An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Combatting Scam SMS

Preliminary Consultation on potential network-based interventions

Preliminary Consultation

Reference: ComReg 26/24

Date: 31/03/2026

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Content

Section **Page**

Contents

1 Introduction

Background

1.1 Voice calls and SMS messages are among the most direct and immediate means of connecting with people. These platforms are unique among calling and messaging applications as they are available on every mobile phone right out of the box. It is this ubiquity that makes these platforms popular for business, consumers and government agencies alike. Around 40 million voice calls are made, and 6.5 million SMS messages are sent every single day in Ireland. People need to trust that those contacting them are genuine; otherwise, avoidance will result in legitimate and important calls going unanswered and SMS messages going unread.

1.2 Scammers exploit this convenience and ubiquity, to defraud Irish citizens by impersonating friends, family, businesses and state bodies. Not so long ago, these platforms were universally trusted, and scam calls and SMS were a sporadic and occasional annoyance rather than an almost everyday occurrence. Moreover, scams were usually recognisable because they tended to be unsophisticated, poorly phrased, use far-fetched premises (e.g., the Nigerian prince or long lost relative), and originate from foreign caller IDs.

1.3 This changed following the COVID-19 pandemic, which forced more daily activities online, with consumers increasingly purchasing products and registering for services by online channels. Scammers capitalised on this change in consumer behaviour, and the volume of scam calls and scam SMS messages increased markedly in 2020 and 2021.

1.4 Today, scam calls and SMS messages have become a constant irritation and an unavoidable negative consequence of simply using a phone. ComReg's research tells us that over 90 per cent of adults in Ireland have received a scam call to their mobile phone, while 84 per cent have received some form of scam text[1]. These scams have become more sophisticated due to scammers spoofing local and national numbers, deploying better technology, using more convincing scripts and premises, and combining these with AI generated voices and deep-fake videos. With scams becoming ever more convincing, consumers now need to be more vigilant than ever before.

1.5 ComReg previously established that the **total quantifiable harm to Ireland's economy and society arising from scam calls and texts was conservatively estimated at over €300 million per annum** with around 1,000 people defrauded of money every single day. It is therefore a serious concern that the financial loss from

[1] Document 24/24 *"Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications"* Link

scams appears to be growing; in fact the Central Bank of Ireland finds that the total value of fraudulent payments is growing each year.[2]

1.6 Much of this fraud originates from or uses SMS, **over 2 billion of which are sent annually in Ireland**. Recent research by AIB found that SMS channel accounted for **nearly 60% of reported frauds**[3] in the first ten months of 2025. This should come as no surprise and ComReg had forewarned that the SMS gap and the lack of a SMS Scam Filter (with content scanning) would lead scammers to specifically target Ireland[4]. Trust in telephone numbers and the ubiquitous messaging services that rely upon them is now being lost to the detriment of consumers, businesses, important public sector services such as health and taxation, as well as telecommunications service providers themselves.

ComReg's work to combat scam calls and texts

1.7 In response to this scam plague, ComReg established a Nuisance Communications Industry Taskforce ("NCIT") in early 2022 – comprising of fixed and mobile network operators, whose networks collectively carry more than 90% of fixed voice traffic and 100% of mobile voice traffic in Ireland. The purpose of the NCIT was to identify and develop interventions that the telecommunications industry could then implement across their networks and services to mitigate this problem. Under the auspices of the NCIT[5], some operators implemented certain static measures – such as Fixed CLI blocking, to tackle nuisance communications. While this went some way to address scam calls, ComReg was of the view that a more complete package of interventions was necessary (including dynamic interventions that could adapt to scams in real time), to reduce the risk of fraudsters pivoting across different technologies and services in response to one or more interventions.

1.8 In June 2023, ComReg published a consultation (ComReg 23/52) on potential interventions informed by, among other things, a report by Europe Economics[6] (the "Europe Economics Report" or ComReg 23/52a)[7] and surveys of Irish businesses and consumers conducted by Behaviour & Attitudes[8] ("B&A") (the "2023 Consumer survey" [9] and the "Business Survey")[10]. ComReg received 31 submissions from stakeholders in telecommunications and financial services. In April 2024, ComReg mandated the following six interventions in its Response to Consultation and

[2] See Payment Fraud Statistics | Central Bank of Ireland
[3] AIB press release "*Scam humbug*" 18 December 2025 Link
[4] See paragraph 1.42 of Document 24/24 and Section 5.6 of Document 23/52
[5] In the intervening period, ComReg convened a new industry forum, the Nuisance Communications Industry Forum ("NCIF"), which succeeds the former NCIT and which will oversee the implementation of each of these interventions.
[6] Europe Economics is a leading economics consultancy providing trusted economic analysis and advice to some of the most well-known and respected national and international firms and organisations.
[7] Document 23/52a, Europe Economics "*Scam calls and texts in Ireland – costs and benefits of interventions*", 16 June 2023 Link
[8] B&A Ipsos, formerly Behaviour & Attitudes, is a leading Irish market research company, offering a comprehensive suite of tailor made quantitative and qualitative methodologies and advice on all aspects of consumer behaviour and its implications.
[9] Document 23/52b, Ipsos B&A "*Research on Nuisance Communications - Consumer*", 16 June 2023 Link
[10] Document 23/52c ComReg 23/52c, Behaviour & Attitudes "*Research on Nuisance Communications - Business*", 16 June 2023 Link

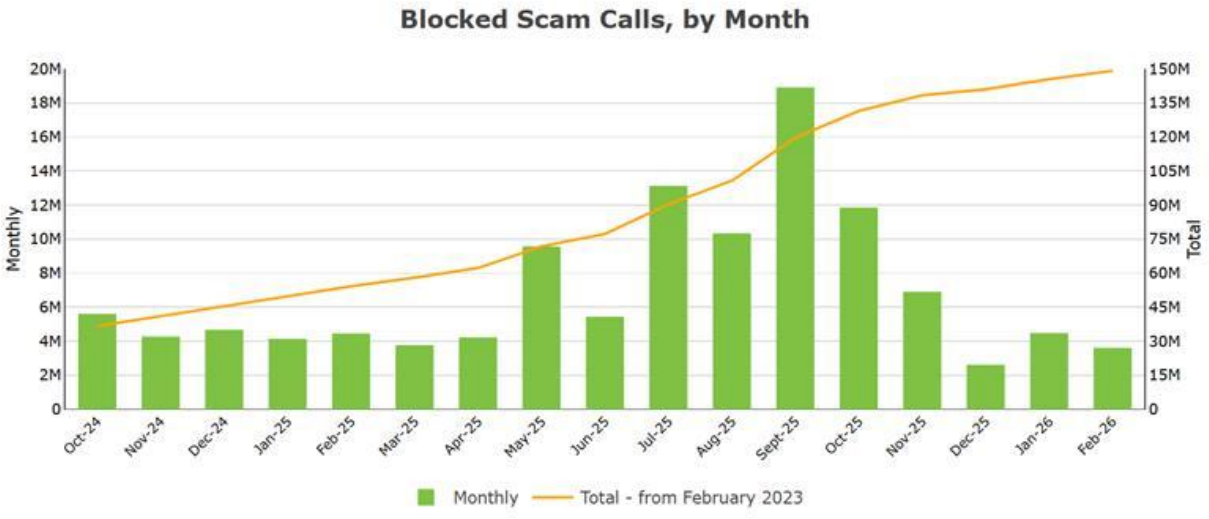
Decision (ComReg 24/24)[11]:

1. **Do-Not-Originate list:** To allow businesses/organisations to secure their numbers by blocking those numbers not used to contact consumers.
2. **Protected Numbers list:** To stop fraudsters using numbers that are not in service.
3. **Fixed CLI Blocking:** To stop fraudsters abroad spoofing Irish geographic numbers (e.g., 01-) to make scam voice calls.
4. **Mobile CLI Blocking:** To stop fraudsters abroad spoofing Irish mobile numbers (e.g., 087-) to make scam voice calls.
5. **Voice-firewall**: To block spam calls wherever they arise (i.e., Ireland or abroad) and protect against future more sophisticated scams.
6. **SMS Sender ID Registry:** To allow businesses/organisations to register an SMS Sender ID while blocking those that are not on the Register.

