this RIA. Instead, ComReg will undertake a separate consultation on the SMS Scam Filter matter to explore the mechanisms available.

Conclusion.

---

line identification (CLI) numbers, calls that don't present call-back details to the destination network, and CLIs that don't correspond to the range allocated to a particular carrier.
https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf

[343] 185 million malicious texts blocked and counting (telstra.com.au)

[344] https://exchange.telstra.com.au/tag/scams/

[345] https://www.optus.com.au/connected/leaders-insights/optus-fight-against-fraud

[346] Indeed, ComReg is entirely dependent on a Government Department to progress this matter.

[347] ComReg continues to engage with DECC on this matter.

6.206 In summary, ComReg identified eleven potential interventions and following an assessment of the technical feasibility and effectiveness and timelines for implementation, seven interventions were identified for assessment in one or more RIAs.

Table 9: Assessment of long list of potential interventions

Interventions	Suitable?	Assessment
Do Not Originate	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Protected Numbers	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Fixed CLI Call Blocking	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Mobile CLI Call Blocking	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Voice Firewall	**Yes**	Technically feasible, as evidenced by its implementation by many MNOs. Many "off the shelf" solutions are available and are reported as being effective.
Stir/Shaken	**No**	Technically feasible, as shown by implementation in other jurisdictions. However, STIR/SHAKEN is unsuitable at present as • success depends on effective deployment in all countries; • few countries have implemented it; • there is no coordinated plan for its broad implementation; and • is relatively expensive relative to alternative interventions.
Shortening the chain	**No**	Technically feasible, as agreed by the NCIT. However, shortening the chain has proven challenging to implement due to high reliance on companies such as financial institutions which appear unable or unwilling to undertake necessary actions. As the success is entirely dependent on these companies, ComReg is not minded to pursue this intervention further.
Sender ID Ban	**Yes**	Technically feasible and would prevent Sender ID spoofing.
Sender ID Registry – Full or partial	**Yes**	Technically feasible, as evidenced by its implementation by other NRAs, notably in Singapore. The complexity and burden of intervention rests primarily with ComReg.
SMS Origin-Destination verification	**No**	Relies upon a hypothetical process which does not yet exist in practice. While this appears technically feasible, no examples exist in practice to confirm its feasibility and/or effectiveness. Would require a long lead in time to allow consideration (further research, feasibility studies, proof of concept etc.).
SMS Scam Filter	**No**	Technically feasible, as evidenced by its implementation in other jurisdictions. ID scanning was already agreed by NCIT members. Many "off the shelf" solutions are available and are reported as being effective. However, a legislative change by the Irish Government, similar to that in Belgium and Poland, so that it can be implemented via an "All-in". ComReg to consult on SMS Scam Filter separately.

6.207 Given the above, ComReg notes that there are seven valid regulatory options (summarised below) that are technically feasible and would likely be effective in reducing nuisance communications. These will now be assessed in the RIAs against ComReg's broader statutory objectives and duties including the obligation to promote competition and protect consumers. ComReg again

notes that it will be separately consulting on how best to introduce the SMS Scam Filter.

Table 10: Suitable interventions for this consultation

	Interventions
1.	DNO
2.	PN
3.	Fixed CLI Call Blocking
4.	Mobile CLI Call Blocking
5.	Voice Firewall
6.	Sender ID Blocking
7.	SMS Sender ID Registry (partial and full)

6.2.3 Grouping the interventions into RIAs and regulatory options

6.208 The inclusion of seven potential interventions poses a challenge because some of the interventions are mutually exclusive while others are interdependent. It is therefore necessary to group interventions and assess across one or more different RIAs. Within each RIA, ComReg must then determine what interventions constitute separate Regulatory Options and how those options relate to one another. In doing so, ComReg considers not only economic, but practical matters, such as the implementation of the interventions.

6.209 Key to this analysis is the impact of interventions on one another's effectiveness. The ability of fraudsters to switch between scams exploiting different vulnerabilities and 'gaps' leads to complementarities between interventions plugging those 'gaps. Therefore, interventions that plug gaps which are substitutable from the perspective of a fraudster are therefore complementary. In effect, such interventions support one another, as only if both interventions are introduced is any benefit achieved. Otherwise, fraudsters merely reroute their scams to reach Irish consumers exploiting other 'gaps'.

6.210 With that in mind, ComReg assesses the seven regulatory options in the following way (illustrated in Figure 26 below).

I. Firstly, interventions are divided between those targeting SMS and Voice scams. These interventions target a specific communications technology and are independent of each other (i.e., an SMS intervention does not directly target a scam conducted over only a

voice call and vice-a-versa) and, while multi-channel scams have been reported at some level, the majority of fraudsters are currently thought to face some barriers to switching between technologies.

II. Secondly, the SMS interventions are assessed as follows.

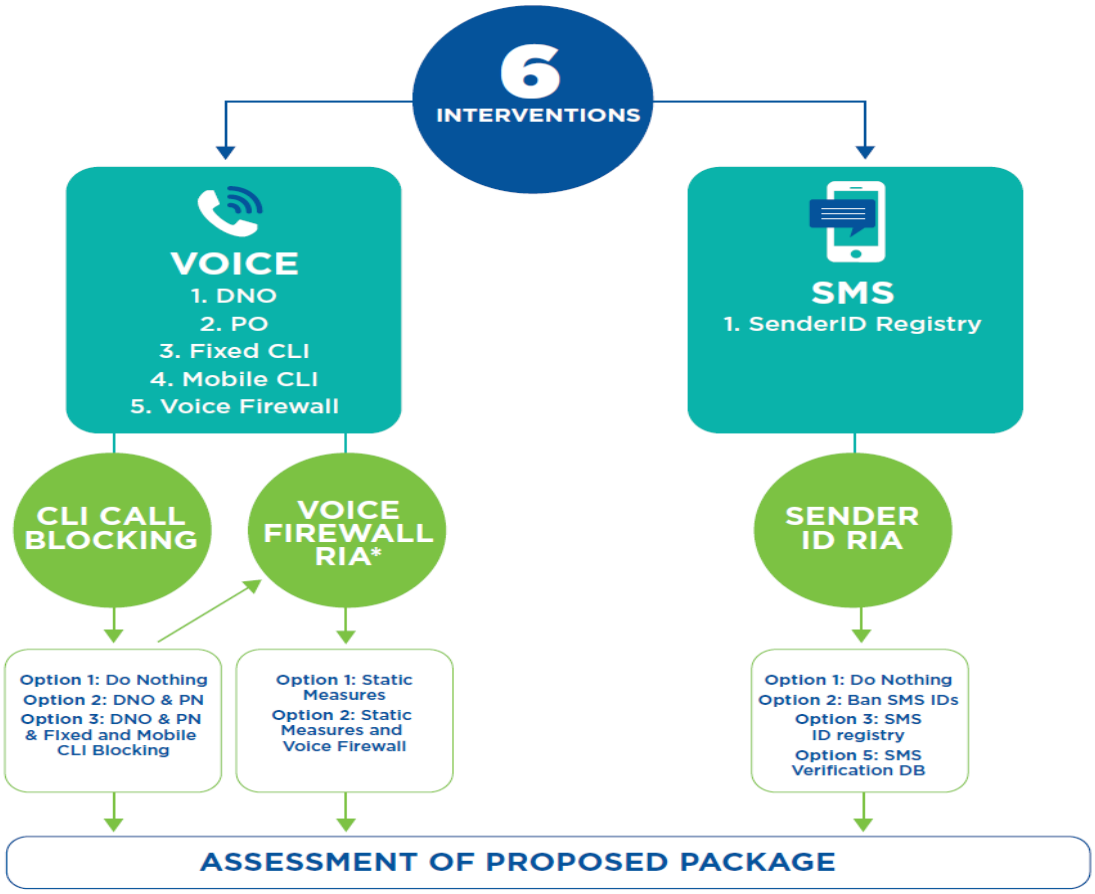
- Sender ID Blocking and the SMS Registry relate to regulating the use of Sender IDs and can be considered together in the '**Sender ID' RIA**. Only one preferred option is available because the interventions are substitutes for one another. (i.e., a SMS Registry and Sender ID Block cannot be implemented together.)[348]

III. Thirdly, the voice interventions are assessed as follows.

- All voice interventions besides the voice firewall relate to blocking the use of certain numbers and closing gaps in networks that fraudsters may target and switch between and are considered together in the **'CLI Call Blocking' RIA**. These interventions are complementary and therefore ComReg's overall preferred option may consist of one or more options.
- Within this RIA, the DNO and PN are assessed jointly, given the advanced state of implementation by operators. Similarly, Fixed and Mobile CLI Call Blocking are assessed jointly, given neither have been fully implemented to date and both are likely highly substitutable from the perspective of an international fraudster, which could merely switch from spoofing of fixed to mobile CLIs or vice versa in the face of one but not both interventions.
- The Voice Firewall is complementary to the other Voice interventions and targets all Voice calls. While the Voice Firewall may overlap to some degree[349] with other voice interventions, it targets scams through a different mechanism and achieves distinct benefits. This intervention is therefore considered separately in the '**Voice Firewall' RIA.**[350]

[348] The SMS Scam Filter is complementary to the Sender ID interventions and targets all SMS communications regardless of the format (i.e., whether an SMS has a Sender ID or otherwise). This intervention is considered separately in a forthcoming consultation.
[349] For example, a Voice Firewall could block scam calls prevented by DNO, Protected Numbers, and Fixed CLI Blocking interventions.
[350] In theory, SMS and Voice firewalls may prevent some scams prevented by the other interventions. However, firewalls would also block scams not targeted by static measures. Firewalls may therefore substitute or complement static interventions, depending which effect dominates. Which effect dominates depends on a number of factors such as whether any overlap in prevented scams is significant, whether the firewall would block all scams covered by static measures, and on how many further scams the firewall would block.

Figure 26: The assessment of the proposed interventions as regulatory options across the three RIAs



Implications of the Preferred Options on each RIA

6.211 The RIAs herein are not in any particular order and the issues they address can overlap. If an option in one draft RIA has or may have implications for any option in the other RIA, then this is considered.

6.2.4 Identification of stakeholders (Joint Step 3)

Identification of stakeholders

6.212 The focus of Step 3 is to assess the impact of the various regulatory options on stakeholders. A precursor to the subsequent steps in the RIA, therefore, is to identify the relevant stakeholders.

6.213 Stakeholders consist of three main groups:

- Consumers, which for the purposes of this RIA, relates primarily to residential consumers and businesses (the impact on consumers is assessed within each RIA under "*Impact on Consumers*");

- Impersonated businesses (e.g., An Post, DHL, AIB, BOI, PTSB, eFlow) and impersonated or otherwise affected Government agencies (e.g., HSE or An Garda Síochána); and
- Industry stakeholders (the impact on stakeholders is assessed within each RIA under "*Impact on Stakeholders*").

6.214 There are several key industry stakeholders in relation to the matters considered in this Chapter, namely operators that:

1. Originate Voice traffic[351];
2. Terminate Voice traffic[352];
3. Transit inbound traffic via an International Gateway[353];
4. Terminate SMS traffic[354];
5. SMS aggregators[355]; and
6. Other operators (Resellers, including MVNOs).

Determining which providers each intervention must apply.

6.215 The effectiveness of an intervention is a function of the operators that implement it – (i.e., if all operators implement each intervention, full coverage of effectiveness would be provided). However, it may not be proportionate to impose certain regulatory options and the associated costs on smaller operators with a small base of customers. In other cases, 100% coverage is essential over a reasonable period and required in order to prevent any gaps than might undermine the implementation of the interventions (s) on a national basis.

6.216 In this section, the interventions are assessed to determine which operators would be required to implement each of the interventions should one or more form part of ComReg's preferred option(s). This assessment is undertaken in three parts.

I. **First,** ComReg assesses which interventions require 100% coverage to achieve effectiveness, such that the intervention would apply to all relevant operators.

[351] Operators that originate Voice calls capable of connecting with public networks. This includes domestic voice operators as well as CSPs.
[352] Operators that terminate Voice calls capable of connecting with public networks.
[353] Operators that carry Voice calls from international PSTNs into the State.
[354] Operators that terminate SMS on public mobile networks.
[355] SMS aggregators that carry SMS traffic that terminates on public mobile networks in the State.

II. **Second,** ComReg assesses how to apply the interventions in a manner that achieves the greatest coverage while being proportionate in their implementation.

III. **Third,** ComReg provides information on the number and type of operators that would be required to implement each intervention.

I. Which interventions require 100% coverage such that the intervention would apply to all relevant operators.

6.217 The implications for each type of traffic and intervention are shown in Table 11. below. A key point is that complete coverage is required for any intervention targeting call origination or international transit. Any 'gap', or uncovered operator that handles this traffic could potentially undermine the entire intervention as fraudsters would likely exploit that 'gap' to potentially reach all Irish consumers. Indeed, this may happen even without conscious switching by the fraudster due to inter-operator agreements on automatic call rerouting. Therefore, it is critical that interventions targeting call origination or international transit (i.e., DNO/PN, Fixed and Mobile CLI) be applied to all operators that service this traffic.

Table 11: Coverage required to ensure the effectiveness of each intervention

Traffic Type	Intervention	Applies to operators that...	Coverage required for effectiveness
Origination	**DNO & PN**	Originate Voice calls capable of connecting with public networks	**Complete coverage** - a single gap can be used to reach many Irish consumers. Exacerbated by "least-cost routing".
International	**DNO & PN Fixed & Mobile CLI Call Blocking**	Transit Int' voice traffic (IGOs)	**Complete coverage** - a single gap can be used to reach many Irish consumers. Exacerbated by automatic call re-routing agreements
Termination	**Voice Firewall**	Terminate voice calls on public networks	**Near complete coverage –** a single gap only allows for scams to reach a limited number of subscribers on its own network. (e.g., covering 90% of subs protects 90% of subs).
	Sender ID Ban Sender ID Registry SMS Content Scanning	Terminate SMS on public networks	**Near complete coverage –** as a single operator only allows for scams to reach subscribers on its own network. (e.g., covering 90% of subs protects 90% of subs).

Phase 1 of Mobile CLI Call Blocking

6.218 Phase 1 of Mobile CLI Call Blocking, which relies on IGOs checking a mobile number roaming status by using a MAP protocol will only be applied for a period of 18 months before the implementation of Phase 2 of Mobile CLI Call Blocking (which relies on a shared roamer database). Phase 1 was always envisaged as a measure aimed at combatting scam calls before Phase 2 begins.

6.219 In Consultation 23/52, ComReg had envisaged that Phase 1 would be applied by all IGOs, with larger IGOs facilitating roamer check for smaller IGOs that could not achieve MAP capabilities in 6 months. This would allow for 100% coverage to be obtained during Phase I. ComReg noted this was reliant on operators making sufficient progress in implementing inter-operator processes, having noted in Consultation 23/52 that the proposed implementation of Phase 1 envisaged in 23/52 was dependent on voluntary cooperation between industry players.

6.220 However, based on the submissions received to Consultation 23/52 and bilateral meetings with operators, ComReg has now formed the view that some modifications to the implementation of Phase 1 are required. Phase 1, as previously proposed, could provide larger IGOs significant bargaining power over smaller IGOs and could potentially result in excessive costs or harm to competition because the cost to a smaller IGO of not having its traffic scrubbed potentially could be very high (i.e., a smaller IGO would not be able to route international traffic). Furthermore, in circumstances where a smaller IGO decided not to carry the traffic, consumers would likely be harmed if that traffic from abroad was not carried or was blocked.

6.221 ComReg now includes a financial threshold to identify which operators must implement Phase 1. Implementation of Phase 1 is only being required of IGOs with revenues from the provision of ECS in the State of €50,000,000 in 2023[356]. The use of this financial threshold is based on the €50 million value already set out in Commission Recommendation (2003/361/EC) which is the instrument the Commission currently uses to define small and medium-sized enterprises (i.e. firms below €50 million would be classified as a SME). This approach is appropriate because it identifies the larger IGOs that are able to implement Phase 1 from the smaller IGOs that are unable to utilise MAP or achieve this capability through investment in a short period of time (six months)[357]. The impact of this change is that ComReg will not now require Phase 1 to be implemented by smaller IGOs that are unable to handle MAP queries without the assistance of a larger IGO[358].

6.222 Importantly, this does not alter ComReg's view that 100% coverage of mobile CLI is required for any intervention targeting call origination or international transit. Rather, this modification is time bound given that Phase 1 only applies

[356] To provide regulatory certainty, ComReg fixes the threshold to revenues in 2023. Otherwise any IGO that exceeded the threshold in 2024 but not in 2023, could be required to participate in the blocking for the remaining period of Phase 1, with little time to prepare.
[357] ComReg also notes that such an investment if it were made by smaller IGOs would likely be inefficient because Phase 1 only applies only for a 18-month period, beginning 6 months after the publication of the DIs.
[358] ComReg is unaware of any reason to extend this exemption to MSPs, noting that MSPs would have the required technical expertise and familiarity with MSPs processes to enable this. Moreover any such exemption would reduce the impact of the blocking undertaken by the Phase 1 IGOs.

for a 18-month period, beginning six months after the Decision. At the end of this period, Phase 2 will achieve 100% coverage across all relevant operators.

6.223 ComReg considers that this approach balances the need to take immediate action to prevent scams, noting that most of the larger IGOs have already made significant progress in implementing Phase 1, against promoting competition. ComReg has only considered this approach as the resulting 'gap' will be closed within a period of 18 months – at which time Phase 2 will result in 100% of international voice transit being screened for mobile roaming status.

Table 12: The total number of minutes, market shares and total revenues of identified IGOs.

IGO	Minutes		Revenues from QKDR
	Total	%	Total
Eircom	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Colt	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Virgin Media Ireland	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
BT Ireland	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Three	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Vodafone	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Verizon Ireland	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Voxbone SA	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Magrathea Telecommunications	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Viatel Group	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Orange	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Regional Broadband	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Carrier2.network	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]
Magnet Networks Limited	[✂[redacted]✂]	[✂[redacted]✂]%	[✂[redacted]✂]

II. What approach best provides the greatest coverage for all remaining interventions.

6.224 The remaining interventions all concern terminating traffic (or combinations of originating and terminating traffic) and that such interventions (i.e., all SMS interventions and the Voice Firewall) may:

- be implemented by placing the obligation on either the service providers (e.g., MVNO and/or MNO) or the network operator itself (e.g., MNO); and
- achieve broadly the same effect by applying such interventions on all operators or only the largest, as such interventions are effective in proportion to its coverage (i.e., the number of consumers that receive

its protection) because fraudsters cannot find an alternative network to connect to a consumer's device and thereby reach that consumer.

6.225 ComReg considers this further below.

Network Operators

6.226 ComReg proposes to place the responsibility primarily on the network operators to ensure that all relevant traffic (including third party traffic e.g., MVNOs) terminating on its network has been subject to each of the relevant interventions outlined above if adopted (i.e., Voice Firewall, Sender ID Ban, Sender ID Registry), where technically feasible.

6.227 ComReg understands that this is only technically feasible where the network operator operates the core network elements on behalf of these virtual operators. For example, a network operator is capable of applying a Voice Firewall to the traffic of those Resellers or virtual operators that rely upon it for their core of their network (e.g., in the case of a MVNO this refers to Gateway Mobile Switching Centre (GMSC) or Home Location Register (HLR)). A network is not required to implement the intervention on behalf of Virtual operators with independent core network or provided by third parties.

6.228 Notably, respondents to Consultation 23/52 have not raised any concerns in relation to this approach.

Virtual Network Operators with independent core network

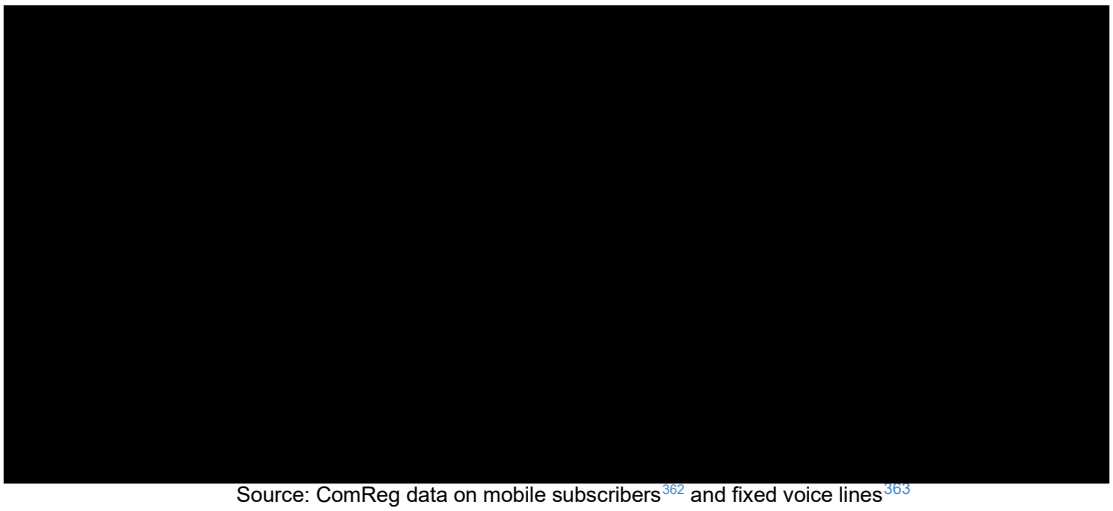
6.229 A number of virtual operators do not rely upon their host network operators[359] for core network services, instead relying on third party service providers.[360]. These virtual operators would also be required to apply these interventions to the traffic[361] (subject to reaching the subscriber cut-off, see below).

Smaller networks or operators

6.230 There are many public Voice network operators across both fixed and mobile in Ireland, of varying sizes, as shown below.

[359] In the case of MVNOs, the host network is the provider of RAN services.
[360] Specifically, ComReg understands from discussions with operators that [✂ ✂].
[361] In the case of MSPs, full MVNOs have their own network-switching infrastructure and negotiate their own interconnect agreements and generate revenues not only from outgoing traffic, but also for incoming traffic. Therefore, distinguishing these operators from 'lighter' MVNOs without any core elements is appropriate.

Figure 27: Voice capable subscriptions and lines on public networks, at a wholesale level, 2022 Q4 [✂]



Source: ComReg data on mobile subscribers[362] and fixed voice lines[363]

6.231 ComReg considers that requiring all such networks to implement these measures may be disproportionate, provide little additional benefit while imposing a large cost on smaller firms, potentially distorting competition. ComReg is therefore of the view that it would be appropriate to provide a threshold for the mandate of these interventions to account for the smaller fixed networks providing Voice services that would otherwise be included.

6.232 ComReg considers that a cut-off of approximately 5% (roughly 270,000 subscribers for SMS and 330,000 subscribers for Voice[364]) appears appropriate as this covers most Voice subscriptions including landlines while not covering overly small networks, noting the figures in Figure 27 above. In this way, the interventions would only apply to MSPs that are above this threshold. ComReg is satisfied that this approach is proportionate as it only includes sufficiently large operators, while ensuring the majority of consumers benefit from the protection of Voice Firewall.

[362] Fixed Voice is measured using lines, both residential and non-residential, as a proxy for subscribers as this is the most appropriate data available. ComReg considers this a conservative estimate of end-users for landlines, noting that the true number of users may be higher in the case of non-residential lines. This data is the best data available to ComReg for attributing landlines at a wholesale level. ComReg will update this data where an operator can demonstrate with adequate evidence that a sufficient number of attributable Fixed Voice Lines on their network are either a) inactive or b) account for a negligible share of Fixed Voice.

[363] In Consultation 23/52, ComReg cited specific numbers of subscribers in the Draft Decision Instruments for these interventions – 270,000 for SMS and 330,000 for Voice. Absolute values were provided to give operators greater legal certainty. These figures have now been consulted upon with industry, over a consultation period which lasted 10 weeks. To update the value for the either threshold now could undermine regulatory certainty and ComReg therefore does not update these figures using the latest data available.

[364] These figures are rounded to the nearest multiple of 10,000 for convenience. These figures are based on subscriptions that are attributable at a wholesale level. The effect on the cut-off of using the QKDR data for each data is marginal (<15,000 subscribers at the 5% cut-off). No firms are affected by this, noting that all operators that exceed the higher cut-off by over 100,000 subscriptions/lines.

Table 13: The coverage achieved and impacted companies for different cut-offs.

Technology	Cut-off (subs/lines)	Affected Companies	Coverage Achieved[365]
Sender ID Registry	>5% (>270,000)	MNOs	94% subscribers and 97% of SMS traffic
	>1% (>54,000)	MNOs and MVNEs of [✂ ✂]	100% of subscribers and SMS traffic
Voice Firewall	5% (>330,000)	MNOs (incl. Eircom and Vodafone Fixed Voice), Virgin (incl UPC)	94% of Voice subscribers • **Mobile** – 97% of subscribers • **Fixed** – 83% of subscribers
	>1% (>66,000)	MNOs (incl. Eircom and Vodafone Fixed Voice), and MVNEs of [✂ ✂]	98% of Voice subscribers • **Mobile** -99% of subscribers • **Fixed** -95% of subscribers

Source: ComReg data on mobile subscribers[366] and fixed voice lines[367]. Preferred approach highlighted in yellow.

6.233 In relation to virtual operators that are not captured by the 5% measure above (either directly or via their host network), ComReg notes that there remains scope for these entities to implement such interventions voluntarily (e.g., voice firewall). ComReg has had discussions with a number of vendors which suggests that there are a variety of business models available.

6.234 ComReg considers this approach is appropriate and proportionate for the following reasons.

I. The costs imposed on network operators from implementing these interventions (e.g., voice firewall) on behalf of its virtual operators that do not own their own core infrastructure is likely to be small and limited to the higher throughput that would result from servicing the virtual operators' traffic. For example, MVNOs traffic accounts for less than [✂ ✂]% of all mobile traffic (and no more than [✂ ✂]% for any one operator) - given the likely economies of scale associated with operating any of the interventions targeting terminating traffic, the marginal costs of servicing a virtual operators traffic (on the same core) are likely to be small and less than what would be the case if such virtual operators had to implement such an intervention themselves. It is therefore appropriate that the host

[365] This table present coverage in terms of subscribers not traffic, as information on traffic is not readily available at a network level for Fixed. ComReg considers this a conservative but appropriate approach as while mobile generates more traffic any device that could be answered may be used to reach a end-user. This includes the subscribers of [✂ ✂] as ComReg understands from discussions with both [✂ ✂] core network in the next [✂ ✂] months. Should this migration not proceed this MVNO would be treated as a separate entity and therefore [✂ ✂].

[366] This is mobile subscriptions excl. MBB and M2M.

[367] Fixed Voice is measured using lines, both residential and non-residential, as a proxy for subscribers as this is the most appropriate data available. ComReg considers this a conservative estimate of end-users for landlines, noting that the true number of users may be higher in the case of non-residential lines.

operator bears the costs associated with this traffic. ComReg also considers that implementing these interventions at a network level better protects a wider range of consumers in a more proportionate manner because networks necessarily carry a greater level of subscribers and traffic than service providers.

II. Extending the obligation on network operators to include all virtual operators regardless of their network infrastructure would likely impose disproportionate costs on the network operators (e.g., MNOs) and seems unlikely to be proportionate. The network architecture associated with virtual operators that build their own core elements (including network-switching infrastructure) is different to those that do not own any core network infrastructure (i.e., network operator operates the core on its behalf), and traffic cannot be serviced in the same way without imposing additional costs on network operators. In any event, such an approach would create obvious issues for the virtual operator retaining the independence of its core network (if an MNO for example was filtering traffic on its core network) and the advantages that such architecture brings. Such an approach would also not promote infrastructure-based competition in line with ComReg's statutory objectives.

III. The thresholds discussed above prevents this measure from being disproportionately costly to smaller network and virtual network operators.

6.235 ComReg considers that applying a Voice Firewall and a Sender ID registry only to networks with at least 5% of all Voice capable subscriptions or SMS subscribers respectively would achieve significant benefits and ensure that such a measure is applied in the least onerous manner. Based on this threshold, the Sender ID Registry would apply to Three, Vodafone and Eir (incl. Eircom). ComReg estimates that such measures (and depending on technical feasibility as described above) would cover:

- 100% of SMS traffic on public networks[368]; and
- over 90% of Voice subscriptions on public networks covering approximately:
    - over 95% voice capable mobile subscriptions; and
    - over 80% of voice capable landlines lines.

[368] Noting that any MSP that is not a Participating MSP will no longer be permitted deliver a SMS with a SenderID to an Irish number.

III. To which firms would each intervention apply?

6.236 Given the above, ComReg now summarises what interventions would potentially apply to whom.

6.237 Not all operators carry all types of traffic (e.g., SMS or Voice), therefore which operators an intervention applies to depends primarily on the type of traffic carried on its network. To identify what firms carry the relevant traffic, ComReg has analysed the following datasets:

- The Electronic Register Of Authorised Undertakings ("ERAU")[369];
- The Telephone Numbering database[370]; and
- The QKDR database[371].

6.238 ComReg has combined these datasets to identify what firms each intervention is likely to apply to - the outcomes of which are summarised in Table 14 below. This has in turn informed Europe Economics' assessment of the aggregator and average cost of interventions to industry stakeholders contained within the RIAs.

Table 14: Identifying the companies to which each intervention applies.

Technology	Interventions	Identified firms[372]
Voice	**DNO List & PN List**	**Originators of Voice traffic: approximately** • c. 30 firms identified from the Numbering database. **IGOs (subset of above)** • 14 identified (from the IGO RFI)
	Fixed CLI Call Blocking & Mobile CLI Phase 2	**IGOs:** • 14 identified (from the IGO RFI)
	Mobile CLI Call Blocking Phase 1	**IGOs:** • 5 identified (from the IGO RFI and QKDR revenues)
	Voice Firewall	**Network with >5% of Voice-capable subscriptions and lines on public networks:** • Three, Vodafone, Eir (incl. Eircom), Virgin (incl. its Fixed Voice)
SMS	**Sender ID Ban**	**Filtering by MSPs** **Network with >5% of SMS subscriptions on public networks:** • Three, Vodafone and Eir **SMS aggregators** • All participating aggregators
	Sender ID Registry *partial or full*	

[369] The ERAU is a register which captures all providers of ECS services, managed by ComReg.
[370] The numbering database contains information on all operators assigned telephone numbers by ComReg.
[371] The QKDR compiles data provided to ComReg by ECS with a turnover of over €500,000.
[372] It should be noted that these are simply firms ComReg has identified as being likely to be required to implement specific interventions. It is the responsibility of all ECS providers to ensure their compliance with their legal requirements.

6.3 CLI Call Blocking RIA

6.240 This Section sets out the CLI Call Blocking RIA.

6.3.1 Policy Issues

6.241 ComReg previously noted, and discussed in detail, the two overarching policy issues relevant to all RIAs.

i. Reducing the harm to consumers and businesses from scam calls; and

ii. Protecting and renewing trust in ECS Networks and Services.

6.242 ComReg is mindful of these policy issues in determining its preferred option for this RIA. The remainder of this section further defines these main policy issues as they relate to this CLI Call Blocking RIA in order to appropriately assess the available regulatory options.

6.243 Overseas fraudsters often use inexpensive and readily available technology to present calls with maliciously spoofed Irish CLIs to display a number more familiar or recognisable to the person receiving the call. The numbers which fraudsters use to defraud people include:

- Mobile numbers where consumers may recognise the mobile prefix (e.g., 08x) and assume someone (whether for business or social purposes) who is not on their contacts is trying to reach them.
- Geographic numbers (e.g., 061 for Limerick, 043 for Longford) where consumers may recognise their local numbers and assume a person or business is trying to contact them from a fixed line number.
- Non-geographic numbers (e.g., 1800 or 0818) where consumers assume that a business (e.g., bank or credit card company) is trying to contact them using a freephone or 0818 number.

6.244 Both domestic and overseas fraudsters may present calls with maliciously spoofed fixed or mobile CLIs to display a number of a trusted or well-known organisation to the person receiving the call. The numbers that fraudsters often use includes the in-bound only numbers of:

- Irish companies (e.g., banks)
- Irish government agencies (e.g., Department of Social Welfare)
- Postal and delivery service providers (e.g., An Post)

- Other legitimate organisations (e.g., NGOs)

6.245 Consumers have a high level of awareness of these numbers[373] and fraudsters take advantage of this by spoofing such numbers which makes it more likely that the call would be answered. This can result in significant harms to consumers either through fraud taking place and/or through annoyance or distress from receiving calls). The ensuing objectionable experiences can in turn lead to Irish consumers no longer trusting the number displayed on their phone when it rings.

6.246 The spoofing of numbers primarily stems from international networks which present as an Irish mobile or fixed CLI (e.g., appear as a valid mobile or geographic range). There are also some numbers which should not appear as a CLI because they are either unassigned to any operator or are outbound calls from trusted numbers which are used for inbound calls only (e.g., a bank's non-geographic number).

6.247 With that in mind, the main policy issue associated with this RIA is to reduce the harm from scam calls on consumers and trust in ECN by:

I. identifying and blocking calls originating from international networks and presenting with Irish CLIs; and

II. identifying and blocking calls which should not appear as a CLI to consumers (regardless of where they are originated) because they are either unallocated or inbound only numbers.

6.248 The above two policy questions are related noting that the preferred option could comprise one or more of the available options.

6.3.2 Regulatory Options (Steps 1 & 2)

6.249 As outlined in Section 5.2.2, the available interventions for the purpose of this RIA are:

- **Option 1** – No new regulatory measure(s).
  - This approach would maintain the status quo position with no intervention(s) proposed by ComReg.
- **Option 2** – Implement the DNO and PN intervention.
  - This approach would implement DNO and PN intervention as outlined in the technical specification.

[373] See Document 21/82b and Document 17/70b

- **Option 3** – Implement Fixed and Mobile CLI Call Blocking in addition to DNO and PN.
  - This approach would implement DNO, PN, Fixed and Mobile CLI Call Blocking as outlined in the technical specifications. Fixed and Mobile CLI Call Blocking are assessed together because the implementation of one but not the other could not achieve the stated policy objectives for both fixed and mobile calls.

6.3.3 Impact on industry stakeholders, consumers, and competition (Steps 3 & 4)

I. Impact on consumers

6.250 This section provides information on the impacts on consumers arising from the regulatory options outlined above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the direct impacts on consumers arising from the regulatory option is assessed (e.g., the reduction in harm due to fraud and time lost to scam calls etc); and

II. Second, other relevant impacts (e.g., impact on trust) arising from the implementation of the regulatory options are assessed.

Option 1: Do Nothing

I. Direct impacts

6.251 Under Option 1, each of the harms from scam calls are likely to remain high. There are numerous factors that could cause this harm to increase (such as fraudsters increasing the rate of scams, or it is becoming more difficult to perpetrate scams in other jurisdictions and relatively easier in Ireland) or decrease because consumers adapt their behaviour towards scams and become less susceptible to fraud)[374].

[374] Europe Economics have estimated how this harm could potentially develop, depending on which factors dominate.

6.252 However, fraudsters are dynamic and adapt their tactics with new forms of scams emerging. ComReg notes that the harm is more likely to increase as the fraudsters become ever more sophisticated even where consumers adapt to older scams[375]. Further, as noted earlier, other English-speaking countries are already implementing various interventions (e.g., CLI Call Blocking and voice firewalls) and fraudsters would inevitably direct more scams towards unprotected Irish consumers under this Option.

6.253 As described in Section 6.2.1[376], Europe Economics estimates that the current level of harm to Irish consumers and businesses arising from scam calls is approximately €187 million per annum[377]. Therefore, under Option 1 the harm to society is likely to remain substantial and at least at these levels.

