An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Know Your Customer (KYC) Guidance - Draft

Information Notice

Reference: ComReg 24/24c

Date: 03/04/2024

Content

Section Page

1 Summary

1. Protecting consumers from harm is an enduring priority for ComReg, and ComReg continues to be very concerned by the continuing proliferation of scams facilitated by telephone calls and text messages.

2. A common tactic for scammers is to contact people using a call or text, often claiming to be from a legitimate organisation, to trick their victim into providing personal details or making a payment. Using a valid Irish telephone number can add to the perceived legitimacy of the scam. However, if operators have processes in place to reduce access to valid phone numbers by those who intend to misuse them, and respond appropriately when number misuse is reported, this should significantly reduce harm to consumers.

3. Operators providing telephone numbers should therefore know their customers, consider their relationship with each customer, and have processes in place to report on and deal with any issues arising with the use of those numbers. To that end, Know Your Customer (KYC) processes can play a critical role in identifying and mitigating fraud.

4. This document outlines the important role that KYC plays in helping to identify and mitigate fraud and looks at how other jurisdictions are implementing effective KYC checks and practices.

5. This document also provides an update to the draft KYC Guidance set out in ComReg 23/52, taking account of submissions received to Consultation 23/52 and some of the checks and practices used in other jurisdictions.

6. ComReg recognises that some services present particular challenges for operators, including prepaid mobile and cloud-based telephony. As such:

    - In the prevailing absence of requiring prepay SIM registration, ComReg expects operators to take proactive KYC measures to prevent prepay SIMs and eSIMs falling into the wrong hands. ComReg therefore strongly recommends that mobile operators introduce electronic KYC (eKYC) measures for the purchase of all new prepay eSIMs, in accordance with the updated guidance set out in this document.

    - Knowing that scam calls originating from genuine Irish numbers, unwittingly assigned by Cloud Service Providers (CSPs) to fraudsters, are a particular problem, ComReg expects these providers to implement sufficient KYC checks to ensure geographic numbers are assigned only to those customer's located in the relevant minimum numbering area (MNA) by verifying the customer's identity and

address. ComReg expects such validation to be achieved through the use of an appropriate eKYC solution capable of supporting the measures set out in the updated guidance.

7. ComReg welcomes comments on this document. The comment period will run for a period of four weeks. Comments should be sent by email to kyc@comreg.ie by 5.30pm on Wednesday 1 May 2024. ComReg will then publish a final version of this document.

2 Background

8. In this Chapter, we highlight ComReg's recent work on combatting scam calls and texts and set out background information relevant to ComReg's administration of Ireland's telephone numbers under the Communications Regulation Act 2002 ("the 2002 Act").

2.1 ComReg's work to combat scam calls and texts

9. In June 2023, ComReg released the consultation entitled "Combatting scam calls and texts - Consultation on network-based interventions to reduce the harm from Nuisance Communications" (ComReg 23/52[1]) which outlined measures to combat telephone scams and proposed, inter alia, Know Your Customer guidelines ("KYC Guidance") to encourage checks to be carried out by mobile and fixed telecoms operators in Ireland.

10. As part of ComReg 23/52, an overview of nuisance communications was provided, and a summary of the negative impact scam calls and texts have on the public in Ireland, causing both financial and economic damage to all sectors of society including consumers, business, and public bodies. Scams also result in significant stress and anxiety, particularly to those most vulnerable who often rely on their phone as the main means of staying connected with friends and loved ones.

11. The impact of nuisance communications on the public can be minimised by the use of KYC processes to increase the barriers to entry for "bad actors" who carry out scam calls and texts using Irish telephone numbers. These processes have been proven to be effective in other countries, as outlined throughout this document, and are essential for the future security of the telecoms industry.

12. The draft KYC Guidance set out as part of ComReg 23/52 was intended as a starting point for developing a best practice guide for all telecoms operators in Ireland. The draft guidance set out minimum checks for operators to follow when assigning Irish phone numbers to customers. As part of the consultation, operators were invited to provide feedback to ComReg on the draft guidance and ComReg has fully considered all of the responses when developing the guidance in this document (see Chapter 4).