Scam calls

1.9 The **first four interventions which target scam calls** have now been implemented by industry. Together, these interventions **have blocked approximately 150 million scam calls**. This is a significant, as these are all scam calls that would have otherwise been received by consumers, wasting their time, and, in the worst case, leading to people being scammed out of their hard-earned money if the industry had not acted.

Figure 1: Scam calls blocked, October 2024 - February 2025



1.10 However, there is more to be done, as scam calls are still being received by consumers. Scammers switch away from the original avenues as they are closed off,

[11] Document 24/24 *"Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications"* Link

using more sophisticated methods in order to sidestep the static interventions. In that regard, the Voice Firewall, the fifth voice intervention, is being put in place by the Mobile Network Operators ("MNOs") at present and should provide an even more robust defence against scam calls. A Voice Firewall is designed with advanced real-time call data analytics, capable of using machine learning and AI techniques to detect and block scam calls. As such, a Voice Firewall is a dynamic intervention and can be updated in real time to account for fraudsters' ever-adapting strategies to reach consumers.

Scam SMS

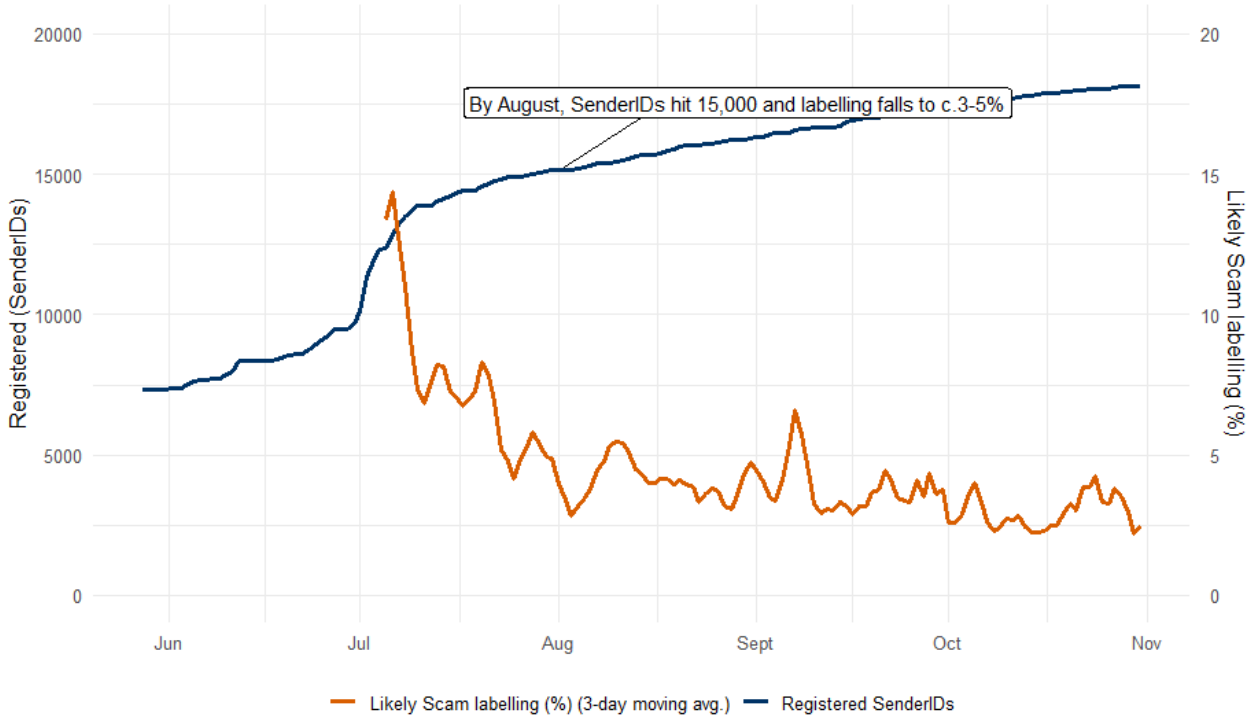
1.11 In July 2025, ComReg launched a SMS Sender ID Registry ('Registry') to help prevent scam SMS which used spoofed SMS Sender ID's, and to restore trust in SMS as a reliable and trustworthy one-way communications channel for businesses and organisations[12]. From 3 July 2025, SMS from unregistered Sender IDs were modified to "Likely Scam" to alert the recipient that the SMS may not be genuine. To date, over 14,000 organisations have registered over 20,000 Sender IDs, illustrating the appeal of A2P SMS channel for business and organisations. The intervention is now performing reliably and providing meaningful safeguards for consumers and businesses, promoting vigilance, restoring trust, and protecting from harm.

1.12 Labelling an SMS with the Sender ID "Likely Scam" also engages and reminds consumers to be extra vigilant about the SMS that they receive. This is important because the experience of those scam victims shows that fraud typically occurred when a victim was not paying full attention, being distracted by the interruptions of everyday life (getting children ready, making dinner, rushing to work, texting and talking, etc.), or tiredness at the end of a long day. Labelling concentrates minds and allows consumers to properly engage with the message to determine whether the message is a scam or not. In a world full of constant interruptions, that reminder can be the difference between staying safe rather than becoming a victim of fraud.

1.13 In the first few weeks of July 2025, the number of registered organisations and Sender IDs increased dramatically. Consequently, the number of SMS being labelled fell, as labelling became more accurate with far fewer 'false positives'. By August 2025, the labelling rate had already stabilised at approximately 3% - 4% of SMS with Sender IDs.

[12] In Q4 2024 and Q1 2025, ComReg engaged closely with MSPs and PAs through ComReg's NCIF to pre-register as many legitimate Sender IDs as possible in advance of Registry launch to help ensure a smooth transition to the new regulatory regime for A2P SMS. The objective of this approach was to minimise any negative impact on legitimate A2P SMS traffic in advance of the Modification and Blocking Phases. Data submissions from the Bulk Upload Phase were validated, authenticated and deemed to be "registered" in advance of registry launch. Over 7000 Sender IDs from over 5000 Sender ID Organisations were registered during the Bulk Upload Phase. On 28 May 2025, the Sender ID Registry was officially launched and SIDOs, or PAs acting on their behalf, were able to register Sender IDs on a "first come, first served" basis at https://comreg.ie/senderid .

Figure 2: Registration and labelling of SMS with Sender ID's



Source: ComReg's analysis of data reported by MNOs.