II. Other Impacts

Trust in voice calls

6.254 There is strong evidence to suggest that until recently Irish consumers had a high degree of trust in Numbers. For example, in relation to Geographic Numbers, consumers had relied to a large degree on the information provided by the number (e.g., the geographic area and the CLIs which consumers see upon receipt of a call). In 2021 (ComReg 21/28b[378]) (the "GN Survey"), B&A found that Irish consumers understood and desired geographic numbers to provide information on the geographic location of the call. For example:

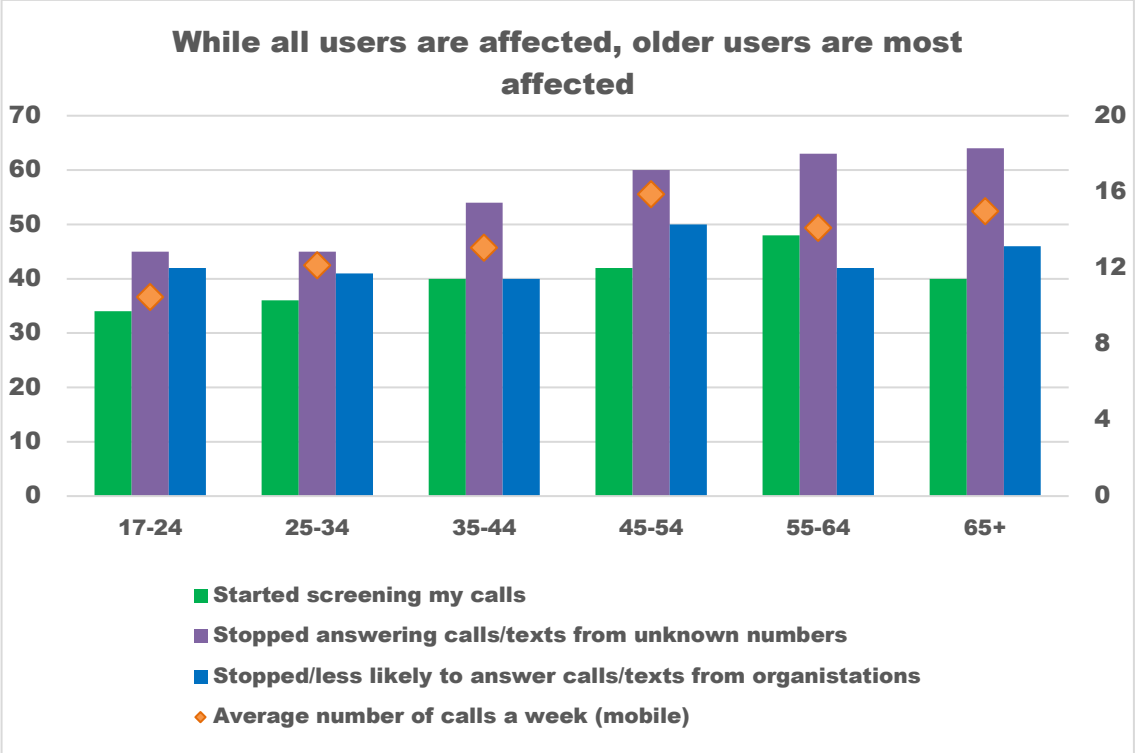
- 83% of Irish consumers know their local area code[379].
- 81% of Irish consumers are satisfied that a household or business must have a physical presence in an area to avail of its area code.
- 74% of Irish consumers consider it important to know the geographic location of the number when they are called[380].
- 72% of Irish consumers trust that a call with an Irish CLI is from the geographic location associated with that number[381].
- Around 60% of Irish consumers will answer a call from an Irish CLI that is not a regular contact, if it has geographic number[382]. This makes

[375] For example, Cyber attackers are diversifying their tactics and finding new ways of scamming customers. As outlined in: HP Wolf Security Threat Insights Report Q4 2022 | HP Wolf Security
[376] See also Section 4.4 – 4.6 of the Europe Economics Report.
[377] Comprising €116 million (consumers) and €71 million (businesses)
[378] B&A "*Geographic Numbering Survey: Quantitative report*" Link
[379] In response to the Question 8 "*Do you know the Area Code associated with Geographic Numbers in your area (i.e. your local area code)?*"
[380] In response to the Question 13 "*When receiving a call, how important is it to know the geographic location of a number calling you (i.e. where the caller is calling from)?*"
[381] In response to the Question 19 "*To what extent do you agree or disagree with the following statement (I trust that the caller is making the call from the Geographic location associated with the number)*"

voice calls a reliable means of contacting the majority of Irish consumers, which is valuable to businesses that need to contact consumers for their business.

6.255 Scam calls have clearly damaged the trust consumers place in the authenticity of Voice calls from consumers and organisations. Many consumers have stopped answering or screening calls, or otherwise reducing their use of Voice calls as illustrated in Figure 28. This is particularly true of older users, who happen to be more dependent on Voice calls.

Figure 28: Loss of trust in calls as a result of scams, by age[383]



Source: ComReg analysis of data from the B&A Consumer Survey

6.256 As outlined above, nuisance communications create a series of distinct effects that reduce trust and threaten the efficient and effective functioning of the numbering platform. ComReg now assesses each of these effects (i.e., contagion, call reduction, feedback, and social effects) with respect to voice calls under Option 1.

Contagion

[382] In response to the Question 16 "*How likely are you to answer a call from a Geographic Number that is not one of your regular contacts*?"
[383] In relation to Question 40c "*Has your experience of scam calls and texts affected your trust in communications from the organisations that provide the aforementioned services?"* and Question 38 "*In relation to your awareness of scam calls and texts, has any of the following happened?"* Average number of calls is displayed on the right axis.

6.257 Contagion refers to the uncertainty caused by the prevalence of scam calls and/or a previous scam call experience which may infect a consumers' beliefs across all calls regardless of who is calling. Under Option 1, it is likely that contagion would spread as consumers become increasingly suspicious about the calls they receive. There are already a number of clear examples of contagion across the numbering platform. For example:

- 70% of consumers are concerned or very concerned about scam calls.[384] Those who have experienced a financial loss have a heightened level of being 'very concerned'.
- 60% of businesses are concerned or very concerned about scam calls[385], with businesses that use mobile numbers to communicate also showing higher levels of concern.

6.258 ComReg is of the view that the numbering platform already suffers from contagion and that this would likely increase under Option 1.

Call reduction

6.259 Call reduction refers to reductions in the volume of calls made and received over the numbering platform due to contagion. Contagion is causing consumers to accept less calls due to the fear of being scammed. Notably, consumers are now not accepting calls from people they may know or from business or public bodies providing services that consumers would ordinarily be interested in (e.g., deliveries, hospital appointments etc). This is because fraudsters primarily impersonate organisations that a consumer would likely be interested in. This reduces the volume of calls received over the numbering platform as consumers decide to answer less and less calls. For example:

- 56% of consumers have stopped answering calls from unknown numbers due to the prevalence of scam calls[386]; and
- 43% stopped answering calls/texts that may be from businesses or government agency[387] due to the prevalence of scam calls.

6.260 ComReg is of the view that there is clear evidence that nuisance communications are supressing the volume of voice calls to the detriment of consumers and businesses.

Feedback effect

[384] B&A Consumer Survey, Slide 12
[385] B&A Business Survey, slide 11
[386] B&A Consumer Survey, slide 31
[387] B&A Consumer Survey, slide 31

6.261 The feedback effect refers to the reduced incentives for people and organisations to use voice calls because of the reduction in people answering calls. Businesses may decide not to provide services over the numbering platform because of the low answer rate (i.e., the call reduction creates a feedback effect). Businesses and consumers would reduce their reliance on Voice calls given the level of harm being borne by Irish consumers and businesses. In particular, businesses are likely to switch to alternative means of contacting consumers even though their preference may be to contact consumers using voice calls on public networks. For example, 39% of businesses have already made changes to how they communicate with consumers.[388]

6.262 These changes often avoid the use of public phone networks and rely more on an alternative means of communications (e.g., email, secure messages, online portal etc.).[389] Notably, 23% of consumers already ignore calls purporting to be from organisations due to scam calls. While only a small share of consumers has moved to alternative instant messaging platforms as a result of scams to date, this figure is likely to grow as the harms persist and such consumers may not transition back to traditional voice.

6.263 Critically, any movement to alternative platforms would have occurred due to nuisance communications and the misuse of the numbering platform rather than any underlying preference for those alternatives. The numbering platform needs to compete with alternative ways of delivering services to some or all users, such as web-based messaging, and social media; however, such choices should be made neutrally, rather than because the numbering platform has been compromised in some manner. Any move to alternatives should ensue from informed decisions made by consumers and businesses, rather than being the result of having to deal with nuisance communications, as is currently the case.

6.264 ComReg is of the view that there is clear evidence of a feedback effect with organisations particularly affected as they consider moving to alternative ways of contacting consumers.

Social effect

6.265 The social effect arises in cases where some services that would normally be provided over voice switch to alternative platforms (due to prevalence of nuisance communications) that are not readily available to some social groups. People's reluctance to engage with voice calls due to fear of being scammed could have a particularly negative impact on vulnerable consumers

[388] B&A Business Survey, slide 23.
[389] B&A Business Survey, slide 23.

for whom voice services provide important access to essential services (e.g., healthcare, social security). The social effects of reduced voice calls resulting from call avoidance can be very detrimental for those who may be dependent on one or more social services.

6.266 For example, older people are more likely to be affected by people and organisations (in particular) moving to alternatives because older people use these alternative services at a much lower rate. The use that over 65s make of alternative voice-calling platforms (e.g., WhatsApp, video calls, social media) is three times lower than the average person and up to 6 times lower compared to younger groups. The over 65s are also the only group currently using voice calls primarily using traditional voice calls. They use voice calls three times as much as other alternatives to voice (e.g., video calls, VOIP calls etc).

6.267 Older people are also more likely to be concerned or very concerned about scam calls (84%)[390] and are the most likely to stop answering unknown calls, with 64% of over 65s not answering unknown numbers[391]. Many organisational numbers are unlikely to be known to older people (or consumers generally for that matter) and the most commonly impersonated organisations are those which older people are most likely to require (e.g., banks, HSE, delivery companies and other public bodies).

6.268 For example, several banks have outlined to ComReg the potentially serious repercussions of this lack in trust in calls such as being unable to assist older customers with issues relating to their account through alternative means (e.g., online or chat). Similarly, a 75-year-old person who primarily relies on voice communications may be greatly impacted if he/she is less contactable by their healthcare providers. Indeed, ComReg has evidence from the HSE of such situations arising in practice. The HSE has outlined to ComReg the potentially serious repercussions of this lack of trust in calls (See Section 6.2.1). It is for such reasons that the possible impacts of reduced trust on more vulnerable consumers must be carefully considered.

6.269 ComReg is of the view that that nuisance communications are having detrimental social impacts.

6.270 Overall, consumers are therefore unlikely to prefer Option 1 because it would perpetuate the harm caused by nuisance communications and would be highly unlikely to restore any trust to the numbering platform.

Option 2: DNO and PN

[390] B&A Consumer Survey responses to Q.5a "*How concerned are you about … Scam Calls*"
[391] B&A Consumer Survey, slide 32

I. Direct impacts

6.271 Under Option 2, the DNO and PN would directly reduce the harm from scam calls in two ways.

- First, Option 2 stops fraudsters spoofing business numbers that are not used for inbound calls by preventing consumers receiving calls from such numbers. ComReg understands from An Garda Síochána that this constitutes a small, but material share of total scam calls. (i.e., while the volume of calls to such numbers are small, they are likely to be more effective at scamming than other numbers because consumers are more likely to recognise them).

- Second, Option 2 stops fraudsters spoofing numbers that have not yet been assigned and reduces the range of numbers that are available to be spoofed. Option 2 also reduces the effectiveness of scams by removing the use of numbers that can be used for impersonating businesses. For example, fraudsters have spoofed unassigned non-geographic numbers in order to give the appearance of coming from a business or from the Dublin area (which has high consumer recognition).

6.272 Europe Economics notes there is considerable evidence on the effectiveness of the DNO and PN approach from international case studies. Further, information provided by a large IGO that has implemented DNO, PN and CLI Call Blocking shows that scam calls using CLI Spoofing of legitimate businesses appears to account for a small share of all scams calls in Ireland[392]. Europe Economics estimates that under Option 2 the net present value of the incremental reduction in harm would be €20 million over seven years, or roughly €3 million per annum.[393]

II. Other Impacts

Trust in voice calls

6.273 Option 2 would improve the trust consumers place in voice calls relative to the status quo under Option 1. While appearing to account for just a small share of all scam calls, ComReg notes that calls impersonating key businesses and organisations are very likely to undermine the trust of consumers in business communications. For example, consumers are unlikely to know that some organisations only use certain numbers for inbound calls only and would never contact a consumer using that same number. Consumers may check a

[392] This is based on calls blocked by the IGO from its implementation of DNO, PN and Fixed and Mobile CLI Blocking over a 5 month period.
[393] See Tables 9.9 and 9.11 the Europe Economics Report.

number online to see whether a number belongs to a particular organisation and be more likely to answer and engage as a result. DNO should assist in restoring some trust in voice calls because these numbers are an easy target for fraudsters to spoof given that they are actively being used for inbound calls. PN should also be expected to protect the trust of consumers by reducing the number of calls using unassigned Irish numbers.

6.274 This option is likely to reduce each of the effects assessed under Option 1 (e.g., contagion, feedback social effect) but only to a limited extent because consumers would still receive scam calls from other sources. However, it is likely to reduce the feedback effect because organisations would be less likely to move to alternative platforms because their number would not be spoofed if placed on the DNO list. This would also have the benefit of reducing the social effects because organisations may be less likely to switch to alternative platforms that some demographics (e.g., older people) are less accustomed. By protecting the important numbers that businesses use, a DNO list can enable businesses and organisations to secure their own numbers. This can protect the use of voice for business communications.

6.275 ComReg is of the view that consumers would likely prefer Option 2 to Option 1. However, consumers would also likely prefer additional protections beyond the use of DNO/PN because spoofed CLIs appear in a variety of different forms and are likely to continue to occur under Option 2.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

I. Direct Impacts

6.276 Under Option 3, Mobile and Fixed CLI Call Blocking would reduce the harm from scam calls by preventing overseas fraudsters from spoofing Irish numbers. Europe Economics notes that there is strong evidence demonstrating the effectiveness of both Fixed and Mobile CLI Call Blocking interventions from international case studies and also from discussions with early adopter operators in Ireland. Further, information provided by An Garda Síochána and a large IGO that implemented DNO, PN and Fixed and Mobile CLI Call Blocking suggests that CLI Spoofing accounts for the majority of identifiable scam calls experienced in Ireland in recent months[394].

6.277 In relation to its implementation in Ireland, Europe Economics notes that:

> *"Approximately 88 per cent of all call minutes in Ireland are accounted for by mobiles, and there are 3.6 times more mobile*

[394] This is based on calls blocked by the IGO from its implementation of DNO, PN and Fixed and Mobile CLI Blocking over a 5 month period.

international/roaming minutes than the total number of fixed international outgoing minutes.[395] *This intervention is therefore likely to be especially effective at limiting the risk of fraud caused by CLI spoofing scams in general".*

6.278 Accordingly, Europe Economics considers that Fixed and Mobile CLI Call Blocking should mitigate a large share of current scams. Europe Economics estimates that under Option 3, the net present value of the reduction in harm could be as high as €900 million over seven years, or roughly €129 million per annum.[396] This is an upper bound for the impact of the static voice interventions, as it assumes no adaptation by fraudsters.

Table 15: Reduction in harms under Option 1-3, relative to status quo

Option	Benefits to Irish society relative to status quo (Option 1)
Option 1 (No regulatory measures)	-
Option 2 (DNO&PN)	Over 7 year – €21 Million Annually - €3 Million
Option 3 (DNO&PN, Fixed and Mobile CLI Call Blocking)	Over 7 year – €900 Million Annually - €129 Million

II. Other Impacts

Trust in voice calls

6.279 Option 3 would block calls that originate from abroad and are spoofing Irish numbers. Because most scam calls currently arise due to Fixed and Mobile CLI spoofing, it would better protect Irish numbers compared to Option 1 and Option 2. Consumers would be assured that Irish numbers appearing on their caller ID are calls originating within Ireland. While caution would still need to be exercised, as scams do and will continue to originate in Ireland, consumers would be able to rule out the possibility that these calls are coming from abroad. This would be a notable improvement on the current case where some consumers ignore the geographic information provided by the caller ID because they suspect it is a scam from abroad. This option is likely to reduce each of the effects (e.g., contagion, feedback etc) assessed under Option 1 and be particularly effective at reducing contagion as the largest source of scam calls would be reduced. Therefore, consumers are likely to prefer Option 3.

[395] Europe Economics analysis of ComReg data. Source: Fixed Line Statistics and Mobile Statistics, Total Fixed International Outgoing Minutes (000's) and Mobile International/Roaming Minutes (000's), Q2 2022 [online].
[396] See Table 9.9 and 9.11 of the Europe Economics Report. The present-value of the value of the harm is the sum of the incremental values for DNO, PN, Fixed CLI Blocking, Mobile CLI Blocking.

Conclusion on impacts on consumers

6.280 Based on the assessment above, ComReg is of the view that consumers are unlikely to prefer Option 1 because the large harms on consumers would continue to occur or worsen, as other countries, particularly those in the Anglosphere, take preventative steps. While Option 3 is preferred to Option 2, consumers are also likely to value Option 2 and the implementation of the PN/DNO Lists. Option 3 could in some respects negate the need for a PN/DNO list over time – however, scams can and do originate in Ireland also and a PN/DNO list would provide a necessary protection against scams that impersonate important businesses or social services.

6.281 Therefore, consumers and businesses are likely to prefer a combination of PN/DNO and Fixed and Mobile CLI because, in combination, they offer the greatest potential for a reduction in the harm from scam calls and best safeguard the trust in and use of Voice calls and Irish numbers more generally.

II. Impact on industry stakeholders

6.282 For the purposes of this RIA the relevant industry stakeholders, among those outlined in Section 6. 2.2, are considered to be operators that:

1. originate Voice traffic;
2. terminate Voice traffic;
3. transit traffic via an International Gateway; and
4. provide other services (Resellers, including MVNOs).

6.283 This section provides information on the impacts on such industry stakeholders arising from the potential adoption of the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this regard:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

6.284 Several operators have made progress in implementing fixed and mobile CLI Call Blocking, with some associated financial costs having already been incurred. Nevertheless, for the clarity and purpose of this assessment,

ComReg assumes that no costs have been incurred to date[397]. This practical approach considers the maximum impact of each option and assumes all costs lie ahead of the operators. (i.e., a greenfield approach.)

Option 1: No regulatory intervention

I. Financial impacts

6.285 Option 1 would not impose any financial costs on any of the operators.

II. Other Impacts

6.286 Under this option, the harms to operators (e.g., commercial benefits from being able to offer networks of trust etc) would continue to occur and the scope for operators to benefit commercially from being able to offer networks of trust would be reduced because the prevailing level of scam calls is diminishing trust in voice calls and Irish numbers which in turn lowers the use of Voice services. Operator reputations would also continue to be damaged as scams proliferate across society negatively impacting the revenues generated by operators from providing Voice services. For example, as little as 16% of consumers think that operators have done enough to protect them from nuisance communications[398].

6.287 Therefore, operators are likely to prefer interventions that reduce the rate of scam calls and are unlikely to prefer Option 1.

Option 2: DNO and PN

I. Financial impacts

6.288 Under Option 2, the DNO and PN list would be applied by fixed line and mobile originating operators on all originating voice traffic. ComReg estimates that there are approximately thirty such operators[399] and each would incur some expense arising from the implementation of this option. Europe Economics has estimated both the one-off costs (e.g., implementing the initial list) and on-going costs (e.g., updating the list periodically) of the DNO/PN per operator as follows.

- A one-off cost of approximately €33,000 in the year of implementation; and

[397] Under the status quo, operators may choose not to incur costs by electing not to undertake any technical measures to combat scams. Indeed, certain operators have informed ComReg that they would await a regulatory requirement before undertaking further work on technical specifications in this RIA.
[398] B&A Consumer Survey, slide 42.
[399] Based on the number of operators in receipt of numbers directly from ComReg. the numbering conditions.

- On-going OPEX costs of approximately €3,000 per annum[400].

6.289 The costs referred to above only concern those operators which have yet to implement the intervention. Several operators have made significant progress in implementing DNO and PN and thus would likely prefer Option 2 to Option 1 because it would offer better protection for their customers with little additional costs. Overall, ComReg considers that few if any operators would prefer Option 1 over Option 2 given the improved customer outcomes that would be achieved at minimal cost.

II. Other Impacts

6.290 The sustained level of scam calls impersonating businesses threatens the continued use of voice calls. Option 2 would safeguard trust to some extent in business numbers and the use of voice calls for businesses which should benefit the long-term commercial interests of Voice operators.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

I. Financial impacts

6.291 Mobile and Fixed CLI Call Blocking are applied on transiting traffic and therefore the cost of this intervention is borne by IGOs. Roughly half of the operators impacted under Option 2 (e.g., non-IGOs) are unaffected by Option 3. ComReg assumes that such operators would prefer Option 3 given the improved consumer outcomes that would likely result. ComReg now focuses on the IGOs that are affected by Option 3.

6.292 ComReg estimates that there are 14 IGOs based on its request for information[401]. Furthermore, it should be noted that over [✂ [redacted] ✂] % of traffic is carried by 6 operators, which are [✂[redacted]✂] (the "Big 6 IGOs"). The value and distribution of costs differ between Fixed and Mobile CLI Call Blocking. For example:

- Fixed CLI Call Blocking is borne by all IGOs who must block calls using Irish CLIs originating abroad and facilitate *'long-lining'*[402] by operators. Europe Economics estimates the one-off cost of this at approximately €46,000, based primarily on the cost of testing the blocking capability of the intervention[403].
- By contrast, the cost of Mobile CLI Call Blocking Phase 1 would only be borne by the larger IGOs and Europe Economics estimates

[400] See Table 9.3 of the Europe Economics Report.
[401] All IGOs originate traffic and are therefore a subset of the 30 known Fixed line and mobile Originating Operators.
[402] As described in Section 5.2.2.
[403] See Table 9.3 of the Europe Economics Report.

this cost at approximately €350,000 for each of the MNO, BT and Virgin Media. The costs of Phase 2 could be bourne by all IGOs.

6.293 Operators that have already implemented Fixed and/or Mobile CLI Call Blocking would prefer Option 3. Indeed, the investments already made in implementing this intervention would be weakened if other operators failed to do so because fraudsters would likely exploit that 'gap' to reach Irish consumers, including the customers of operators that have already implemented the intervention. To maximise their return on investment such operators would prefer if Option 3 applied to all relevant operators. In relation to those operators that have not implemented this option – the knowledge of knowing that this intervention has been implemented by other operators already provides some assurance that a return on their investment would be earned soon after implementation. This intervention also provides a higher degree of protection for customers at a relatively low cost.

6.294 It is difficult to foretell whether IGOs would prefer Option 2 or Option 3, given the trade-off between cost and customer protection. Option 3 would provide better customer protection, but would also impose a greater cost, in particular on the three MNOs and BT, as outlined in Table 16 below. BT, Three, Vodafone and Eir may prefer Option 2 over Option 3, if motivated by cost alone, but may prefer Option 3 if they prioritise consumer protection. ComReg assumes given the responses to consultation that other IGOs would likely prefer Option 3 to Option 2, given the small incremental costs that would be borne under Option 3 (again, noting that some operators are already implementing these interventions)

6.295 All the operators identified above would appear able to afford these measures, with annual revenues far in excess of one-off costs. Furthermore, and for context, the Phase 1 IGOs collectively earned approximately €[✂✂] million in 2022[404] from providing this transit service to third parties (noting that a number transit traffic for their own networks).

Table 16: One-off costs per stakeholder for each Option, relative to status quo

Option	Originating Operators (excl. IGOs)	Smaller IGOs	Phase 1 IGOs
Option 1 (Do nothing)	-	-	-
Option 2 (DNO&PN)	€33,000	€33,000	€33,000
Option 3 (DNO&PN, Fixed and Mobile CLI call Blocking)	€33,000	€79,000	€435,000

[404] IGO RFI.

II. Other Impacts

6.296 The same impacts described under Option 1 would apply here – however Option 3 would better reduce the harms from nuisance communications (e.g., fraud and emotional harm) and best protect trust in the numbers that are used to deliver telecommunications services. Therefore, Option 3 would also best protect the long-term commercial interests of providers of voice services as trust underpins the use of Voice services.

6.297 Certain operators, such as CSPs, that originate traffic in the state, which may leave the Irish PSTN, before returning to terminate in Ireland. These operators may have to re-route their traffic to conform with these interventions. ComReg is not aware of any technical reason that CSPs cannot engage with MSPs to ensure minimal interruption to their services, noting that such issues should be reduced with time as CSPs and IGOs enable better use of the exceptions (e.g., long-lining).

Conclusion on impact on industry stakeholders

6.298 Based on its assessment, and the response to consultation which generally supported this approach, ComReg is of the view that Option 3 is likely to be preferred by most stakeholders, particularly those that have already implemented this intervention.

III. Impact on competition

6.299 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the statutory objectives as they relate to competition, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the promotion of competition and the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on efficient investment arising from the regulatory option is assessed.

Option 1: No regulatory intervention

6.300 ComReg notes that the assessment provided under this option is also relevant to the 'Voice Firewall' RIA because it provides an appropriate benchmark with

which to measure the effectiveness of that intervention regardless of the preferred option in this RIA. (i.e., this is the status quo absent any intervention at all).

Efficient use of numbers

6.301 Against the objective of ensuring the efficient and effective use of numbers, it is evident under Option 1 that the numbering resource is not being used efficiently or effectively and that this is resulting in observable and significant consumer harm. A situation where 51 million annoying and 17 million distressing scam calls are made to consumers each and every year, and approximately 500 consumers a day are being defrauded by scam calls, is clearly not consistent with the efficient and effective use of the numbering platform and also constitutes the misuse of numbers.

6.302 As noted above, numerous scam calls exploit the lack of protection afforded to Irish numbers at present, with fraudsters using CLI spoofing to impersonate Irish businesses and government agencies. In this way, telephony numbers are being used to perpetuate fraud and undermine ECS networks. The status quo is therefore not consistent with the efficient use of numbers noting that this constitutes misuse. If scam calls continue at their current rate, consumers may adapt by not answering voice calls at all, thereby further undermining the legitimate use of Irish numbers.

6.303 Finally, it is clear that operators under Option 1 do not have processes in place to reduce access to valid numbers by those who intend to misuse them. The misuse of the numbering resource is likely to continue and multiply in Ireland under Option 1 as fraudsters become more sophisticated and other English-speaking countries continue to put in place interventions of their own. ComReg discusses how operators could improve their number assignment processes through Know Your Customer measures in Chapter 5.

Promoting Competition

6.304 Competition is not currently providing adequate levels of protection to consumers from the harm caused by nuisance communications. There has been little attempt by operators to differentiate themselves from rivals by making investments in consumer protection measures that would reduce the nuisance communications arising on their networks[405]. Consumers would likely switch to alternative operators if nuisance communications could be avoided by doing so – however, operators have not distinguished themselves from rivals in any serious way or not at all in most cases. This stifles the

[405] For example, EE in the UK regularly tout the number of scam calls and texts their Voice Firewall and SMS Scam Filter block. See How EE is leading the fight against scams

competitive process because consumers have little incentives to switch between operators if there are no differences between them in relation to protecting against nuisance communications. This is particularly relevant in light of the serious harm caused to consumers as identified above.

6.305 The lack of protection against nuisance communications arises for a number of reasons.

- First, the incentives to provide protections are not sufficiently high because the majority of the harm/damage of scams are not borne by operators themselves but rather are being borne by their customers, be they consumers or businesses (i.e., €187 Million p/a)[406]. As noted by Europe Economics, without such an incentive, the level of investment by operators is likely to be less than socially optimal, as much of the cost of scam calls represents an "externality" to operators (e.g., not being borne by either contracting party) from the narrow perspective of cost.

- Second, operators are likely concerned that such investments, even if they were made, would prove inefficient if other operators did not replicate similar interventions.[407] Absent regulation, operators may underinvest in interventions whose effectiveness relies upon the coordinated implementation by many other operators. Otherwise, any such investment might prove inefficient. Hence, industry-wide interventions may ultimately be required in order properly address some aspects of nuisance communications.

- Third, the current lack of investment may also be borne from the fact that operators may be unconvinced that competing for customers on the basis of protection against nuisance communications would cause sufficient switching to justify relevant investments. Absent this competitive pressure, operators face little incentive to invest in scam protection in the short run. For example;

    - Competition in mobile markets is multifaceted and involves more than just price – however, adding an additional facet to competition would increase the informational load that consumers must bear when making a product decision.

[406] Europe Economics Report page 63.

[407] This is true of a number of the interventions being considered in the Consultation, including:
- DNO and PN - which relies upon implementation by all originating operators and IGOs.
- Fixed and Mobile CLI Blocking – which relies upon implementation by all originating operators and IGOs.
- Mobile CLI Blocking – which also relies upon the implementation of supporting inter-operator processes (i.e., MAP protocol and Share Solution).

Research conducted by the ESRI Price Lab found that consumers are unable to make good purchasing decisions when descriptions of products force them to think about too many things at once;[408]

- Consumers would not be able to directly observe the actual level or effectiveness of protection offered by operators' ex-ante, and choice could easily become distorted by perceived rather than actual level of protections afforded by an operator. Consumers may experience the same level of scam calls after switching having compromised on other aspects of competition.

- Fourth, there may be an understanding to maintain the status quo so as to avoid making network investments, such as might be needed to reduce nuisance communications. Such arrangements might be fairly easy to maintain given the small number of network operators and the comparative ease with which one network operator can monitor any significant investment in interventions by a rival operator. In effect, there could be an understanding to delay investments to save additional network costs.

6.306 Given the incomplete consumer information, negative externalities, and coordination failures outlined above, it would appear that competition has not provided sufficient incentives to protect consumers, leading to a market failure and socially suboptimal levels of investment in measures to tackle scam calls. If networks are not timely in offering sufficient protections, despite the significant harm caused by these communications, it would suggest a competitive failure that requires regulatory intervention. Clearly identifiable harms (as evidenced in detail above) for important services (e.g., voice and SMS) should be addressed in a well-functioning competitive market over an appropriate period. However, that is clearly not the case with respect to nuisance communications in Ireland.

6.307 That is not to say operators would not undertake any investment but rather that the level of investment necessary to protect consumers is currently insufficient. There are measures that operators can take independently, and some overseas operators have been proactive in implementing measures that significantly reduce the threat in their countries. Indeed, there are examples of operators attempting to distinguish their voice service from rivals as most protected from scams (e.g., EE in the UK and Telenor in Norway). However,

[408] Lunn, Pete et al, 2016, PRICE Lab: An Investigation of Consumers' Capabilities with Complex Products, ESRI.

this represents only a handful of examples internationally despite the worldwide plague of scam calls.

6.308 Furthermore, this option does not promote infrastructure-based competition between voice calls and other VOIP based platforms (e.g., WhatsApp) for a number of reasons including:

- Consumers and businesses may no longer see Voice calls as a viable option given the preponderance of nuisance communications which reduces reliance on the numbering platform.
- Consumers and businesses may move to alternative messaging platforms, despite preferring SMS at present[409] (e.g., OTT for P2P[410] and B2C[411]) ; and
- Declining use of SMS may lead to reduced investment and further reduce competition between providers of SMS services and alternative instant messaging platforms[412].

6.309 More generally, the declining use of voice calls owing to nuisance communications under Option 1 distorts the incentives that providers of voice services (e.g., fixed and mobile network operators) have to compete and invest in their networks and services thereby reducing infrastructure-based competition. For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform. Businesses may switch to alternative technologies to provide such services, that are inferior for serving these specific consumer and business needs at present (e.g., OTT delivery of VOIP for P2P, or apps, email or push notification for B2C[413]) but may have the notable advantage of not suffering from nuisance communications to the same extent as traditional voice calls. This would also greatly reduce the competition between Voice communications and alternative networks for P2P and B2C communications, as Voice calls decline in utility. As operators will

[409] These can be considered inferior in the sense that at present consumers and businesses choose voice for certain services, revealing a current preference for Voice calls as a means of communications for those services.
[410] Which is subject to more QoS issues due to latency and potentially less trusted due to a lack of numbers. Notably during the pandemic Irish mobile consumers returned to fixed and mobile voice calls for P2P communications.
[411] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish Geographic Numbers.
[412] For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform.
[413] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish Geographic Numbers.

know, once consumers and businesses switch to alternative means these switching decisions tend to be for a long period or permanent.

Efficient investment

6.310 Under Option 1 there is a risk that the investments already made voluntarily by some operators would become inefficient. For example, investments by some operators who have already implemented or begun implementing Fixed or Mobile CLI interventions (or would do so in the future under this Option) could become inefficient if other operators do not make concurrent investments. As previously noted, any operator that has yet to take appropriate steps potentially undermines other operator's investment as fraudsters would likely exploit that 'gap' to reach all consumers including those that made an investment.

6.311 Further, under Option 1, operators would face lower incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications (i.e., 2018/2019) may now become inefficient because such investments were made on the basis of an effectively functioning numbering platform. This may also reduce the incentive for future investments if operators are of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

Option 2: DNO and PN

Efficient use of numbers

6.312 Under Option 2, the DNO and PN should reduce the present misuse of Irish numbers and result in a more efficient use of numbers compared to Option 1 given that the numbers used by businesses and included in the DNO and PN lists would only be used for valid purposes. The DNO and PN List should also decrease the volume and effectiveness of scams impersonating Irish businesses and government agencies while also reducing the susceptibility of consumers to fall for scams by removing numbers of particular importance and credibility (e.g., banks).

6.313 This more efficient use of numbers however would only apply to those numbers on the DNO and PN lists and its impact, while positive, would be limited given the many other avenues used by fraudsters to commit fraud.

Promoting competition

6.314 Under Option 2, DNO and PN should reduce both scam calls and the resulting fraud. In particular, the DNO should improve trust and thereby consumers use of such numbers. This would increase the use of numbers more generally by

consumers to contact businesses relative to Option 1. In this way the DNO and PN can help preserve the use of voice communication by business to communicate with consumers, thereby protecting the incentive for operators to compete to provide such services to businesses and also compete on issues such as quality of service for those services.

6.315 Furthermore, reducing the level of scams impersonating businesses may also increase consumers' confidence in answering calls from businesses, potentially reducing the share of legitimate calls that go unanswered and improving the efficiency of businesses that contact consumers by Voice call.

6.316 However, because Option 2 only extends to numbers on the DNO/PN lists, its ability to promote competition and reduce the existing distortions to competition as outlined under Option 1 is clearly restricted to this specific use.

Efficient Investment

6.317 Option 2 better protects the investments that have already been made in voice services compared to Option 1 because it better preserves the use of and demand for voice calls. Absent the protection provided by Option 2, service providers and businesses that use certain numbers to allow consumers to contact them may need to invest in alternative communications channels to contact consumers. Such behaviour could result in existing investment becoming inefficient such that those investments would never have been made had operators been aware of the damage nuisance communications would inflict on the numbering platform. Therefore, Option 2 is less likely to result in inefficient investments compared to Option 1.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

Efficient use of numbers

6.318 Under Option 3, Mobile and Fixed CLI Call Blocking should further reduce the effectiveness of scams impersonating both businesses and government agencies relative to Option 1 and 2. This is because these interventions reduce scams through the avenue currently most used by fraudsters (i.e., CLI spoofing). In particular, it would prevent scam calls being spoofed from abroad using Irish Geographic Numbers, Non-Geographic Numbers or Mobile Numbers (which are popular with fraudsters at present). Further, it would prevent scam calls originating from the numbers of businesses or agencies which have not been included on the DNO or by entities currently unaware of the DNO under Option 1. Fixed and Mobile CLI Call Blocking should greatly reduce the present misuse of Irish numbers better ensuring that where numbers are used, they are used more efficiently than is currently the case.