13. While the KYC guidance is not mandatory, it does, for example, address the need for operators to carry out checks on the geographic location of their customer's residence or place of business when assigning geographic

[1] ComReg 23/52: Consultation on combatting Nuisance Communications, 16 June 2023

numbers. This is to ensure compliance with the conditions of use that attach to geographic numbers.

14. ComReg will keep KYC practices under review and, if needed, may explore introducing mandatory KYC checks, if KYC practices do not improve and the level of scam calls and texts persist across society as a result.

2.2 ComReg's responsibility for numbering management

15. The Commission for Communications Regulation ("ComReg") is the statutory body responsible for the regulation of the electronic communications (telecommunications, radiocommunication and broadcasting networks), postal and premium rate sectors in Ireland in accordance with European Union ("EU") and Irish Law. ComReg also manages the national numbering resource, among other responsibilities.

16. 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.

17. Further to section 12(1)(a)(iii) of the 2002 Act, one of ComReg's objectives in exercising its functions is, in relation to the provision of electronic communications networks, and electronic communications services, and associated facilities, to promote the interests of users within the Community.

18. ComReg's Numbering Conditions of Use and Application Process document (ComReg 15/136R4) (the "Numbering Conditions") sets out the rules to be adhered to for the provision and use of phone numbers in Ireland. Know Your Customer relates to number provision and number use as operators are expected to ensure that they only provide numbers to customers who intend to use them properly. KYC processes protect operators in the number provision process and reduce the risk of consumers experiencing scams.

2.3 Structure of this Information Notice

19. The remainder of this document is structured as follows:

- Chapter 3 outlines the important role that KYC plays in helping to identify and mitigate fraud, the key components of effective KYC frameworks, the benefits of implementing robust KYC practices, how other jurisdictions are implementing KYC, risk assessment, adapting existing processes, responding to incidents of number misuse, eKYC, particular challenges,

organisational awareness and support, collaboration and shared responsibility, as well as the future of KYC.

- Chapter 4 provides an update to the draft KYC Guidance set out in ComReg 23/52, taking account of submissions received to Consultation 23/52 and building on some of the checks and practices identified in Chapter 3.

3 KYC: Its role and implementation

3.1 Overview

20. In general terms, Know Your Customer (KYC) refers to the policies and procedures put in place by organisations to verify the identities of customers and manage risk. KYC standards are typically used to protect financial institutions against fraud, corruption, and money laundering, but are increasingly being used in other industries and sectors, including telecommunications.

21. In this Chapter we consider the important role that KYC plays in helping to identify and mitigate fraud, the key components of effective KYC frameworks, and the additional benefits to telecoms operators of implementing robust KYC practices.

22. The Chapter also looks at how other jurisdictions are implementing effective KYC checks and practices, before considering how Mobile Service Providers ("MSPs") i.e., MNOs and Mobile Virtual Network Operators ("MVNOs") can use electronic KYC ("eKYC") to verify document authenticity and determine whether new subscribers are legitimate.

23. The Chapter then considers the particular KYC-related challenges posed by prepaid mobile and cloud telephony, before highlighting the importance of organisational awareness and support for KYC at a senior level within organisations. The Chapter also highlights the importance of collaboration and knowledge sharing before concluding with a discussion on the future of KYC in the telecommunications industry.

3.2 Importance of KYC in identifying and minimising fraud

24. Protecting consumers from harm is an enduring priority for ComReg, and ComReg continues to be very concerned by the continuing proliferation of scams facilitated by telephone calls and text messages.

25. A common tactic is for scammers to contact people using a call or text, often claiming to be from a legitimate organisation, to trick their victim into providing personal details or making a payment. Using a valid Irish telephone number can add to the legitimacy of the scam. If operators have processes in place to reduce access to valid phone numbers by those who intend to misuse them, and respond appropriately when number misuse is reported, this should significantly reduce harm to consumers.

26. Operators providing telephone numbers should therefore know their customers, consider their relationship with each customer, and have processes in place to report on and deal with any issues arising with the use of numbers. To that end, KYC processes can play a critical role in identifying and mitigating fraud.