1.14 Since August 2025, millions of SMS have been labelled "Likely Scam", alerting consumers of potential scam SMS. The Sender ID Registry has likely deterred or prevented millions of scam SMS spoofing/falsely using a Sender ID to impersonate Irish businesses or State agencies in order to defraud Irish consumers. Indeed, one large Irish retail bank has informed ComReg that since the introduction of the Sender ID registry last summer it has not had a single reported spoofed SMS scam, or imitation of its Sender ID's. Given the success of SMS labelling to date in warning consumers of likely scam SMS, ComReg will maintain the labelling intervention for now. However, ComReg may revisit blocking non-compliant SMS with Sender IDs in the future.[13]

[13] ComReg is engaging with SMS aggregators and will continue to monitor the performance of PAs and MSPs in complying with the relevant Decision Instrument. ComReg may revisit this position in the future.

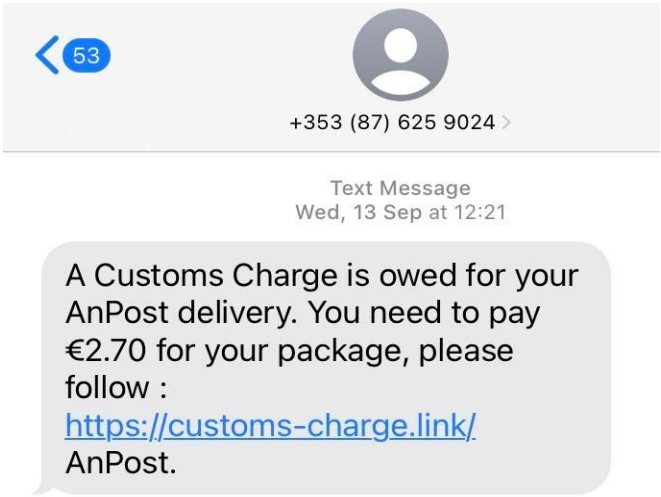
2 The gap in Ireland's anti-scam defences

2.1 The 'SMS Gap'

2.1 Notwithstanding the value of the SMS Sender ID Registry, it focuses on a specific use case where a Sender ID is used in so called Application-to-Person ("A2P") messages.[14] In its Consultation 23/52, ComReg observed that there are two main areas that cannot, by definition, be addressed by the SMS Sender ID Registry[15].

2.2 **First**, fraudsters are resourceful and so do not always use Sender ID spoofing. Instead, scammers may impersonate a business within the body of a message or impersonate an ordinary person. By design, the Sender ID Registry only combats scam messages mimicking Sender ID. Fraudsters can continue to send scam messages without a Sender ID (e.g. instead of displaying "An Post" as the Sender ID a telephone number is shown – see Figure 1).

Figure 3: Impersonating An Post without a Sender ID



2.3 Many common types of scam SMS do not use a Sender ID, including those that rely on users clicking on URLs (e.g., An Post scam, eFlow scam, and those impersonating government departments[16]) or impersonating individuals (e.g., the "Hi Mam" scam). ComReg flagged that this gap in Ireland's SMS scam defences could be exacerbated by a number of "*waterbed effects*", including that in response to the Sender ID Registry, scammers may increasingly use SMS without a Sender ID to target consumers. Such scams continue to degrade trust in government services and

[14] A2P (Application-to-Person) messages are automated SMS or text messages sent from a software application to a user, rather than from another person. These messages are generally used by businesses for one-way, high-volume communication like 2FA codes, appointment reminders, marketing alerts, and notifications.
[15] In addition to these factors, there have been recent reports of state actors attempting to exploit similar gaps in telecommunication defences to engage in cyber-attacks. For example, see this press release from the United States Secret Service, "*U.S. Secret Service dismantles imminent telecommunications threat in New York tristate area*" 23 September 2023 Link
[16] DECC pinned tweet on scam texts in relation to energy credit. Posted 24 November 2024. Link

communications. In recent weeks, there were reports of new scam text waves impersonating the HSE in relation to medical cards[17], the Department of Social Protection and gov.ie in relation to energy bills[18] and the Housing Agency in relation to offers of accommodation[19].

2.4 **Second**, future scams seem likely to become more sophisticated as fraudsters use advanced artificial intelligence (AI) based software to create more realistic and believable text while instantly messaging people. There are clear signs that a number of the risks identified by ComReg are beginning to materialise. In Document 23/52, ComReg identified that AI had the potential to supercharge scams acting as an accelerant, by enabling scammers to create compelling real time conversations at scale, or by personalising scams with voice cloning or deepfakes, and that scams could fuel domestic organised crime. Since then, there have been numerous reports of fraudsters incorporating AI into their scams to dupe consumers[20] and these scams are fuelling the growth of criminal gangs[21].

Figure 4: How AI can power scams

2.2 SMS Scam Filter

2.5 In order to address this gap, ComReg also consulted on the need for a SMS Scam Filter (with content scanning)[22]. Such an intervention would target all SMS messages regardless of the format (i.e., whether an SMS has a Sender ID or otherwise) and would complement ComReg's SMS Sender ID Registry by providing protection to the majority of SMS that do not have a Sender ID. Under this approach, anti-scam software scans the content of an SMS for potentially suspicious or malicious content

[17] HSE "*Fraudulent texts in circulation - HSE does not seek payments by SMS*" 27 March 2026 Link
[18] RTE "Warning of scam text messages for reduced electricity bill" 30 January 2026 Link
[19] Dept. Housing, Local Government and Heritage "*Statement from Department of Housing, Local Government and Heritage regarding online scams*" 12 March 2026 Live
[20] Euronews "*Scammers clone Italian defence minister's voice with AI in ransom scheme*" 10 February 2025 Link
[21] The Irish Times "*Black Axe gang behind bank account takeover fraud swells to network of 1,600 people in Ireland*" 13 May 2025 Link
[22] Content scanning is critical to the effectiveness of a SMS Scam Filter, not least as key elements of the scam (e.g., the premise, request for money, payment details, instructions) are transmitted within the content of the message.

(e.g., fraudulent URLs).[23]

2.6 ComReg is unable to mandate a SMS Scam Filter with content scanning as it requires a legislative basis. In April 2025, Minister Darragh O' Brien noted in response to a parliamentary question, that legislation to support this intervention by default for all consumers would not be forthcoming. Instead, other approaches, including those that would seek consumer consent in advance of the introduction of a SMS filter, are being explored.[24]

2.7 The government position was subsequently confirmed to ComReg, along with the possibility of legislation to underpin a consumer 'Opt-in' measure. It will be appreciated that such considerations if it brings forward legislation, is unlikely to deliver consumer protection in the short or medium term.

2.8 Therefore, ComReg in this preliminary consultation is seeking to protect Irish consumers by proposing other possible interventions that may mitigate the harm to consumers, that do not rely on SMS content scanning. Given the harm already caused by SMS scams, despite the Sender ID Registry (which covers only A2P SMS), ComReg simply cannot countenance a situation where telephone numbers continue to be misused and, as a consequence, consumers are so egregiously harmed.

2.9 There is of course no impediment to any mobile operator voluntarily implementing interventions to combat SMS scams. Such actions would demonstrate a strong commitment to protecting customers and signal to scammers that operators are and will be proactive in response to scams on their networks and services wherever they arise.