6.319 Therefore, Option 3 would better promote the efficient use of numbers than

Option 1 or Option 2.

Promoting competition

6.320 Option 3 should reduce the distortions to competition outlined under Option 1 because all originating operators would be required to put in place the Mobile and Fixed CLI intervention and this would close one of the main avenue (spoofing numbers) through which scam calls are currently made in Ireland. Operators would then compete on the basis that such calls would be blocked rather than under Option 1 where competition failed to deliver the same protections that could be reasonably expected to arise in an effectively functioning market.

6.321 Furthermore, if this intervention is applied to all originating operators, it would not lead to any competitive distortions such that only some operators and their associated consumers would benefit from the intervention. By imposing a common, minimum standard for consumer protection across all operators, Option 3 is less distortionary to competition than relying on operators implementing solutions of their own accord. As outlined above, if left to competitive forces alone there is reason to believe that Mobile and Fixed CLI Call Blocking would not be implemented across industry as operators face a collective action problem.

6.322 Option 3 also represents a reinforcement of all the benefits provided under Option 2 because it strengthens the benefits of DNO/PN by extending its protection to all inbound international voice traffic and improves trust in numbers relative to Option 1 or 2 given that otherwise such numbers would be unprotected by DNO and only partially covered by PN. This should capture further scam calls targeting businesses not captured by DNO (e.g., nearest neighbour).

6.323 Finally, Option 3 would also improve trust in numbers and thereby enhance the likelihood of consumers answering calls from unknown Irish mobile numbers. In this way, Option 3 can help preserve the use of voice communication to provide services between Irish consumers and therefore protects the incentive for MNOs to compete to provide such services to businesses, and relatedly to compete on issues like the QoS for those services.

6.324 Therefore Option 3 would better promote competition that either Options 1 or Option 2.

Efficient Investment

6.325 Under Option 3, the addition of Fixed and Mobile CLI Call Blocking should bring the greatest reduction in inefficient investment resulting from scam calls

and CLI spoofing. In particular, Option 3 removes the risk that that investments by some operators who have already implemented or begun implementing Fixed or Mobile CLI interventions (or would do so in the future under this Option) could become inefficient. As we have noted, any uncovered operator potentially undermines an operator's investment as fraudsters would likely exploit that 'gap' to reach all consumers including those that made an investment. In summary, Option 3 would best promote efficient investment and innovation in new and enhanced infrastructures by facilitating MNOs to make investments in the knowledge other MNOs would be subject to the same consumer protection measures.

6.326 Further, under Option 3 operators would face better incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications, and which were made on the basis of an effectively functioning numbering platform would also be better protected under this option. This option would also increase the incentives for future investments if operators were of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

6.327 By best promoting the use of and demand for Voice calls for P2P and B2C communication, Option 3 benefits operators that may otherwise need to invest in alternative communications channels in order to contact consumers. Absent this protection, service providers and businesses may need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient as it would be driven not by unmet need but by a degradation of existing voice network's ability to continue to meet the existing need for such services. Therefore, Option 3 is less distortionary to investment than Option 2.

Conclusion on impact on competition

6.328 Based on the assessment above, ComReg is of the view that a combination of Option 2 and Option 3 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

6.329 The above assessment and the accompanying Europe Economics Report demonstrate that there is significant consumer and societal harm present under Option 1. On the other hand, Option 2 and Option 3 address the policy issues described at the outset of this RIA by identifying and blocking calls stemming from international networks and presenting with Irish CLIs and identifying and blocking calls which should never appear as a CLI in the first place. This would promote competition and the more effective functioning of

the numbering platform. Therefore, ComReg is of the view that, on balance, Option is the preferred option in terms of its impact on stakeholders, competition and consumers. These interventions are referred to as the ‘static interventions’ in the subsequent RIAs in this consultation.

6.330 It should be noted this view only concerns the policy issues described at the outset of this RIA. (e.g., identifying and blocking calls stemming from international networks and presenting with Irish CLIs etc). This preferred option may not be sufficient to address all scam calls, and this is discussed further in the ‘Voice Firewall’ RIA which follows.

6.4 Voice Firewall RIA

6.4.1 Policy Issues

6.331 In Section 6.2.1, ComReg noted that the two overarching policy issues relevant to all RIAs are:

i. to reduce the harm to consumers and businesses from scam calls; and

ii. to protect and renew trust in ECS Networks and Services.

6.332 The remainder of this section further defines these main policy issues as they relate to this RIA in order to appropriately assess the available regulatory options. With that in mind, ComReg notes that this RIA builds on the previous CLI Blocking RIA, where the main policy issue was, among other things, to reduce harm by identifying and blocking calls making illegitimate use of Irish CLIs from international networks. While the preferred option appropriately addresses that policy issue, it does not address all nuisance voice communications and readers will obviously appreciate that it may become less effective over time depending on how fraudsters react to its implementation.

6.333 In that regard, there are three areas of scam voice calls that are not addressed by the preferred option in the CLI Blocking RIA, and which are of relevance to this RIA.

- **First**, scam calls that originate in Ireland are unaffected by Fixed or Mobile CLI Call blocking but there is increasing evidence that scams are now originating in Ireland in scale – primarily through the use of pre-pay burner phones. It is also possible that fraudsters could exploit other unknown or unidentified vulnerabilities in network that have not already been identified.
- **Second**, fraudsters from abroad do not always use CLI spoofing of Irish numbers and on occasion use their own numbers from where the scam originates or spoof the numbers of a foreign country trusted by Irish consumers (e.g., certain scams have used +44, the UK's dialling code). Such scams can travel by what is ostensibly legitimate traffic and cannot simply be blocked on the basis of the CLI and route alone.
- **Third**, future scams seem likely to become more sophisticated as the Fixed and Mobile CLI Call Blocking takes effect. Any call a consumer might receive from whatever location could potentially be

a scam call. Blocking such traffic requires an assessment of characteristics of the traffic itself, and not merely whether the route matches the CLI.

6.334 With that in mind, the main policy issue associated with this Voice Firewall RIA is to reduce the harm from scam calls and protect and renew trust in ECN by identifying and blocking scam calls regardless of how and where they originate and with an emphasis on scams that would not be blocked under the static interventions (i.e., DNO/PN Lists and/or Fixed and Mobile CLI Call Blocking).

6.4.2 Regulatory Options (Steps 1 & 2)

6.335 The available interventions for the purpose of this RIA (and previously discussed in Section 6.2.1 and 6.2.3) are as follows.

- **Option 1 –** No Voice Firewall – Preferred Option from the 'Voice CLI' RIA' only
  - No additional interventions to the Preferred Option outlined in the 'CLI Blocking RIA ', which is to implement the DNO, PN and Mobile and Fixed CLI Call Blocking.
- **Option 2** – Implement a Voice Firewall (in addition to the Preferred Option from the 'Voice CLI' RIA')
  - This approach would implement the Voice firewall, alongside the DNO, PN and Mobile and Fixed CLI Call Blocking.

6.4.3 Impact on industry stakeholders, competition and consumers (Steps 3 & 4)

I. Impact on consumers

6.336 This section provides information on the impacts on consumers arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the direct benefits to consumers arising from the regulatory option are assessed (i.e., reduction in time lost to scam calls and monies to fraud); and

II. Second, other relevant impacts arising from the implementation of the regulatory is assessed (i.e., trust in numbers, use of Voice calls etc.).

I. Direct impacts

Option 1

6.337 The static voice interventions should significantly reduce the number of scam calls and fraud. Europe Economics estimate that these interventions could reduce the value of the present harm to consumers and businesses by approximately €900 million over a 7-year period[414]. However as noted above, these interventions would not prevent all scam calls being made or received and there are three areas that would not be addressed under Option 1

6.338 In relation to I, currently the bulk of scam calls originate abroad and reach Irish consumers via these channels. However, ComReg understands from An Garda Síochána that scam calls originating in Ireland are scaling up- primarily through the use of pre-pay burner phones. There has also be a noted increase in these scams being report in the media, including the successful interception by An Garda Síochána of a criminal enterprise based in Ireland that targeted Irish and international consumers[415]. Such scams cannot be easily identified and blocked because they use valid Irish SIMs to perpetuate fraud. These types of scams are likely to increase significantly under Option 1 because fraudsters will recognise that the static interventions are focussed on stemming calls from international networks and presenting with Irish CLIs etc. Scams using valid SIMs (whether in Ireland or abroad) would not be captured by this intervention.

6.339 In relation to II (scams using valid CLI from abroad)[416] primarily use Wangiri calls (a Japanese word, literally means one ring and cut). Fraudsters will use international numbers to dial users in other countries and immediately disconnect the calls. The scam lies in the hope that they will be called back, and the unassuming caller will then be routed to a premium rate number, overseas, and billed a large sum of cash to listen to a pre-recorded message. These types of scams have been experienced in Ireland previously by taking advantage of peoples trust in Geographic Numbers. For example, in Mayo, people received Wangiri calls which appeared to come from a local number because the numbers '94' (the prefix to all landline telephones number in the Castlebar district) - appeared on screen but were instead fraudsters from Tunisia.[417]

6.340 Other related scams from abroad include impersonating banks and government agencies without CLI spoofing and instead spoofing using the prefix +44). Scams using the UK international code +44 are particularly

[414] See Table 9.9 and 9.11 of the Europe Economics Report.
[415] Waterford gardaí investigating scams seize €1.12m in 'first major seizure of cryptocurrency' (irishexaminer.com)
[416] For example, calls that appear with an international dialling code (e.g., +44),
[417] Mayo being targeted today by 'Wangiri' phone fraudsters | Connaught Telegraph (con-telegraph.ie)

prominent in Ireland as many people typically have family and friends based in the UK and may be more likely to answer compared to other international codes. These scams would continue to occur under Option 1 because there is no intervention that would protect against them.

6.341 In relation to III (more sophisticated scams), there is a high likelihood of scam calls becoming significantly more sophisticated through criminal's use of advanced AI technologies such as ChatGPT and Microsoft's Vall-E (a tool that converts text to speech)[418]. Emerging evidence suggests that fraudsters abroad are using these technologies to imitate the voice of businesses or family members in distress in order to commit fraud[419]. These scams can combine the relative strengths of different AI tools such as voice mimicry and Chat GPT to generate convincing speech or text in real time and perpetuate such scams on a large scale[420].

6.342 Family emergency calls have already been initiated in the United States and Canada where money is requested based on a voice mimicking a family member[421][422]. Such a call could come from someone who sounds just like a friend or family member but is actually a fraudster using a clone of their voice. Using a short sample of anyone's voice, this technology can accurately convert written sentences into convincing sounding audio. A sample of anyone's voice can be obtained[423] and used to impersonate that person and can appear highly credible.

6.343 It is inevitable that these types of scams will arrive on Irish shores and can be expected to have a higher rate of fraud compared to the current wave of scams. A large share of Irish consumers could be targets for impersonation by voice-mimicry software, given the ubiquity of video content publicly available on social media. Next-generation AI based scam calls should be expected to reach Ireland and increase with time as the underlying technology becomes more widely available (e.g., software like VoiceLab for calls[424]).

6.344 Therefore, a significant amount of scam calls and associated harm will inevitably remain following the implementation of the static interventions.

[418] Vall-E is not yet available to the public, but other companies, like Resemble AI and ElevenLabs, make similar tools that are.
[419] For example, AI based voice recognition has been used to verify identity by Centrelink and Australian tax office. AI can fool voice recognition used to verify identity by Centrelink and Australian tax office | Artificial intelligence (AI) | The Guardian
[420] For example, robocalls can reach many consumers but rely on recorded messages, whereas scam callers are more convincing but can only make one call at a time.
[421] Scammers use AI to enhance their family emergency schemes | Consumer Advice (ftc.gov)
[422] For example, a couple in Canada were reportedly scammed out of $21,000 after getting a call from an AI-generated voice pretending to be their son" 6th March 2023 Link
[423] This can be obtained through a number of means by ringing a person and recording them for a very short period or obtaining it through social media or recoding in public.
[424] https://beta.elevenlabs.io/.

Moreover, the present volume and prevalence of such scam calls would likely increase with time, as domestic and international fraudsters adapt their operations to circumvent the static interventions. Therefore, while effective and beneficial, the impact of the static interventions should be expected to degrade over time.

6.345 Consequently, consumers are highly unlikely to prefer Option 1.

Option 2

6.346 The static interventions only target scam calls arriving from a specific route (i.e., fixed and mobile CLI spoofing target scam calls from abroad that spoof Irish numbers). However, the voice firewall is a dynamic intervention that is designed to intercept scam calls regardless of how or where they originate. In this way, voice firewalls do not directly target each of the gaps outlined above, rather these gaps are captured through an assessment of each inbound call made to an individual caller. In this way, the voice firewall would complement the static interventions by covering other avenues that fraudsters use.

6.347 As noted by Europe Economics: "*In the longer term (after a year) the voice firewall could be implemented, which would enhance the benefits of the other interventions by adding a more dynamic element. As scammers become confronted by the blocks on their activities caused by those interventions in the shorter term, they will likely evolve their methods to maintain access to the pool of* potential *victims in Ireland. A voice firewall has the potential, in the longer term, to help combat the problems more dynamically and address scam calls that get around the previous interventions*".[425]

6.348 While Voice Firewalls do not target specific gaps directly, it is likely that it would reduce the scams described above because voice firewalls logs, monitors (e.g., the route taken to arrive onto the network), and controls all inbound voice network activity regardless of where the call originates (i.e., not just international traffic) which should reduce the rate of scam calls. Furthermore, behavioural analysis in firewalls using AI or machine learning ("ML") to conduct advanced data analytics to predict potential attacks and to identify patterns. Such technologies allow operators to analyse and monitor network traffic and activity for signs of suspicious or malicious behaviour, and to remediate the threats. The data subject to these analytics depends on the firewall provider but typically includes:

- Information and logs that the Voice Firewall gathers locally, and scams assessed by the Voice Firewall other countries, including pre-created watch lists.

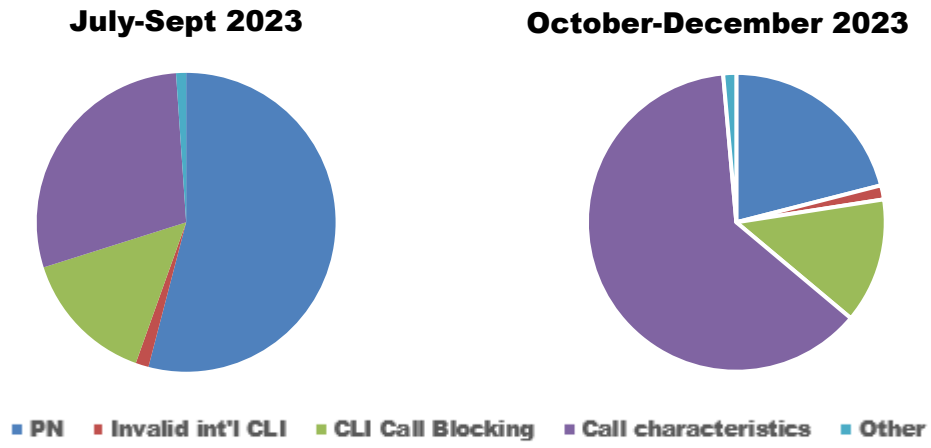
[425] Europe Economics Report, p75.

- phone call characteristics (e.g., numbers that are making a large number of calls) and number owner details.
- previous call histories and recipient reports of fraud.
- network probes strategically positioned across the globe.
- Intelligence gathered from law enforcement agencies.

6.349 The importance of the Voice Firewall grows as fraudsters adapt to the static interventions by either sidestepping (e.g., scam calls without CLI spoofing, originating scams within Ireland, bringing Irish SIM cards abroad) or overcoming them (e.g., impersonating businesses not on the DNO). The Voice Firewall would provide annual benefits of €152m over 7 years in addition to the static voice interventions even where fraudsters do not adapt because they offer protection that simply cannot be provided by the static interventions (e.g., against scams originating in Ireland etc).

6.350 Evidence from Australia indicates that scammers quickly adapt to static interventions at which point dynamic interventions such as the Voice Firewall become ever more important. Since the publication of Consultation 23/52, the ACMA has published a detailed breakdown of the number of scam calls blocked by each intervention which shows that between Q3 and Q4 of 2023 alone, blocking based on call characteristics (which is dynamic in nature) rose from 29% to 62%, while calls blocked on the basis of Protected Numbers fell from 54% to 21%.

Figure 29: Scam calls blocked by different interventions in Australia.



Source: The ACMA's "*Phone Scams: Intelligence Report Q2 (Oct-Dec) 2023-24*"[426]

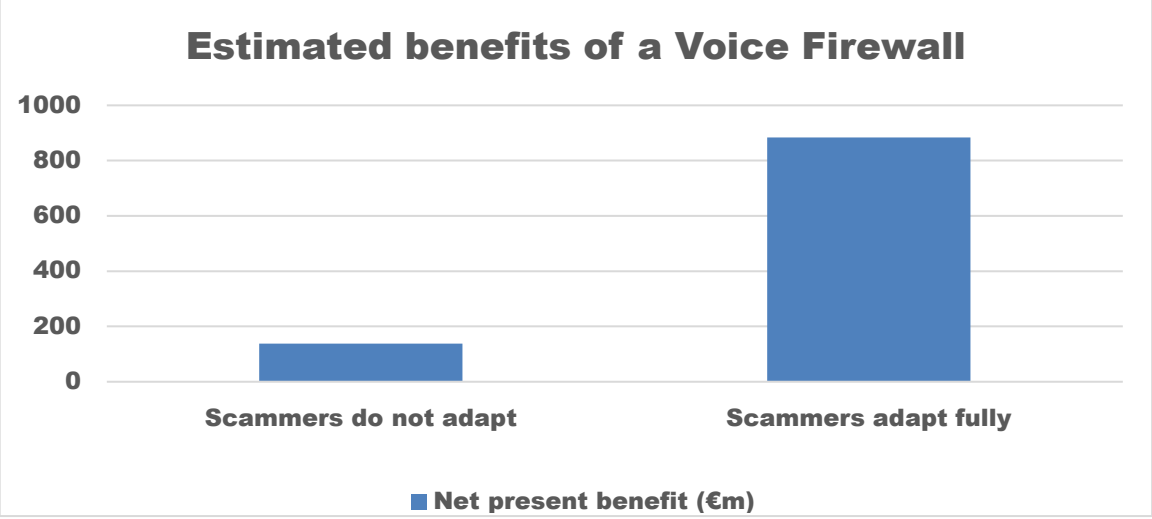
[426] For simplicity, ComReg has relabelled the ACMA interventions using the terminology contained throughout this report. 4.2.1-Invalid or unallocated Australian numbers – Protected Numbers, 4.2.3-Invalid international numbers (unallocated country code or digit length) – Invalid International CLI
4.2.5-Australian Calling Line Identification (CLI) from international source – Fixed CLI Call Blocking

6.351 Similarly, recent reports from Traficom indicate that the number of calls blocked by Mobile CLI Call Blocking has fallen from approximately 200,000 a day, to 500,000 a month as scammer adapt to the intervention: "*The model has proven indispensable, helping prevent as many as over 200,000 attempted scam calls a day. Although criminals have of course noticed the preventive measures, the service still prevents approximately half a million scam calls a month*". [427]

6.352 It should be noted that the importance of the Voice firewall would increase as fraudsters adapt to ComReg's static interventions, rising to €892m where fraudsters fully adapt. The exact benefits of the voice firewall would depend on the reaction of fraudsters to the static interventions – however it is highly likely to be closer to €892m in the longer run given how sophisticated scams are expected to become in the future. Europe Economics find that the Voice firewall represents a healthy social return on a relatively modest investment, with this improving the as fraudsters adapt to the static interventions.

6.353 Therefore, consumers are likely to prefer Option 2 and the introduction of a Voice Firewall.

Figure 30: Impact voice firewall in addition to the static voice interventions, for different levels of fraudster adaptation



II. Other Impacts

Trust in voice calls

[427] Traficom recognises cooperation for preventing scam calls and messages with the Information Security Trailblazer award | Traficom (kyberturvallisuuskeskus.fi)

Option 1

6.354 Option 1 would improve the trust of consumers in Voice calls, relative to the status quo where no regulatory measures would be implemented. The static voice interventions should reduce the prevalence of scam calls and the number of scam calls received by consumers, in particular those using CLI spoofing. Option 1 would therefore protect the trust consumers place in key numbers relative to status quo. However, the impact is likely to be temporary as fraudsters can be expected to adapt to the implementation of the static interventions. There is no reason to think that consumers would trust voice calls more in the long run because a subset of those communications (i.e., spoofed numbers from abroad) are blocked. In effect each of the effects outlined above (e.g., contagion, feedback etc) would continue diminishing trust in the numbering platform in the longer run.

Option 2

6.355 Under Option 2, the combination of a Voice firewall and the static voice measures would provide the greatest protection to Irish consumers, by both blocking scam calls making illegitimate use of CLIs but also by blocking suspicious voice traffic originating in potentially legitimate uses. Absent the static voice measures, some of those nuisance calls may end up being received by consumers because, while effective, the voice firewall cannot provide full protection all of the time due to the rapid evolution of nuisance calls[428]. Furthermore, to the extent that the static interventions would restore trust, this would only be in the short term and before fraudsters could adapt to the implementation of the Fixed and Mobile CLI Call Blocking. As noted by Europe Economics: "*the ability to adapt to evolving threats from scammers gives this intervention the potential to improve consumer and business trust in voice communication in the longer term. Knowing that a voice firewall is in place to respond to CLI spoofing and potentially other forms of threats could imbue call receivers with trust that the calls they receive are legitimate*"[429]

6.356 As this regulatory option would block the most scam calls, ComReg considers that it would be most likely to restore trust in Voice calls, particularly in the short run. As previously noted, two out of three adults state that regulatory intervention would increase their trust in calls and texts, rising to 9 out of 10

[428] Absent the static measures, fraudsters would likely continue to spoof Irish numbers, given the importance of such numbers to Irish consumers. As a Voice Firewall assesses many millions of calls, even a with high degree of accuracy a large number of scam calls would not be blocked and still reach consumers. Even were only a small share of attempted scam calls using CLI spoofing to reach consumers, this is still a large number of scam calls. Therefore, absent the static interventions, a Voice Firewall is unlikely to protect trust fully as fraudsters would likely continue to spoof Irish numbers.
[429] Europe Economics Report, page 73

once adults that are unsure of its effect are excluded[430].

6.357 Consequently, Option 2 and the combination of the static interventions and the voice firewall would result in the greatest reduction in scam calls, while protecting the use of Irish numbers. Therefore, Option 2 would best safeguard the trust in Voice calls and Irish numbers and is likely to offer the best defence, thereby promoting the continued use of Voice by Irish consumers and businesses.

Conclusion on impacts on consumers

6.358 Based on its assessment, ComReg is of the view that Option 2 is likely to be preferred by consumers and businesses as it offers the greatest reduction in the harm from scam calls and best safeguards the trust in and use of voice calls and Irish numbers more generally.

II. Impact on industry stakeholders

6.359 As this RIA relates solely to voice interventions, the relevant industry stakeholders, among those outlined in Section 6.2.4, are operators that:

a) Originate Voice traffic;

b) Terminate Voice traffic;

c) Transit traffic via an International Gateway; and

d) Other operators (Resellers, including MVNOs).

6.360 This section provides information on the impacts on industry stakeholders arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

Option 1: No voice firewall, preferred option in CLI Call Blocking RIA only.

I. Financial impacts

[430] Q.45 "*If regulatory interventions were made to block scam calls and texts, to what extent would this impact the level of trust you have in calls and texts you receive in the future?*". 27% of respondents answered that they were "Unsure of the impact" of such regulatory actions on their trust in calls and texts. Upon implementation, such consumers trust either would or would not be affected, therefore we consider the estimated of consumers whose trust will be positively impacted to be a lower bound estimate.

6.361 Under Option 1, no financial costs would be incurred by operators other than those already incurred through the implementation of the DNO, PN lists and both Fixed and Mobile CLI Call Blocking.

II. Other Impacts

6.362 The benefits to operators in terms of the protecting their consumers and commercial interests from this option are as previously outlined above. However, as some level of scam calls should be expected to remain and negatively impact trust and use of Voice calls these scams would continue to threaten operators' long-term commercial interests.

Option 2: Voice Firewall and preferred option from the 'CLI Blocking RIA'

I. Financial impacts

6.363 A Voice firewall is applied on terminating voice traffic and therefore the cost of this intervention is borne by terminating operators. The requirement to implement a Voice Firewall would apply to Eir, Three, Vodafone and Virgin. To inform ComReg's assessment, Europe Economics has estimated both the one-off costs (e.g., the cost of software purchase and installation) and on-going cost (e.g., on-going cost of software) of Voice Firewall per operator.

6.364 Under Option 2, most operators would pay the same as under Option 1 as only operators required to implement a Voice firewall would pay more. However, Option 2 would impose an additional cost on Eir, Three and Vodafone and Virgin, as shown in Table 17 below.

Table 17: One-off costs per stakeholder for each Option, relative to status quo

Intervention costs	Originating Operators	Small IGOs	Large IGO w/o Voice Firewall [431]	MNOs [432]
Option 1 DNO&PN, Fixed and Mobile CLI call Blocking	€33,000	€79,000	€435,000	€435,000
Option 2 DNO&PN, CLI Call Blocking & Voice Firewall	€33,000	€79,000	€435,000	€1.6 Million

II. Other Impacts

[431] This includes IGOs which bears the cost of implement CLI Call Blocking.
[432] This includes any IGO(s) which meet the threshold to be required to implement the Voice Firewall.

6.365 Under Option 3, the harms outlined from scam calls we outlined in Section 6.2.1 would be most reduced, thereby best protecting trust in Voice calls and Irish numbers.

6.366 Any intervention that utilises probabilistic predictions inevitably introduces a risk of inadvertent blocking, where some legitimate calls may be blocked. Based on the experience of vendors and international NRAs ComReg considers that in practice this risk is quite low, noting that the Decision Instrument allows MSPs to take a number of actions other than blocking the call (e.g., CLI modification). ComReg also does not specify what probability an operator should take any action.

Conclusion on impact on industry stakeholders

6.367 Based on its assessment, some operators may be of the view that the implementation of voice firewall is unnecessary given its additional costs. Conversely, however, operators may also prefer Option 2 given the additional protections provided by that option, including improved consumer outcomes for voice calls, thereby safeguarding their long run commercial interests.

6.368 In particular, such operators may value the future-proofed protections provided by the voice firewall with regard to scam prevalence. Indeed, the UK MNO EE has implemented a voice firewall and relayed its benefits to consumers. While cost-conscious MNOs may prefer Option 2, ComReg suspects few would be so blinkered as to prioritise costs in the short term over the continued use of Voice services in the long run – not to mention the higher rate of consumer fraud and harm.

III. Impact on competition

6.369 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the relevant statutory objectives on competition, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on the efficient investment arising from the regulatory option is assessed.

Option 1: No Voice Firewall, preferred option in CLI Blocking RIA only.

Efficient use of numbers

6.370 Implementing the static interventions would represent a significant improvement in terms of the efficient use of numbers. However, such interventions on their own would not prevent all scam calls being made and certain scam calls would continue to be made through other routes. In particular, ComReg notes that scams could still occur through (i) calls that originate in Ireland and (ii) through the use of Irish SIMs abroad. The use of these numbers to commit fraud could not be considered efficient and would remain a misuse of Irish numbers. Therefore, while Option 1 would increase efficiency due to the implementation of static interventions the impact would be limited to calls that originate over those routes.

Promotion of competition

6.371 The static interventions would promote competition but only insofar as identifying and blocking calls stemming from international networks and then presenting with Irish CLIs or by identifying and blocking calls which should never appear as a CLI because the numbers are either unassigned or are inbound only numbers. Importantly, these interventions would be highly unlikely to promote competition in the long run given that the effectiveness of the static interventions can be reasonably expected to wane as scams become more sophisticated. Consequently, the distortions to competition previously identified above (under Option 1 of the CLI Call Blocking RIA) would continue to exist in the long run. Furthermore, even in the short run, where the static interventions would have the greatest impact on promoting competition, scam calls would continue to be made using other routes as we have discussed.

Efficient Investment

6.372 The static interventions would encourage efficient investment in ECS because all relevant operators would be required to implement those interventions and therefore there would be no ‘gaps’ to be exploited by fraudsters. Notably however, and unlike the fixed and mobile CLI interventions, the effectiveness of the Voice Firewall reducing nuisance communications is not dependent on implementation by other operators. In effect, an operator implementing a firewall would reap the full benefit of that investment independent regardless of other operator decisions.

6.373 However, Option 2 would promote efficient investment and innovation in new and enhanced infrastructures because the investment made in the firewall would be forward looking and there is a high degree of likelihood that the firewall would provide protection against scams in the future – scams that would otherwise have occurred. Therefore, there is a lower risk that any

investments made in a voice firewall would become inefficient. Further, its speedy implementation would prevent operators from having to make further future investments to address the damage caused by nuisance communications. This may be particularly acute for Voice services for B2C which has a more diverse and specialised ecosystem (e.g., the operators serving the call centres serving Irish businesses).

Option 2: Voice Firewall and preferred option from the 'CLI Blocking RIA'

Efficient use of numbers

6.374 Given the investment made by the industry in the work of the NCIT, ComReg is satisfied that the 'static' interventions are robust and powerful. However, on their own they are unlikely to offer sufficient protection because there are other avenues, as we have discussed earlier, that fraudsters could use Under Option 2. The combination of a Voice firewall and the static interventions would provide the greatest protection to Irish numbers, by both blocking scam calls that are clearly making illegitimate use of CLIs but also by blocking suspicious voice traffic originating in potentially legitimate uses. In this way, it is less likely that numbers would be used inefficiently.

6.375 In particular, the voice scam calls that originate in Ireland are unaffected by Fixed or Mobile CLI Call Blocking but there is growing evidence that scams are originating in Ireland. These particular cases of fraud directly use Irish numbers so the use of a voice firewall is particularly important as otherwise such scam calls would not be stopped. Further, because the voice firewall provides protection against future scams it better promotes long run efficiency effects. Therefore, Option 3 clearly best promotes the efficient use of numbers, by minimising their misuse and promoting their legitimate use.

Promoting competition

6.376 Option 2 would maximise benefits to consumers by appropriately and proportionately addressing significant consumer harms (as evidenced in Section 6.2.1) for clearly important services. Option 2 would complement the static interventions in reducing the rate of nuisance communications. Option 2 would also play an important role in reducing any competitive distortions by mandating measures that that one would expect to be provided in a well-functioning competitive market over an appropriate period.

6.377 Because the static interventions can only target specific sources of scams, the addition of the voice firewall would importantly broaden the scope of consumer protection to better cover current scams. Further, it is unlikely that the static interventions of themselves would protect long run competition

because it is highly likely that scams would evolve in response to the static interventions. Indeed, absent the implementation of the voice firewall it is highly likely that further regulatory interventions would be required in the short-term as scams inevitably become more sophisticated.

6.378 Finally, under Option 2 there remains a high degree of flexibility in terms of how the voice firewall is implemented by operators and the features and functionality it would use. There are a variety of different types of firewalls that can be implemented, and the technical specifications afford operators a degree of discretion over how this is done. Competition may even drive protection beyond the levels envisaged by ComReg thereby underpinning the role of competition in driving benefits for consumers. This provides assurance that there is little risk of the obligation itself creating unintended distortions or imposing due costs.

Efficient Investment

6.379 A Voice Firewall would act as a strong complement to the static interventions in promoting efficient investment, by reducing potential distortions to competition and the misuse of numbers. Option 2 would encourage efficient investment and innovation in new and enhanced infrastructures by encouraging the rollout of voice firewalls to protect consumers, promoting innovation and ensuring the efficient use and effective management of the national numbering resource. Such investments would be efficient because there is a clear requirement for these interventions given the harms outline in Section 6.2.1 and it is highly likely that such technologies would be implemented at some point by some operators in the future. However, the implementation of this infrastructure now would address the current ongoing harm to both consumers and operators. Option 3 best prevents inefficient investment by protecting the current and future investment in current Voice services and networks, and the use of Irish numbers.

Conclusion on impact on competition

6.380 In light of the above, ComReg is of the view that Option 2 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

6.381 The above assessment, together with the Europe Economics Report, demonstrate that there is currently a significant consumer and societal harm present due to nuisance communications. While the static interventions are effective for their intended purpose, there are other forms of scams that would still occur. Under Option 2, the Voice Firewall would complement the static interventions and provide additional and proportionate consumer protection

measures. Option 2 clearly address the policy issues described at the outset of this RIA because a voice firewall would reduce the rate of scam calls generally but would also address scam calls that originate in Ireland as well as scams through valid non-Irish numbers from abroad. It would also provide protection against future more sophisticated scams designed to circumvent the static interventions as fraudsters make increased use of AI and ML technologies.

6.382 Therefore, ComReg is of the view that Option 2 is the preferable option.

6.5 Sender ID RIA

6.5.1 Policy Issues

6.383 In Section 6.2.1, ComReg noted that the two overarching policy issues relevant to all RIAs are:

i. being to reduce the harm to consumers and businesses from scam calls; and

ii. to protect and renew trust in ECS Networks and Services.

6.384 ComReg is mindful of these policy issues in determining its preferred option. The remainder of this section further considers these main policy issues as they relate to this RIA in order to appropriately assess the available regulatory options.

6.385 Fraudsters, be they overseas or based here in Ireland use relatively inexpensive and readily available technology to send SMS with maliciously spoofed Sender IDs to impersonate an individual or trusted businesses/organisation. Such businesses/organisations include:

- Irish companies (e.g., banks or delivery services)
- Irish government agencies (e.g., Department of Social Welfare)
- Other legitimate organisations (e.g., NGOs)

6.386 Consumers have a high level of awareness of these organisations and fraudsters take advantage of this by impersonating them by means of a fake Sender ID. This makes it more likely that the consumer will read and comply with the instructions contained within the SMS. This can result in significant harms to consumers either through fraud and/or through annoyance or distress at receiving such SMS (See Section 6.2.1). The ensuing objectionable experiences can in turn lead to Irish consumers no longer being able to trust the Sender ID displayed on their SMS messages.

6.387 Unfortunately, there is significant incidence of impersonation through scam text messages. ComReg understands from An Garda Síochána, who itself has been recently impersonated, that this constitutes a major share of total SMS fraud. ComReg's research reveals that around 9 in 10 consumers claim a legitimate organisation was impersonated, with the most prevalent organisations impersonated being banks, followed by postal services (An Post), Revenue and the HSE.[433] For organisations, this level of impersonation

[433] B&A Consumer Survey, slide 37.

is impacting mainly organisations with a large consumer base and who would typically have a regular requirement for them. On average, 3 in 4 businesses claim to spend around 25 hours resolving scam texts in the past year – though rates are significantly higher depending on the organisations affected. More pertinently, the scamming reduces trust consumers have in SMS and consequently are less willing to engage with SMS.

6.388 With that in mind, the main policy issue associated with this RIA is to reduce the harm to consumers arising from scam SMS using spoofed Sender ID that impersonate organisations.

6.5.2 Regulatory Options (Steps 1 & 2)

6.389 Having regard to the interventions described in Section 6.2.2, ComReg considers that the four regulatory options available to it are:

- **Option 1 –** No regulatory Intervention
  - This approach would maintain the status quo position with no intervention(s) proposed by ComReg.
- **Option 2 –** Ban Sender IDs
  - This approach would ban the use of SMS IDs and businesses/organisations would be unable the send SMS using a Sender ID.
- **Option 3** – Full Sender ID registry
  - This would require senders and aggregators to follow a set of rules or a code of practice which requires that they register their Sender ID thereby authenticating the source of such messages. This approach would implement a Full Sender ID registry as stated in the technical specification.
- **Option 4** – Partial Sender ID registry
  - This would be a hybrid of Option 2 and Option 3 whereby some Sender IDs are permitted, but all others are blocked. Sender ID Registration would be available for businesses/organisations that plan to send more than a certain volume of SMS per month (e.g., Banks, delivery companies), all other SMS using Sender ID would be blocked.