27. While KYC is more generally associated with financial and banking services, as well as related sectors such as financial trading, KYC requirements are increasingly becoming necessary for a growing number of other industries to verify the identity of clients either before or during the commencement of business. KYC can be used to help the telecommunications industry combat the misuse of telephone numbers, by further enabling operators to assure that individuals and businesses are '*who they claim to be*' before assigning Irish telephone numbers to them.

28. In the banking and financial services sector, KYC involves the verification of customer identities and the monitoring of their transactions. Financial institutions are required to authenticate personal information, develop risk profiles for each customer, and continually monitor their transactions for signs of illegal activity. These processes not only protect customers and investors but also help safeguard the reputation of the institutions and the integrity of financial markets.

3.3 Key components of KYC frameworks

29. All effective KYC frameworks are made up of three key components: identity verification, customer due diligence, and ongoing monitoring (see Figure 1).

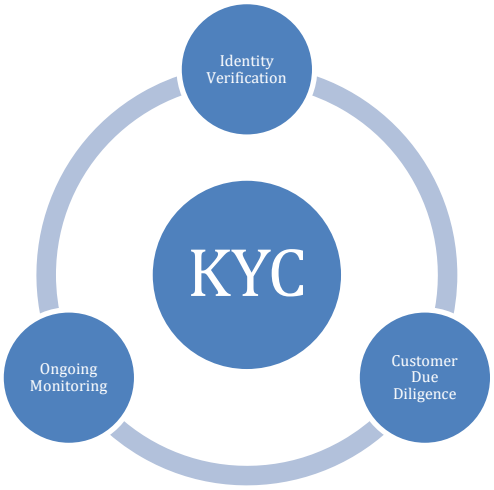

Figure 1: Key components of KYC Frameworks

Identity verification

30. Identity verification sits at the core of any KYC framework. This requires any customer, both individual and business, to have their identity verified via the provision of appropriate documents and/or proof of address.

31. An effective ID verification system can assist operators in ensuring that the customer is who they claim they are and not an impostor. Increasingly, AI-powered ID verification solutions are enabling operators to assess the risk associated with clients through different identification checks, such as biometric face recognition.

Customer due diligence

32. Once a customer's identity has been verified, the next step is to complete customer due diligence (CDD) by using available information to determine what risk, if any, the customer carries, and how this could be impactful to the business. CDD aims to identify potential risk factors by analysing information from a number of sources including information provided by the customer themselves, sanctions lists maintained by official authorities, publicly available data, and private data sources from third parties.

33. Customers that are deemed to be high risk are typically subject to enhanced due diligence (EDD) checks, such as searches of credit histories, additional checks with agencies or public sources, or further investigation into accounts/transactions/usage.

Ongoing monitoring

34. Ongoing monitoring is used to identify changes in customer activity that may warrant an adjustment in risk profile or further investigation. The level and frequency of monitoring will depend on the customer's perceived risk and the strategy adopted by the organisation.

3.4 Benefits of robust KYC practices

35. In addition to the critical role that KYC can play in identifying and mitigating fraud, there are many benefits for telecoms operators including:

- Improved risk management
- Better customer experience
- Improved data quality
- Compliance with legislation

Improved risk management

36. KYC processes help operators to manage the risk of illegal activity on their networks by providing them with a better understanding of who is using their services. Common scam activity includes nuisance calls and text messages, and schemes like the Wangiri scheme (where a call rings once and is then disconnected).

37. KYC enables operators to verify the identity and legitimacy of their customers by carrying out identity checks to ensure that information provided is accurate, whilst recording and retaining basic customer information. This allows for improved risk management as such verification reduces the likelihood of bad actors accessing the network and helps protect consumers from fraud. By recording information gathered through KYC processes, operators are able to respond swiftly by taking direct action on those who may have misused the service.

Better customer experience

38. Improved customer experience can enhance customer satisfaction and loyalty and help cultivate trust between the customer and operator. The more operators seek to optimise their KYC processes, the better the customer experience delivered.