2.3 Fraudsters' incentives

2.10 ComReg's approach in this preliminary consultation is similar to that first set out in Consultation 23/52, where interventions are aimed at targeting fraudsters' *financial incentives* to engage in scams. Fraudsters are entrepreneurial and thus have an inducement to perpetuate scams wherever the revenues generated by a scamming operation exceed costs. The profitability of scam calls and texts is determined by several 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.

[23] Document 23/52 page 15.

[24] Minister O'Brien stated that "*Some EU Member States have introduced legislation to enable blanket SMS filtering on all network contracts, without seeking consumer consent. My Department carried out an extensive evaluation of this approach and has concluded that legislation to allow this application of the SMS filter would not meet the bar of proportionality necessary to dampen privacy protections provided for in other areas of Irish law. This conclusion was reached after weighing the proportionality of such a response, and the impact on consumer's privacy rights, against the scale of the problem and the potential positive benefits of this course of action*" See Telecommunications Services: 29 Apr 2025: Written answers (KildareStreet.com)

2.11 The success rate is highly critical to the profitability of a scam and most scams require only a small percentage of the recipients to fall victim to a scam to achieve profitability.[25] While a certain level of scam SMS is always likely to endure, the aim of the interventions proposed in this consultation is to introduce friction which will have the effect of reducing their effectiveness and the profitability of Irish targeted scam SMS campaigns. If previously a scam campaign only required a success rate of 1/10,000 to be profitable, then reducing the hit rate to 1/100,000 may make a scam unprofitable and be sufficient to deter the fraudster. In this regard, even where the impact of an individual intervention is small, the cumulative impact of this combination of interventions, along with those previously implemented in 2024 may be enough to deter scammers from launching at least some scam campaigns in Ireland.

2.12 Moreover, any package of interventions must be cognisant of the ability of fraudsters to readily switch across scams, technologies, and territories. 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. Indeed, Ireland is the only Anglosphere country without an SMS Scam Filter (the UK, the USA, Canada, Australia, New Zealand, South Africa, Hong Kong and Singapore have SMS Scam Filter), leaving Ireland more exposed to English language scam texts, on top of being one of the shrinking number of countries in the EU/EEA not to have an SMS Scam Filter (See Annex 1).

[25] 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.

2.4 The preliminary consultation

2.13 In this preliminary consultation, ComReg is seeking to protect Irish consumers by proposing a number of specific interventions that may mitigate the harm from scam SMS to consumers. These interventions build upon the beneficial impact of ComReg's existing SMS scam intervention, the SMS Sender ID Registry. However, there are known gaps in our SMS defences which must be addressed, as ably highlighted by the recent AIB Report[1]

2.14 ComReg is proposing a number of interventions to reduce harm caused by scam SMS which are summarised below:

1. **A SMS Base Filter:** The SMS Base Filter would use the metadata associated with a message (e.g., phone number, country code, source network node or route, time stamp and frequency) to determine whether a message is from a scammer – it would not use any of the SMS message content. The SMS Base Filter would apply predictive modelling to this metadata to estimate the probability of a SMS being a scam. It could be upgraded to an SMS content filter at a later date, if legislation was forthcoming.

2. **A SMS Cap**: A SMS cap would limit the number of SMS that could be sent over a defined period of time (e.g., number of SMS per hour/minute). The cap would need to be set at a level that would not restrict genuine users in their use of SMS, but frustrate and/or introduce friction to scammers who tend to send high volumes of scam SMS over a short period (e.g. every minute)This would limit the extent to which a scammer could send potentially thousands of SMS with an individual SIMs. This could be implemented on a fixed or dynamic basis (where the cap would be adjusted based on consumer behaviour). ComReg is also considering the introduction of rules regarding the activation of SIMs and eSIMs, to combat their use by scammers abroad.

3. **Automated SIM Blocking**: With a SMS Base Filter, MNOs could automate the blocking of SIMs that send scam SMS, where such SIM blocking could happen in minutes (or less), instead of the current manual process. ComReg is also considering the blocking of devices used by scammers, to combat domestic scam operations.

4. **DNS Scam Filter**: A DNS (Domain Name System) filter would block or restrict access to specific websites by preventing their domain names from being resolved to the correct IP addresses, instead redirecting to a website warning consumers that they have clicked on a URL used by scammers.

2.15 Succeeding in the fight against scams demands a united effort from all of society, including government, media, businesses and consumers but particularly the

telecommunications industry – which has been instrumental in the success of the interventions implemented to date.

2.16 ComReg would therefore encourage network operators (including relevant virtual operators) to build on their collective and essential efforts in the voice space to date and respond to this preliminary consultation with consumer protection as their foremost priority. Indeed, operators are also encouraged to consider implementing these and similar interventions voluntarily, as many ISPs already do so across the western world – including the United Kingdom, Australia and Canada, all with the goal of helping to speedily safeguard consumers.

2.17 This preliminary consultation provides interested parties with an opportunity to provide comment on any aspect of the proposed interventions or to propose other interventions that could reduce the harm caused by scam SMS. **All input, including proposals for other network interventions are welcome.** Please set out your reasoning and all supporting information for any views expressed. It would make the task of analysing responses easier if comments were referenced to the relevant section/paragraph number in each chapter and annex in this document.

3 Potential interventions

3.1 Background information

3.1 This section identifies and describes the potential interventions that ComReg has identified as being available to combat scam SMS.

3.2 ComReg also welcomes the views of industry on each of these proposed interventions, including potential cost of implementation and timelines for implementation. ComReg would also welcome views on other potential interventions that would mitigate the harm currently caused the SMS Gap.

3.2 Identifying the regulatory options

3.3 In identifying regulatory options, ComReg uses the same approach as used and consulted upon in Documents 23/52 and 24/24 to assess the list of interventions and their intended impact. It should be noted that these proposals are complementary interventions and so, some or all, could be implemented.

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 to its intended purpose ("Technical feasibility and effectiveness"); and

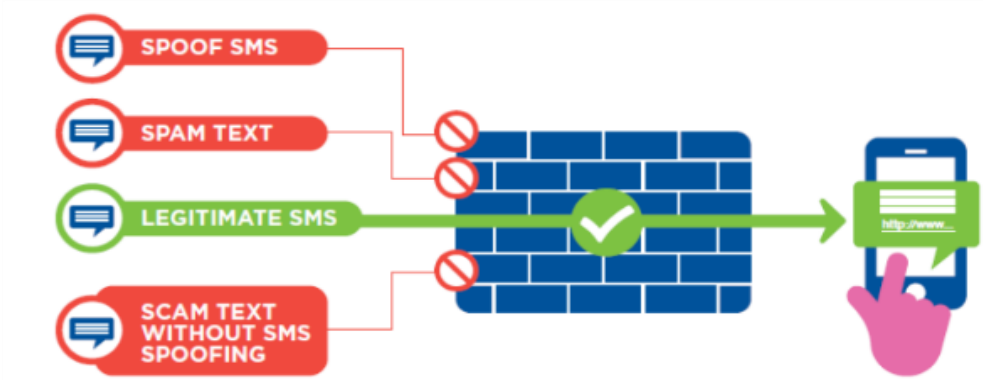
III. Third, ComReg assesses whether the intervention is implementable over a reasonable period ("Timelines")

1. SMS Base Filter

Overview

3.4 A SMS Base Filter typically refers to the initial, network-level, or system-level defence mechanism designed to stop fraudulent text messages before they leave/reach the consumer's phone. This layer operates independently of the consumer, filtering out known malicious content at the carrier level.