6.5.3 Impact on industry stakeholders, competition and consumers (Steps 3 & 4)

I. Impact on consumers

6.390 This section provides information on the impacts on consumers arising from the regulatory options outlined above. ComReg notes that there are two broad

categories of impacts relevant in this section:

I. First, the direct benefits to consumers arising from the regulatory option is assessed (i.e., the reduction in monies lost to scam texts); and

II. Second, other relevant impacts (e.g., impact on trust) arising from the implementation of the regulatory options are assessed (i.e., other impacts).

Option 1: No regulatory intervention

I. Direct impacts

6.391 Under Option 1, the prevalence and harm (detailed in Section 6.2.1) from scam texts would likely remain high. There are numerous factors that could cause this harm to escalate (such as fraudsters increasing the rate of scam attempts) or moderate (consumers adapting their behaviour). However, absent any intervention, there is a notable risk that scams which impersonate organisations using Sender IDs would increase. Text scams are dynamic in nature and fraudsters adapt and evolve tactics to target consumers and so new forms of scams emerge over time. The harm is also likely to increase as the fraudsters become more ingenious even where consumers adapt to older scams.

6.392 As outlined in Section 6.2.1 [434], Europe Economics estimates that the annual level of harm to Irish consumers and businesses from scam texts is approximately €115 million per annum[435]. For the purpose of the analysis in this RIA, it is sufficient to note that the harm to society under Option 1 is likely to remain substantial with the potential to increase even further.

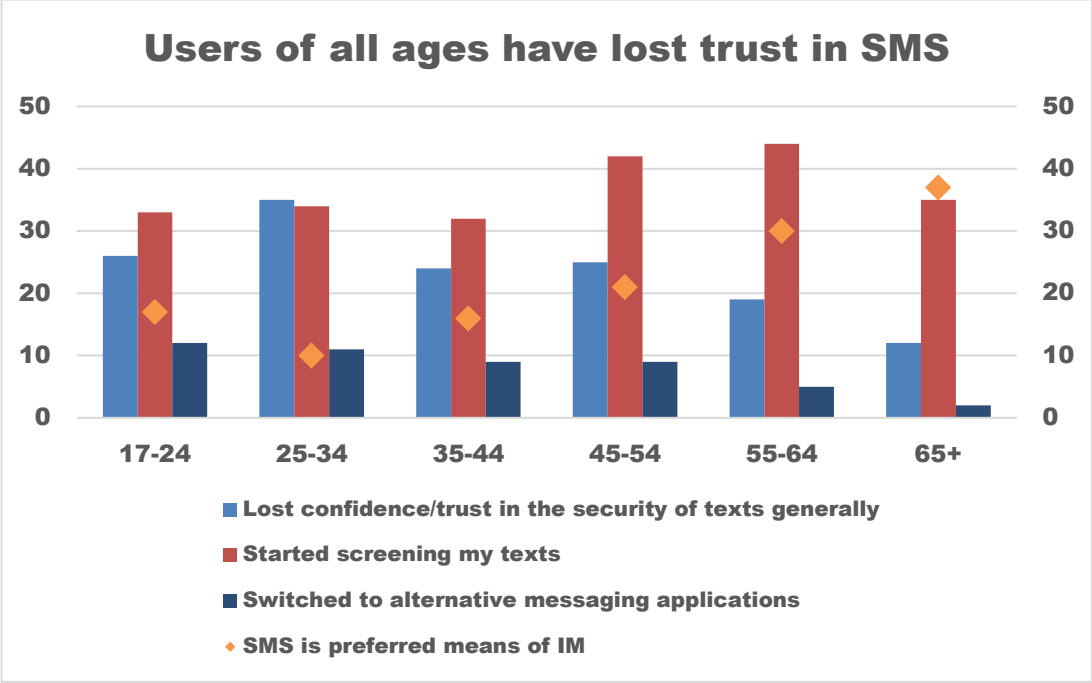
II. Other Impacts

Trust in SMS

6.393 Scam SMS reduce consumer trust with many consumers now screening or ignoring SMS altogether. Unsurprisingly, nearly 1 in 4 consumers have begun to lose trust in SMS, with issues of trust higher among younger consumers (see Figure 31 below), a fact of itself that does not bode well for the longer term future of the SMS service.

[434] See also Chapter 4 of the Europe Economics Report.
[435] Europe Economics Report page 63.

Figure 31: Loss of trust in texts as a result of scams[436]



Source: ComReg analysis of B&A Consumer survey data

6.394 Scam calls and texts create a number of distinct effects that reduce trust and threaten the efficient and effective functioning of the numbering platform. Below we assess each of these effects (i.e., contagion, call reduction, feedback, and social effects) in relation to SMS.

Contagion

6.395 Contagion refers to the uncertainty caused by the prevalence of scam SMS and/or a previous scam SMS experience which may infect a consumers' beliefs across all SMS regardless of who the sender is. Under Option 1, it is likely that contagion would multiply as consumers become increasingly suspicious about the SMS medium. As identified in Section 6.2.1, there are already a number of clear examples of contagion across the numbering platform. For example:

- Nearly 70% of consumers are concerned or very concerned about scam SMS. Those who have experienced a financial loss have a heighted level of being 'very concerned'[437].

[436] Q.38 In relation to your awareness of scam calls and texts, has any of the following happened? Q.5 Main way of sending and receiving instant messages?
[437] B&A Consumer Survey, slide 13.

- Over 59% of businesses are concerned or very concerned about scam SMS. Those using mobile numbers to communicate also show higher levels of concern[438].

6.396 ComReg is of the view that SMS provided over the numbering platform already suffers from contagion and this would likely intensify under Option 1.

SMS Reduction

6.397 SMS reduction refers to reductions in the utility of SMS due to contagion. Contagion is causing consumers to read fewer SMS than they would otherwise, due to fear of being scammed. Consumers are now not reading SMS even from people they may know or from businesses providing services that consumers would ordinarily be interested in (e.g., deliveries, hospital appointments etc). ComReg's Consumer Survey results show that fraudsters impersonate organisations that a consumer would potentially be open to receiving information from. This reduces the volume of SMS received over the numbering platform as consumers decide to read less and less SMS. For example:

- 43% of consumers have stopped reading SMS that may be from businesses or government agencies[439] due to the prevalence of scam texts.
- 23% of consumers have lost confidence/trust in the security of SMS generally.

6.398 While only 8% of respondents have switched to OTT providers to date due to scams[440], this can be expected to grow as the harms further manifest. Absent intervention, it appears that this level of switching could increase, and amount to a serious threat to the use of SMS for P2P and B2C in the future. This risk is heightened as younger consumers, who are less likely to prefer SMS for messaging to begin with and consumers that lost money to a scam call or text (which grows cumulatively year on year) are more likely to move to alternatives. These groups represent an important and growing share of the market, and such consumers may not transition back to SMS as they gradually adopt other OTT services (e.g., instant messaging combined with voice & video).

6.399 As we have noted, this can occur not because consumers necessarily prefer alternative applications or because they view these alternatives as being essentially equivalent to one another. Rather, such migration usually occurs

[438] B&A Business Survey, slide 11
[439] B&A Consumer Survey, slide 31.
[440] B&A Consumer Survey, slide 31.

because the consumer decides that the harms and nuisance associated with using calls and/or SMS are so high that they try to avoid using SMS altogether. It stands to reason that if SMS messaging operated more effectively then consumers (or at least some consumers) would have less need to migrate to alternative means that they may not prefer or are uncomfortable using.

6.400 ComReg is of the view that the evidence it has gathered demonstrates that nuisance communications are supressing the volume of SMS to the detriment of consumers and businesses.

Feedback effect

6.401 The feedback effect refers to the reduced incentives for people and organisations to use SMS because of the reduction in people reading SMS. Businesses may decide not to send SMS because of the low answer rate (i.e., the SMS reduction creates a feedback effect). In such circumstances, businesses are likely to switch to alternative means of contacting consumers even though their preference may be to contact consumers using SMS on public networks. For example, 39% of businesses have made changes to how they communicate with consumers, with 23% relying more on alternative means of communications (e.g., email, secure messages, online portal, WhatsApp etc.).[441] Nevertheless, many businesses continue to make use of SMS for B2C. While some businesses report reducing their reliance on mobile networks (10%) or SMS aggregators (7%) to contact consumers[442], these remain in the minority. Therefore, SMS has not yet been abandoned and its further decline may be avoided if actions are swiftly taken.

6.402 ComReg is of the view that there is clear evidence of feedback effect under Option 1 with organisations particularly affected as they move to alternative ways of contacting consumers.

Social effect

6.403 The social effect arises where some services that would normally be provided through SMS moves to alternative platforms not readily available to some social groups. People's reluctance to engage with SMS due to fear of being scammed could have a particularly negative impact on vulnerable consumers for whom SMS provides an important social outlet or access to essential services (e.g., healthcare, social security). The social effects of reduced SMS volumes resulting from avoidance can therefore be particularly detrimental for those who may be dependent on one or more social services and such

[441] B&A Business Survey, slide 23.
[442] B&A Business Survey, slide 23.

persons can often be the most vulnerable members of our society.

6.404 For example, older people are more likely to be affected by people and organisations (in particular) switching to alternative messaging services because older people are more reliant on SMS for instant messaging. The use by over 65s of alternative instant messaging platforms (e.g., WhatsApp, video calls, social media) is only a third of average users, and up to 5 times less when compared to younger groups[443]. Notably, fewer older users report switching to alternative messaging applications due to the prevalence of nuisance communications.

6.405 Older people are also more likely to be concerned or very concerned about scam SMS (83%)[444]. The most commonly impersonated organisations are those which older people are likely to require (e.g., banks, HSE and other public bodies such as An Post). For example, the HSE has outlined to ComReg the potentially serious repercussions of this lack of trust in SMS in particular for its elderly patients, given its impact on missed appointments. It is for such reasons that the possible impacts of reduced trust on more vulnerable consumers must be carefully considered.

6.406 ComReg is of the view that there is clear evidence that scam SMS are having social effects under Option 1.

Option 2: Ban Sender IDs

I. Direct impacts

6.407 Under Option 2, a Sender ID ban would reduce the harm from scam SMS by preventing the use of Sender IDs entirely, including from businesses and government agencies. This would reduce the volume and effectiveness of scam SMS impersonating businesses/organisations because it prevents scam SMS using Sender ID spoofing. It would also reduce the susceptibility of consumers to fall for scams by reducing the ability of fraudsters to accurately impersonate businesses and organisations. Because many scam SMS arise from the impersonation of businesses/organisations using scam Sender IDs, there would be a reduction of around half of the current €166m in harms. However, this reduction in harm is likely to be only temporary as fraudsters inevitably divert all SMS scams to messages without Sender ID.

6.408 However, while effective at cutting scams using Sender ID any reductions in harm (even in the short run), would come at the cost of preventing businesses and organisations from using Sender ID to communicate with consumers. This

[443] Mobile Consumer Experience Survey, slide 37. Link
[444] B&A Consumer Survey, responses to Q.5a "*How concerned are you about … Scam texts*"

option would unavoidably reduce the utility of SMS for B2C communications given that Sender ID, even in its current polluted form, is still valued by businesses/organisations in communicating with consumers. Indeed, consumers would likely value Sender ID if they were assured that such communications were valid and originating from the intending organisation/business.

6.409 The overall impact on consumers is therefore likely to be mixed and would depend on the consumer demographic and on how businesses/organisations agencies react to a ban on Sender IDs. Businesses/organisations may use SMS without Sender ID where SMS communications would display an originating number rather than a Sender ID. Ostensibly, consumers seem unlikely to prefer this because this simply moves the scam SMS using Sender ID to SMS more generally.

6.410 Alternative technologies (e.g., OTT) for B2C may be effective, particularly for younger demographics that are familiar with these technologies. In that regard, some consumers are likely to be indifferent about this option particularly for those who may already be wary of scam texts using Sender IDs. Indeed, some consumers may prefer all Sender ID's to be banned because it removes a potential avenue for fraudsters particularly for scams that appear within a genuine "thread" of text messages, and which is particularly egregious. For example, of consumers who did not respond to texts, 58% chose not to because they would prefer to communicate with the organisation in other ways[445].

6.411 However, these could be an inferior service to SMS because the use of alternatives may make it more difficult for organisations/businesses to communicate with older demographics who are less likely to engage with such forms of communications. This would result in lower effectiveness or efficiency of B2C and therefore higher cost to businesses. Conversely, SMS is universally used by all demographics which explains why businesses/organisations use it so widely but also why it is a target for fraudsters. Overall, the impact on consumers is likely to be mixed and consumers are likely to become more open to this Option in the event that scam SMS increase further.

I. Other Impacts

Trust in SMS

6.412 Under Option 1, there would be no trust issues in relation to SMS using a Sender ID since all such communications would be blocked. However, Option

[445] B&A Consumer Survey, slide 38.

1 would be unlikely to significantly improve trust in SMS generally. Fraudsters would still send scam SMS regardless of whether Sender IDs were blocked or not. Contagion and related effects would still occur as fraudsters would also continue to impersonate businesses through copying text their language format using normal or spoofed numbers. There is no reason to think that consumers would trust SMS communications more because a subset of those communications (i.e., Sender ID) are blocked.

Option 3: Full Sender ID registry

I. Direct impacts

6.413 Under Option 3, a full Sender ID registry would reduce the harm from scams by preventing fraudsters using Sender ID spoofing. Only businesses with Sender IDs that are registered would be permitted to send SMS to consumers using a Sender ID – all other Sender IDs would be blocked. This would be available for all businesses and organisations that are registered and would not be limited to the larger users of Sender IDs. Consumers could be confident that any SMS that they receive with a Sender ID is from a reputable organisation.

6.414 Europe Economics estimates that Option 3 would reduce the value of the present harm to consumers and businesses by €372 million over a seven-year period, or roughly €53 million annually[446]. However, similar to Option 2, this reduction in harm could be temporary as fraudsters divert any remaining SMS scams to messages without Sender ID.

II. Other impacts

Trust in SMS

6.415 Option 3 would restore and safeguard trust in SMS that use a Sender ID because consumers would have a high level of assurance that such SMS are valid and sourced from genuine businesses and organisations. This would prevent contagion from occurring at the outset and consumers would be significantly more likely to engage with such SMS thereby lowering the 'SMS reduction effect' and promoting the efficient use of the underlying number used to deliver such SMS. Higher rates of SMS engagement increase the effectiveness and efficiency of SMS as a means of communication, thereby increasing the utility and use of SMS by senders.

6.416 Most importantly, Option 3 preserves the benefit of Sender IDs to SMS as a means of B2C communications, as noted by Twilio: "*Benefits of messaging*

[446] See Table 9.10 and Table 9.11 the Europe Economics Report.

with Alphanumeric Sender ID….Higher message deliverability…Improved brand recognition…Increased open rates…Alternative to 10DLC A2P messaging"[447]. The effectiveness of SMS for B2C would recover as Sender ID spoofing is prevented and consumers become more likely to trust, open and read SMS that use IDs. This is turn would lower the feedback effect by encouraging organisations and businesses to use SMS as a means to communicate with their consumers. Finally, such organisations that deliver important public and social services would be able to register their Sender ID allowing vulnerable groups to receive services without the worry of knowing whether such SMS are genuine or from fraudsters. For most businesses the cost of registration would be likely to be of little consequence[448].

Option 4: Partial Sender ID registry

I. Direct impacts

6.417 Under Option 4, businesses and/or organisations that send a large amount of SMS using Sender IDs (e.g., banks, delivery companies etc) would be required to register their Sender IDs and all other Sender IDs would be blocked. The purpose of this approach would be to ensure that only those businesses/organisations that are currently being impersonated or have a specific requirement for Sender IDs would be permitted to use them. This would reduce the range of Sender IDs that consumers receive, reducing confusion and potentially increasing engagement with businesses/organisations that have a strong requirement for using Sender IDs (i.e., banks and important public services).

6.418 The reduction in scams (and associated harm) would be substantial, noting that the majority of the Sender ID spoofing relates to a small number of businesses. Under Option 4, scam SMS using Sender ID spoofing would be significantly reduced because all the main Sender ID users (e.g., banks, postal delivery, etc.) would be included in the SMS Registry. This should reduce the effectiveness of scam SMS more broadly by removing key Sender IDs which can be used by fraudsters to impersonate businesses. Option 4 would be an enhancement compared to Option 1 and Option 2 because the largest users of Sender ID could continue using this method of communications and consumers would have a higher level of confidence that messages received with such Sender IDs would be valid. This would reduce the harm to consumers because a main avenue for impersonation would be closed off. Europe Economics estimate that Option 2 could reduce the present

[447] Twilio Website "Alphanumeric-Sender-ID-for-Twilio-Programmable-SMS" Link
[448] ComReg has not determined what fee, if any, would apply to Sender ID registration. By design, any such fee should be so low as to not prevent use, even to small companies that could realistically wish to make use of Sender IDs. This would be a matter for future consideration once ComReg has more information regarding the cost of a Sender ID registry and the demand for Sender IDs.

harm by as much as €317 million over a 7-year period[449].

6.419 However, Option 4 would restrict the business/organisations that would be able to use the registry. Some businesses/organisations that would prefer to be included in the registry would need to use alternative methods of communications which could be inferior to the current arrangements. The extent of this approach would depend on where the threshold for inclusion was drawn (not an insignificant task that could lead to other economic effects[450]) but ultimately some businesses/organisations would not be permitted to use Sender IDs.

6.420 Such businesses/organisations would likely include social clubs, local delivery services etc. While these businesses/organisations are not widely impersonated at the moment they may have a use for Sender IDs. Furthermore, placing a restriction on those businesses/organisations who currently use Sender IDs to only display their originating number instead would likely create some consumer confusion for those who are used to receiving SMS with Sender ID. Indeed, consumers may inadvertently become suspicious of genuine SMS received from those businesses/organisations that previously used Sender ID.

II. Other impacts

Trust in SMS

6.421 Option 4 would restore and protect trust in SMS in a similar way as described in Option 3 because consumers would have a higher level of confidence that such SMS are valid and sourced from genuine businesses and/or organisations. However, as previously noted, some consumers may consequently distrust valid SMS from smaller businesses/organisations who previously used Sender ID but would not be permitted to do so under this option.

Conclusion on impact on consumers

6.422 Based on the assessment above, ComReg is of the view that Option 3 (Full Registry) is likely to be preferred by consumers and businesses as it balances the benefits of preventing Sender ID spoofing with safeguarding the trust in and use of SMS, Sender ID and Irish MNs more generally. In particular, this option provides consumers a high degree of confidence that any SMS with Sender IDs are valid and that these Sender IDs are available to all businesses/organisations.

[449] See Table 9.9 of the Europe Economics Report.
[450] For example, ComReg's threshold could create unintended consequences of allowing some business in the registry but excluding competing businesses simply because the volume of texts used is smaller.

Table 18: Reduction in harms under Option 1-4, relative to status quo

Option	Benefits to Irish society
Option 1 (No regulatory measures)	-
Option 2 (Sender ID Ban)	No precise figure – Reduction in harm from scam SMS offset by loss of Sender IDs
Option 3 (Full Sender ID Registry)	Over 7 year – €327 Million Annually - €53 Million
Option 4 (Partial Sender ID Registry)	Over 7 year – €317 Million

II. Impact on industry stakeholders

6.423 The relevant industry stakeholders among those outlined in Section 5.2.4, are the following:

1. Networks that terminate SMS traffic;
2. SMS aggregators; and
3. Other operators (Resellers, including MVNOs).

6.424 ComReg does not gather information on SMS aggregators sending SMS traffic into Ireland, which likely includes firms with no presence in Ireland[451]. Based on discussions with different MNOs and businesses, ComReg estimates that there are approximately 30 such SMS aggregators.

6.425 This section provides information on the impacts on industry stakeholders (as outlined above) arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., Implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

6.426 For the purpose of this assessment, ComReg assumes that no costs have been incurred to date[452]. This approach appears most reasonable, as it considers the maximal impact of each option, as it presupposes all costs lie ahead of the operators. In this way, the assessment examines the impact of the Options on the "least prepared" or "greenfield" operator and is therefore

[451] Therefore not subject to ERAU registration.
[452] Under the status quo, operators may choose not to incur costs by electing not to undertake any technical measures to combat scams. Indeed, certain operators have informed ComReg that they would await a regulatory requirement before undertaking further work on technical specifications in this RIA.

conservative assuming no progress to date. MNOs have made some progress in implementing Sender ID filtering, and many of the relevant financial costs have already been incurred.

Option 1: Do Nothing

I. Direct impacts

6.427 Under Option 1, no regulatory interventions to combat scam SMS would be mandated on operators. Therefore, this option would not impose any direct financial costs on those operators.

II. Other Impacts

6.428 The present level of scam SMS is reducing trust in Sender IDs and SMS and ultimately reducing the use of SMS for B2C.Therefore, absent intervention, scam SMS could negatively impact the revenues generated by operators from providing SMS services, and operating networks over which SMS services are generated. Under this option, the harms to operators would continue to occur and the scope for operators to benefit commercially from being able to offer networks of trust would be reduced because the present level of scam SMS are reducing trust in SMS.

6.429 Operator reputations would also continue to be damaged as scam SMS proliferate across society negatively impacting the revenues generated by operators from providing such services. Further, as consumers and businesses move away from SMS communications there is less scope for operators and aggregators to generate commercial opportunities. For example, Europe Economics notes that the survey shows that consumers have been moving away from traditional telecommunication by reducing their reliance on public phone networks and SMS aggregators for contacting customers (i.e., the feedback effect referred to earlier), a fact which should be concerning for operators and SMS aggregators.[453]

6.430 Therefore, operators are likely to prefer measures that reduce the rate of scam SMS and are unlikely to prefer Option 1.

Option 2: Ban Sender IDs

I. Financial impacts

6.431 Under Option 2, the three Irish MNOs (Eir, Three and Vodafone) would block all SMS messages containing a Sender ID. ComReg understands that all MNOs have this capability at least to some extent and could implement this

[453] Europe Economics, page 53

measure at a relatively low cost.

II. Other Impacts

6.432 Despite its low cost and effectiveness in reducing the harms in the short run ComReg expects that no MNO or aggregator would likely prefer this Option over any of the alternatives, given the unavoidable negative impact this option would likely have on the use of SMS for B2C and resulting revenues (i.e., operators would be unable to provide an SMS with Sender ID service to businesses/organisations) This would also negatively impact the business of SMS aggregators which originate and transit SMS for B2C on behalf of businesses (often with Sender IDs).

Option 3: Full Sender ID registry

I. Direct impacts

6.433 Under Option 3, MNOs would block all SMS with a Sender ID except those registered and sent from the registered owner via an approved participating aggregator. Interested organisations could apply to register Sender IDs via an online portal, open to all businesses/organisations meeting certain eligibility criteria. A list of protected Sender IDs would be maintained by ComReg and shared with MNOs.

6.434 The costs of operating the registry would fall on ComReg, however it also imposes certain costs on the Irish MNOs and aggregators.

- For MNOs, the blocking component would entail some costs (including those SMS scams that could spoof Irish mobile numbers) to operators to implement, such as internal project activities i.e., design, implementation, testing. However, as noted above these are expected to be relatively modest.
- Aggregators would incur costs of setting up new connections to local MNO(s), if not in place already. They would also incur business costs of onboarding and authenticating new Sender ID owners and implementing and validating the required Sender ID filtering.

6.435 To inform ComReg's assessment, Europe Economics has estimated both the one-off costs (e.g., the cost of software purchase and installation) and on-going cost (e.g., on-going cost of software) of a partial Sender ID register for MNOs and aggregators. Europe Economics estimates one off costs of approximately €150,000 for each MNO with annual on-going costs of approximately €20,000[454], and one-off costs of €123,000 for each

[454] Europe Economics Report, Table 9.3.

aggregator[455].

6.436 Therefore, Option 3 would impose a greater cost on Three, Vodafone, Eir and participating aggregators[456], as shown in Table 19 below.

II. Other Impacts

6.437 SMS aggregators may incur greater costs under Option 3 because they will no longer use least cost services which are difficult to secure and will instead connect a greater number of Sender IDs and Sender ID owners. However, it should be noted that there are commercial opportunities for participating aggregators in providing trustworthy services to businesses/organisations. In particular, under this option, any business/organisation in the State could register their Sender ID increasing the number of participating businesses/organisations compared to Option 1 where all Sender IDs would be banned or Option 4 where only businesses/organisations above certain thresholds would be included. A more secure Sender ID regime would provide even greater value to SMS for B2C for large businesses, potentially generating greater revenues for MNOs and participating aggregators (either through increased demand at existing prices or through higher prices.).

6.438 Furthermore, any increased costs may be offset by increased revenues under Option 4, as a result of greater demand for SMS for B2C, potentially generating greater revenues for operators (i.e., increased demand at existing prices or through higher prices). This should be expected given the greater number of potential organisations using Sender ID and generating SMS traffic and improved trust in Sender IDs more generally.

Option 4: Partial Sender ID registry

I. Direct impacts

6.439 The direct impacts under Option 4 are the same as under Option 3 because both involve the implementation of the registry, and the same costs of implementation would be incurred by MNOs. This would impose slightly lower one-off costs of approximately €107,000 per SMS aggregator.

II. Other Impacts

6.440 Option 4 would reduce the harms from Sender ID spoofing and restore and protect trust in Sender IDs. This should help protect the long-term commercial interests of MNOs and SMS aggregators. However, because Option 4 would exclude many businesses from using Sender IDs for B2C, operators and

[455] Europe Economics Report, Table 9.4
[456] Any operator willing to undertake the necessary actions could become a patriating aggregator.

aggregators are unlikely to prefer this option. This could reduce the number of businesses using Sender IDs which would limit the demand for these services.

6.441 Non-participating aggregators could be negatively impacted by a partial SMS registry through a reduction in transiting of SMS with Sender IDs. This is an unavoidable consequence of a Sender ID registry, which relies upon the actions of known and compliant aggregators. However, an aggregator can easily address this by undertaking the necessary actions to become a compliant participating aggregator. ComReg expects that most, if not all, SMS aggregators that send significant volumes of SMS traffic to Ireland currently would participate.

Table 19: One-off costs per stakeholder for each Option, relative to status quo

Option	MNOs	SMS Aggregators
Option 1 (Do nothing)	-	-
Option 2 (Ban Sender IDs)	Some loss of revenue	Some loss of revenue
Option 3 (Full Sender ID Registry)	€150,000	€123,000
Option 4 (Partial Sender ID Registry)	€150,000	€107,000

Conclusion on impact on industry stakeholders

6.442 Based on the assessment above, ComReg is of the view that Option 3 is likely to be preferred by most stakeholders because it balances the benefits of preventing Sender ID spoofing with the costs of implementation. More generally, the wider business community would prefer Option 3 because any businesses/organisations could continue to use Sender IDs. Those Sender ID owners excluded under Option 4, would therefore likely prefer Option 3 because SMEs are less likely to feature on a partial registry.[457]

III. Impact on competition

6.443 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the statutory objectives outlined in 6.2.2, there are three broad categories of impacts relevant in this section:

[457] The threshold for inclusion on any potential partial Sender ID registry is currently unknown at this time and therefore only a small number of companies could be sure to access a Sender ID registry under Option 3 (e.g., banks)

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on the efficient investment arising from the regulatory option is assessed.

Option 1: Do Nothing

Efficient use of numbers

6.444 Against the objective of ensuring the efficient and effective use of numbers for the benefit of consumers, it is evident that under Option 1 the numbering resource is not being used efficiently or effectively and this is resulting in observable, significant consumer harm (as described in Section 6.2.1). In summary, a situation where 38 million nuisance SMS and 14 million distressing SMS are made to consumers every year, with approximately 500 consumers a day being defrauded by scam SMS, is clearly not consistent with the efficient and effective use of the numbering platform and constitutes a serious misuse of numbers.

6.445 As noted above, numerous scam SMS exploit the lack of protection afforded to Sender IDs at present, with fraudsters using Sender ID spoofing to spoof businesses/organisations, including important public services. In this way, Sender IDs are being used to perpetuate fraud and undermine ECS networks more generally. Option 1 is therefore not consistent with the efficient use of Sender IDs (a form of numbers), and this constitutes misuse of an important national resource. As outlined above, should scam SMS using Sender ID continue, consumers may adapt by not reading SMS messages potentially undermining the legitimate use of Irish numbers.

6.446 Finally, given that such misuse has been allowed to proliferate over the last number of years, it is clear that operators do not have processes in place to reduce access to valid numbers by those who intend to misuse them. The misuse of the numbering resource is therefore likely to continue and multiply under Option 1 as fraudsters become more sophisticated. Operators do not have processes in place to reduce access to numbers by those who intend to misuse them. In particular, the lack of or inadequacy of any assignment processes used by operators has led to bad actors getting access to numbers that are ultimately used to perpetrate fraud. See Chapter 5 for more information on ‘Know Your Customer’ initiatives that operators could be enforcing in order to reduce the misuse of numbers.

Promoting competition

6.447 Competition has not delivered a satisfactory level of scam text protection to date. ComReg considers that there are a number of reasons for this which are similar to those previously set out in respect of voice services. These are outlined in paragraphs - above but in summary are as follows.

- The incentives to provide SMS protections are not sufficiently high because the majority of the harms due to scam SMS are not borne by operators themselves and are instead being borne by consumers and businesses that they serve. Absent this competitive pressure operators face little incentive to invest in scam protection in the short run.
- Operators are likely concerned that such investments even if they were made would prove inefficient if other operators did not replicate similar interventions. For example, operators may rationally underinvest in interventions whose effectiveness relies upon the coordinated implementation by many other parties. As outlined in Section 5.2.2, this is true of a number of the interventions being considered in the Consultation, including the Sender ID registry – which relies upon implementation and coordination between operators and a large number of SMS aggregators.
- There is little evidence of key businesses attempting to procure better protected SMS services for B2C. This view is corroborated by the lack of action, and in certain cases the apparent indifference, of key businesses in attempting to procure better protected services (e.g., ComReg is unaware of any business or bank switching SMS messaging provider to improve the protection to date[458]).
- Operators may be sceptical that competing for customers on the basis of protection against nuisance communications would cause sufficient switching to justify relevant investments. This creates a feedback effect where consumers who may be willing to switch due to impact of scam SMS cannot do so because protected services are not being provided.

6.448 Given the prevalence of scam SMS, it would appear that competition has not provided sufficient incentives to protect consumers, leading to a market failure and socially suboptimal levels of investment in measures to tackle scam SMS. If networks are not timely in offering sufficient protections, despite the significant harm caused by these communications, it would prima facie suggest a possible competitive failure. Clearly identifiable harms (as evidenced in Section 6.2.1) for important services (e.g., voice and SMS) should be addressed in a well-functioning competitive market over an

[458] ComReg has discussed this with key businesses and found little to no willingness or intention to switch SMS provider to reduce SMS scams and fraud.

appropriate period. However, that is clearly not the case with respect to scam SMS in Ireland. ComReg notes that industry-wide interventions may ultimately be required in order to properly address nuisance communications.

6.449 Therefore, ComReg remains of the view there is a serious risk of continued under investment absent intervention. This is highly undesirable as, absent intervention, the present level of scam SMS and fraud may distort competition between providers of the following.

I. SMS services because declining use of SMS due to 'the SMS reduction effect' would lead to a reduced incentive to compete between providers of SMS services. It is unlikely that the current uncoordinated approach would lead to a similar level of protection across all operators and choice between operators could become distorted by perceived, and not actual level of protections afforded. The impact of any such distortions could be uneven as operators have different businesses, services and subscriber bases.

II. SMS services and OTT/Instant Messaging platforms (e.g., WhatsApp) because consumers and businesses may no longer see SMS as a viable option which would reduce infrastructure-based competition. Consumers and businesses may move to alternative messaging platforms, despite preferring SMS at present[459] (e.g., OTT for P2P[460], or apps, email or push notification for B2C[461]). Such transitions to alternative messaging platforms may become permanent if consumers lose trust in SMS entirely as would likely be the case absent interventions. Finally, the declining use of SMS may lead to reduced investment and further reduce competition between providers of providing SMS services and alternative instant messaging platforms[462].

Efficient Investment

6.450 Under Option 1 there is a risk that the investments already made voluntarily by some operators would become inefficient. For example, investments by some operators who have already implemented or begun implementing Sender ID filters (or would do so in the future under this Option) could become inefficient if other operators do not make concurrent investments. As

[459] Inferior in the sense that at present consumers and businesses choose SMS for certain services, revealing a current preference for SMS as a means of communications for those services.
[460] Which is potentially subject to more QoS issues due to latency and potentially less trusted due to a lack of numbers.
[461] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish Geographic Numbers.
[462] For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform.

previously noted, any uncovered operator potentially undermines an operator's investment as fraudsters would likely exploit that 'gap' to reach all consumers including those that made an investment.

6.451 Further, under Option 1, operators would face lower incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications (i.e., 2018/2019) may now become inefficient because such investments were made on the basis of an effectively functioning numbering platform. This may also reduce the incentive for future investments if operators are of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

Option 2: Ban Sender IDs

Efficient use of numbers

6.452 Option 2 would prevent Sender ID spoofing, leading to reduced misuse of Sender IDs (which as previously discussed is a form of number). This would also reduce the misuse of mobile numbers by reducing the volume and effectiveness of scam SMS impersonating businesses/organisations because it would prevent scam SMS using Sender ID spoofing (which are popular with fraudsters at present). However, it is likely that fraudsters will continue to use scam SMS without Sender ID Spoofing. Indeed, it is likely that scam SMS that do not use Sender ID (because it would now be unavailable) are likely to increase as scammers adapt. Therefore, while there would be some short-term efficiency benefits to Option 2, they are likely to reduce over time.

6.453 Further, while fraudsters use Sender ID to impersonate businesses, the vast majority of text messages using Sender ID are valid and represent an efficient use of the numbering platform[463]. Option 2 would block the use of all these numbers in the same breath as blocking those which may be used for scam SMS. In effect, this option could result in a large number of what would have been efficiently made SMS being restricted in order to combat a comparatively smaller number of scam SMS. The extent to which this would impact the current efficient use of numbers would depend on how businesses/organisations react to potential implementation of Option 2. It could be the case that what previously constituted an efficient use of numbers would move to an alternative (and potentially inferior) platform because of the imposition of this Option. This would be particularly likely to occur absent any measures to protect other SMS communications (i.e., those that don't use a

[463] Sender ID Ban would reduce the legitimate use of Sender IDs to contact Irish consumers. As noted in Sections 3.1-3.2, this is valued as an efficient and effective way businesses/organisations (including public services) to communication with citizens.

Sender ID).

6.454 Therefore, while this Option would clearly reduce the misuse of numbers compared to Option 1 the overall impacts on the efficient use of numbers are unclear and would depend on how businesses/organisations react to the blocking of Sender IDs.

Promoting competition

6.455 Currently, despite the prevalence of scam SMS, providers of SMS services compete to provide B2C services to businesses/organisations. Even if this competition is currently limited due to scam SMS (reducing the utility and use of SMS) there is at least some competition for these services. By contrast:

I. Under Option 2, competition between providers of SMS services would likely be distorted further because Sender IDs which are required by businesses/organisations, could not be offered because of the restriction created by Option 2. Further, it is not clear whether businesses/organisations would use SMS (without Sender ID) for B2C communications under Option 2 because consumers would face even greater difficulty in identifying legitimate SMS from businesses without a Sender ID.

II. Under Option 2 competition between SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would also be distorted because Option 2 removes a key product characteristic of SMS (i.e., the ability to use Sender IDs) and businesses/organisations may be forced to use alternative channels to reach consumers due to the reduced utility of SMS for B2C communications.