39. High quality KYC can expedite the requirement for additional checks during interactions between customers and operators, enabling customers to access services more efficiently. By optimising KYC checks, the need for customers to provide redundant or excessive information can be avoided helping to alleviate customer frustration and boost overall satisfaction. If customers are satisfied with their experience, they are more likely to have a positive perception of the operator leading to increased trust and loyalty, which can drive customer acquisition and retention.

Improved data quality

40. In collecting data through optimised KYC processes, and analysing it in the right way, operators can become better informed of their customer base and make more informed business decisions. Operators can, in turn, utilise this data to tailor their products and services and refine their sales and marketing strategies.

Compliance with legislation

41. By using KYC to efficiently verify customer identity, operators can also help eliminate suspicions of fraud and money laundering and further enable compliance with Anti-Money Laundering (“AML”) requirements.

42. KYC is also of relevance to the proposed Payment Services Regulation ("PSR")[2], as it strengthens the protection of payment service users and confidence in payments, including by improving strong customer authentication (SCA) rules (including improved accessibility of SCA for users with disabilities, older people and others facing challenges using SCA) (Article 85). However, obligations under the PSR are primarily upon payment service providers.

43. Similarly, KYC can also help operators to meet aspects of the General Data Protection Regulation ("GDPR"), which requires that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing (Article 5(1)(f)). The GDPR also requires that personal data must be accurate (Article 5(1)(d)).

3.5 KYC guidance and measures in other jurisdictions

44. Many National Regulatory Authorities ("NRAs") have developed KYC guidance and other related measures to help operators reduce access to valid telephone numbers by those who intend to misuse them. For example:

- In November 2022, Ofcom published its good practice guide to help prevent misuse of assigned numbers[3], which sets out the steps Ofcom expects operators to take to help prevent valid telephone numbers being misused, including to facilitate scams.
- The Infocomm Media Development Authority ("IDMA") in Singapore has published guidelines for a *subscriber verification process*[4], whereby potential customers are required to furnish information, according to the details requested by their operators, for the verification of their identity before signing up to new services or making changes to existing subscriptions.
- In support of the industry's fight against illegal robocalls, the Federal Communications Commission ("FCC") in the USA instituted its own KYC requirements for originating voice service providers in 2020.

45. It is also worth noting that in 2022 the Japanese telecoms regulator, the Ministry of Internal Affairs and Communications of Japan ("MIC"), published

[2] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010) COM/2023/367 final - EUR-Lex - 52023PC0367 - EN - EUR-Lex (europa.eu)

[3] https://www.ofcom.org.uk/consultations-and-statements/category-2/good-practice-guide-on-sub-allocated-assigned-numbers

[4] https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/guidelines-for-subscriber-verification-process.pdf

its guidelines on money laundering and terrorist financing ("AML/CFT")[5]. The guidelines outline requirements for customer management, or customer due diligence, which encompasses investigating the information of each customer and the transactions conducted by that customer. The guidelines also propose recommendations for management including the creation of a specific compliance and risk management function, as well as a unit focused on internal audits as an additional line of defence.

46. Some of the guidance and related measures summarised above include a number of important practices which should be considered by telecoms operators in Ireland. In particular, consideration should be given to the adoption of a risk-based approach to determine the types of checks and level of scrutiny applied according to the perceived risk posed by the customer, the need for operators to be proactive to stay up to date in their ability to identify and respond to areas of vulnerability, and the benefits of adopting a robust framework for responding to incidents of number misuse. Each of these are now considered in further detail.

3.6 Risk assessment

47. In the guidance published by Ofcom, operators are encouraged to tailor the types of checks and level of scrutiny applied according to the perceived risk posed by the customer. Additionally, operators are asked to look out for indicators of higher risk customers, such as customers which present inaccurate, vague, or unclear information.

48. Similarly, the IMDA requires operators to complete enhanced due diligence checks on higher risk customers (i.e., customer's background, source of income or revenue, country of origin and residence, and the nature and purpose of their accounts) when the initial CDD raises red flags.

49. ComReg considers that a KYC risk-based approach, similar to those summarised, will help enable operators to implement a better customer onboarding experience as the verification levels can be adjusted based on risk factors. In other words, low-risk customers can be onboarded more quickly, while higher-risk customers can have additional verification procedures to meet.