Figure 5: SMS Base Filter



3.5 SMS Metadata consists of a variety of information that accompanies a SMS (i.e., not the message content), such as details contained within network signalling, timing, and sender characteristics. This data may be of use in determining the likelihood of a scam, including volumetric analysis of the originating number or route. Operators can also use SMS Metadata to block scammers from sending SMS to their users where any suspicious patterns are detected.

3.6 The SMS Base Filter applies predictive modelling to this Metadata to estimate the probability of a SMS being a scam. Network based interventions that utilise probabilistic assessment are inherently dynamic, adapting to scammers evolving tactics by identifying new emerging patterns in traffic. Leading vendors have begun to deploy AI as part of such interventions to improve the effectiveness of such probabilistic assessment[26].

3.7 A SMS Base Filter would be applied to originating and terminating traffic in order to combat scam SMSs effectively by utilising all available information on the volume of SMS sent by individual SIM cards (e.g., no knowledge of sender, SIM, location or other patterns in these variables). It is important to apply the scanning to both types of traffic as:

- Originating traffic can be particularly useful as it can prevent scam generation by using indicators of scams unique to origination as well preventing malware related SMS (e.g. 'flubot')[27]
- Terminating traffic can provide a last line of defence to all end-users, and combat international scam SMS, but does not stop the origination of large numbers of scam SMS.

Technical Feasibility

[26] Mavenir press release "*Mavenir's AI-Driven Fraud Defense Solutions Win FutureNet Asia Award for Customer Experience Innovation*" Link
[27] Proximus (2022) "*Dealing with Flubot, an operators experience*" Link

3.8 ComReg understands from discussions with vendors that a SMS Base Filter whereby the Content Filtering functionality is not enabled is technically feasible. The assessment of SMS metadata is a key component of SMS Scam Filters, which are widely used internationally.

Effectiveness

3.9 A SMS Base Filter is effective at blocking scam SMS where there are indications of the scam contained within the metadata (e.g. signalling, timing, volumetric trends, source network node or route and sender information). This can reduce the volume of scam SMS received by consumers, thereby reducing the harm to consumers. Therefore, to the extent that scam SMS are determined based on their metadata alone, the SMS Base Filter would be effective at reducing scam SMS.

3.10 Importantly, once a SMS Base Filter is installed, the "content scanning" functionality could be activated if legislated for at a future date. The introduction of a SMS Base Filter would allow some consumer harm to be mitigated in the period while the Department of Culture, Communications and Sport ("DCCS") considers any potential legislation for a SMS Scam Filter with content scanning. However, regardless of the approach used by DCCS, the metadata would continue to contain some valuable information that could assist in determining the probability of a SMS being a scam.

Timelines

3.11 ComReg is of the preliminary view that the SMS Base Filter could be implemented by operators within 6 months of a Decision, because it is clearly defined and relatively straightforward to apply from a technical perspective.

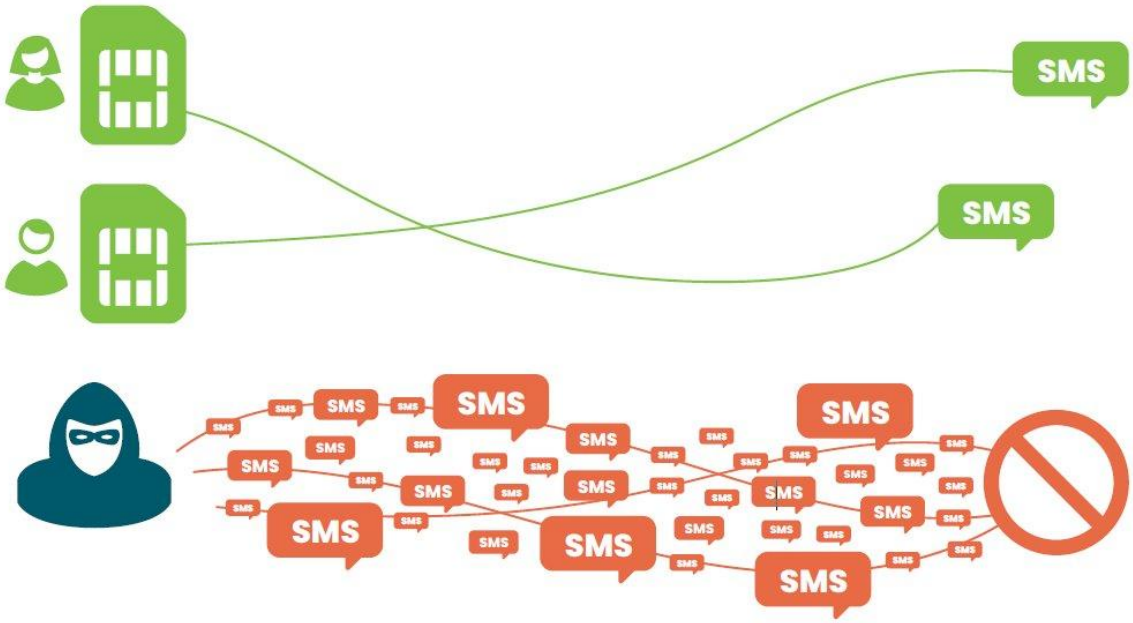
2. Limiting SMS Origination (Volume Cap)

Overview

3.12 The SMS Cap involves limiting the number of SMS a subscriber[28] can send from their subscription over a specific period. It should be noted that this cap would not apply to A2P subscriptions such as those that are registered on the SMS Sender ID Registry. At present, mobile operators initiate a fraud-check on a subscriber once the SIM has reached a threshold, however, and understandably, a check can take time to complete.

[28] This intervention applies at subscriber level to prevent easy circumventions by swapping SIMs across devices.

Figure 4: SMS Cap



3.13 This proposed intervention could be implemented in one of two main forms. Either a cap could apply either to all subscriptions, or to only those considered to be most at risk (e.g., pre-pay SIMs[29] or newly activated SIMs). ComReg seeks views from interested parties on which subscriptions this potential intervention should be targeted towards.

I. A static cap

3.14 A static cap means that the number of SMS that a subscriber may send over a certain period (e.g., every day/minute) is capped at a certain number of SMS (e.g., 200 SMS per day). In order to be effective, the cap would need to be set at a level that would not restrict genuine users in their use of SMS, but frustrate and/or introduce friction to scammers abilities because the volume of scam SMS that could be sent would be capped, reducing the hit rate of each batch of SMS sent within a period.

II. A smart cap

3.15 A smart cap is a volume cap which would adjust depending on the behaviour of each individual subscription. It could start with a baseline limit on the number of outgoing SMS per subscription (e.g., per phone number) and then adaptively changes that limit over time based on observed behaviour. This means that a given pattern of subscriber behaviour might trigger the cap on operator X but not on operator Y. In summary, it could work as follows:

[29] A Bill pay subscriptions requires the use of a payment service, which entails KYC (e.g., banks may perform a fraud check on the transaction, banks have KYC on the payment account).