6.456 Therefore, competition would likely be reduced under Option 2.

Efficient Investment

6.457 As noted previously, Option 2 would likely reduce the utility of SMS services to businesses/organisations. Accordingly, service providers and businesses /organisations may need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient because it would be driven by the inability to use Sender ID rather than the underlying effectiveness of Sender ID as a method to communicate with consumers. Investment in alternative platforms would entail an unnecessary and avoidable duplication of investment particularly for those businesses/organisations that are already using Sender ID, having invested in the provision of same.

6.458 Therefore, Option 2 is likely to lead to inefficient investment by service

providers and businesses/organisations.

Option 3: Full Sender ID registry

Efficient use of numbers

6.459 As noted in Section 5.2.2, international experience indicates that full Sender ID registries are highly effective at reducing scam SMS that use Sender ID, and the evidence in Ireland demonstrates that many of the most common and effective scams utilise Sender ID spoofing. Under Option 3, scam SMS using Sender ID spoofing (and the underlying numbers) would be significantly reduced. In this way any of the SMS with Sender IDs that are used through the registry would be genuine and would constitute an efficient use of numbers because those SMS do not have the intention to commit fraud and may be of interest to receiving customers. This reduces the potential for numbers to be misused in a way that harms consumers, increasing the overall efficiency of the numbering platform. Furthermore, by reducing the current prevalence of Sender ID Spoofing, Option 3 should enable even greater use of Sender IDs (compared to all other options) because consumers are more likely to trust, open and read SMS containing Sender IDs. This increases the overall utility of the numbering platform as businesses/organisations become satisfied that consumers are engaging more with the communications that they make via SMS.

6.460 Under Option 3, the reduction in misuse should be large because the majority of the scams and fraud appear to relate to a small number of Sender IDs (i.e., those Sender IDs that would be included in the Sender ID Registry). Therefore, Option 3 would likely be effective at preventing the misuse of Sender IDs, particularly in the short term prior to fraudsters adapting to the implementation of the registry. Importantly, and unlike Option 2, it would allow businesses/organisations (above certain volume thresholds) and who are currently using numbers efficiently to register their Sender ID and continue communicate with their customers using this preferred approach. This would allow these numbers to continue to be used efficiently. Further, by reducing the current prevalence of Sender ID spoofing, businesses/organisations should have increased confidence in using Sender ID to communicate with customers enabling even greater use of Sender IDs than at present further increasing the efficient use of the underlying numbers.

6.461 Therefore, Option 3 would likely result in the more efficient use of numbers.

Promoting competition

6.462 Option 3 represents a reduction in the competitive distortions resulting from scam SMS and Sender ID spoofing, as a result of its greater impact on scam

SMS, Sender ID spoofing and trust in and use of Irish numbers relative to Option 1 or Option 2. Therefore, Option 3 represents a reduction of competitive distortions in in general sense. In that respect, Option 3 would better incentivise the competition between aggregators and providers of ECS.

6.463 There are a number of reasons why competition has not delivered a satisfactory level of scam text protection to date, these are summarised under Option 1 above. With that in mind, Option 3 would assist in resolving the coordination problem that operators face in ensuring that only SMS with valid Sender ID are received by consumers. Currently operators have no way of discerning which messages bearing Sender IDs are valid and which are genuine, and this information asymmetry provides opportunities for fraudsters to commit fraud. The Sender ID Registry allows businesses/organisations to select which Sender IDs are valid and this information is provided to operators who block Sender ID's not on the registry. Therefore, Option 3 provides all operators with important information about which Sender IDs are genuine. This would not be possible absent a registry because operators currently only have a limited insight into which Sender IDs are genuine (i.e. based on the services it already provides to businesses/organisations). Furthermore, under Option 3:

I. between providers of SMS services would likely increase because Sender IDs which are required by businesses/organisations would continue to be provided to those that require them. Further, providers would be able to offer SMS with Sender ID services that provide significant protection against Sender ID spoofing. Businesses/organisations should therefore have increased confidence in using Sender ID to communicate with customers enabling even greater use of Sender IDs – This is likely to attract new businesses/organisations which providers would compete for.

II. between SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would also be increased because Option 3 provides protection against spoofed Sender ID meaning the choice made by businesses/organisations would be based on the underlying effectiveness of the SMS platform rather than because of scam SMS. Option 3 preserves competition between providers of SMS services and other alternative messaging services, through protecting the use of SMS more generally.

6.464 Therefore, Option 3 would better promote competition compared to Option 1 and Option 2.

Efficient Investment

6.465 Option 3 would accord with and further the regulatory principle of promoting efficient investment and innovation in new and enhanced infrastructure by allowing operators to avoid what would otherwise be inefficient infrastructure investment. In particular, by preserving the use of and demand for SMS communication, Option 3 benefits operators that may otherwise need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient being driven not by unmet need but by a degradation of existing SMS network's ability to continue to meet the existing need for such services. Furthermore, SMS aggregators' investments in their business model may be unnecessarily supplanted by third parties offering B2C communications via OTT or via App.

Option 4: Partial Sender ID registry

Efficient use of numbers

6.466 Option 4 is similar to Option 3 in that it would block all spoofed Sender IDs. However, not all businesses/organisations would be able to benefit from the protection provided by the registry. In particular, small businesses/organisations would need to use alternative platforms in order to communicate with consumers. This would lead to the same inefficiencies as identified under Option 2 save that it would apply to smaller number of potential users. The extent of these inefficiencies would depend on the criteria for inclusion in the registry, but it would, by definition include only a subset of businesses/organisations. This reduces the efficiency of the numbering platform because the volume of SMS used by those businesses/organisations would be reduced arising from a restriction on legitimate use of Sender IDs. Further, Option 3 would potentially restrict the use of what would have been genuine communications (and their underlying numbers) for the sake of a potentially smaller amount of scam SMS.

6.467 Therefore, while Option 4 would prevent the misuse of number in the same way as Option 2, it would not lead to the more efficient use of numbers compared to Option 3 because the numbers used by certain businesses/organisations would be restricted from using the Sender ID Registry.

Promoting competition

6.468 Similar to Option 3, Option 4 would also assist in resolving the coordination problem that operators face in ensuring that only SMS with valid Sender ID are received by consumers. This Option allows businesses/organisations to select which Sender IDs are valid and this information is provided to operators who block Sender ID's not on the registry. Importantly, however, Option 4 restricts the protection offered by the registry to certain

businesses/organisations. These businesses/organisations would be even less likely to use SMS services for B2C because the restriction would prevent operators from competing to provide Sender ID services to businesses/organisations who would normally avail of such services. Furthermore, businesses/organisations that are currently availing of Sender ID services may be below any threshold for inclusion noting that Sender ID services are currently being availed of by businesses/organisations with relatively low SMS volumes (e.g., GAA clubs and local businesses). Operators that are currently providing these services may be unable to facilitate such businesses/organisations in the future and there would be no alternative providers that could provide SMS using Sender ID.

6.469 Further under Option 4, competition between:

I. providers of SMS services would likely remain relatively static. While Sender IDs which are required by the largest businesses/organisations would continue to be provided to those that require them, there would be restrictions because only a subset of businesses/organisations would be eligible for inclusion in the registry. In particular, the scope for competition would be limited by the extent of the restriction on the registry.

II. SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would be limited by the extent of the restriction on the registry. Option 3 provides protection against spoofed Sender ID for larger businesses/organisations thereby increasing competition between providers of SMS services and other alternative messaging services. However, the restriction would mean that some businesses/organisations would use alternative platforms not because SMS is ineffective but because SMS using Sender ID would be unavailable.

6.470 Therefore, while Option 4 is better for competition than Option 1 or Option 2, it is less likely to promote competition compared to Option 3.

Efficient Investment

6.471 Under Option 4, operators would be required to implement each of the processes and associated costs required for the implementation of Sender ID Registry. However, because of the restriction imposed by this option it would be unable to reap the full benefit of those costs and would therefore be an inefficient investment.

Conclusion on impact on competition

6.472 Based on the assessment above, ComReg is of the view that Option 3 best

promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

6.473 The above assessment and the Europe Economics Report demonstrate that there is currently a significant consumer and societal harm present due to scam SMS and much of this harm arises from spoofed Sender ID. Blocking all SMS that use Sender ID under Option 2 would clearly stop fraudsters spoofing and remove the harm created by spoofed Sender IDs. However, this would prevent genuine use of Sender ID and reduce the viability of the SMS platform, reducing competition between providers and across platforms. A partial registry under Option 4 would provide protection to those businesses/organisations that are most impersonated by fraudsters. However, its restriction to a subset of businesses/organisations means that the benefits of a viable SMS platform would be denied to those that require it, again reducing competition and creating inefficient investments. Option 3 however extends the benefit to all businesses/organisations who wish to use Sender IDs and because of this the protection it would provide would encourage other businesses/organisations that may have concerns to engage with the SMS platform. This would promote greater competition between providers and across platforms. Therefore, ComReg is of the view that, on balance, Option 2 and is the preferred option in terms of its impact on stakeholders, competition and consumers.

6.474 ComReg notes that this RIA relates to scam SMS using Sender ID only, and other scam SMS (e.g., those that do not use Sender ID) will be discussed separately in a RIA in the forthcoming consultation on a SMS Scam Filter.

6.6 Assessment of the Overall Preferred Option (Step 5)

6.475 ComReg is of the view that the Interventions as discussed in each of the RIAs above are the best means of combating scam call and SMS at this time in terms of its impact on consumers, industry stakeholders and competition and in line with its statutory objectives.

6.476 ComReg now examines the cumulative cost and benefit of all interventions assessed in Consultation 23/52 (i.e., the Proposed Package)[464] on identified industry stakeholders given the interdependencies between interventions. This informs ComReg's assessment of the Overall Preferred Option.

6.477 The remainder of this section summarises the Overall Preferred Package in terms of its:

I. Impact on Irish consumers and businesses;

II. Impact on industry stakeholders; and

III. Against ComReg's statutory objectives (Step 5)

6.6.1 Impact on Irish consumers and businesses

6.478 ComReg considers that the Overall Preferred Option best reduces the current and future harm described in Section 6.2.1 and is also best placed to protect and restore trust in Irish numbers as described in each of the RIAs. EE estimates that all the Interventions have positive estimated net benefits[465]. However, the total benefit of the Overall Preferred Option depends on the reaction of the fraudsters to each of the individual interventions again noting that fraudsters have the capability to switch between technologies and scams in response to each of the interventions[466].

6.479 As noted by Europe Economics, dynamic interventions such as the Voice Firewall are important and provide net benefits in the hundreds of millions even where fraudsters only minimally adapt to the static interventions, because they offer protection that cannot be provided by the static

[464] For the purpose of this section, ComReg has retained the SMS Scam Filter despite it not forming part of the Interventions, to provide a better overview of the potential impact of all potential interventions. Otherwise, important context could be overlooked by underestimating the potential ultimate cost of interventions to operators (which could include a SMS Scam Filter), or the net benefit of interventions (noting that the SMS Sender ID Registry is supported by the SMS Scam Filter). It should be noted that none of the conclusions in this section are affected by the inclusion of the SMS Scam Filter, noting the figures provided by Europe Economiocs demonstrate the large positive net benefit of the intervention with, or without, the SMS Scam Filter.
[465] This is shown by examining the effectiveness of the firewalls as a standalone intervention, which leads to a far greater impact. This is the result of the firewalls, in this case, hoovering up the same share of the now greater remaining harm.
[466] Each of the RIAs above carefully considered the impact of other relevant interventions (e.g., the Voice Firewall RIA took into consideration that Mobile and Fixed CLI blocking would also be implemented.).

interventions (e.g., against scams originating in Ireland). However, they become increasingly more important the more fraudsters adapt to ComReg's static interventions, rising to over a Billion euros collectively in a scenario where fraudsters fully adapt (i.e., where the benefits of the static interventions come to zero). Emerging international evidence indicates that scammers have already begun adapting to static interventions in the countries which were first to implement them (e.g., Protected Numbers in Australia).

6.480 In reality, fraudsters will use a mix of methods, and while fraudsters are likely to adapt to ComReg's static interventions, this will require time and it cannot be ruled out that they may reinitiate old scams in the future. The reaction of fraudsters will fall somewhere between not reacting at all or fully adapting to the interventions. However, regardless of how fraudsters adapt, the benefits of the Overall Preferred Option will range between €1.3 and €.9 billion over seven years, with an average value of €1.2 Billion across the modelled scenarios[467]. This corresponds to a benefit of €55 for every €1 spent on the interventions[468].

Table 20: Europe Economics estimates of benefit of the interventions, dependent on level of adaptation by fraudsters.

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers fully adapt to static interventions
Voice interventions			
Static Voice interventions	€4.5m	€899m	-4.5m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS Scam Filter [469]	€6.2m	€197m	€514m
Combined			
Total	**€27m**	**€1.6bn**	**€1.4bn**
Combined without SMS Scam Filter			
Total	**€21m**	**€1.3bn**	**€.9bn**

6.481 Failure to take comprehensive action to protect Irish consumers could result in Irish consumers being targeted by international scammers. This risk will

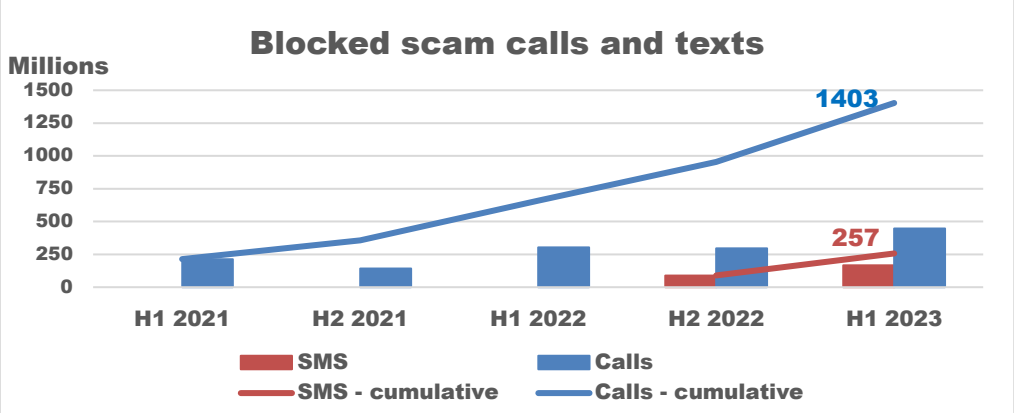
[467] ComReg accepts the average of this range, €1.2 billion, as the expected net benefit of the Interventions, as scammers will undoubtedly adapt to some degree.
[468] See Europe Economics 24/24a for further information.
[469] Once again, ComReg has left in the SMS Scam Filter to highlight its interaction with the Sender ID Registry. The SMS Scam Filter provides interlocking support for the Sender ID registry as scammers switch from forms of smishing which do not utilise SenderID spoofing.

increase with time as other NRAs take action and are successful in deterring scammers from targeting their citizens. For example, Australian operators, government and regulatory agencies have introduced a range of measures that could leave Ireland more exposed than its peers in the Anglosphere.

Case study – the work to combat scams in Australia.

Following the ACMA's registration and enforcement of rules to identify and block scam calls in December 2020, and scam text messages in July 2022, telcos have reported over 1.4 billion scam calls and over 257 million scam messages have been blocked to the end of the quarter.

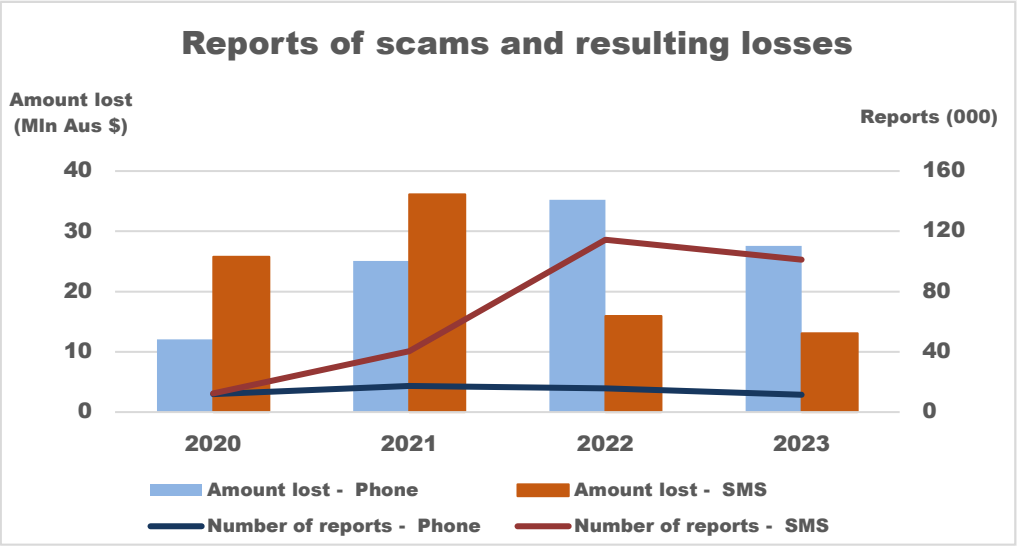
Figure 32: Scam calls and texts blocked by Australian telecommunication operators, H1 2021-H1 2023



Source: ACMA Blocking statistics

There is evidence that the efforts of Australian telecommunication operators to block scam calls and texts is having real impact and protecting consumers. Data from Scamwatch, a government website aimed at raising consumer awareness and enabling consumers to report scams, indicates in 2023 the number of reported scams and monies lost to both "Phone" and "SMS" scams falling.

Figure 33: Scams calls and texts reported by Australian consumers to Scamwatch, 2020-2023



Source: ACCC Scamwatch's scam statistics

6.6.2 Impact on industry stakeholders

6.482 ComReg considers that the Overall Preferred Option best protects the business interests of affected operators in the long-term by protecting and promoting the trust in and use of Voice and SMS as described in each of the RIAs. However, ComReg is cognisant that it is primarily operators that bear the cost of implementing such interventions (with the exception of ComReg for Sender ID registry). ComReg has taken care to ensure that the Interventions is delivered in the least onerous form (see Section 6.2.2-6.2.4 as well as the changes made to certain interventions in relation to operators concerns)[470] and without imposing an excessive cost on any individual operator (see "Impact on Stakeholders" within each RIA).

6.483 Further, while the cost of individual interventions was assessed in each RIA, it is the total cost of all interventions that will be borne by operators. Therefore, ComReg assesses the burden of the interventions on identified industry stakeholders, by examining the cumulative one-off cost[471] associated of the Overall Preferred Option.

6.484 For each of the MNOs, the cumulative upfront cost of all the Interventions is approximately €2 million per MNO or €5-6 million for the mobile industry (i.e., the three mobile operators). This corresponds to a fraction of a per cent of total retail revenues earned in 2023. These revenues are all likely to increase in 2024 and beyond, in line with operators well flagged price increases. ComReg notes that some operators have defended their annual price increases based on generating revenues to finance investment in the upgrade of networks and services[472]. It is inconceivable that such upgrades would not include measures to protect their customers from criminals who are committing fraud using the very same services provided over their networks.

6.485 The annual ongoing costs of these interventions to mobile operators is a modest cost of doing business (given the benefits it provides) and very minor relative to other annual operating costs (e.g., some operators spend over €10 million annually on marketing[473]).

6.486 Similarly, in relation to Virgin and BT the proposed interventions across both its fixed and mobile customers would amount to approximately €1 million or a

[470] ComReg made changes to certain interventions in response to submissions by respondents, which have the effect of reducing their cost (e.g., Mobile CLI Phase 1, Mobile CLI Phase 2, Sender ID Registry).
[471] One-off costs are used here to provide simple single-year comparison. Europe Economic estimates the one-off and on-going going costs, both of which are included in the estimated Net-Benefits.
[472] For example, Eir stated that "*In light of the significant and continued investment in our fibre and mobile network and the rising cost of inflation, we are writing to let you know of some changes to your eir service(s).*" Home (eir.ie)
[473] For details on the latest price increases (April 2024) please see CPI Price Increase (three.ie) Annual Price Adjustment | Vodafone Ireland Annual price change (eir.ie)

fraction of a percent of eithers annual revenues. Similarly, the annual operating costs are approximately €100,000, a fraction of a percent of eithers current annual cost of sales. Virgin Media has also announced significant annual price increases from April 2024 to invest in technology and give a better experience to customers, among other things[474].

6.487 The one-off costs for remaining operators are all low and represent a small cost of doing business relative to the size and scale of those operations. For example, while there are potentially small voice originators that would be required to implement the DNO/PN List, the estimated one-off cost is approximately €30,000. Furthermore, ComReg has adjusted its proposals on Phase 1 of Mobile CLI in order to reduce the costs further on smaller operators (i.e. those operators do not now bear any costs for Phase 1 of Mobile CLI).

6.488 More generally, the one-off costs for all affected parties of implementing their respective interventions are dwarfed by their annual revenues, as shown in Table 21 below. Indeed, the entire NPV cost of the interventions to industry (i.e., from 2024-2030) is €21 million, which is only a fraction of total capital expenditure in a given year[475]. In other words, a fraction of a single year's investment in networks would protect mobile and landline users for many years to come[476]. Moreover, the annual ongoing costs of these interventions to operators is a modest cost of doing business (given the benefits it provides) and very minor relative to other annual operating costs. It therefore appears unlikely that the cumulative cost of the interventions is excessive on any of the firms that are required to implement the interventions.

6.489 Finally, while ComReg takes account of costs likely to arise from its proposed measures, it also recognises that any such impacts should be balanced against the benefits of achieving relevant statutory objectives, including promoting the interests of other users (i.e., consumers), protecting consumers more generally, promoting competition, and ensuring the efficient and effective use of numbers.

[474] Price increase 2024 | Virgin Media
[475] QKDR Q2 2023 - Investment in mobile telephony
[476] Noting that operating costs are small relative to one-off costs.

Table 21: Estimated one-off costs per stakeholder for all interventions.

Operator Type	Interventions	Approximate total cost	Annual ECS revenues in Ireland in 2022/23[477]
MNOs	All Voice and SMS	€1.8 million	**Three** - €619 million[478] **Vodafone** - €981 million[479] **Eir** - €1.2 billion[480]
Large IGO with a Voice Firewall	All Voice, lower cost for Mobile CLI	€1.6 million	€385 million[481]
Large IGO	All Voice excl. Firewall	€435,000	€343 million[482]
Other IGOs	DNO/PN, Mobile and Fixed CLI Call Blocking	€80,000	€10 million-€100 million[483]
SMS Aggregator	Sender ID registry	€123,000	€1 million -€10 million[484]
Voice originator	DNO/PN	€33,000	€1 million -€10 million [485]

6.6.3 Preferred Options across the RIAs – Mandate all measures (Step 5)

6.490 Considering the above, ComReg is of the view that the preferred option in terms of the impact on stakeholders, competition and consumers (the "Overall Preferred Option") is to require:

a) DNO/PN by all originators of Voice traffic capable of terminating on public networks;

b) Fixed and Mobile CLI Call Blocking by all IGOs carrying Voice traffic capable of terminating on public networks into the State;

c) A Voice Firewall by all operators of public networks in the State with more than 330,000 subscribers or lines capable of receiving Voice calls;

d) A full Sender ID registry by all operators of public mobile networks in the State capable of terminating SMS; and

[477] These represent the most recent data available to ComReg. Where data was unavailable ComReg has provided expected lower bounds. Revenues and expected revenues are presented to enable comparison between the implementation cost and operators' revenues, to highlight the difference in magnitude.
[478] Three Ireland (Hutchinson) Limited, "*Directors' Report and Financial Accounts for the year ended 31 December 2022*".
[479] Vodafone Ireland Limited, "*Annual Report and Financial Statements for the year ended 31 March 2023*".
[480] Eircom Limited, "*Directors' Report and Financial Statements for the year ended 31 December 2022*".
[481] Virgin Media Ireland Limited "*Directors' Report for the year ended 31 December 2022*".
[482] BT Communications Ireland Limited "*Directors' Report and Financial Statements for the year ended 31 March 2023*"".
[483] This broad range is informed by CRO filings, noting that information was not available for all operators.
[484] This broad range is based on judgement, noting that SMS Aggregators are not necessarily based in Ireland and ComReg therefore has limited visibility of such operators' revenues.
[485]This estimated lower bound is informed by CRO filings, noting that information was not available for all operators.

6.491 This assessment has considered the impact of the various options from the perspective of industry stakeholders, as well as the impact on competition and consumers, and should aid stakeholders' understanding of the relative merits of the different regulatory options.

6.492 The following section assesses the Overall Preferred Option against ComReg's other relevant functions, objectives and duties.

Assessment of the Overall Preferred Option against ComReg's other relevant statutory objectives

6.493 The preceding RIAs considered a number of interventions potentially available to ComReg within the context of the RIA analytical framework as set out in the ComReg's RIA Guidelines (i.e., impact on industry stakeholders, impact on competition and impact on consumers). It necessarily also involved a complex evaluative analysis of the extent to which various interventions would serve to facilitate ComReg in achieving certain statutory objectives in the exercise of its functions. In particular, it involved an analysis of the extent to which the proposed interventions would serve to promote competition and ensure that there would be no distortion or restriction of competition in the electronic communications sector, whilst at the same time promoting innovation and encouraging the efficient use and ensuring the effective management of the national numbering resource This would in turn enable ComReg to ensure that users would derive maximum benefit in terms of choice and quality.

- The CLI Blocking RIA concluded that a combination of Option 2 and Option 3 and the implementation of the DNO/PN List and the Fixed and Mobile CLI Blocking (i.e., the static interventions) are, on balance, the Preferred Options in terms of its impact on stakeholders, competition.

- The Voice Firewall RIA concluded that, on balance, Option 2 and the implementation of a Voice Firewall is the preferred option in terms of its impact on stakeholders, competition and consumers because it was needed to address scams not covered by the static interventions, including protection against future scams which are likely to become more sophisticated.

- The Sender ID RIA concluded that Option 3 and the implementation of a full Sender ID Registry is the preferred option in terms of its impact on stakeholders, competition and consumers.

6.494 In this section, ComReg assesses the Preferred Option in the context of other statutory provisions relevant to management of Ireland's numbering resource

(which are summarised in Annex 2 of this document). It is not proposed to exhaustively reproduce those statutory provisions here. However, set out below is a summary of all statutory provisions which ComReg considers to be particularly relevant to the management and use of numbering resource with an assessment (to the extent not already dealt with as part of the RIAs) of whether, and to what extent, the Preferred Option accords with those provisions. In carrying out this assessment, ComReg has highlighted below some of the relative merits / drawbacks which would arise if it was to select some of the alternative options assessed under the RIA above.

6.495 For the purposes of this section, the statutory provisions which ComReg considers to be particularly relevant to the management of the radio frequency spectrum in the State are grouped as follows:

- general provisions on competition;
- contributing to the development of the internal market;
- to promote the interest of users within the Community;
- efficient use and effective management of numbers;
- regulatory principles;
- relevant Policy Directions and Policy Statements; and
- general guiding principles:
    - Objective justification;
    - Transparency;
    - Non-discrimination; and
    - Proportionality.

General provisions on competition

6.496 There is a natural overlap between the aims of the RIAs and an assessment of ComReg's compliance with its statutory remit including, in particular, its core statutory objective under section 12(2)(a) of The Communications Regulation Act 2002 (as amended)[486] (the "2002 Act") to promote competition by, amongst other things:

[486] The Communications Regulation Act 2002 (as amended), the Communications Regulation (Amendment) Act 2007, the Communications Regulation (Premium Rate Services and Electronic Communications Infrastructure) Act 2010 and the Communications Regulation (Postal Services) Act 2011.

- ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality;
- ensuring that there is no distortion or restriction of competition in the electronic communications sector; and
- encouraging efficient use and ensuring effective management of numbering resources.

6.497 In so far as the promotion of competition is concerned, Regulation 4(3)(b) of S.I. No. 444 of 2022[487] further requires ComReg to promote competition in the provision of electronic communications networks and associated facilities, including efficient infrastructure-based competition, and in the provision of electronic communications services and associated services. A further relevant general objective is set out in Regulation 4(3)(d), namely, to promote the interests of the consumers and businesses in the State, by enabling maximum benefits in terms of choice, price and quality on the basis of effective competition.

6.498 Certain other provisions also relate to ComReg promoting and protecting competition in the electronic communications sector including:

- Regulation 4(5)(d) of S.I. No. 444 of 2022 which requires ComReg inter alia to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles by promoting efficient investment and innovation in new and enhanced infrastructures;
- Regulation 4(5)(b) of S.I. No. 444 of 2022, which requires ComReg to ensure that, in similar circumstances, there is no discrimination in the treatment of providers of electronic communications networks and services; and
- General Policy Direction No. 1 on Competition (26 March 2004) which requires ComReg to focus on the promotion of competition as a key objective, including removing barriers to market entry and supporting new entry (both by new players and entry to new sectors by existing players).

6.499 Based on the assessment provided in the RIAs above, ComReg's view is that the Overall Preferred Option would best safeguard and promote competition

[487] S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022.

to the benefit of consumers. In particular, ComReg refers to '*Impact on consumers' and 'Impact on competition'* within each RIA.

Contributing to the development of the internal market

6.500 In achieving the objective of contributing to the development of the Internal Market, another of ComReg's statutory objectives under section 12 of the 2002 Act[488], ComReg considers that the following factors are of particular relevance in the context of combatting Nuisance Communications:

- the extent to which the Overall Preferred Option would encourage the establishment and development of trans-European networks and the interoperability of pan-European services, by facilitating, or not distorting or restricting, entry to the Irish market by electronic communication services providers based or operating in other Member States; and

- to ensure the development of consistent regulatory practice and the consistent application of EU law, the extent to which ComReg has had due regard to the views of the European Commission, BEREC and other Member States in relevant matters, in selecting an option and considering any regulatory action required by ComReg in respect of such an option.

6.501 These are assessed in turn below.

I. Encouraging the establishment and development of trans-European networks and the interoperability of pan-European Services

6.502 ComReg notes the overlap between this objective and the objective of promoting competition in the provision of ECN/ECS. Encouraging the establishment and development of trans-European networks requires that operators from other Member States seeking to develop such networks are given a fair and reasonable opportunity to obtain numbers required for such networks. Accordingly, options which would restrict or distort competition or otherwise unfairly discriminate against potential entrants (such as through exposing entrants to greater security risk or lower QoS) would not, in ComReg's view, satisfy the requirements of this objective.

6.503 In this regard, ComReg refers to the RIAs and the finding that the Overall Preferred Option would likely be preferred by those stakeholders that wish to protect consumers and enhance their network security. This is because the

[488] Section 12(1)(a)(ii) of the Communications Regulation Act 2002, as amended.

Preferred Option would reduce the prevalence and harm from scam calls and reduce the potential distortions to competition. In particular, businesses/organisations from other Member States are currently impacted by scam calls in Ireland. For example, a consumer that purchases goods and services from abroad (e.g., online) may receive a call or SMS from a foreign businesses/organisation. However, research shows that consumers are less likely to engage in such communications due to fear of scams and because they are less likely to recognise an international number. Because the Overall Preferred Option reduces scam communications, consumers are more likely to engage with calls and SMS from abroad. Therefore, the Overall Preferred Option best promotes the establishment and development of trans-European networks and the interoperability of pan-European Services.

II. Promoting the development of consistent regulatory practice and the consistent application of EU law

6.504 In relation to contributing to the development of the internal market, ComReg continues to cooperate with other National Regulatory Authorities ('NRAs')[489] which includes closely monitoring developments in other Member States to ensure the development of consistent regulatory practice and consistent implementation of the relevant EC harmonisation measures and relevant aspects of the European Electronic Communications Code as transposed. For example:

- ComReg has considered international trends in the regulation of CLI and Sender IDs, as well as use of Voice Firewall (see Section 6.2.2) and this has informed its consideration in developing its Overall Preferred Option.
- ComReg has held meetings with other NRAs to better understand their views on the regulation of CLI and Sender IDs, as well as Voice Firewall (see Section 2.7).
- ComReg issued a Request for Information and received 19 responses from members of the IRG provided a response to the IRG RFI which ComReg issues in order to gather, among other things, the most up to date information on actions being undertaken by other NRAs in relation to the regulation of CLI and Sender IDs, as well as Voice Firewall to combat scam calls (see Section 2.7);

[489] In accordance with section 12(2)(b)(iv) of the Communications Regulation Act 2002 as amended, which provides that: "In relation to the objectives referred to in subsection (1)(a), the Commission shall take all reasonable measures which are aimed at achieving those objectives, including— in so far as contributing to the development of the internal market is concerned—co-operating with electronic communications national regulatory authorities in other Member States of the Community and with the Commission of the Community in a transparent manner to ensure the development of consistent regulatory practice and the consistent application of Community law in this field".

- Europe Economics has had clear regard to the effectiveness of DNO, PN, Mobile CLI Blocking and Fixed CLI Blocking, Voice Firewalls, Sender ID registries used in other countries in forming its recommendations[490]; and
- ComReg has held meetings with members of the NCIT, and bilateral meetings with individual NCIT members to discuss, among other things, their views on the potential interventions that could be implemented in relation to the regulation of CLI and Sender IDs, as well as Voice Firewall (see Section 2.7).
- ComReg has also monitored legislative developments in other EU countries with a view to implementing optimal interventions. For example, ComReg has identified legislative developments in Belgium, Poland and Spain with a view to whether similar approaches would be required in Ireland.

6.505 Furthermore, ComReg met with and considered the detailed views of the European Union Agency for Law Enforcement and Cooperation (Europol) the law enforcement agency of the European Union. ComReg also considered the recent Europol report titled "*ChatGPT: The impact of Large Language Models on Law Enforcement*" published in in March 2023[491].

To promote the interest of users within the Community

6.506 The impact of the Overall Preferred Option and other options on users within the community and other stakeholders and in the context of ComReg's objective to promote competition has been considered in the context of the RIAs and it is not proposed to consider this matter further here. In particular, ComReg refers to '*Impact on stakeholders'* and *"Impact on Consumers"* within each RIA.

6.507 ComReg also observes that most measures set out in Section 12(2(c) (i) to (vii) of the 2002 Act, aimed at achieving this statutory objective, are more relevant to consumer protection, rather than to the management of numbers.

Efficient use and management of numbers

6.508 Under section 10(1)(b) of the 2002 Act, it is one of ComReg's functions to manage the national numbering resources in accordance with a Policy Direction under section 13 of the 2002 Act. Importantly, in pursuing its objective to promote competition under section 12(1)(a) of the 2002 Act, ComReg must ensure the efficient use and management of numbers (section

[490] See Europe Economics Report Appendix 1 and Appendix 2, in particular Table 9.8.
[491] ChatGPT - the impact of Large Language Models on Law Enforcement | Europol (europa.eu)

12(2)(a)(iv)). Section 12(3) of the 2002 Act also requires that in carrying out its functions, ComReg shall seek to ensure that measures taken by it are proportionate having regard to the objectives set out in section 12.

6.509 ComReg is of the view that the Overall Preferred Option is one that would safeguard and promote those interests. In addition, the Overall Preferred Option best encourages the efficient use of numbers and reduces the misuse of numbers. ComReg refers to '*Efficient use of numbers'* within each RIA. In summary, the Overall Preferred Option would prevent or reduce the misuse of numbers, through reducing the ability of fraudsters to

- spoof the CLI of key Irish businesses and government agencies, as well as the ability of international fraudsters to spoof Irish Fixed and Mobile CLIs more generally; and
- spoof CLIs within the state, exploit any gaps or otherwise circumvent the Voice CLI interventions (e.g., taking an Irish Mobile SIM abroad to originate calls from abroad using an Irish mobile number, hacking an Irish company to originate calls with Irish CLI); and
- to spoof the Sender ID of key Irish businesses and government agencies initially, and any business and government agency once fully implemented; and
- send scam SMS to Irish mobile users, which may include spoofing the Sender ID of key Irish businesses and government agencies.