50. The broad intention is to encourage operators to adopt a risk-based approach by focusing resources on areas of higher risk. That does not detract, however, from the need for operators to do their own analysis of where their risks lie, in order to make a risk-based approach effective. Such an approach will, for

[5] https://www.dataguidance.com/news/japan-mic-publishes-guidelines-amlcft-telephone

example, ensure that lower risk customers do not suffer from unduly burdensome procedures and requirements. And, on the other hand, it will ensure that operators undertake greater due diligence whenever that is required, i.e., for customers that may pose higher risk.

3.7 Adapting existing processes to introduce additional KYC checks

51. Existing checks implemented by operators present a base level of KYC processes to build upon. However, ComReg considers that operators need to be proactive and stay up to date in their ability to identify and respond to areas of vulnerability. Some of the ways operators can continuously adapt and improve their KYC measures include:

- Conduct regular risk assessments to identify areas of vulnerability and prioritise resources accordingly.
- Provide ongoing education and training to internal teams to keep them informed of best practices.
- Leverage technology to automate certain KYC processes and improve the accuracy of risk assessments.
- Collaborate with other operators, ComReg and other stakeholders to ensure a coordinated and consistent approach to KYC checks.

52. Ofcom's guidance expects operators to consider routinely testing and/or monitoring specific risks associated with particular customers, with the frequency of testing being based on the level of risk associated with each customer. For example, a customer with no history of number misuse may require less frequent monitoring than one with a history of number misuse. ComReg considers this approach sensible, appropriate, and reasonable.

53. The financial services sector is very aware of the need for staff to be well-trained and knowledgeable about KYC procedures. For example, in Ireland Section 54(6) of the CJA 2010[6] requires firms to ensure that:

> "…persons involved in the conduct of the [firm's] business are—
>
> (a) instructed on the law relating to money laundering and terrorist financing, and

[6] The primary piece of legislation in Ireland on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) is The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by Part 2 of the Criminal Justice Act 2013 and by the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 ("the CJA 2010")

(b) provided with ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified."

54. ComReg acknowledges that processes underpinning the manual collection and verification of KYC can take time to gather and analyse. ComReg therefore encourages operators to consider the use of technology to enable an interactive and automated process for gathering data quickly, giving internal teams the necessary time to focus on the investigation of potential misuse and suspicious activity. Developing and utilising analytical technology is likely to be of even greater importance when working with high-volume and repetitive manual activities, in order to achieve the greatest benefits in a cost-effective manner.

3.8 Responding to incidents of number misuse

55. ComReg clearly expects operators to respond in an appropriate and timely way to evidence of number misuse to help ensure that where issues do arise, action is taken quickly and decisively to ensure the potential harm to customers is minimised.

56. In this regard, Ofcom's guidance encourages providers to set target Service Level Agreements ("SLAs") for reviewing reports of misuse. The Ofcom guidance also provides some examples of how misuse (including scams utilising mobile numbers) should be responded to, including by applying temporary blocks to numbers or customer accounts, suspending some services and/or using contractual controls. ComReg considers this approach appropriate and necessary in the ongoing fight against nuisance communications.

3.9 eKYC

57. In a retail environment, MSPs can verify the identity of the customer by performing their normal KYC checks. However, with the growth of eSIM devices, MSPs will increasingly come under pressure to offer a similar onboarding experience but in a remote/virtual environment and without the support of a trained retail representative.

58. Electronic Know Your Customer, or eKYC, is the real-time, remote, and paperless version of the traditional KYC verification process, which will be widely used in the activation of eSIM subscriptions. In addition to enhancing

the simplicity of the KYC process and speeding up onboarding of new customers, MSPs can use eKYC to verify document authenticity and determine whether new subscribers are legitimate.

59. For example, taking a sufficiently high-quality photograph of an official ID document means that it can be analysed and verified for authenticity, with more accuracy than an in-store representative is likely to be able to provide. Similarly, a selfie portrait can be taken on a smartphone, its biometric template extracted, and then compared with the portrait in the ID document.