- A cap could be based on a large number of SMS issued over a short period (e.g., 50 per minute) [30] but this could also be combined with an overall daily limit (e.g., 100 per day, or a limit set according to that subscriber's historical usage).
- The level of the initial cap would be based on evidence from operators of actual usage, experience of vendors in fighting scams and/or market research.
- The cap would then be adjusted periodically[31] for each subscription based on a probabilistic assessment (e.g. using the base filter) on the likelihood of a scam arising from that subscription.
- Over time, this would result in an increase or decreases in the SMS cap for a particular subscription(s)[32].
- Operators would be required to report to ComReg on a periodic basis across a number of metrics, including, the number of subscriptions whose cap was increased or decreased.

3.16 Separately, ComReg is considering requiring that pre-pay SIMs can only receive SMS and calls once they have topped-up with credit. In the UK, Stop Scam UK[33] has implemented this activation policy in order to combat the use of UK SIMs by international fraudsters to conduct romance and investment scams. These SIM cards are used to receive the one-time-passwords required to set up the fake digital identities which fraudsters use. This appears effective as noted by Stop Scam UK: *"BT's evidence has shown a dramatic, almost complete eradication of reported Romance fraud via the PAYG SIM route*". [34]

Technical feasibility

3.17 ComReg understands from discussions with vendors that each version of this intervention is technically feasible. Further, MNOs have long monitored and counted the number of SMS sent by each user for billing purposes and "*fair use*" and prevented users sending SMS above a certain level. Further, the Smart Cap is technically feasible once the SMS Base Filter (as described above) has been installed, although there may be other means and ComReg is open to proposals from interested parties.

3.18 MNO can implement a 'Smart' Cap virtually, via their SMS Base Filter which typically assess originating numbers and can limit SMS sent by individual users (also known

[30] Scammers use "SMS blasting" services or bots to send hundreds or thousands of messages in seconds to minutes, creating a "burst" of activity, making them hard to trace and stop.
[31] ComReg suggests that this period should be short in order to avoid scams being sent when they could have been identified as scam if the period of review was shorter.
[32] Operators could implement a "white-list" of end-users that contact their operators in relation to the SMS Cap, permitting their higher SMS use.
[33] Stop Scams UK describes itself as "*a membership organisation of responsible businesses from across banking, technology and telecoms*." Link
[34] Stop Scams UK "*UK Dismantles organised crime infrastructure in fight against fraud*" Link

as “Volumetric analysis”).

3.19 ComReg also notes the recent announcement of similar messaging caps by:

- WhatsApp - introduced a cap on messages to unknown senders in October 2025 - link
- Ofcom - proposed a volume limit on SMS in October 2025– link

Effectiveness

3.20 This approach would undermine the ability of scammers to send large volumes of scam SMS to Irish consumers over networks. This would also reduce the incentive for fraudsters to send scam SMS, by raising the cost of doing so (e.g., more SIMs and administrative overhead required to send the same volume).

Timelines

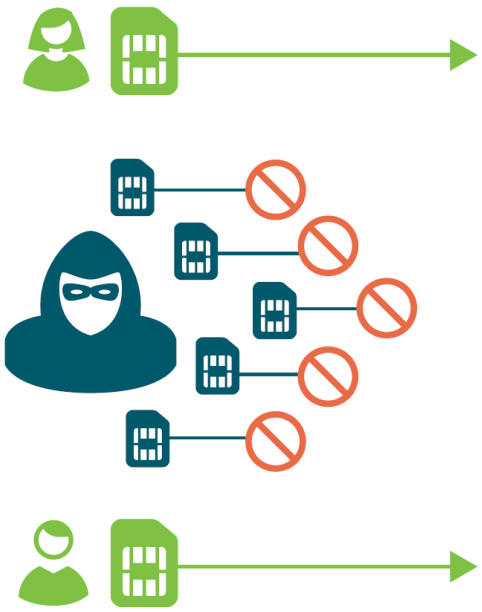
3.21 ComReg is of the preliminary view that, in combination with the implementation of a SMS Base Filter, either cap could be implemented within 6 months, because it is clearly defined and relatively straightforward to apply from a technical perspective.

3. Automated SIM and device Blocking

Overview

3.22 SIM Blocking refers to preventing the SIMs or eSIMs used by scammers from connecting to a mobile network and sending any SMS. Once a MNO deploys a SMS Base Filter, SIMs that are in use by scammers could be blocked automatically (rather than manually), based on the SIM/eSIMs’ individual traffic.

Figure 7: SIM Blocking



3.23 ComReg is also considering whether IMEI Blocking warrants consideration as an intervention. An IMEI (International Mobile Equipment Identity) is a unique 15-digit number identifying mobile devices on a network. Once blocked, the device cannot be used with any SIM card on that network and often shared with other carriers to prevent use on their networks. This may also increase the cost to scammers from perpetuating fraud. The Equipment Identification Register (EIR) enables MSPs to share blocked IMEIs.

Technical Feasibility

3.24 With a SMS Base Filter, MNOs can automate SIM blocking. A number of Irish MSPs already block SIMs on their own network using a manual process. This is a standard feature in the SMS Base Filter, which typically assess originating traffic and blocks SIMs found to send scam SMS as standard (also known as "Originating-number analysis"). A number of Irish MSPs also block IMEI's to combat scams.

Effectiveness

3.25 With a SMS Base Filter, MNOs could automate the blocking of SIMs that send scams. This would mean that scammers' SIMs are blocked in minutes (or less) after a determination that the SMS have a high probability of being scams. Automated blocking would greatly reduce the ability of scammers to send large volumes of scam SMS.[35]

3.26 Irish mobile operators existing process for blocking SIM is manual, and

[35] Primarily where a SIM has breached the cap on SMS sent.

understandably, takes time to complete. However, this means that scammers can send many scam SMS before a SIM is blocked giving them an opportunity to recoup the cost of the SIM. For example, while Irish mobile operators blocked approximately 9,500 SIMs used by scammers in the first six months of 2023, these SIMs sent between 38-46 Million scam SMS before being blocked.[36] International experience indicates that automated SIM blocking can reduce the time a SIM is active to minutes[37], greatly reducing a scammers ability to send large volumes of SMS.

Timelines

3.27 ComReg is of the preliminary view that, in combination with the implementation of a SMS Base Filter, automated SIM blocking could be implemented within 6 months, because it is clearly defined and relatively straightforward to apply from a technical perspective.

4. DNS Scam Filter

Overview

3.28 A DNS (Domain Name System) filter blocks, restrict or limit access to specific websites by preventing their domain names from being resolved to IP addresses. It acts as a safety barrier by protecting consumers from harmful or illegal content in many EU countries (e.g., illegal gambling sites, copyright content, terrorism content and child sexual abuse material).