6.510 Furthermore, it would safeguard the legitimate use of numbers by reducing the harm from scam calls and SMS which could reduce the trust and use of Voice calls and SMS by Irish consumers and businesses (e.g., as consumers either switch to alternative channels or stop answering certain types of calls (e.g., answering calls from Irish numbers, or stop reading SMS messages, with or without Sender ID)).

Regulatory principles

6.511 Under Regulation 4(5) of S.I. No. 444 of 2022, ComReg must, in pursuit of its policy objectives under Regulation 4(3), apply impartial, objective, transparent, non-discriminatory, and proportionate regulatory principles by, amongst other things:

a) promoting regulatory predictability by ensuring a consistent regulatory approach over appropriate review periods; and

b) promoting efficient investment and innovation in new and enhanced infrastructures.

Regulatory Predictability

6.512 ComReg notes that it places importance generally on promoting regulatory predictability and as illustrated below, has complied with this principle in carrying out the current process.

6.513 In the present context, ComReg considers the following objectives to be of particular importance to achieving the aims of this regulatory principle:

- promoting regulatory predictability in relation to use of numbers by applying an open, transparent, and non-discriminatory approach to accessing and using numbers; and

- promoting regulatory predictability in relation to ensuring that the use of numbers is predictable and not subject to significant change such that it would compromise efficient investments.

6.514 In relation to the first objective, ComReg's Overall Preferred Option is consistent with its general treatment of a scarce national resource that is subject to misuse such that ComReg would stipulate rules on its use or make interventions that promote legitimate use and prevent misuse. Noting the significant harm from scam calls and SMS to Irish consumers and businesses, and the potential for its persistence to compromise the use of such services in the future, operators should expect that ComReg would seek to implement rules regarding the use of CLI and SMS and require technical interventions. Further, as noted in Section 2.6, ComReg has dealt with instances of Nuisance Communications in the past and made proportionate regulatory interventions to alleviate harm to consumers. Similarly, ComReg introduced measures to address the cost of using non-geographic numbers to tackle confusion among consumers about the differences between the numbers[492].

6.515 In relation to the second objective, ComReg refers to its assessment under 'Efficient *Investment'* within the RIAs, and its view that the conditions for promoting efficient investment and innovation in new and enhanced infrastructures investment involves ComReg taking its regulatory functions in an appropriate and predictable fashion as provided under the Overall Preferred Option.

6.516 Considering the above, ComReg is of the view that the Overall Preferred Option complies with the regulatory principle of promoting regulatory

[492] Non-Geographic Numbers | Commission for Communications Regulation (comreg.ie)

predictability.

Relevant Policy Directions and Policy Statements

6.517 ComReg notes that the core policy objectives, principles and priorities set out therein are broadly in line with those set out in the 2002 Act and in the European Electronic Communications Code (which has repealed the Common Regulatory Framework), as transposed in S.I. 444 of 2022 (and the Act of 2023) and, in turn, with those followed by ComReg in identifying the Overall Preferred Option.

6.518 Section 12(4) of the 2002 Act requires ComReg, in carrying out its functions, to have regard to policy statements, published by or on behalf of the Government or a Minister of the Government and notified to it, in relation to the economic and social development of the State. Section 13 of the 2002 Act requires ComReg to comply with any policy direction given to ComReg by the Minister as he or she considers appropriate to be followed by ComReg in the exercise of its functions.

6.519 ComReg has taken due account of relevant Policy Directions contained in the February 2003 Ministerial Policy Direction, namely:

- Policy Direction 5 – Regulation only where necessary;
- Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; and
- Policy Direction 7 – Policy Direction on consistency with other Member States.

6.520 In relation to I and II, the three RIAs considered a variety of different options against each other, including the option of doing nothing. In all cases there was strong evidence in support of the Preferred Options and the Overall preferred Option. In relation to III, ComReg refers to the discussion within each RIA as to how ComReg has promoted the development of consistent regulatory practice and the consistent application of EU law.

General guiding principles (in terms of number management and conditions).

6.521 ComReg notes that it is required to comply with the guiding principles of objectivity, transparency, non-discrimination and proportionality in carrying out its functions under the 2002 Act and under the European Electronic Communications Code (which has repealed the Common Regulatory Framework), as transposed by S.I. 444 of 2022. In relation to the current process, ComReg considers that these principles are most relevant in terms of its functions concerning use and management of numbers and attaching

conditions to rights of use.

6.522 In relation to number management and use, ComReg notes that:

a) ComReg's function under section 10(1)(b) of the 2002 Act is to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act are to ensure the efficient management and use of numbers from the national numbering scheme in the State;

b) Regulation 79 of SI 444 of 2022 provides that ComReg:

- shall grant rights of use for numbers for all national numbering resources for all publicly available ECS by application of procedures which are objective, transparent, non-discriminatory; and
- shall ensure that adequate numbering resources are provided for the provision of publicly available electronic communications services.

c) Regulation 79(4) of S.I 444 of 2022 provides that: "any *person who assigns to locations, terminals, other persons or functions on public communications networks numbers from the national numbering plan that the regulator has not specifically allocated to the person in connection with the provision of publicly available electronic* communications services commits a hybrid offence".

6.523 ComReg notes that the above guiding principles are Irish and EU legal principles that ComReg abides by in carrying out its day-to-day regulatory functions.

6.524 ComReg also notes a relevant power under Regulation 83(2) of SI 444, which provides that "*ComReg may require providers of public electronic communications networks or publicly available electronic communications services to block on a case by case basis, access to numbers or services where this is justified by reason of misuse or fraud and to require that in such cases those providers withhold relevant interconnection or other service revenues, where this is justified by reason of fraud or misuse and to require undertakings to withhold relevant interconnection or other service revenues*".

6.525 ComReg further notes a relevant power under Regulation 4(1) of SI 444 which provides: "*The Regulator and other competent authorities, in carrying out their regulatory tasks specified in these Regulations insofar as it gives effect to the Directive, shall take all reasonable measures which are necessary and proportionate for achieving the objectives set out in paragraph (3)*." Relevant general objectives listed in Regulation 4(3), which ComReg has to pursue in

the context of its tasks, are the following: "*promote the interests of the consumers and businesses in the State, …, by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules* …"

6.526 ComReg notes that each of the RIAs and the supporting Sections (i.e., Section 6.2.1 and Section 6.2.2) provide strong evidence of the misuse of numbers in relation to both voice and SMS which are used to perpetuate fraud. For example, Europe Economics estimates that 59 million scam calls were received by consumers which equates to approximately 161,000 scam calls being received each and every day and over 47 million scam messages a year were received which equates to an average of approximately 129,000 scam texts being received each and every day.

6.527 Overall, it is estimated that there were approximately 365,000 cases of fraudulent scams in Ireland over the last 12 months with losses ranging from €5 to €5,000, with scam calls accounting for a higher share of large scams (e.g., >€500). In effect, around 1,000 people are defrauded every single day over telephony networks.

6.528 A further relevant power is ComReg's power under Regulation 104 of SI 444, which gives ComReg the power to, for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the SI 444 Regulations, to issue directions to an operator or undertaking to do or refrain from doing anything which the Regulator specifies in the direction.

6.529 ComReg is of the view, having regard to the applicable legislation and legal principles, its RIAs and other analyses, its expert advice and reports, and the material to which it has had regard, that the Preferred Option is objectively justified, transparent, proportionate, and non-discriminatory. In particular, the Preferred Option:

a) is objectively justified given the detailed assessment provided in the RIAs, including that it would be unlikely to distort or restrict competition and it better encourages the efficient use of the numbers;

b) would not give rise to discrimination in the treatment of undertakings because:

   - any difference in costs incurred as a result of the Overall Preferred Option arise because the situation of some operators is materially different from others.

- the cost of combating scam calls is not dependent on the stakeholder but rather on their traffic and how scams are originated.

c) is transparent because, among other things:

- ComReg provides an assessment of the potential impact of DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, and a Sender ID Registry on affected stakeholder groups by types of traffic carried, including an estimated cost to affected operators, in the RIAs above;
- Europe Economics and ComReg have published the estimates of the costs and benefits to society from a DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, and a Sender ID Registry and the CBA based on same, with detailed explanation of the underlying methodology set out in Chapter 5 of the Europe Economics Report;
- Europe Economics and ComReg have considered the responses to Consultation 23/52 and responded to same including some adjustments and clarifications to proposed interventions: and
- Europe Economics has provided the necessary information for operators to understand its estimated cost of DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, and a Sender ID Registry which may assist operators in understanding and seeking necessary internal approvals for undertaking the actions and budget required for implementation.

d) is proportionate because, among other things:

- in relation to the Overall Preferred Option
  - it would accord with ComReg's statutory objectives and regulatory principles as described above;
  - there does not appear to be less onerous means by which these objectives and principles could be achieved, and wherever possible, ComReg has scoped the interventions to reduce their cost and complexity on industry and allow operators to implement the decision in a cost efficient way (e.g., allowing MNOs to implement Mobile CLI blocking on behalf of MVNOs or smaller IGOs, only applying a

Voice Firewall to networks exceeding a subscriber-based threshold);

- the majority of affected stakeholders are members of the NCIT and have previously agreed to implement some of these measures; and
- these measures are in line with measures implemented by operators in several other EU member states to protect their consumers, in many cases without any regulatory requirement.

- in relation to costs specifically:
  - The social cost of these interventions are not excessive to its benefits. Europe Economics has found that the social benefit of preferred package vastly outweighs the social cost of the interventions. ComReg has already established that the social benefit of the preferred package far outweighs its social cost (see above). Indeed as noted in the Irish Governments Public Spending Code "*The difficulty for the public sector is that it must consider the wider implications for society – the social costs and benefits*."[493]; and
  - The cost of the preferred package to affected operators does not appear prohibitive, relative to the size of revenues generated and capital expenditures made by those operators from providing ECS in the State.

- In relation to timelines specifically:
  - the deadline for implementing each intervention takes into account the scale of the work and time necessary involve, as determined as reasonable (see Section 5.2.2);
  - ComReg commissioned additional expert advice from Plum Consulting on the timelines for each intervention who considered both Consultation 23/52 and the responses to same, when forming the view that the timelines were appropriate.

[493] Department of Public Expenditure and Reform "*A Guide to Economic Appraisal: Carrying Out a Cost Benefit Analysis*"

- in each case this timeline exceeds and extends the voluntary deadlines of the NCIT by a number of months; and
- the majority of affected stakeholders are members of the NCIT and have previously agreed to implement these measures well in advance of these timelines.

Conclusion

6.530 In light of the above, ComReg is of the view that the Overall Preferred Option complies with those statutory functions, objectives and duties relevant to its management of the national numbering resource.

Chapter 7

7 Decision Instruments

7.1 Decision Instrument for Do Not Originate (DNO) – D09/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“DNO list” means a list of numbers maintained by ComReg of telephone numbers assigned to organisations which are never to be used for outgoing calls;

“DNO number” means a number on the DNO List;

“E.164 number” means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"Originating Voice Operator” or “OVO” means an Irish Undertaking originating calls on the Irish PSTN capable of terminating on public networks;

“Presentation CLI” means a number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Public Switched Telephone Network” or “PSTN” is the collection of global telephone networks which provide services available to the public for originating and receiving national and international calls and access to emergency services using E.164 telephone numbers.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52 and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely those undertakings that are:

- either OVOs or IGOs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all calls that use a number on the DNO List as a Presentation CLI;

b. update their blocking systems with the DNO numbers which are to be blocked no later than five working days after receipt from ComReg of updates to the DNO List;

c. record the daily number of:

i. calls blocked under (1) a; and

ii. all calls completed by the undertaking; and

d. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked under (1) a; and

ii. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply as from the date of the making of this Decision Instrument and shall be implemented no later than six months after the date of making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.2 Decision Instrument for Protected Numbers – D10/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"Originating Voice Operator” or “OVO” means an Irish Undertaking originating calls on the Irish PSTN capable of terminating on public networks;

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Protected Numbers” means telephone numbers which have not been assigned by ComReg;

“Protected Numbers List” means a list of Protected Numbers, managed by ComReg;

“Public Switched Telephone Network” or “PSTN” is the collection of global telephone networks which provide services available to the public for originating and receiving national and international calls and access to emergency services using E164 telephone numbers.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52, and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- either Originating Voice Operators or IGOs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all calls that use a number on the Protected Numbers List as a Presentation CLI;

b. update their blocking systems with the Protected Numbers which are to be blocked no later than five working days after receipt from ComReg of updates to the Protected Numbers List;

c. record the daily number of:

iii. all calls blocked under (1) a; and

iv. all calls completed by the undertaking; and

d. provide to ComReg, on a monthly basis no later than 10 working days from the final day of the calendar month, the daily number of:

v. all calls blocked under (1) a; and

vi. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply as from the date of the making of this Decision Instrument and shall be implemented no later than six months after the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.3 Decision Instrument for Fixed CLI Call Blocking – D11/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“E.164 number” means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"Fixed Numbers” means Irish numbers which are Geographic Numbers (numbers linked to a particular geographic region that is identifiable from the area code) or Non-Geographic Numbers;

“Geographic Numbers” means a telephone number that are linked to a particular geographic region that is identifiable from the area code;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

“M2M” means Machine to Machine;

“Mobile Service Provider” or “MSP” means an Irish Undertaking providing End Users with land based/terrestrial publicly available mobile telephony services using a mobile network;

‘MSRN’ means Mobile Station Roaming Number;

“Non-Geographic Numbers” means a telephone number that is not linked to a particular geographic location identifiable from the number;

“PSTN” or “Public Switched Telephone Network” means any network providing transmission and switching functions as well as features which are available to the general public, not restricted to a specific user group. The PSTN provides access points to other networks or terminals only within a specific geographical area;

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation23/52, and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- IGOs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all inbound international calls where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 fixed number except where:

i. the called party number for the call is an Irish E.164 number assigned for use for MSRN.

ii. the Presentation CLI for the call is an Irish E.164 number from the 088 range assigned for M2M applications;

b. record the daily number of:

i. calls blocked as a result of the Fixed CLI Call Blocking; and

ii. all calls completed by the undertaking; and

c. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked as a result of the Fixed CLI Call Blocking; and

ii. all calls completed by the undertaking.

(2) Relevant undertakings that are Mobile Service Providers shall inform ComReg three months in advance of any changes to their Irish MSRN number ranges.

PART V– EFFECTIVE DATE

Decision (1) above shall be implemented no later than six months after the date of the making of this Decision Instrument.

Decision (2) above shall be implemented no later than three months after the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.4 Decision Instrument for Mobile CLI Call Blocking – D12/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Block" means to prevent a call from terminating, with a tone;

"Commission" or "ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"E.164 number" means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"E.146 Mobile Number" means a mobile number that has a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"International Gateway Operator" or "IGO" means an Irish Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"Phase 1 IGO" means an IGO with annual revenues from the provision of ECS in the State of over €50,000,000 annum in 2023;

"IP" means Internet Protocol;

"M2M" means "Machine to Machine";

"MAP Protocol" means a Signalling System No. 7 ('SS7') Mobile Application Part protocol;

"Mobile Number" means a number assigned to the use of Mobile telephony services, primarily for P2P communications (e.g., 083, 085, 086, 087 and 089);

"Mobile Service Provider" means an Irish Undertaking providing End Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network;

MSRN means "Mobile Station Roaming Number";

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Public Switched Telephone Network” or “PSTN” means any network providing transmission and switching functions as well as features which are available to the general public, not restricted to a specific user group. The PSTN provides access points to other networks or terminals only within a specific geographical area;

“Roamer check” means the facility provided by MSPs to IGOs, through the use of network signalling protocols and for the purposes of verifying whether the Presentation CLI of an international call is from an Irish mobile user who is roaming internationally;

“Roaming Proxy Server” means an interworking facility operated by MSPs with the purpose of handling Roamer check queries without requiring IGO direct access to individual MSP networks;

“VoLTE” means Voice over Long Term Evolution, that is, a managed voice service that benefits from prioritisation over other traffic.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is hereby made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52, and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- IGOs;

- MSPs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings that are Phase 1 IGOs shall:

a. block all inbound international calls where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 mobile number, except where the:

i. the user of the mobile number has been determined, by the IGO or another undertaking on its behalf, to be roaming internationally, by verifying against the Roamer Check facility of the user's MSP.

ii. the called party number for the call is an Irish E.164 number assigned for use as a MSRN.

iii. the Presentation CLI for the call is an Irish E.164 number from the 088 range assigned for M2M applications.

b. record the daily number of:

i. calls blocked under (1) a; and

ii. all voice calls completed by the undertaking.

c. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked under (1) a; and

ii. all voice calls completed by the undertaking.

(2) Relevant undertakings that are MSPs shall:

a. provide a Roamer Check facility based on use of MAP protocol to all Phase 1 IGOs; and

b. ensure that ComReg is informed three months in advance of any changes to their Irish MSRN number ranges.

(3) Relevant undertakings that are MSPs shall implement the Roaming Proxy Server.

(4) Relevant undertakings that are IGOs shall:

a. block all inbound international calls where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 mobile number, except where the:

i. the user of the mobile number has been determined, by the IGO or another undertaking on its behalf, to be roaming internationally, by either verifying against the Roamer Proxy Server or the Roamer Check facility of the user's MSP.

ii. the called party number for the call is an Irish E.164 number assigned for use as a MSRN.

iii. the Presentation CLI for the call is an Irish E.164 number from the 088 range assigned for M2M applications.

b. record the daily number of:

i. calls blocked under (4) a; and

ii. all voice calls completed by the undertaking.

c. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked under (4) a; and

ii. all voice calls completed by the undertaking.

d. IGOs who do not implement 4(a) shall not convey calls from international PSTNs to the Irish PSTN where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 mobile number.

PART V– EFFECTIVE DATE

Undertakings that are Phase 1 IGOs shall implement Mobile CLI blocking, that is Decision (1), no later than six months after the date of the making of this Decision Instrument.

Undertakings that are MSPs shall implement Decision (2) above, no later than five months after the date of the making of this Decision Instrument.

Undertakings that are MSPs will implement Decision (3) no later than twenty one months after the date of the making of this Decision Instrument.

Undertakings that are IGOs will implement Decision (4) no later than twenty four months after the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.5 Decision Instrument for Voice Firewall Specification – D13/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Block" means to prevent a call from terminating, with a tone;

"Classification" means assigning each terminating call into one of multiple categories of probability that such a call is a Scam call;

"Commission" or "ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"Fixed Service Provider" or "FSP" means an Undertaking providing End-Users with publicly available voice telephony services using a Fixed Number at a fixed location, irrespective of the underlying technology over which such services are delivered;

"M2M" means "Machine to Machine";

"MBB" means a wireless broadband connection delivered via a mobile network;

"Mobile Service Provider" or "MSP" means an Undertaking providing End-Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network;

"Modify" or "Modified" means to allow the call, but modify the presentation CLI to alert the consumer of the potential risk of a scam;

"Network FSP" means an FSP that operates a network for the purposes of providing End-Users with publicly available voice telephony services using Fixed Numbers at a fixed location, irrespective of the underlying technology over which such services are delivered;

"Network MSP" means a MSP that operates a 2nd, 3rd, 4th, or 5th Generation digital wireless network, or any intermediate evolution of those, using Mobile Numbers, in which seamless handover and roaming features are provided;

"Scam Calls" mean voice calls aimed at defrauding end users by deceiving them into revealing personal or financial details, taking actions that would cause them to be defrauded and/or into making a payment;

"Voice Capable Subscriber" means a subscriber to Voice Capable Subscription;

“Voice Capable Subscription” means any mobile subscription or fixed line that is capable of originating and terminating a voice call on a public network;

“Voice Firewall” means a network platform that monitors in real-time each terminating call and provides a Classification for these calls using a process incorporating the use of data including signalling information for the call, patterns of traffic volumes and call durations, and phone number data.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52, and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- MSPs or FSPs with over 330,000 Voice Capable Subscribers (except those MSPs or FSPs whose requirements below are satisfied by a Network MSP and/or Network FSP); and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

Relevant Undertakings who are also a Network MSP and/or Network FSP shall satisfy the requirements below for other Undertakings who are MSPs and/or FSPs and for whom they provide a voice call origination and termination service, where technically feasible.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. use a Voice Firewall:

i. to identify any terminating voice calls that have a Classification with the highest probability of being a Scam Call

ii. to identify any terminating voice calls that have a Classification with a high probability of being a Scam Call other than the highest probability of being a scam call.

b. block all terminating voice calls that have a Classification with the highest probability of being a Scam Call;

c. Modify all terminating voice calls that have a Classification with a high probability of being a Scam Call, other than the highest probability of being a scam call

d. record the daily number of all

i. calls blocked under 1 (b)

ii. calls modified under 1 (c); and

iii. calls completed by the undertaking.

e. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of

i. all calls blocked under 1 (b) ~~and~~

ii. modified under 1 (c); and

iii. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply from the date of the making of this Decision Instrument and shall be implemented no later than 18 months after the date of making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.6 Decision Instrument for Sender ID Registry – D14/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Already Modified" means that the Sender ID has already been replaced with "LikelyScam" or other Sender ID as defined by ComReg, by a previous PA;

"Block" means to prevent a SMS from originating or terminating or being transited or forwarded;

"ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"ComReg Quarterly Key Data Report" means the statistical data collected by ComReg from authorised undertakings on a quarterly basis, and published on ComReg's website on a quarterly basis;

"Directly Connected" means that the computer system which originates SMS within the SIDO or its third-party technical contractor, uses and maintains a connection at the application protocol level, directly with the systems which accept SMS within the PA;

"M2M" means "Machine to Machine";

"MBB" a wireless broadband connection delivered via a mobile network;

"Mobile Service Provider" or "MSP" means an undertaking providing End-Users with land based/terrestrial publicly available mobile telephony services using a mobile network;

"Modify" means that the Sender ID is replaced with "LikelyScam" or other Sender ID as defined by ComReg;

"Network MSP" means a MSP that operates a 2nd, 3rd, 4th, or 5th Generation digital wireless network, or any intermediate evolution of those, using Mobile Numbers, in which seamless handover and roaming features are provided;

“Participating Aggregator (“PA”)” means a SMS Aggregator that is registered with ComReg to transit or forward a SMS carrying a Sender ID destined for an Irish number;

“Participating MSP” means an MSP in the State, which is registered with ComReg to transit, deliver or forward a SMS carrying a Registered Sender ID bound for a subscriber with an Irish number, that has deployed the necessary technical filtering functions and business processes to enable it to accept SMS messages bearing a Sender ID from PAs;

“Registered Entities” means the SIDOs, Participating Aggregators and Participating MSPs;

“Registered Sender ID” means a Sender ID which is registered with ComReg for use in mobile terminated SMS;

“Securely Authenticated” means the process of verifying the identity of the SIDO using technical means such as a secure username/password combination or other cryptographic means;

“Sender ID” means an alphanumeric originating address sent in SMS messages;

“Registered Sender ID owner” or “SIDO” means the entity to which a Sender ID is assigned by ComReg for use with SMS. A SIDO could contract a third party to send their messages on their behalf via an PA rather than send them directly;

“Sender ID Registry” means the registry managed by ComReg of all Registered Sender IDs, the associated SIDOs, PAs and other relevant data;

“SMS Aggregator” means a service provider that acts as an intermediary between businesses or individuals that wish to send or receive SMS messages, and an SMSC function within mobile telecommunication networks.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. Having had regard to the powers, functions, objectives and duties of ComReg, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of 2022 Regulations, for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to ComReg's statutory duty under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to ComReg's statutory duty under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to ComReg's general objective under Regulation 4(3) of the 2022 Regulations of promoting the interests of consumers and businesses in the State by maintaining the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services) and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard, inter alia, to ComReg's duty under Regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Regulation only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52, and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely those undertakings that are:

- MSPs;
- Participating Aggregators; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

Network MSPs with over 270,000 Mobile Subscribers (excluding M2M and MBB,) are required to register with ComReg as Participating MSPs.

Relevant Undertakings who are also a Network MSP shall satisfy the requirements below for other Undertakings who are MSPs and for whom they terminate SMS, where technically feasible.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) When delivering an SMS with a Sender ID, relevant undertakings that are Participating MSPs shall Modify the Sender ID unless it is Already Modified where that Sender ID:

a. is not a Registered Sender ID; or

b. is a Registered Sender ID, but sent by a source other than a Participating Aggregator or a Participating MSP.

(2) When delivering an SMS with a Sender ID, relevant undertakings that are Participating MSPs shall block SMS where the Sender ID:

a. is not a Registered Sender ID; or

b. is a Registered Sender ID, but sent by a source other than a Participating Aggregator or a Participating MSP.

(3) Relevant Undertakings that are Participating MSPs shall apply the same treatment as in (1) and (2) to all SMS except for SMS sent:

a. to visitors within the State who are roaming; and

b. to their own end users roaming in another country, where technically feasible.

(4) Relevant Undertakings that are MSPs but are not Participating MSPs, or that do not have a Network MSP applying Decision 1, 2 and 3 on their SMS traffic on their behalf, shall not deliver any SMS bearing a Sender ID to an Irish number.

(5) Following any updates to the SMS Sender ID Registry, and within five working days, relevant undertakings that are Participating MSPs or Participating Aggregators shall update all information related to the Registered Entities used by the undertaking to achieve (1) and (2).

(6) Relevant Undertakings that are Participating Aggregators shall Modify any SMS which is destined for an Irish number which has a Sender ID that is:

a. not a Registered Sender ID; or

b. a Registered Sender ID, but sent by a source other than a:

i. Directly Connected and Securely Authenticated Registered SIDO for that Sender ID; or

ii. Participating Aggregator.

(7) Relevant Undertakings that are Participating Aggregators shall Block any SMS which is destined for an Irish number which has a Sender ID that is:

a. is not a Registered Sender ID; or

b. is a Registered Sender ID, but sent by a source other than a:

i. Directly Connected and Securely Authenticated SIDO Registered for that Sender ID; or

ii. Participating Aggregator.

(8) All undertakings shall:

a. record separately for each connected source the daily number of SMS with a Sender ID destined for Irish numbers:

i. which have been blocked or modified for each Sender ID; and

ii. which were not blocked or modified for each Sender ID;

b. provide to ComReg, on a monthly basis in a format and manner to be determined by ComReg, no later than 10 working days from the final day of the calendar month, the daily number of SMS with a Sender ID destined for Irish numbers separately for each connected source:

i. which have been blocked or modified for each Sender ID; and

ii. which were not blocked or modified for each Sender ID;

c. upon request from ComReg, provide information pertaining to any SMS or SMSs bearing a Sender ID which ComReg suspects may have been in breach of the blocking requirements in Decision (1), (2), (6) and (7) including, but not limited to, the name of the sending party, the date and time of delivery, a record of what checks the operators performed on the incoming message before relaying or delivering it , and the total number of identical or similar SMS which were sent at that time.

(9) Undertakings that are MSPs must block any SMS bearing an originating number in the Irish number range, fixed, mobile or a short code, when presented for delivery from an SMSC which is not operated by or on behalf of an Irish MSP.

PART V– EFFECTIVE DATE

Decision (1) and (6) above shall apply from 15 months after the date of the making of this Decision Instrument, for a period of 3 months.

Decision (3), (5), and (8) above shall apply 15 months after the date of the making of this Decision Instrument.

Decision (2), (4), (7) and (9) above shall apply 18 months after the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

7.7 Decision Instrument for Numbering Conditions of Use and Application Process – D15/24

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. Having had regard to the powers, functions, objectives and duties of ComReg, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to the Commission's statutory duty under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to the Commission's statutory duty under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to the Commission's general objective under Regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act, and pursuant to ComReg's power to grant rights of use for numbering resources under Regulation 79(1) and 79(5)(a) of the 2022 Regulations;

i. pursuant to ComReg's power to specify conditions to be attached to a right of use for numbering resources under Regulation 10(1) of the 2022 Regulations;

j. pursuant to ComReg's power under Regulation 14(1) of the 2022 Regulations to amend the rights of use for numbering resources;

k. having regard, inter alia, to its duty under Regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

l. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

m. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

n. having considered all relevant evidence before it, including from Voluntary Information Requests;

o. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation 23/52 , and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

p. having regard to the consultants' reports commissioned in relation to this matter;

q. for the reasons set out in its written Response to Consultation document (response to Consultation 23/52) to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to undertakings that:

- use numbers or have been assigned numbers from the national numbering resource; and
- are deemed to be authorised under Regulation 6 of the 2022 Regulations.

The requirements below shall also apply to a "Sender ID owner" or "SIDO", meaning the entity to which a Sender ID is assigned by ComReg for use with transiting or terminating SMS, so far as applicable.

PART III – THE DECISIONS

Thereby makes the following decisions:

(1) The Numbering Conditions of Use and Application Process (currently Commission Document 15/136R3, version four) shall be amended as follows (and shall be titled 15/136R4, with consequential numbering and pagination updates):

(A) Insert the following text as a new paragraph 4 in Section 1 "Introduction", as follows:

(4) As set out in its Response to Consultation 24/24 and Decision on Nuisance Communications, ComReg supports industry by managing the following:

i. Do Not Originate ("DNO") List;

ii. Protected ("PN") List;

iii. Mobile Station Roaming Number ("MSRN") List; and

iv. Sender ID Registry.

(B) Add the following underlined text in Section 3.1 (5)(a) :

(a) "the undertaking which originates a call *on the Irish PSTN* shall ensure:"

and add the following underlined text as a new paragraph "i", with consequential numbering updates:

(i) *that the CLI for the call shall be the assigned number for the calling party;*

and delete the indicated text and add the underlined text in paragraph "ii" as follows:

(ii) that the presentation CLI for the call shall be ~~the assigned~~ a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number *appropriate to the designated MNA for that number*, a Harmonised Code of Social Value, a Mobile Number, or a Standard Rate Number ~~for the calling party~~ .

and add the underlined text as paragraph "iii" as follows:

(iii) *that the presentation CLI for the call may be the single European emergency number 112 or the national emergency number 999 when the call originates from the national PSAP, but not otherwise.*

(C) that the current Section 3.1(5)(d) and Section 3.1(5)(e) be deleted as indicated and replaced with the text of a new Section 3.1 (5)(d) as follows:

~~(d) for international calls originating from outside the State, the CLI may be modified with appropriate prefixes including "00", "+" and the relevant country code; and~~

~~(e) a presentation CLI may be marked as "Caller ID unknown" or equivalent if an operator cannot ensure that the presentation CLI information is valid~~.

(d) That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code, or setting the correct ISUP "Nature Of Address" flag. If the international call is untrusted and the CLI not in E164 a correct format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".

(D) insert the following text as new paragraphs "f" and "g" in Section 3.1(5) as follows:

(f) An end-user organisation may give permission to its call centre contractor to use the organisation's assigned number as CLI while providing the service.

(g)An employer may give permission to its remote working employees to use the employer's assigned number as CLI while carrying out their employment duties.

(E) insert the following text as a new paragraph "e" in Section 3.1 (5) in the Numbering Conditions:

(*e) For the avoidance of doubt, Undertakings shall carry out CLI-analysis on all calls originating on the Irish PSTN. This is to ensure that such undertakings can comply with the CLI conditions of use.*

Where it is not technically feasible for an undertaking to carry out CLI-Analysis with its existing systems, it shall notify ComReg of its plan to ensure compliance by the Effective Date.

(F) Add the following underlined text to paragraph 1 of Section 3.2 "Rights of Use Conditions" as follows:

(1)Unless ComReg otherwise consents, a number shall be activated by its holder (a) within 12 months of the date on which the right of use for the number was first granted to the holder; or (b) within 3 months of the date on which the right of use for the number was transferred, as applicable. "In the case of 1800 Freephone and 0818 Standard Rate Numbers, applications shall be submitted on the Fixed Number Portability (FNP) system which shall support the activation of these numbers on networks. *In the case of SMS Sender ID, and unless ComReg otherwise consents, a SMS Sender ID shall be activated by its holder (a) within 6 months of the date on which the right of use for the SMS Sender ID was first granted to the holder; or (b) within one month of the date on which the right of use for the SMS Sender ID was transferred, as applicable".*

(G) insert the following text as a new paragraph 9 in Section 3.2 as follows:

(9) Long-lining – For clarity, undertakings implementing long-lining must ensure that CLI-Analysis is carried out on calls originating on the Irish PSTN.

(H) Add the following underlined text to paragraph 2 of Section 4.3 in the case of 1800 Freephone and paragraph 2 of Section 4.4 in the case of 0818 Standard rate:

(2) An authorised undertaking shall only be granted the Rights of Use of 1800 Freephone/0818 Standard Rate Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for together with the end-user's unique identifier. This identifier shall be the end-user's name, or suitable alternative such as account number or order number which enables ComReg to validate the authenticity of the assignment order. Furthermore, as 1800 Freephone/0818 Standard Rate numbers are only provided to organisations, to demonstrate its eligibility to be assigned an 1800 Freephone/0818 Standard Rate number, an organisation end-user shall be required to provide at least one of the following:

i. A company's Irish CRO number, Revenue VAT or business number;

ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration;

iii. For a trademark holder that holds a trademark that is enforceable in the State, the trademark number or a digital copy of the trademark certificate;

iv. Registered charity number from the Charities Regulator or evidence of registration as a voluntary non-profit making organisation in the State; or

v. Evidence that the organisation's premises is in the State, e.g. organisations such as schools, clubs etc;

For clarity, any organisation that does not meet the above criteria but wishes to submit other evidence of its need for an 1800 Freephone/0818 Standard Rate number may do so. ComReg reserves the right to refuse any application that does not meet the above criteria.

This condition shall apply to new 1800/0818 applications only, from the date of commencement of this Decision Instrument.

(l) Carry out the following which concerns the assignment of Sender IDs and the attached Numbering Conditions;

insert the following text at the end of paragraph "a" of Section 2.2 on RoU Conditions;

(a)In the case of Sender IDs, end-users, which are non-ECS/ECN and are therefore non-authorised entities, may be assigned such numbers based on Article 79(5)(a) of SI No 444 of 2022.

insert a new Section 6 entitled "Conditions for SMS Sender ID" with the Rights of Use Conditions as follows, with subsequent numbering changes:

(1) SMS Sender IDs ("Sender ID") are encoded according to the GSM 7-bit default alphabet (section 6.2.1 of [2]) and as such a SMS Sender ID can have a maximum length of 11 characters

(2) The following are the valid characters which are permitted:

*a-z 0-9 @ ! # % & ( ) * + , - . / : ; < = > ? Fada [Space]*

Any character not on the above list is not permitted.

Include a footnote clarifying the characters permitted as follows;

"For example: Not permitted are all characters with accents (E.g. è Ç), Greek letters (E.g. Ω Ψ) and the following: £ $ " ' ¡ €, with the exception of the Irish Fada which is permitted."

(3) Sender ID registration and filtering is case insensitive. A given Sender ID is assigned to a SIDO to use in whatever choice of case they prefer, however the messages should be treated identically irrespective of the case used.

(J) Add Sender ID as a class of number in the Numbering Conditions by inserting the following table in Appendix 10 "Classes of Numbers" as follows;

Code	Designation	Notes
Alpha-numeric	SMS Sender ID ("Sender ID")	Recognised Sender IDs are included in the SMS Sender ID Registry intervention. The Registry shall include information such as the Sender ID, Sender ID Owner (SIDO) and Participating Aggregator (PA).

(K) insert the following underlined text in paragraph 1 of proposed Section 7.1 "General Application Criteria" of the Numbering Conditions";

(1)ComReg will grant rights of use for numbers to authorised undertakings in an open, objective, transparent, non-discriminatory and proportionate manner and generally on a "first come, first served" basis though ComReg may hold open competitions before granting rights of use for newly-opened number ranges. <u>For the avoidance of doubt, SMS Sender IDs will also be assigned on a "first come, first served" basis.</u>

(L) Insert the following text as new paragraph 2 and new paragraph 3 of Section 7.1 "General Application Criteria" of the Numbering Conditions;

(2) Undertakings are not encouraged to engage in sub-assignment of numbering resources, where sub-assignment means the assignment of numbering resources by an assignee to another entity that is not an end user. Transfer of numbers between undertakings is to be preferred. Where sub-assignment is necessary, it is subject to the prior notification of ComReg, and the consent of the Primary Assignee. The responsibilities regarding the compliance with the Numbering Conditions in relation to the assigned number(s) shall be shared between the Primary Assignee and the Sub-Assignee.