60. Some NRAs are beginning to provide guidance in relation to the use and implementation of eKYC. For example, as part of a roadmap to identify and recommend solutions needed to secure Singapore's connectivity infrastructure, in 2019 the IMDA released an eKYC implementation guide[7] – the aim of which is to make it more convenient for consumers to register for mobile services online in a trusted manner by enabling operators to digitally verify mobile services registrations without the need for physical face-to-face transactions.

61. The IMDA eKYC implementation guide requires operators to implement the following minimum measures in their eKYC solutions to identify and verify a subscriber's identity:

> "(a) [when] collecting the subscriber's information for the purposes of validating the subscriber's identity, [this must include]…
>
> (i) performing a live scan of the […] subscriber's identity document; and
>
> (ii) taking live photos (or live video) of the subscriber,
>
> or
>
> (b) establishing that information about the subscriber's identity is provided from a trusted database."

62. ComReg notes the increasing availability of biometric face recognition and other technologies used to provide remote identity verification to meet the requirements set out in the IMDA eKYC implementation guide. Whilst there will be a cost to operators of implementing such solutions, the implementation costs can be offset against the benefits these solutions will bring.

63. As highlighted in ComReg 23/52, operators can use the opportunity provided by the growth in eSIM deployments to implement eKYC policies to ensure all

[7] https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/licensing/telecommunication/services-based-operations-licence/ekyc-implementation-guide.pdf

new customers are registered and known to them. This would result in most consumers being registered over time as consumers upgrade to new devices, which in the future are likely to be eSIM only. Therefore, operators should view eSIM as an outstanding opportunity to implement better KYC policies via eKYC.

3.10 Particular challenges

64. ComReg recognises that some number services present particular KYC-related challenges for operators, including prepaid mobile and cloud telephony. This section considers these services in greater detail and highlights particular measures being implemented in other countries to minimise fraudulent activity.

Prepaid mobile

65. Convenience of use is one of the key reasons for the success of prepaid mobile SIMs, but the anonymity associated with them continues to attract a growing number of bad actors looking to use prepaid mobile SIMs to implement voice and text scams.

66. As noted in ComReg 23/52, Ireland is now one of only a few countries without mandatory SIM registration (for prepaid mobiles). As of February 2021, the GSMA found that governments of 157 countries mandate prepaid SIM registration (see Figure 2). A number of other markets including the USA and the UK have also chosen not to impose registration obligations. In these markets, this decision appears to reflect a balance between the effectiveness of a possible solution, the cost of implementing a solution (including the cost to the consumer and limitations on the prepaid market) and potential privacy concerns relating to the use of the registration information by local authorities and/or operators.

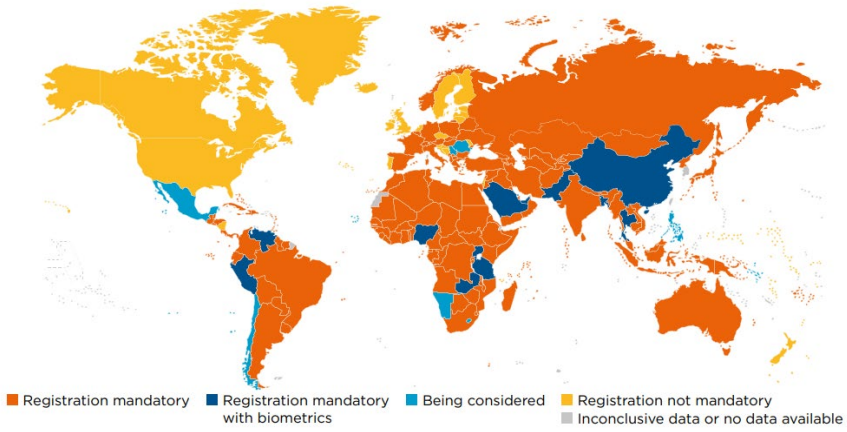

Figure 2: SIM Registration status globally [Source: GSMA, 2021[8]]

67. Other alternatives to mandatory SIM registration include the setting up and maintenance of an International Mobile Equipment Identity ("IMEI")[9] registry. For example, operators in Mexico were asked to set up a database of handset IMEIs using their networks.[10]

68. The IMEI database is used to identify all homologated (type approved) and legally imported and acquired IMEIs that are permitted to be used in the country, while the database is also used to establish and maintain a blacklist of IMEIs that should not have access to the networks (blocked), where the device is believed to be stolen or is suspected of being used for fraudulent or criminal activity.