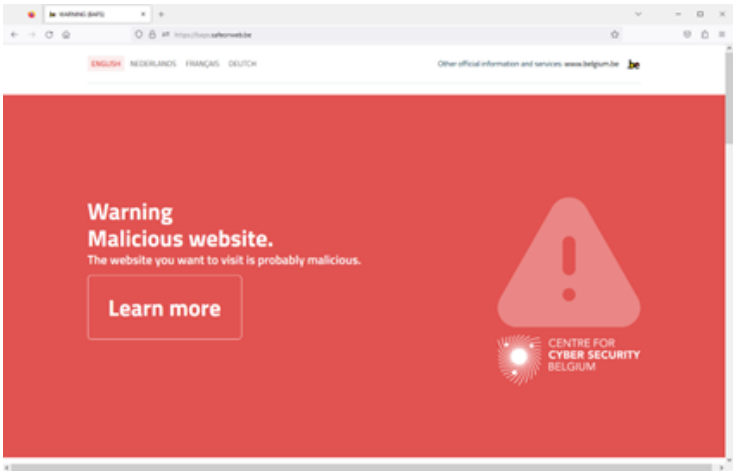
Figure 8: DNS Scam Filter

3.29 A DNS Scam Filter applies this to a list of known scam domains (websites)[38]. In practice, many DNS Scam Filters do not block the website, but present a "pop-up" webpage that warns end-users that they have clicked on a link to a URL for a

[36] This data is from a request for information issued by ComReg to MNO and MVNOs in 2024.
[37] For example, the UK Home Office "SIM farm regulation: economic note (accessible)" 18 December 2023 Link
[38] The list of websites would be updated (by the fraud team in a MNO, a vendor or a provider of DNS scam lists) to identify scam websites in (near) real time.

fraudulent/scam website (e.g., the DNS Scam Filters in Belgium and Lithuania). ComReg's preference would be for a warning page which allows the end user to accept the risk and continue to the site if desired, as opposed to blocking websites.

Figure 9: The warning page of the Belgian "Anti-phishing shield"



Source: European Cyber Security Centre – European Union

Technical Feasibility

3.30 A DNS Scam Filter requires ISPs to apply a blacklist, which can be drawn from multiple sources, which is then cross-checked once a user clicks on a URL. From the perspective of the Internet Service Provider ("ISP"), implementing a DNS Scam Filter appears straightforward[39]. Across Europe, ISPs use DNS Filters for a variety of other purposes, such as gambling, copyright content, and child sexual abuse material. Indeed, Irish ISPs already block access to certain websites.

3.31 A DNS Scam Filter would require a list of domains that host scam URLs, which requires continuous updating. Several EU/EEA countries have deployed a DNS Scam Filter (e.g., Belgium, Norway, Lithuania, Poland, UK[40]). ComReg is aware of other EU/EEA countries that are considering a DNS Scam Filter.

Effectiveness

3.32 Most DNS Scam Filters have been deployed recently, with a number of sources only recently publishing metrics for their DNS Scam Filter. Notwithstanding, the publicly available examples indicate it is a highly effective intervention:

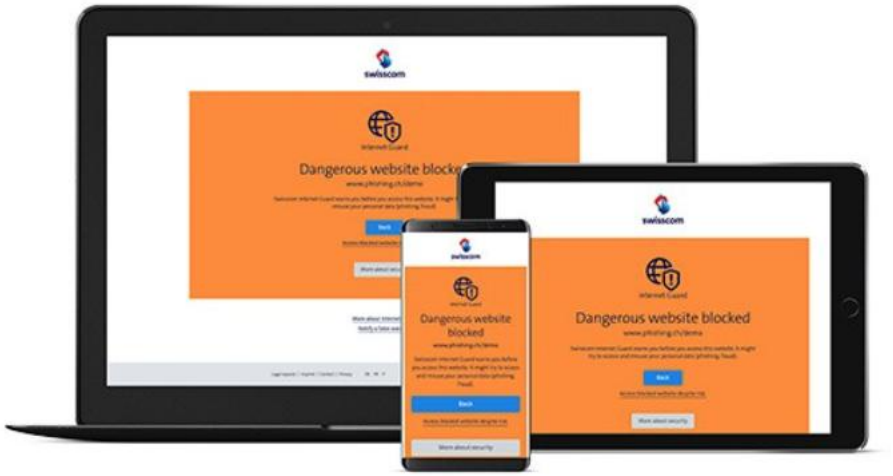
- In 2025, Telenor Norway[41] blocked over 2 billion DNS attempts in Norway alone[42].

[39] Indeed, many smaller organisations manage their own DNS Filter in the form of a company or organisations firewall.
[40] NCSC.gov.uk Press release "*Share and Defend capability"* 14 May 2024 Link
[41] Telenor Group is a major international telecommunications company primarily operating in the Nordic region (Norway, Sweden, Denmark, Finland) and Asia (Thailand, Malaysia, Bangladesh, Pakistan).
[42] Telecomaper "*Telenor Norway blocks over 2 bln online scam attempts*" Link

- In 2025, Airtel in India launched its multi-channel Fraud Detection Solution, which prevent approximately 30,47,727 fraud attempts daily[43].
- In 2024, Poland's DNS Scam Filter blocked over 72 Million visits to fraudulent websites[44].
- In 2022, Belgium's DNS Scam Filter blocked 14 Million visits to fraudulent websites[45].

3.33 The impact of a DNS Scam Filter is not surprising as it is a multi-channel solution – an Irish DNS Scam Filter would also prevent scams originating on non-SMS channels (e.g., WhatsApp, Messenger, RCS,[46] email). Consequently, a DNS Scam Filter could achieve far greater coverage than other network-based interventions. Moreover, the DNS Scam Filter is a dynamic intervention, as the blacklist can be updated as scammers create new URLs.

Figure 10: Swisscom scam warning "pop-up", across different device types



Source: Swisscom[47]

3.34 A DNS Scam Filter and SMS Base Filter are highly complementary as a DNS Scam Filter does not stop scam SMSs, or combat scam SMSs without URLs, and a SMS Base Filter does not combat scam messages over other platforms, or which contain a URL, or which evade detection. Consequently, by adding a DNS Filter to an SMS Base Filter, a country gains the ability to:

[43] GSMA "*Airtel: Fraud Detection Solution*" 24 September 2025 Link
[44] CERT Polska "*RAPORT ROCZNY 2024 z działalności CERT Polska*" [translated by Google Translate PDF] Link
[45] Safeonweb.be "*14 million clicks to suspicious websites avoided in Belgium thanks to unique Anti-Phishing Shield*" 14 July 2023 Link
[46] Rich Communication Services ("RCS") is an IP-based communication protocol that upgrades traditional SMS/MMS to a rich-media experience directly in the native messaging app.
[47] Swisscom, "*Head of Product Management for Internet Services talks about Internet Guard*" 2018 Link

- **Combat scam SMS containing a URL, that evade detection** – a DNS Scam Filter can provide protection against scams with URLs that evade detection by a SMS Scam Filter (with content scanning).
- **Block "clicks"** – blocking URLs is highly effective as users that have clicked on a link have already been misled by the scam.
- **Protect multiple text channels –** by applying to scam URLs sent via alternative messaging apps (e.g., WhatsApp and Messenger).

3.35 ComReg has met with NRAs in Belgium and Lithuania where DNS Scam Filters are in operation[48], as well as Telenor. In each case, the NRA considered the DNS Scam Filter highly effective in combatting scam communications in addition to the SMS Scam Filter, typically blocking a greater number of scam attempts[49]. Notably, in addition to the 2 Billion scam DNS attempts blocked in 2024, Telenor Norway blocked 64 Million Scam SMS and 56 Million scam calls[50] using its SMS Scam Filter (with content scanning) and Voice Firewall, respectively.

Timelines

3.36 ComReg is of the preliminary view that a DNS Scam Filter could be implemented by relevant operators within 6 months, because it is clearly defined and relatively straightforward to apply from a technical perspective.

[48] In each case, the MNOs also apply a SMS Scam Filter (with content scanning).
[49] It should be noted there are difficulties in comparing scam metrics between SMS and DNS.
[50] Telenor "*Sikkerhetsåret 2024*" [translated by Google] Link

4 Submitting comments and next steps

4.1 Submitting comments

4.1 The consultation period will run until 17:00 on Friday 15 May 2026 during which time ComReg welcomes written comments on any issues raised in this paper.