(3) In providing services to its end-users, an undertaking shall only use numbers for which it solely, or jointly in the case of sub-assignment, holds the rights of use.

This condition that, in providing services to its end-users, an undertaking shall only use numbers for which it solely, or jointly in the case of sub-assignment, holds the rights of use, shall apply to new applications only, from the date of commencement of this Decision Instrument.

The process for sub-assignment is set out in Appendix 9 of the Numbering Conditions.

Insert the following text as new paragraph 13 of Section 3.1 as follows;

(13)For the avoidance of doubt, number hosting is permitted in Ireland.

Insert the following underlined text as new paragraphs (l) and (m) in Section 3.2 (8) "Rights of Use Conditions"

(8)*For the purposes of ComReg making any information requirement under regulation 99 of the 2022 Regulations, holders shall maintain accurate and current records in respect of rights of use for all classes of numbers granted to them, to include the following:*

(l)rights of use for numbers sub-assigned to them;

(m)rights of use for numbers sub-assigned by them.

Where "transfer" is indicated in Sections 3.2(1), 3.2(3), 3.2(4), 3.2(5) and 3.2(6) add "or sub-assign"

(M) Insert the following text as Section 7.1 paragraph 16(b) as follows:

(b)*Applications for Sender IDs must be submitted via the automated system designated by ComReg.*

(N) Insert the following text as new paragraph 8 of Section 7.2 "Eligibility Criteria" which identifies the information to be supplied with the customer order:

(8)Rights of use for Sender ID may only be granted once the following criteria are met

(a) The applicant must be a legitimate organisation and have a need to register a Sender ID in the State. The SIDO shall demonstrate that it meets these criteria by submitting at least one of the following;

i. A company's Irish (or international equivalent) CRO number, Revenue VAT or business number or international equivalent;

ii. A partnership/sole trader's Irish (or international equivalent) VAT

number in their name(s) or proof of their business or Irish income tax registration;

iii. *For a trademark holder that holds a trademark that is enforceable in the State, the trademark number or a digital copy of the trademark certificate;*

iv. *Registered charity number from the Charities Regulator or evidence of registration as a voluntary non-profit making organisation in the State; or*

v. *Evidence that the organisation's premises is in the State, e,g. organisations such as schools, clubs etc;*

Note; For clarity, any organisation that does not meet the above criteria but wishes to submit other evidence that it is a legitimate organisation and has a need to register a Sender ID in the State may do so. ComReg reserves the right to refuse any application that does not meet the above criteria.

(b). ComReg reserves the right to refuse applications where the proposed name is likely, in ComReg's view, to lead to confusion; to facilitate fraud or misuse; to incorrectly suggest state sponsorship; or cause offence.

(c) The applicant for a Shared Sender ID shall be a Registered PA.

(O) Insert the underlined text in Section 2(4) as follows;

(*4)In addition to the conditions set out herein, undertakings which use numbers or which have been granted rights of use for numbers are expected to adhere to applicable international standards and established best practices in relation to numbers and number usage, <u>including in relation to Know Your Customer ("KYC")</u>.*

(P) Insert the underlined text in Appendix 12 "Definitions" of the Numbering Conditions as follows;

<u>"Sender ID Registry" means the register managed by ComReg of all Registered Sender IDs, SIDOs and the Registered Entities which may transmit or terminate specific Registered SMS Sender IDs;</u>

<u>"Sender ID owner" or "SIDO" means the entity to which a Sender ID is assigned by ComReg for use with transiting or terminating SMS. A SIDO could contract a third party to send their messages via an PA rather than send them directly;</u>

"Registered Entities" means the SIDO and Registered PA(s) for a given Registered SMS Sender ID;

"Registered Sender ID" means a Sender ID that has been approved by ComReg for addition to the Sender ID Registry.

"Shared Sender ID" means a Sender ID which is assigned to a Registered PA for use by its customers who do not wish to register their own Sender ID.

"PA" means participating aggregator. This is an SMS aggregator that signs up to the relevant Sender ID registry rules and carries messages bearing a registered sender ID from SIDOs via an Irish MSP;

In the definition of "*Holder"* insert the following underlined text *"holder" means an undertaking which has been granted a right of use for any class or description of number by ComReg, or to which such a right of use has been transferred or ported by another undertaking or which jointly holds the rights of use under a sub-assignment agreement with an aforementioned undertaking;*

"Sub-Assignment" means, the assignment of numbering resources by a Primary-Assignee to a Sub-Assignee.

"Primary Assignee" means, in the context of the sub-assignment of numbers, an undertaking which has been granted a right of use for any class or description of number by ComReg.

"Sub-Assignee" means an undertaking which has been sub-assigned a number by a Primary Assignee.

"Long-lining" means the implementation by an undertaking of a dedicated SIP or alternative trunk type to serve an end-user to ensure that calls from that end-user originate on the Irish PSTN;

"Number Hosting" means the implementation of numbers, which are held by an undertaking, on another undertaking's network; this is to enable connectivity for the number holders end users.

"Mobile Service Provider" or "MSP" means an authorised undertaking providing End-Users with land based/terrestrial publicly available mobile telephony services using a mobile network;

- In the definition of "Network CLI" add the following text *"In SIP based networks, the Network Number is carried in a "P-Asserted-Id" header field, as defined in RFC 3325[494] as amended".*

- In the definition of "*Presentation CLI"* add the following text *" In SIP based networks, the Presentation Number is carried in the "From" header field, as defined in RFC 3261[495] as amended"*;

Public Safety Answering Points ("PSAP") means the entity that answers all emergency calls and text messages and connects the caller to the required emergency service. This service is currently provided by ECAS in Ireland

Know Your Customer ("KYC") means, in general terms, the policies and procedures put in place by organisations to verify the identities of customers and manage risk.

Part IV– EFFECTIVE DATE

A revised version of the Numbering Conditions of Use and Application Process (currently Commission Document 15/136R3, version four), which shall be titled Numbering Conditions of Use and Application Process, ComReg 15/136R4, reflecting the decisions above, shall come into effect immediately subject to the following:

Decisions "A(iv)", "D", "F", "I", "J", "K","M","N", "O" and "P" shall apply from the date of the making of this Decision Instrument;

Decisions "A(i)", "A(ii)", "A(iii)", "B", "C", "G", "H" and "L" and shall apply no later than three months after the date of the making of this Decision Instrument; and

Decision "E" shall apply no later than six months after the date of the making of this Decision Instrument.

The fourth version of the "Numbering Conditions of Use and Application Process" (Commission Document No. 15/136R3) shall stand revoked with immediate effect (save that this document shall remain in full effect insofar as it may apply to any relevant matters as may occur prior to its revocation).

PART V – STATUTORY POWERS NOT AFFECTED

[494] RFC 3325 Private Extensions to the Session Initiation Protocol for Asserted Identity within Trusted Networks. Available here: RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (rfc-editor.org)
[495] RFC 3261 SIP: Session Initiation Protocol. Available here: RFC 3261: SIP: Session Initiation Protocol (rfc-editor.org)

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

The 28th day of March 2024

Annex: 1 Basic background on Nuisance Communications

A 1.1 This Annex sets out some relevant background information to ComReg's assessment of the harm due to nuisance communications and the potential interventions that could reduce same, including information on the following:

- The importance of Voice and SMS communications;
- The importance of Irish telephone numbers;
- What are Nuisance Communications;
- Fraudsters and scams.

A 1.2The importance of Voice calls and SMS to Irish society

A 1.3 Telecommunications services are essential to our everyday lives and allow us to keep in touch with our family and friends while engaging with businesses for goods and services. Voice calls and SMS are unique among calling and messaging services in that they are universally installed and activated on mobile devices by default, unlike alternatives which are reliant upon a consumer downloading the application to their device (e.g., WhatsApp etc).

A 1.4 Irish businesses rely upon Voice and SMS texts for conducting their sales and business operations (with only 13% of Irish companies reporting no use of either technology). Firms that use voice and text communications as part of their revenue generating strategies earn revenue of approximately €48 billion through the use of these services, and scam communications puts this in jeopardy by making it more difficult for organisations and consumers to communicate with one another.[496]

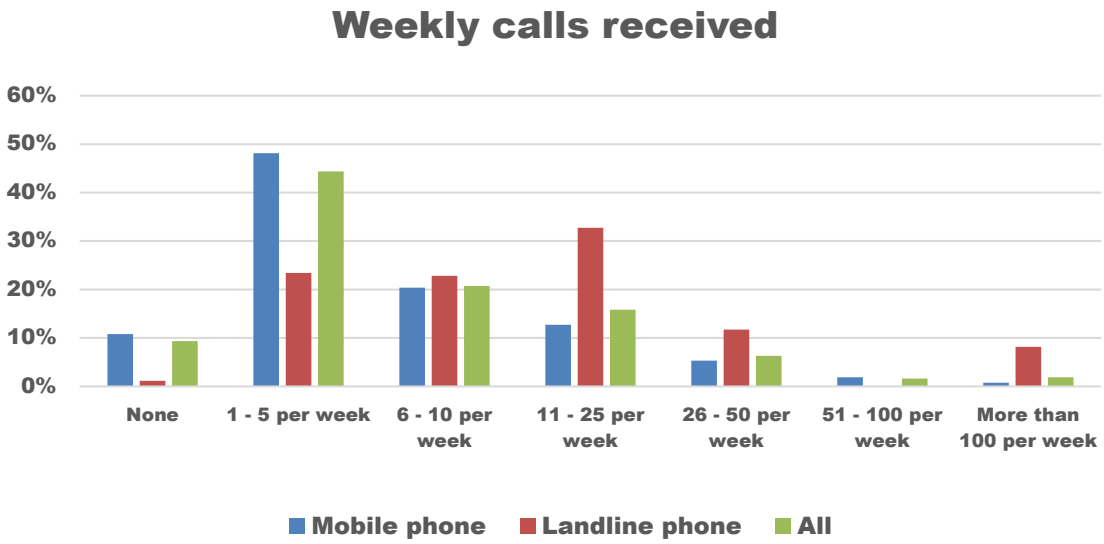
Voice calls

A 1.5 A Voice Call is a connection over a telephone network between the called party and the calling party that enables people to hold conversations and communicate information in real time. This makes Voice Calls an instantaneous means of transmitting information between people, critical to the daily life of many consumers and organisations.

[496] See Europe Economics Report – Page 54.

A 1.6 There are approximately 7 million voice capable subscriptions[497]. Irish mobile and fixed networks carried over 11 billion Voice minutes in the 12 months to Q4 2023[498]. On average mobile users receive an average of 10 calls per week.

Figure 34: Weekly voice calls received by mobile or landline, Q4 2022



Source: ComReg analysis of B&A Consumer Survey[499]

A 1.7 Voice services are also critical to delivery of important public and social services. This was ably demonstrated during the Covid-19 period where services were increasingly required through calls and text message (e.g., an extra 1.5 billion minutes a year were received due to Covid-19). While new communications channels have emerged, consumers use of Voice and SMS remains high and continues to facilitate consumer and business communications. Voice services are critical to Irish businesses, with 84% reporting using Voice calls for their business operations, 72% to contact other business, 58% to facilitate communication between staff and 56% to connect with end-customers[500].

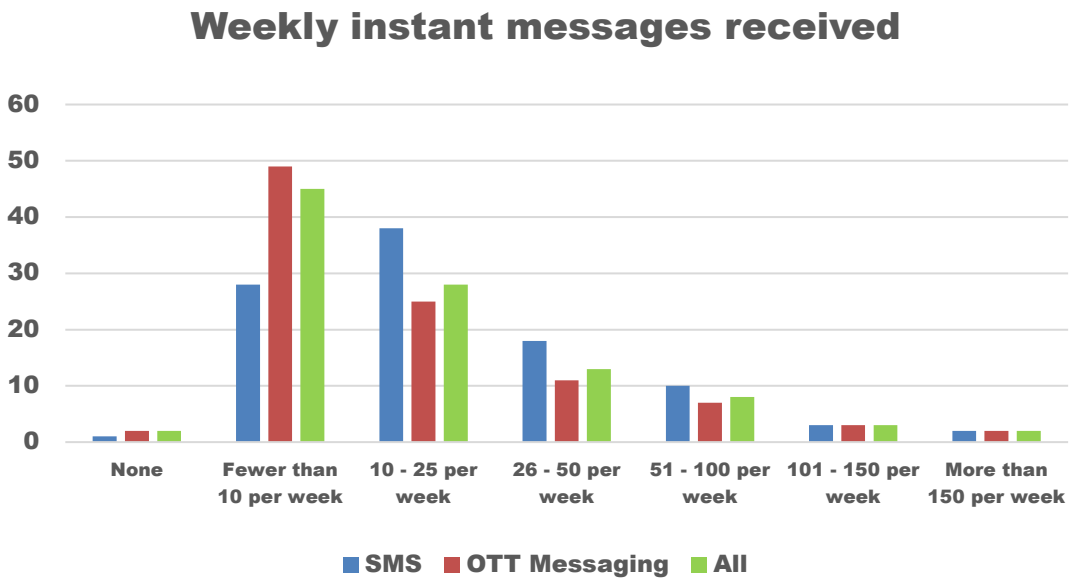
Short Messaging Service

[497] ComReg QKDR data for Q2 2024. Using the traditional Voice networks - this excludes other devices (e.g., laptops) which may receive Voice calls transmitted using VOIP.
[498] ComReg QKDR data for Q2 2024.
[499] Q3 "*Approximately how many calls do you receive on your mobile phone per week?*" and Q4a "*What is the main way in which you make and receive calls, by mobile or landline?*"
[500] B&A Business Survey, slide 9.

A 1.8 Short Messaging Service ("SMS") is a text messaging service component of all mobile phone networks. SMS uses standardised communication protocols that let mobile devices exchange short text messages. SMS rolled out commercially as part of 2G mobile networks and became hugely popular worldwide as a method of text communication and transmitting information to mobile devices.

A 1.9 There are approximately 5.7 million subscriptions for consumer devices capable of receiving a SMS[501]. Notwithstanding the success of other messaging apps, significant volumes of SMS are still sent and received every quarter, with 2.1 billion texts being sent in the 12 months to Q4 2023. While many consumers now use OTT messaging applications, such as WhatsApp, as their primary means of P2P messaging, 22% of Irish consumer still rely primarily on SMS[502] with higher rates of use for older people (65+)[503]. On average, consumers receive approximately 25 texts a week.

Figure 35: Weekly instant messages received by preferred channel, Q4 2022



Source: ComReg analysis of B&A Consumer Survey data[504]

[501] As of Q2 2023. Using the traditional Voice networks - this excludes other devices (e.g., laptops) which may receive Voice calls transmitted using VOIP.
[502] B&A Consumer Survey Slide 9
[503] Europe Economics Report, Figure 4.13
[504] B&A Consumer Survey - Q.4b "*Approximately how many text messages do you receive per week?*" and Q.5 "*Main way of sending and receiving instant messages?*"

A 1.10 SMS remains an important means of communication for certain cohorts of the population in particular as it is generally considered to be the only truly universal messaging service, not relying on both parties to have downloaded an OTT app. As a result, SMS continues to be an important method of communications between businesses and their customers ("B2C"). While P2P communications have moved to OTT applications over time, the importance of SMS to B2C has if anything increased, with the majority of Irish:

a) businesses reporting some use of SMS (65%), to either contact other business (35%), communicate between staff (45%) or connect with end-customers (36%)[505]; and

b) consumers reporting some use of SMS for some B2C activity (66%) (e.g., reminders for appointments)[506].

A 1.11 SMS is not only used for the purpose notifying consumers of offers or appointment offers, but also increasingly for new uses such as customer authentication or verification for of services (e.g., Know Your Customer ("KYC")[507] for a new app, two-factor authentication[508] ("2FA") for financial transactions). In contrast with P2P, for B2C SMS can complement (rather than substitute) many OTT applications, being used to facilitate consumer sign up or verification. (i.e., SMS is used for verifications of OTT applications).

Transit of international traffic

[505] B&A Business Survey, Slide 9.
[506] B&A Consumer Survey
[507] Know Your Customer is the often-mandatory process of identifying and verifying a customer's identity, for example when opening a bank account and periodically over time.
[508] Two-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully confirming their identity via a second authentication mechanism, often SMS.

A 1.12 Operators originate voice calls and SMS on fixed or mobile networks before sending the call or text toward its intended recipient. Calls and texts that both originate and terminate in the state are handed over directly between domestic operators, in many cases without ever leaving the state. However, a significant share of calls or texts reaching Irish consumers originate abroad and must be delivered to domestic operators by foreign operators via one of a small number of international gateways (ingress), typically after being carried via a submarine cable terminating on the Island of Ireland. Operators that provide this service for Voice calls are known as International Gateway Operators or IGOs [509]. Although accounting for a small share of overall Voice Calls (approximately 8% by minutes[510]), it is understood that the bulk of scam calls originate abroad and reach Irish consumers via these channels (although ComReg understands from An Garda Síochána that scam calls originating in Ireland are increasing).

A 1.13 The importance of Irish telephone numbers

A 1.14 Telephone numbers are an integral part of both fixed and mobile electronic communications networks and services worldwide. Numbers are critical to the routing of Voice calls and SMS and also convey information which consumers may find useful (e.g., geographic location), enabling consumers to understand of the source and authenticity of incoming Voice calls or SMS.

A 1.15 The trust Irish consumers have in Irish numbers influences the likelihood of consumers and businesses making and receiving calls, and thereby the benefits of ECS and ECN itself. However, this trust has been exploited by fraudsters who now use the numbering platform to perpetuate fraud on consumers. Until the late 20th century, when the vast majority of voice telecommunications consisted of fixed telephony, each telephone number routed calls to a unique subscriber address, with geographic relevance identifiable within each subscriber number. Today such numbers, known as **Geographic Numbers** ("GNs"), are still linked to a particular geographic region that is identifiable from the area code (e.g. '01' for Dublin, '061' for Limerick)[511].

[509] ComReg has identified 14 IGOs from an information request issued in January 2023 to the companies on the numbering list. All IGOs originate traffic and are therefore a subset of the 30 known Fixed line and mobile Originating Operators.
[510] IGO RFI
[511] There are 50 Area Codes (excluding the 048 code for Northern Ireland). Within these Area Codes there are Minimum Numbering Areas (MNAs). There are 106 MNAs in Ireland. See https://www.comreg.ie/industry/licensing/numbering/area-code-maps-2/

A 1.16 But, because of the growth in mobile telecommunications and other telephony services, further number ranges such as Mobile Numbers and non-geographic numbers (NGNs) have been introduced.

- a NGN is a type of telephone number that is not linked to a particular geographic location identifiable from the number i.e., a NGN does not identify the call termination point. ComReg has consulted extensively on NGNs[512] and introduced measures to address the cost of using such numbers and to tackle confusion among consumers about the differences between the numbers. There are now only two Non-Geographic Number ("NGN") ranges, 1800 Freephone and 0818 Standard Rate.

- Mobile Numbers are numbers assigned to the use of Mobile telephony services, primarily for P2P communications (e.g., 083, 085, 086, 087 and 089). Mobile Numbers do not contain geographic information of any significance, other than to indicate that the SIM was provided in Ireland. Nevertheless, Irish consumers likely recognise such numbers as relating to a resident of Ireland. Mobile Numbers have taken on additional importance in recent years, with the increased use of SMS for 2FA, as a means of customer identification.

A 1.17 **Calling Line Identification**[513]**,** Caller ID or CLI, provides the receiving end of a call with a number for the calling phone. CLI is often used to identify the caller or the geographic location from which a call originated, or to enable saved contact names for known numbers to appear on the recipient device. Companies such as those with call centres can often choose a CLI for their outbound calls so that the telephone number used enhances the ability of the call recipient to identify the company trying to contact them (e.g., the customer of a bank may already have the telephone number being used as the CLI stored in their phone address under their bank name)

[512] Non-Geographic Numbers | Commission for Communications Regulation (comreg.ie)
[513] Calling Line Identification (CLI) is the number presented or displayed by the party making a telephone call to the recipient of that call.

A 1.18 Similarly, for SMS a sender may supplant the mobile number with alphanumeric text, known as a **Sender ID**[514]. This is typically done by businesses/organisations to facilitate recognition of their text messages by consumers, who are unlikely to recognise or memorise the business's entire mobile number. For example, for most mobile users the Sender ID is their phone number, while a business or organisation may choose to display its trading name instead of its phone number (e.g. "An Post", "BOI").

A 1.19 What are Nuisance Communications

A 1.20 The daily use of electronic communications networks and services is exploited by criminals, who use social engineering type attacks, with the intention of illegally acquiring personal consumer information, ultimately to abet financial fraud (though a wide array of other harms are caused by it – see Section 6.2.1). Such scams can take many forms, however in each case the fraudster aims to secure a financial payoff from either taking over a consumer account or tricking a consumer into making one or more payments to the fraudster. Such practices include[515]:

- **Vishing** – a phone call designed to get you to share personal information and financial details, such as account numbers and passwords. A seemingly genuine number is displayed to gain your trust and encourage you to share information. The vishing attempt may sound robotic (see Robocall below).

- **Smishing** – a SMS message designed to gain your trust and encourage you to share information) and is where text messages are sent to trick you into clicking on a malicious attachment or link.

- **Wangiri** – short calls or faked missed calls prompt you to call back an international number. The call-back provides financial benefit for the fraudster often at the expense of the caller.

- **Tech Support Scam Calls** – calls where a fraudster claims to offer a technical support service. The fraudster typically attempts to get consumers to allow remote access to their computer. After remote access is gained, the fraudster attempts to gain your trust to pay for supposed "support" services, steal your credit card account information or to persuade you to log in to your online banking account.

[514] Note that the term Sender ID in this document generally refers to the case where an alphanumeric business name is used rather than a phone number.
[515] See Chapter 4 of the Europe Economics Report for further details.

- **Robocall –** calls generated automatically, where you hear a recorded message that often sounds as if it was a robot listing options that, if selected, would connect you to the fraudster

A 1.21 Recent scam calls and texts have also involved "spoofing", whereby the fraudsters impersonate a legitimate Irish business or organisation by presenting their name or number or pretend to be based in Ireland by presenting an Irish number. This greatly increases the effectiveness of scams by misleading consumers as to the identity of the originator of the call or SMS text. There are two main spoofing practices.

- **CLI Spoofing** where the CLI (Caller ID) has been faked by a fraudster and appears to be a call from a genuine number or business. In effect, it appears that an incoming call is coming from a local number that is already known and trusted to the receiver.

- **Sender ID Spoofing** occurs when the number or name as displayed on a recipient device's screen has been faked by a fraudster and appears to be a SMS from a genuine business or organisation. In effect, it appears that an incoming SMS is coming from a local business or organisation that is already known and trusted.

A 1.22 Fraudsters and scams

The stages of a scam

A 1.23 Almost all scams are comprised of four key stages, whereby a fraudster will:

1. **Conspire** – The fraudsters plan their scam, after gathering information on their targets and devising a suitable premise.

2. **Connect** – The fraudsters then connect with the target(s) via communication channels such as Voice call or SMS.

3. **Convince** - The fraudsters then, through conversation or the content of the message, convinces the target of the need to make a payment or provide their personal information.

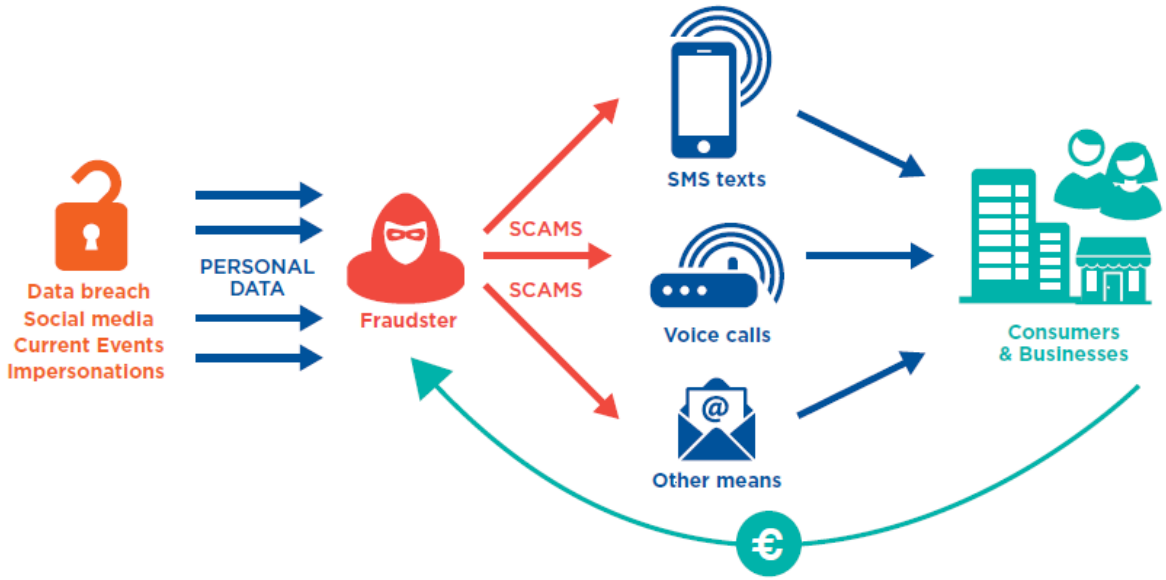
4. **Close** - Finally, the victim either makes the payment or provides their personal information, after which the fraudster will secure or conduct the payment and terminate the connection.

Figure 36: The four stages of a scam.

Fraudsters use telecommunication networks to commit fraud

A 1.24 Fraudsters utilise public, international ECS networks to contact consumers in Ireland and other countries by SMS and Voice calls. Scam operations are typically operated by criminal groups which can commit scam calls and SMS both within the same country and from other countries. International fraudsters often target wealthier countries, in particular those with more common, widely shared languages such as English. Hence, fraudsters have the ability to contact consumers to elicit information and/or payments from a consumer to complete their fraud. Without such networks, fraudsters would be limited in how many potential victims they can reach.

Figure 37: How fraudsters use telecommunication networks to commit fraud



A 1.25 Fraudsters can use consumers own genuine information to persuade them of the authenticity of the scam (e.g., using the targets own name, showing a consumer the last 4 digits of their bank account). In this way, weak network security and data breaches fuel scams. Fraudsters often use lists of personal information in combination with phone numbers that have been obtained through various means, such as

- buying them from illicit data brokers;
- extracting them from malware-infected devices;
- stealing them from other companies in data leaks; and
- increasingly, obtaining or complementing such information with information on potential victims garnered via social media. Using such sites, fraudsters can identify and impersonate the friends, family or colleagues of victims using information or images posted online[516].

[516] DublinLive.com 21st March 2023 "*Expert warns of WhatsApp 'family emergency' scam targeting users across Ireland*" Link

A 1.26 Scam call operations often use large call centres or automated dialling systems to place a large number of calls to potential victims. Once a victim answers the call, the fraudster will typically use a script to try to trick them into providing personal information or sending money. The fraudsters may ask for sensitive information such as Personal Public Service ("PPS") number, credit card information, or bank account numbers, ask the victim to send money through wire transfer, gift card or via cryptocurrency, or even request remote access to the victim's computer. Once they have obtained this information or money, they will often quickly disappear and use it for fraudulent activities.

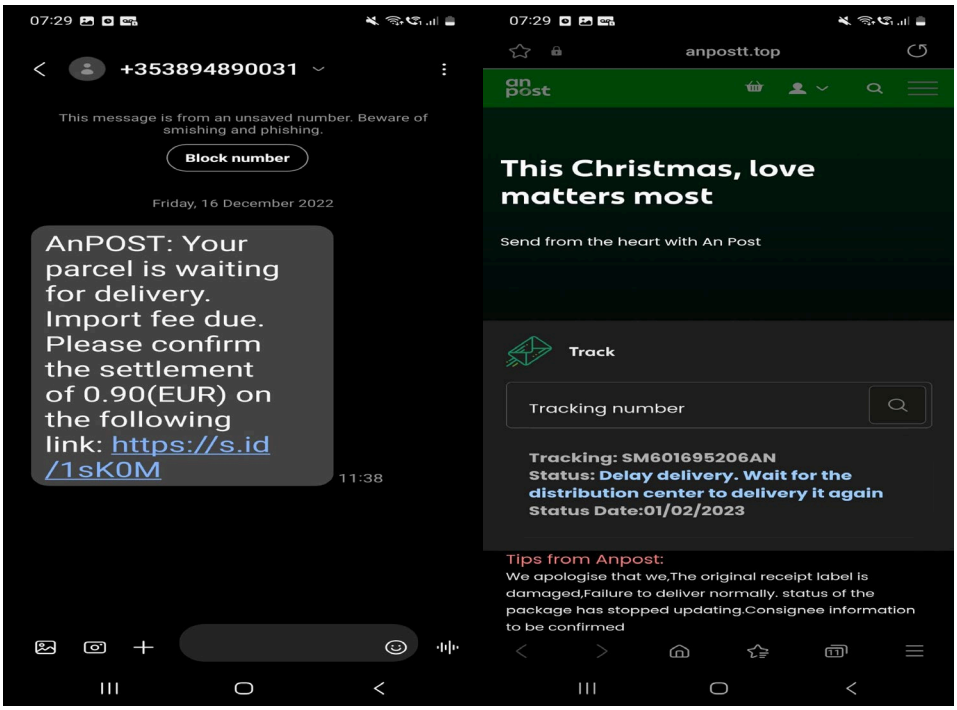
A 1.27 Scam call centres are often based in countries with relatively low labour costs and a large pool of skilled English-speaking workers (e.g., India) in order to target wealthy English-speaking countries. There are reports of centres with hundreds of staff operating 24/7, generating tens of thousands of calls daily. This is crucial to many scam calls given the low success rate for scams, with the consumer survey indicating there are up to 3 successful scams per 1,000 received[517]. While many scam calls have originated from abroad in the past, ComReg understands from An Garda Síochána that a growing share of reported scam calls appear to originate within the State (primarily through the use of pre-pay burner phones).

A 1.28 Scam SMS operations will send text messages to many potential victims at once. Fraudsters may use SIM banks[518] to store and manage a large number of SIM cards, each with a different phone number[519]. They can then use these SIM cards to send a large number of text messages to potential victims. Fraudsters often operate from a moving vehicle to avoid detection and triangulation of their location by MNOs and law enforcement agencies[520].

A 1.29 The text message may appear to be from a legitimate source, such as a bank, government agency, or a well-known company. The scam may request the recipient to provide either personal information or payment details in response. Alternatively, the message may ask the victim to click on a link, which leads to a fake website or app that looks like a legitimate one asking them to enter their personal information, as shown in Figure 38 below. Once the victim enters their personal information into the website, the fraudsters can use it for fraudulent activities.

[517] This is based on scam calls and resulting fraud as reported to the Consumer survey. ComReg considers that underreporting of scam calls is more likely than fraud, and therefore this figure should be considered as an upper bound on scam effectiveness.
[518] A SIM bank is used to store and manage a large number of SIM cards in a single location.
[519] Using different numbers can make it more difficult for victims to block or for authorities to trace fraudsters.
[520] Commsrisk.com, 20 March 2023 "*Sixth Suspect Arrested for Massive Paris IMSI-Catcher SMS Scam*" Link

Figure 38: Example of a scam text impersonating An Post and accompanying website, 16th December 2022



A 1.30 A single 64 port SIM bank (see Figure 39), available online for between €700-€800 and can generate 640,000 scams texts for less than €1,000 per month – as multiple MNOs offer SIM-only mobile plans offer up to 10,000 texts messages per month, for as little as €14.99. A fraudster could well recoup these and other costs (e.g., fake website development) with even a low success rate, noting that the consumers survey indicates there are up to 4 successful scams per 1,000 received.

Figure 3939: Example of a SIM Bank

Source: Advert for a 64 port SIM Bank on sale at AliExpress.

Incentives for criminals to perpetuate scams

A 1.31 Fraudsters have an incentive to perpetuate scams wherever the revenues generated by a scamming operation exceeds its costs. The profitability of scam calls and texts is determined by a number of factors, including: the number of victims targeted; the success rate of the scam; the amount of money each victim is scammed out of; the cost of running the scam; and the likelihood of facing sanctions.[521]

A 1.32 Although the success rate is highly critical to the profitability of a scam, most scams require only a small percentage of the recipients to fall for the scam to achieve profitability. The required success rate of scams is highly variable, with different types of scams needing different levels of success to achieve profitability. For example, a scam that involves tricking victims into providing personal information or wiring money may require far lower success rates to achieve profitability than a fake delivery charge scam where the sums scammed could be much smaller, albeit such scams are often directed at emptying bank accounts as opposed to collecting small sums for purported delivery costs.

A 1.33 To increase the success rate, fraudsters use a number of tactics to gain the trust of their victims, which may include:

- impersonating well-known business or government agencies;
- impersonating family members or friends;
- using the user's personal information gathered through a data leak or via social media to gain trust;
- capitalising on current events which may require a refund, fee or social transfer or submitting personal information (e.g., Revenue at the end the tax year[522], An Post at Christmas); and
- using fear tactics or injecting a false urgency, such as claiming that there is an emergency the consumer must address.

[521] Fraudsters likely factor in the risk of being caught and facing prosecution or penalty into their expected value of launching a scam. Given the difficulty in tracing fraudsters, many fraudsters likely consider the risk of facing sanction low.
[522] Revenue.ie "*Warning: Latest SMS (text message) scam*" Link

A 1.34 Fraudsters react remarkably quickly to current events to maximise their effectiveness. On 8 July 2023, Rogers (one of Canada's largest telecoms companies), experienced a failure lasting approximately 15 hours. The following day, fraudsters were reported as having launched successful campaigns exploiting this network outage, claiming to offer credits to affected customers in lieu of the downtime[523]. Fraudsters tendency to exploit current events, combined with successful scams being copied by fraudsters at home and abroad results in scams coming in waves.

Fraudsters are an enduring threat to consumers and businesses

A 1.35 Each evolution in the use of ECS and smartphones to communicate, make payments and/or share personal information presents new opportunities to fraudsters. Indeed, the recent increase in scams appears to coincide with the increased use of online payments, shopping and banking, during the COVID-19 pandemic, which has created opportunities for fraudsters to steal data and money from unsuspecting users by SMS texts and Voice calls. Past waves of scams have similarly made use of evolutions in consumer purchasing behaviour (e.g., PRS scams exploiting SMS subscription services).

A 1.36 ComReg's proposed approach should constrain the ability of fraudsters to reach consumers and to impersonate trusted organisations and contacts. However, fraudsters will not run out of opportunities and events to capitalise on and data leaks feed and exacerbate scams. Data leaks can occur without warning, and immediately expose a large number of consumers at once to highly targeted scams[524]. Notably, the Irish wave of scams coincided with the leak of the user data including the mobile numbers of over 500 million Facebook users[525], containing over 1.3 million Irish users[526]. Therefore, any package of measures proposed by ComReg must include a *dynamic* component which can tackle nuisance communications in real time and take account of economic and societal developments.

[523] CBA.ca July 10, 2022 "*Rogers warns of text scams 'claiming to offer credits' in wake of service outage*" Link
[524] The Optus hack in Australia resulted in the theft of personal information belonging to 9.8 million customers, including names, birth dates, physical and email addresses, and phone numbers. This information was subsequently used by fraudsters to attempt fraud. Link
[525] Cybernews.com, 27 September 2022 "*Facebook data leak: you should be on the lookout for scams*" Link
[526] Independent.ie "Meta fined €265m in Facebook data-scraping case that exposed millions of mobile phone numbers" Link

Annex: 2 Econometric analysis of victims of fraud

A 2.1 This Annex contains information on ComReg's econometric analysis of the survey data of B&A on scam victimhood and monies lost as a result of scams.

A 2.2 ComReg's work will reduce the prevalence of scams, and thereby restore consumer trust in networks in the long term. This work may be complemented by consumer awareness efforts, which could potentially further reduce the effectiveness of scams[527].

A 2.3 While many organisations have made information available on scams, ComReg is not aware of any organisation that have engaged in proactive targeted awareness campaigns. The purpose of the research is to aid organisations in conducting their own scam awareness campaigns, by enabling them to target information at the most at-risk consumers. By targeting those most at-risk of scams, organisations can use finite budgets to combat scams most effectively.

A 2.4 This research overcomes certain identified information deficits that would otherwise impede such targeted campaigns. ComReg considers that a number of organisations may wish to raise consumer awareness of scams, including:

- Impersonated businesses (e.g., Irish retail banks)
- Impersonated Government agencies
- Enforcement agencies

Targeted campaigns can reach the most at-risk users.

[527] It is the responsibility of organisations to raise their consumers awareness and immunity to scams.

A 2.5 For readability, the key takeaways are presented first, followed by the econometric analysis which is unavoidably technical. Accordingly, this Annex is laid out as follows:

I. How targeted awareness campaigns can combat scams.
   a. The benefit of targeted awareness campaigns.
   b. How a lack of information on scam victims impedes targeted campaigns.
   c. Key findings for organisation undertaking such campaigns.

II. ComReg's econometric analysis of the consumer survey data.

I. How targeted awareness campaigns can help combat scams

a. The benefit of targeted awareness campaigns

A 2.6 Many impersonated organisations engage in passive consumer awareness, by making information available via online press releases or dedicated webpages. This approach relies upon the consumer using key search terms to find the information. In either case, consumers are likely to encounter such information upon searching for it.

A 2.7 Active awareness campaigns are likely to be most important in further raising consumer awareness for a number of reasons, which includes:

- First, consumers that view passive ads are less likely to be susceptible to scams. After all, passive ads are seen by consumers that likely already are suspicious, having searched for this information (e.g., having searched for "scam text an post?").
- Second, as many consumers do not engage with or permit direct communications, a large share of unsuspecting consumers can be reached by indirect communications like advertising.
- Third, as passive campaigns are widespread, they are likely having most if not all of their effect already - further raising scam awareness depends upon further action.

A 2.8 Certain organisations have also raised awareness of scams actively, through attempting to put that information in front of consumers that are not searching for it (e.g., publishing it in a newspaper)[528]. Active campaigns work best where they involve targeting specific groups.

[528] Companies can reach consumers in a number of ways, including via direct communications (e.g., emails, in-app messages) or indirect communications such as via advertising on print, broadcast, online and social media.

A 2.9 Traditionally, proactive campaigns target consumers by choice of media channel[529] However with digital advertising, organisations can choose the audience directly, based on an individual's demographic characteristics, such as their age, gender, income, education, and location); or their online behaviour (e.g., websites they visit, search terms they use, or products they purchase).

A 2.10 In Ireland, online media platforms allow organisations to place information in front of specific user groups, by selecting the demographic profile of the audience[530]. This can greatly enhance the effectiveness of a campaign where certain users are most relevant or at risk. However, to engage in proactive advertising campaign, organisations must know which consumer groups to target.

b. How a lack of information on scam victims impedes targeted campaigns

A 2.11 At present, any organisation planning a proactive awareness campaign to combat scams is impeded by a lack of accurate information on what consumers are likely to be scammed.

A 2.12 ComReg is not aware of the existence of any representative data on scam victimhood in Ireland. Organisations can only be aware of consumers that report having been scammed. ComReg's survey analysis indicates the majority of scams are not reported. Moreover, individual organisations could only be aware of scams reported to them, which represents a small share of the fraction of scam victims that report a scam. Furthermore, organisations may wish to target different outcomes, either scam prevalence or reducing to reduce the total value of monies stolen (i.e., targeting high value fraud more)[531].

A 2.13 This lack of information lowers the effectiveness and return on active awareness campaigns. Unlike passive advertising, proactive advertising necessarily incurs a cost, and organisations have a finite budget for such campaigns. An inability to target most at-risk consumers lowers the return-on-investment to proactive awareness campaigns and thereby inhibit their use.

c. Key findings

[529] For example, advertising in the Irish Farmers Journal to sell to farmers.
[530] See for example, the policies of Google and Meta.
[531] The latter may be an objective for organisations with a greater incidence of high-value frauds, noting that amounts scammed can vary between €5 and €5,000.

A 2.14 Based on the analysis below, ComReg recommends that an organisation attempting to reduce the incidence of fraud target people under 25 years of age.

A 2.15 This is the most statistically and economically significant predictor of an individual's risk of being scammed, with those under 25 years of age being 14 times more likely to report having lost money to a scam, controlling for other variables.

A 2.16 Given the age cohort most at-risk from current scam SMS and calls in the past 12 months, awareness campaigns conducted in schools or universities may also be effective.

II. ComReg's econometric analysis of the consumer survey data

A 2.17 ComReg analysed data on scam victimhood, payments and demographic information gathered as part of the B&A Consumer Survey. ComReg examined the following question: Are certain groups of consumers more likely to become scam victims or lose greater amounts when defrauded.

A 2.18 To ComReg's knowledge, this analysis is unique not only in Ireland, but internationally.

A 2.19 The analysis is divided into the following sections:

a) Literature review;
b) Methodology;
c) Data;
d) Results; and
e) Assessment of the results.

a) Literature review

I. Determinants of scam victimhood

A 2.20 Most research on scam victimhood appears to have focused on the psychological and not demographic determinants of scam victimhood. While interesting, this is of little use to organisations combatting scams, as these traits are not readily observable and targetable characteristics[532]. Research on scam victimhood is complicated by the lack of reliable data on actual rates of victimhood. Much of the literature is based on reported scams, which likely comprise only a fraction of actual scams given the low levels of reporting.

A 2.21 The key findings of ComReg's literature review are summarised below. The literature is inconclusive on whether any specific demographic group is most susceptible to scams overall. Indeed, different demographics appear most susceptible to differ scams, consistent with fraudsters using a variety of scams to target many groups. Indeed, research has found that different groups (male vs. female, young vs. old) are more likely respond to a scam solicitation depends on the type of scams (Button et al. 2009).

A 2.22 By far the most studied characteristic is age. An interesting finding in the literature is that in spite of a widespread belief that older people are most susceptible there is evidence that scam victimhood is spread across age cohorts with different cohorts appearing most susceptible to different scams (Hanoch & Wood, 2021). The scant research on the demographic determinants of SMS and Voice to date, typically carried out by banks such as Barclays and PTSB, indicates that younger consumers are more susceptible to scams.[533] In the Irish context the evidence is mixed regarding what consumers are most at-risk. While research by Amárach on behalf of AIB indicates that consumers "*aged over 55 were more likely to be targeted by fraudsters*", while research conducted by BehaviorWise on behalf of Permanent PTSB[534] found that consumers "*under 45 (are) more likely than older people to fall victim to financial fraud*".

Table 22: Key findings of demographic determinants of scam victimhood

Characteristics	Effect
Age	***Over 65s: Inconclusive – higher for some scams*** While a number of studies have found that that older adults (65 years old and over) are more likely to be targeted by fraudsters (Burnes et al., 2017; Lichtenberg et al., 2016) and more likely to become victims (James et al., 2014), a number of studies have found that older adults face a reduced risk of becoming a victim compared with middle-aged adults (Anderson, 2019; Office for National Statistics, 2016; Titus et al., 1995).

[532] https://onlinelibrary.wiley.com/doi/abs/10.1111/jasp.12158, https://link.springer.com/article/10.1007/s10610-020-09458-z https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2448130
[533] Other NRAs, such as Ofcom, that have studied scams have focused more on scam prevalence and not published any information on the demographic profile of victims.
[534] Reflecting Ireland consumer research, published on 23 November 2022. Link

	Middle age - Inconclusive – appears higher for some scams. Some research indicates that middle-aged adults are the age group with the highest rate of victimization (Office for National Statistics, 2016). Focusing on scams related to COVID-19, a report by the Federal Trade Commission (2021) found that adults between the ages of 30 and 39 reported the highest number of COVID-19 fraud complaints, a finding that roughly matches Anderson's (2019) report that individuals ages 35 through 44 were most likely to report falling victim to mass-marketing solicitations
	Younger adults – appears higher for SMS and Voice scams. In relation to recent scams • In the UK, younger people were significantly more likely to be victims of fraud with those aged 20 to 39 accounting for 39% of all reports to Action Fraud. • Recent research by Barclays band found that 21–30-year-olds being fifteen times more likely to be a victim compared with those aged over 70 . • Recent Research by Permanent TSB found that victims are more likely to be young (under 45, particularly Millennials) living in Dublin or urban areas.
Sex	A survey on scams in 30 European countries (European Commission, 2020) found that males are more likely than females to report being victimized.
	The ACMA has found that men and women report a falling victim to a similar number of scams, however men typically lose money.[535]
Economic Status	The Office for National Statistics (2016) in the United Kingdom, for example, has reported that individuals with higher incomes report higher rates of victimhood. A survey on scams in 30 European countries (European Commission, 2020) has provided similar insights, finding that more educated individuals and individuals with higher incomes are more likely to report being a victim of fraud, and also that males are more likely than females to report being victimized. DeLiema and colleagues (2020) and Whitty (2019a, 2019b) also reported that being better educated was associated with higher rates of reporting being defrauded in investment-type scams. In contrast, studies by Wood et al. (2018) and Mueller et al. (2020) suggest that higher education is associated with a lower intention to respond to mass-marketing solicitations.
Demographic group	Anderson (2019), who reported that Hispanic Americans and Black Americans are more likely than White Americans to report falling victim to fraud

II. Appropriate empirical approach

A 2.23 The econometric analysis of scam victimhood and losses is made complex as a result of the "zero-inflated problem", which arises as few consumers have been scammed. Zero-inflated problem in econometrics is a phenomenon in which an excessive number of zero values are observed in a dependent variable, leading to skewed and biased estimates of the statistical model. A variety of approaches have been used in the literature given the zero problem. In line with Eisenberg et. Al (2015)[536] ComReg has applied both a two-stage hurdle model and separate models for the process of scam victimhood and amounts paid, given that there is no censoring of data or latent structure.

[535] ACMA "*Targeting scams report 2021*" available here
[536] Eisenberg, Theodore and Eisenberg, Thomas and Wells, Martin T. and Zhang, Min, "Addressing the Zeros Problem: Regression
Models for Outcomes with a Large Proportion of Zeros, with an Application to Trial Outcomes," 12 Journal of Empirical Legal Studies
161-186 (2015)

A 2.24 In this instance, as the results of the two-stage model supported the results of the separate models, with the same variables achieving the same level of statistical significance. ComReg considers that it has little additional useful information to offer an organisation designing awareness campaigns. Therefore, to aid readability ComReg only reports the results of the separate models here[537].

b) Methodology

A 2.25 Using logistic regression, ComReg has examined whether certain groups of consumers more likely to become scam victims. A logistic regression, is used to model the relationship between a binary dependent variable (e.g., scammed or not scammed) and one or more independent variables[538]. In this instance, the OLS regression can be used to establish whether a statistically significant relationship exists between a consumer's demographic characteristics and the likelihood of them being scammed. The coefficients in the output of the logistic regression are given in units of log odds. Therefore, the coefficients indicate the amount of change expected in the log odds when there is a one unit change in the predictor variable with all of the other variables in the model held constant. Odds ratios that are greater than 1 indicate that the event is more likely to occur as the predictor increases.

A 2.26 The logit regression can be shown as follows:

$$logit(Y) = log\left(\frac{p(Scammed_i)}{1 - p(Scammed_i)}\right) = \beta_0 + \beta_1 Charateristics_i + \varepsilon_i$$

[537] Moreover, a hurdle model is typically used where the observed party commits two consecutive decisions, whereas in this instance, the consumers make choices that enable the scam, but does not choose the amount being stolen (e.g., the payment is set by the fraudster, or the fraudster empties the bank account).
[538] The goal of logistic regression is to estimate the coefficients of the independent variables that best predict the binary outcome, and to estimate the probability of the binary outcome given the values of the independent variables. Logistic regression assumes that the probability of the binary outcome follows a logistic function, which is an S-shaped curve that ranges from 0 to 1. The logistic function maps a linear combination of the independent variables and their coefficients to the probability of the binary outcome.

A 2.27 Using ordinary least squares ("OLS") regression, ComReg has examined whether certain groups of consumers lose more money if scammed. An OLS regression is a statistical technique used to model the linear relationship between a dependent variable (also known as the response or outcome variable) and one or more independent variables (also known as predictor or explanatory variables) [539]. In this instance, the OLS regression can be used to establish whether a statistically significant relationship exists between a scam victims demographic characteristics and the amount lost to the scam.[540]

A 2.28 The OLS regression can be shown as follows:

$$AmountScammed_i = \beta_0 + \beta_1 Charateristics_i + \varepsilon_i$$

c) Data

A 2.29 This dataset records the experiences of scam calls and SMS for a representative sample of 1,219 consumers above the age of 16. This sample was constructed in terms of the age, gender, socio-economic class and region of respondents to reflect the profile of the adult population of the Republic of Ireland. As part of this survey respondents were asked to report whether they had lost money as a result of a scam call or text, and if so, how much money was lost. The demographic information gathered includes the age, gender, socio-economic class, region of participants.

Table 23: Descriptive statistics for possible predictors of victimhood

Variables	Victims		Non-Victims		Whole sample	
	Mean	SD	Mean	SD	Mean	SD
Male	.55	.50	.50	.50	.50	.50
Age	34.24	13.97	47.33	15.74	46.57	15.94
High SES	.45	.50	.53	.50	.52	.50
Urban	.25	.44	.35	.48	.34	.48
National	.82	.39	.82	.39	.82	.39
Kids	.62	.49	.63	.48	.63	.48
N	71		1,148		1,219	

[539] The goal of OLS regression is to estimate the parameters of a linear equation that best fits the observed data. In an OLS regression, the line of best fit is determined by minimizing the sum of the squared differences between the observed values of the dependent variable and the predicted values based on the independent variables. This is known as the least squares criterion.

[540] In line with Eisenberg (2015), ComReg also examined this effect using a two-stage regression, specifically a hurdle model. ComReg considered this appropriate given that 0 values were observed (i.e., not being scammed). However, in this instance, as the results supported the results of the OLS, with the same variables achieving the same level of statistical significance, ComReg considers that it has little additional useful information to offer organisation designing an awareness campaign. Therefore, to aid readability ComReg only reports the results of the OLS here. Moreover, a hurdle model is typically used where the observed party commits two consecutive decisions, whereas in this instance, the consumers make choices that enable the scam, but does not choose the amount being stolen (e.g., the payment is set by the fraudster, or the fraudster empties the bank account).

d) Regression results

A 2.30 Table 24 below presents the results ComReg's regression analysis.

Table 24: Regression coefficients and their statistical significance

Variables	Victimhood			Amount lost (€)
	Calls	SMS	Any	Calls or SMS
	Logit	*Logit*	*Logit*	*OLS*
Male	1.90** (.62)	1.50 (.48)	1.59* (.44)	-861.76*** (284.39)
High SES	1.05 (.33)	1.00 (.31)	0.95 (.26)	-567.96** (277.51)
GenZ	18.49*** (8.8)	21.56*** (10.87)	14.78*** (6.07)	
Millennials	3.12*** (1.32)	4.59*** (2.02)	2.96*** (1.00)	
Over65s	0.47 (.37)	0.61 (.5)	0.46 (.29)	
Age	-	-	-	-11.76 (10.19)
Kids	2.73** (.98)	2.24** (.77)	2.69*** (.84)	
Non-national	1.26 (.51)	1.20 (.49)	1.03 (.34)	
UrbanRural	0.84 (.31)	0.56 (.21)	0.76 (.29)	
Region 2	1.17 (.47)	1.42 (.56)	1.46 (.5)	
Region 3	0.63 (.29)	0.93 (.4)	0.73 (.28)	
Region 4	0.60 (.30)	0.72 (.35)	0.62 (.27)	
_cons	0.01*** (.01)	0.01*** (.1)	0.02*** (.01)	1554.184 (432.5603)
R^2	0.1355	0.1421	0.1257	0.1586
Observations	1,219	1,219	1,219	68

Standard errors in parentheses, *<p<0.1, ** p<0.05, *** p<0.01

e) Assessment of the results.

Victimhood

Age

A 2.31 The coefficient for the dummy variables *GenZ* and *Millennial* are statistically significant at the 1% level in both OLS regressions for scam calls and SMS[541]. The size of the effect is large, with GenZ and Millennials roughly 14 and 3 times more likely to report having been scammed by call or text in the prior 12 months respectively, compared to older age cohorts.

Sex

[541] As the sign of the coefficient is negative, this means we can reject with 99% confidence that GenZ and Millennials are not more susceptible to scam calls or texts.

A 2.32 The coefficient for the dummy variable male is statistically significant at the 5% level for scam calls or at all, but not for SMS specifically[542]. The size of the effect is moderate, with men roughly twice as likely to report having been scammed in the prior 12 months respectively, compared to women.

Other variables

A 2.33 The coefficient for the dummy variable *Kids* is statistically significant at the 1% level in both OLS regressions. The meaning of *kids* is ambiguous, as this merely records whether children under the age of 18 are in the respondents' households. These may be children or siblings, with the latter more likely in the case of respondents under 25. Nevertheless, this may support parents being more susceptible to scams, noting the evidence of scams targeting parents specifically[543].

A 2.34 None of the other demographic factors demonstrate a statistically significant relationship with victimhood.

Money lost

Sex

A 2.35 The coefficient for the dummy variable male is negative and statistically significant at the 1% level[544]. The size of the effect is large, with scammed women losing approximately 800 euro more on average than men, controlling for age and socio-economic status. This is consistent with the distributions of men and women among payees: while more men report having lost money to scams, women were overrepresented among those who paid more than €100, and in particular above €1,000[545].

Socio-Economic status

A 2.36 The coefficient for the dummy variable *SES* is statistically significant at the 5% for the OLS regressions for the value of amounts reported as being lost to scam calls.[546] This is consistent with the distributions of high and low SES among victims: low SES were overrepresented among those who paid more.

Conclusions

Age

[542] As the sign of the coefficient is negative, this means we can reject with 95% confidence that men are not more susceptible to scam calls.
[543] For example, "Hi Mum" scams.
[544] As the sign of the coefficient is negative, this means we can reject with 99% confidence that women do not pay more than men when scammed by call or texts.
[545] The significance values for these findings were corroborated by the 2SLS hurdle model.
[546] As the sign of the coefficient is negative, this means we can reject with 90% confidence that high SES do not pay more than low SES when scammed by call.

A 2.37 The analysis indicates that younger users are far more likely to report having been scammed. Age is clearly the key predictor of scam victimhood.

Sex

A 2.38 The analysis indicates that men are more likely to fall victim to scams; but women typically lose more money when scammed. ComReg places less weight on this finding in constructing its advice to given the:

- mixed effects of gender on scam victimhood and monies lost; and
- unavoidably small sample for the impact on monies lost.

Other factors

A 2.39 ComReg places less weight on the remaining factors given the difficulty in this into reliable, advice given uncertainty in regarding sample size or the effect.

Annex: 3 Summary of statutory objectives and legal framework relevant to interventions relating to nuisance communications

A 3.1 This Annex seeks to set out the primary legal powers currently available to ComReg in relation to dealing with nuisance communications[547].

A 3.2 The 2002 Act, the Communications Regulation and Digital Hub Development Agency Act 2023, and S.I. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022, set out, amongst other things, powers, functions, duties and objectives of ComReg that are relevant to interventions relating to nuisance communications. For the purposes of this Annex, "nuisance communications" means unwanted, unsolicited communications generally directed at large groups of the population. Nuisance communications often have the intent to mislead the receiver, so that they unknowingly provide sensitive personal information.

A 3.3 The previous European Common Regulatory Framework for ECN and ECS has been superseded by the European Electronic Communications Code[548] ("EECC"). On 20 December 2018, the EECC entered into force.

A 3.4 Most of the EECC (including numbering provisions) has been transposed into Irish law by secondary legislation, namely S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022[549]. The other relevant transposing legislation is the Communications Regulation and Digital Hub Development Agency Act 2023.

A 3.5 All references in this annex to enactments are to the enactment as amended at the date hereof unless the context otherwise requires.

Primary Objectives and Regulatory Principles under the 2002 Act

Relevant statutory functions and objectives

[547] For completeness, relevant criminal law relating to fraud, although enforced by An Garda Síochána rather than ComReg, is also noted below.
[548] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11th December 2018 establishing the European Electronic Communications Code.
[549] pdf (irishstatutebook.ie)

A 3.6 The ComReg statutory functions contained in section 10 of the Communications Regulation Act 2002, as amended, that are particularly relevant to this project are the following:

- Section 10(a): “to ensure compliance by undertakings with obligations in relation to the supply and access to electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such facilities”;
- Section 10(b): “to manage … the national numbering resource, in accordance with a direction under section 13”; and
- Section 10(d): “to carry out investigations into matters relating to- (a) the supply of, and access to, electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such networks…”.

A 3.7 The ComReg statutory objectives contained in section 12 of the Communications Regulation Act 2002, as amended, that are particularly relevant to this project include the following:

- Section 12(1)(a): “the objective of the Commission in exercising its function in relation to the provision of electronic communications networks, electronic communications services and associated facilities shall be as follows: (i) to promote competition; (ii) to contribute to the development of the internal market, and (iii) to promote the interests of users within the Community”;
- Section 12(1)(b): “to ensure the efficient management and use of … numbers from the national numbering scheme in the State in accordance with a direction under section 13”.

A 3.8 Further to section 12(2), in relation to the objectives referred to in section 12(1)(a), ComReg shall take all reasonable measures which are aimed at achieving those objectives, including:

(as set out in section 12(2)(a)), in so far as the promotion of competition is concerned-

(i) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality;

(ii) ensuring that there is no distortion or restriction of competition in the electronic communications sector, …

(iv) encouraging efficient use and ensuring the effective management of radio frequencies and numbering resources,

as set out in section 12(2)(c)) in so far as promotion of the interests of users within the Community is concerned-

- (ii) ensuring a high level of protection for consumers in their dealings with suppliers…;
- (iii)contributing to a high level of protection of personal data and privacy;
- (iv)promoting the provision of clear information…"
- (vii) ensuring that the integrity and security of public communications networks are maintained".

A 3.9 Section 12(3) of the 2002 Act provides that in carrying out its functions, ComReg shall seek to ensure that measures taken by it are proportionate having regard to the objectives set out in section 12.

A 3.10 Section 12(5) of the 2002 Act provides that in carrying out its functions, ComReg shall have regard to international developments with regard to electronic communications networks and electronic communications services, associated facilities… and numbering.

A 3.11 To note that section 10(3) of the 2002 Act provides that ComReg shall have all such powers as are necessary for or incidental to the performance of its functions under the 2002 Act or any other Act.

Powers relating to Numbering

A 3.12 ComReg's powers in relation to the rights of use for numbers are further detailed in the S.I. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022. Part 10 of S.I. 444 of 2020 deals with access to numbers and services, and related provisions, and transposes Articles 93 and 94 of the EECC.

A 3.13 Relevant general objectives listed in Regulation 4(3), which ComReg has to pursue in the context of its tasks, are the following: "promote the interests of the consumers and businesses in the State, by ensuring connectivity and the widespread availability and take-up of very-high-capacity networks, including fixed, mobile and wireless networks, and of electronic communications services, by enabling maximum benefits in terms of choice, price and quality on the basis of effective competition, by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules and by addressing the needs, such as affordable prices, of specific social groups, in particular end-users with disabilities, elderly end-users and end-users with special social needs, and choice and equivalent access for end-users with disabilities".

A 3.14

Under Regulation 79(1) of S.I. 444, the granting by ComReg of rights of use for all national numbering resources for all publicly available electronic communications services is subject to ensuring the proper management of the national numbering plan in accordance with ComReg's objectives under section 12 of the 2002 Act, and Regulation 4 of S.I. 444.

1. Regulation 78(7) of SI 444 provides: "the Regulator may, without prejudice to the generality of Regulation 10, attach conditions to rights of use for numbering resources (a) to ensure the efficient and effective management of all numbering resources, and (b) to ensure that person granted numbering resources does not discriminate against a provider of publicly available electronic communications services".

2. Pursuant to Regulation 10(1) of SI 444, the Regulator shall specify conditions to be attached to a right of use for numbering resources, only as are listed in Part E of Schedule 1 to the Regulations. The key word to be aware of here is "only". There is a relatively narrow list of conditions that that can be attached to a numbering right of use set out in Part E of Schedule 1 – a criminal penalty applies if these conditions are breached (Regulation 10(5) and (6)). Regulation 10(1) transposes Article 13 of the EECC.

3. Relevant conditions which may be attached to rights of use for numbering resources under Part E of the Schedule to SI 444 are: (2) Effective and efficient use of numbering resources in accordance with these Regulations.

Current provisions relating to CLIs

A 3.15 General Authorisation Condition 3.1(5) of the Numbering Conditions of Use[550] (which Condition applies to all authorised undertakings) sets out, amongst other things, that:

(a) The undertaking which originates a call shall ensure:

(i) that the presentation CLI[551] for the call shall be the assigned Customer Support Short Code (for on-network calls), a Freephone Number, a

[550] Numbering Conditions of Use and Application Process, ComReg-15136R3.pdf
[551] "presentation CLI" is defined for the purposes of the Numbering Conditions of Use (in Annex 11) as meaning a number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI.

Geographic Number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number for the calling party;

(ii) that the network CLI for the call shall be the assigned Geographic Number, 076 Standard Rate Number, Mobile Number or M2M number for the calling party; and

(iii) that a Mobile Number is not used as the presentation or network CLI for any call that originates from a fixed terminal.

Power relating to misuse of numbers

Under Regulation 83(2) of SI 444, the Regulator may require providers of public electronic communications networks or publicly available electronic communications services to block on a case by case basis, access to numbers or services where this is justified by reason of misuse and to require that in such cases those provides withhold relevant interconnection or other service revenues. See further discussion on this below.

Powers relating to security

A 3.16 Obligations on operators regarding security and integrity are set out in Part 2 of the Communications Regulation and Digital Hub Development Agency Act 2023.

A 3.17 Further to section 6(1): “Providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services.” It should be noted that further to section 6(2): “Measures taken in accordance with subsection (1) shall ensure a level of security appropriate to the risk presented having regard to the state of the art. It should also be noted that further to section 6(3): “In particular, measures, including the use of encryption where appropriate, shall be taken by providers to prevent security incidents and minimise the impact of any security incident on users and on other networks and services.”

A 3.18 It is important to note that the definition of “security of networks and services” means as per section 5 of the Act of 2023: “the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services”.

A 3.19 There is a statutory duty on ComReg under section 13 of the Act of 2023 to seek to ensure compliance by providers with Part 2: "The Commission shall take reasonable steps to ensure that providers comply with the obligations placed on them by or under this Part."

E-Privacy issues

A 3.20 Regulation 5(1) of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011), provides that: "Without prejudice to section 98 of the Act of 1983[552] and section 2 of the Act of 1993[553] and except where legally authorised under a provision adopted in accordance with Article 15(1) of the Directive on privacy and electronic communications, the listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is prohibited."

A 3.21 It should be noted that if operators obtain the consent of users of their services to the interception of communications in order to prevent nuisance communications from reaching those users, then it would appear that the prohibition in Regulation 5(1) is not breached.

Interception - The 1983 Act

A 3.22 Section 98(1) of the Postal and Telecommunications Services Act 1983 provides that: "A person who- (a) intercepts or attempts to intercept, or (b) authorises, suffers or permits another person to intercept, or (c) does anything that would enable him or another person to intercept, telecommunications messages being transmitted by the company or who discloses the existence, substance or purport of any such message which has been intercepted or uses for any purpose any information obtained from any such message shall be guilty of an offence."

A 3.23 Exceptions to section 98(1) are set out in section 98(2), which provides as follows:

> "Subsection (1) shall not apply to any person who is acting—
>
> *(a)* (i) for the purpose of an investigation by a member of the Garda Síochána of a suspected offence under section 13 of the Post Office (Amendment) Act, 1951 (which refers to telecommunications messages of an obscene, menacing or similar character) on the complaint of a person claiming to have received such a message, or

[552] Postal and Telecommunications Services Act 1983.
[553] Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

(ii) in pursuance of a direction issued by the Minister under section 110 , or

(iii) under other lawful authority, or

(b) in the course of and to the extent required by his operating duties or duties for or in connection with the installation or maintenance of a line, apparatus or equipment for the transmission of telecommunications messages by the company.

3) (*a*) The company may, with the consent of the Minister, make regulations to carry out the intentions of this section in so far as concerns members of its staff.

(*b*) The Minister, after consultation with the company, may direct the company to make regulations under *paragraph (a)* or to amend or revoke regulations made under that paragraph and the company shall comply with that direction.

(*c*) A person who contravenes any regulation under this subsection shall be guilty of an offence.

(4) (*a*) The Minister may make regulations prohibiting the provision or operation of overhearing facilities in relation to any apparatus (including private branch telephone exchanges) connected to the network of the company otherwise than in accordance with such conditions as he considers to be reasonable and prescribes in the regulations.

(*b*) A person who contravenes any regulation under this subsection shall be guilty of an offence.

A 3.24 It should be noted that for the purposes of section 98, “interception” means: “listening to, or recording by any means, or acquiring the substance or purport of, any telecommunications message without the agreement of the person on whose behalf that message is transmitted by the company and of the person intended by him to receive that message” (section 98(5)).

Interception - The 1993 Act

A 3.25 Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 is entitled “Authorisation of interceptions”. Section 2(1) provides as follows: “The Minister may give an authorisation, but only for the purpose of criminal investigation or in the interests of the security of the State”.

A 3.26 Further to section 2(3) of the 1993 Act, the Minister shall not give an authorisation unless he considers that the conditions specified in section 4 or 5 of the Act, as may be appropriate, stand fulfilled, and that there has not been a contravention of section 6 of the Act, in relation to the proposed interception.

Power relating to unsolicited communications

A 3.27 Further to Regulation 13 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011), a person shall not use or cause to be used any publicly available electronic communications service to send to a subscriber or user who is a natural person an unsolicited communication for the purpose of direct marketing by means of- (a) an automated calling machine, (b) a facsimile machine, or (c) electronic mail, unless the person has been notified by that subscriber or user that he or she consents to the receipt of such a communication.

A 3.28 Further to Regulation 13(15), a person who commits an offence under Regulation 13 is liable- (a) on summary conviction, to a class A fine, or (b) on conviction on indictment- (i) in the case of a body corporate, to a fine not exceeding €250,000, or

A 3.29 (ii) in the case of a natural person, to a fine not exceeding €50,000.

A 3.30 Regulation 30(1) which is entitled “Enforcement of Regulations by the Regulator” provides that subject to the performance by the Data Protection Commissioner of the functions under Regulation 17, it shall be a function of the Regulator (i.e. ComReg) to monitor compliance with Regulation 7, 8, 9, 10, 11, 12, 13, 14 or 15 and to issue such directions as may be necessary, from time to time, for their effective implementation. The Regulator, in consultation with the Commissioner, may also specify the form and any other requirements regarding the obtaining, recording and rescinding of consent of subscribers for the purpose of these Regulations.

A 3.31 Pursuant to Regulation 30(3), the Regulator may give directions to an undertaking to which Regulation 7, 8, 9, 10, 11, 12, 13, 14 or 15 applies requiring the undertaking to take specified measures or to refrain from taking specified measures for the purpose of complying with the provision.

A 3.32

Annex: 4 Glossary of terms

Acronym	Full title
2002 Act	Communications Regulation Act 2002, as amended
2FA	Two-factor authentication
2023 Act	Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023
AI	Artificial Intelligence
All-In	An implementation process for a service where consumers and included by default.
B2C	Business to consumer
CLI	Calling Line Identification
ComReg	Commission for Communications Regulation
Decision Instruments	Decision Instruments contained in this document
Draft Decision Instruments	The Draft Decision Instruments contained in Consultation 23/52
DECC	Department of the Environment, Climate and Communications
DNO	Do Not Originate
Dynamic Intervention	Interventions which can adapt over time to counter new and emerging scams.
ePrivacy Directive	ePrivacy Directive
GDPR	General Data Protection Regulation
GN	Geographic Numbers
IGO	International Gateway Operators
IISG	Intervention Implementation steering-group
INA	Individual Number Assignment
The Interventions	The network-based interventions which ComReg has determined that telecommunications operators must take to combat scam calls and texts, in the RIAs.
IRG	Independent Regulators Group
KYC	Know Your Customer
M2M	Machine to Machine
MBB	Mobile Broadband
Mobile Numbers	Numbers assigned to the use of Mobile telephony services
MSP	Mobile Service Providers
MSRN	Mobile Station Roaming Number
NCIT	Nuisance Communications Industry Taskforce
NCIT Version	A version of this document that includes the information on the submissions on the Technical Specifications, which NCIT members will receive upon request.
NGNs	A Non-Geographic Numbers is a type of telephone number that is not linked to a particular geographic location identifiable from the number i.e., a NGN does not

	identify the call termination point.
NIICS	Number Independent Interpersonal Communications Services
NRA	National Telecommunications Regulatory Authorities
Number Holder	The operator to whom the number was assigned, referred to as the assignee in the Numbering Conditions
Opt-In	Opting in means that a user will be only be enrolled in a service after confirming their wish to be included.
Opt-out	Opting out means that a user will be enrolled in a service unless they elect not to be included.
Originating PA	The PA(s) used by the SIDO would validate at the point of ingress that the SIDO
OTT	An over-the-top media service is a media service offered directly to viewers via the Internet.
P2P	Communications between one person and another.
PA	Participating Aggregators
PN	Protected Numbers
Proposed Package	The interventions ComReg to mandate in Consultation 23/52 – DNO, PN, Fixed and Mobile CLI Call Blocking, Voice Firewall, SMS Sender ID Registry, the SMS Scam Filter.
RFI	Request for Information
RIA	Regulatory Impact Assessment
Robocall	calls generated automatically, where you hear a recorded message that often sounds as if it was a robot listing options that, if selected, would connect you to the fraudster
RoU	Rights of Use
Sender ID	Similarly, for SMS a sender may supplant the mobile number with alphanumeric text
Sender ID Spoofing	occurs when the number or name as displayed on a recipient device's screen has been faked by a fraudster and appears to be a SMS from a genuine business or organisation. In effect, it appears that an incoming SMS is coming from a local business or organisation that is already known and trusted.
Smishing	a SMS message designed to gain your trust and encourage you to share information) and is where text messages are sent to trick you into clicking on a malicious attachment or link.
SMS	Short Messaging Service
Static Interventions	Interventions which cannot adapt over time to counter new and emerging scams.
Tech Support Scam Calls	calls where a fraudster claims to offer a technical support service. The fraudster typically attempts to get consumers to allow remote access to their computer. After remote access is gained, the fraudster attempts to gain your trust to pay for supposed "support" services, steal your credit card account information or to persuade you to log in to your online banking account.
Technical Specification Documents	Technical and Functional requirements
Vishing	a phone call designed to get you to share personal information and financial details, such as account numbers and passwords. A seemingly genuine number is displayed to gain your trust and encourage you to share information.
VNO	Virtual Network Operators
Voice Call	A Voice Call is a connection over a telephone network between the called party and the calling party that enables people to hold conversations and communicate

	information in real time.
Wangiri	short calls or faked missed calls prompt you to call back an international number. The call-back provides financial benefit for the fraudster often at the expense of the caller.