4.2 Responses must be submitted in written form (email) to the following recipient, clearly marked – Submissions to ComReg 26/24:

Donnacha Hennessy

Commission for Communications Regulation

Email: marketframeworkconsult@comreg.ie cc: donnacha.hennessy@comreg.ie

4.3 Electronic submissions should be submitted in an unprotected format so that they may be readily included in the ComReg submissions document for electronic publication.

4.4 ComReg appreciates that respondents may wish to provide confidential information if their comments are to be meaningful. In order to promote openness and transparency, ComReg will publish all respondents' submissions to this notice, as well as all substantive correspondence on matters relating to this document, subject to the provisions of ComReg's guidelines on the treatment of confidential information (Document 05/24).

4.5 In this regard, respondents should submit views in accordance with the instructions set out below. When submitting a response to this notification that contains confidential information, respondents must choose one of the following options:

4.6 Preferably, submit both a non-confidential version and a confidential version of the response. The confidential version must have all confidential information clearly marked and highlighted in accordance with the instruction set out below and include the reasons as to why they consider any particular material to be confidential. The separate non-confidential version must have actually redacted all items that were marked and highlighted in the confidential version.

OR

4.7 Submit only a confidential version including the reasons as to why they consider any particular material to be confidential and ComReg will perform the required redaction to create a non-confidential version for publication. With this option, respondents must ensure that confidential information has been marked and highlighted in

accordance with the instructions set out below. Where confidential information has not been marked as per our instructions below, then ComReg will not create the non-confidential redacted version and the respondent will have to provide the redacted non-confidential version in accordance with option A above.

4.8 For ComReg to perform the redactions under Option B above, respondents must mark and highlight all confidential information in their submission as follows:

a) Confidential information contained within a paragraph must be highlighted with a chosen particular colour

b) Square brackets must be included around the confidential text (one at the start and one at the end of the relevant highlighted confidential information)

c) A Scissors symbol (Symbol code: Wingdings 2:38) must be included after the first square bracket. For example, “Redtelecom has a market share of [✂<25%].”

4.2 Next steps

4.9 When it has concluded its review of all submissions received to this Preliminary Consultation, and other relevant material, ComReg’s intention would be to publish a Consultation, and draft Decision(s).

Annex: Countries that filter SMS traffic

The following is a list of countries where public information[51] indicates that a SMS Scam Filter (which typically includes analysis of metadata such as the SMS Base Filter) has been deployed.

Table 1: Countries that filter SMS traffic and reported impact

Region	Country	Public Source(s)	Link	Reported Impact
Anglosphere	*UK*	Media	Link	**2.8 Billion** scam SMS blocked[52] **as of March 2026,** with 49 Million blocked in February 2026 alone
	USA	Aggregator	Link	-
	Canada	Aggregator	Link	-
	Australia	MNO	Link	**969 Million** scam SMS blocked[53] **as of September 2025.**
	New Zealand	Media	Link	-
	South Africa	Media	Link	-
	Singapore	Media	Link	-
EU/EEA member state	*Germany*	Media	Link	-
	Belgium	Media	Link	**Proximus** blocked **16 Million** scam SMS **in 4 months**.[54] **Telenet** blocked **2.4 Million** scam SMS **in 2 months.**[55]
	France	Aggregator	Link	-
	Poland	Media	Link	-
	Finland	MNO	Link	-
	Switzerland	MNO	Link	-
	Denmark	Media	Link	**3.8 Million** scam SMS blocked **in the first 3 months**[56]
	Lithuania	Media	Link	-
	Iceland	Aggregator	Link	-
	Romania	Aggregator	Link	-
	Norway	MNO	Link	**Telenor** blocked 64 **million** scam SMS **in 2024**.[57]
Rest of World	*Turkey*	Vendor	Link	
	Philippines	Media	Link	**Globe**[58] & **SMART**[59] blocked **7 Billion** scam SMS in **12 months.**
	Malaysia	Media	Link	-
	Fiji	Vendor	Link	-
	Nigeria	Media	Link	-
	Ghana	Media	Link	-
	Kenya	Media	Link	-
	Zambia	Media	Link	-
	India	Media	Link	**Airtel** alone has flagged **2.9 Billion** scam SMS **since 2024**[60]
	South America	Vendor	Link	**Telefonica** blocked **40 Million** scam texts **every month**.[61]
	China	Aggregator	Link	-

[51] This list is non-exhaustive, there may be other countries countries with SMS Scam Filters.
[52] Mobile UK "*Total scam messages blocked to date*" Link See also earlier press releases from Three, Vodafone and EE.
[53] ACMA "*Action on scams, spam and telemarketing: July to September 2025*". Link See also press from Telstra and Optus.
[54] Telecompaper.com "*Belgium's Telenet Proximus block millions of smishing messages with ai tool"* 29 February 2024 Link
[55] Telenet, "*Telenet and BASE already blocked over 2 million suspicious text messages thanks to new platform*" Link
[56] Commsrisk *"New Danish Content Filter Blocks 3.8mn SMS Messages in First Quarter"* Link
[57] Telecomtv.com "*Telenor safeguards customers and delivers solid results*" Link
[58] Mavenir, press release "*Mavenir's SpamShield Messaging Technology Drives Steep Decline in Spam and Scam SMS for Globe Telecom*" 29 May 2024 Link
[59] PhilipineStar "*Smart blocks nearly 2 billion malicious text messages*" Link.
[60] EconomicTimes "*Airtel flags 71 billion spam calls, 2.9 billion messages since 2024*" Link
[61] Mavenir, press release "*How Mavenir's Revenue Protection Helped Telefonica Increase Revenue by Preventing Spam and Monetizing A2P Grey Routes*" 2019 Link

Legal Annex: Summary of statutory objectives and legal framework relevant to SMS interventions

The Communications Regulation Act 2002, as amended ("2002 Act"), the Communications Regulation and Digital Hub Development Agency Act 2023 ("2023 Act"), and S.I. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022 ("2022 Regulations"), set out, amongst other things, powers, functions, duties and objectives of ComReg that are relevant to SMS interventions.

The ComReg statutory functions contained in the 2002 Act 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…".

The ComReg statutory objectives contained in section 12 of the 2002 Act, 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".

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) (ii) ensuring that there is no distortion or restriction of competition in the electronic communications sector, …

(iii) (iv) encouraging efficient use and ensuring the effective management of 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".

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.

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.

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

ComReg's powers in relation to the rights of use for numbers are further detailed in the 2022 Regulations. Part 10 of the 2022 Regulations deals with access to numbers and services, and related provisions, and transposes Articles 93 and 94 of the EECC.

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".

Under Regulation 79(1) of the 2022 Regulations, 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.

Regulation 78(7) of the 2022 Regulations 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".

Regulation 104 of the 2022 Regulations 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 2022 Regulations, to issue directions to an operator or undertaking to do or refrain from doing anything which the Regulator specifies in the direction.

Power relating to misuse of numbers

Under Regulation 83(2) of the 2022 Regulations 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

Obligations on operators regarding security and integrity are set out in Part 2 of the 2023 Act. 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."

It is important to note that the definition of “security of networks and services” means as per section 5 of the 2023 Act: “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”.