69. Whilst the blacklisting of IMEIs may provide some level of deterrence, for those resolute in continuing to engage in scam calls and texts, limiting access to devices may prove only a short-term inconvenience.

70. Given the potential for voice and text firewalls, and other types of filters, to combat scam communications, ComReg is not currently minded to require the registration of prepaid SIMs. However, this issue may need to be revisited should firewalls prove to be ineffective at combatting voice and text scams.

71. In the prevailing absence of requiring prepay SIM registration, ComReg expects operators to take proactive KYC measures to prevent prepay SIMs falling into the wrong hands. ComReg therefore strongly recommends that

[8] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf. Note that Denmark, Lithuania and Sweden have introduced mandatory SIM registration since 2021.

[9] IMEI is a numeric mobile equipment identifier

[10] Mexican authorities only imposed this requirement on mobile operators, and not handset vendors. Other countries such as Colombia have implemented IMEI control systems to combat stolen, fraudulent, and counterfeit mobile phones

mobile operators introduce KYC measures for all new prepay SIMs, including eSIMs. The following measures should be considered:

- prevent anonymous purchasing of prepay SIMs.
- limit the number of prepay SIMs that can be purchased per customer (online, at all retail outlets and other points of sale).
- prevent activation of SIM until online registration is complete.
- impose daily thresholds/caps on the number of SMS/calls.

Cloud Telephony

72. Cloud telephony, sometimes referred to as cloud calling, generally means Internet-based voice communication (Voice over Internet Protocol or "VoIP") services where the telephony application is hosted by a third-party provider. Cloud Service Providers can route voice calls, which originate nationally or internationally, to access the Irish Public Switched Telephone Network (PSTN) via a suitable gateway.

73. ComReg understands that some of the traffic that ingresses the Irish PSTN may include scam traffic. This is because bad actors, often but not exclusively based abroad, may "spoof" Irish geographic numbers as their CLI and direct this traffic into the Irish PSTN, knowing that recipients in Ireland are more likely to answer such calls. However, ComReg is also aware of scam calls originating from genuine Irish numbers. These are numbers that may have been unwittingly assigned by a cloud service provider to fraudsters.

74. Other jurisdictions, including Japan and Singapore, have implemented measures to address similar issues. For example, new requirements from the MIC in Japan require every owner of a new Japanese local number[11] to have a physical interconnection on the premises[12]. Only Japanese national (+81 50) and toll-free numbers[13] (+81 800 or +81 120) will be available from cloud telephony providers, with the requirements shown in Figure 3 now in place:

[11] Japanese local numbers have prefixes such as +8144 for Kawasaki, +8152 for Nagoya, or +816 for Osaka

[12] https://support.telnyx.com/en/articles/3739474-japan-did-requirements

[13] Japanese Toll-Free numbers can only be registered to businesses

National number		
Personal identity verification	**Business identity**	**Address verification**
Name, last name	Name, last name	Address (street, building number, postal code, city, and country)
Contact telephone number	Contact telephone number	
Copy of passport or national ID	Company name	
	Copy of company incorporation certificate	
Toll–free number		
	Business identity	**Address verification**
	Name, last name	Address (street, building number, postal code, city, and country)
	Contact telephone number	
	Copy of passport or national ID	
	Company name	
	Copy of company incorporation certificate	

Figure 3: Requirements for obtaining national and toll-free numbers in Japan [Source: Telnyx, 2024]

75. In relation to the new requirements in Japan, it is also worth highlighting that Microsoft has updated its advice on the requirements to obtain a Skype number in Japan, noting that users will have to take a live selfie or upload a headshot photograph, and install the Microsoft Authenticator app on their mobile device, in addition to uploading a suitable form of ID (passport, My Number Card[14], resident card). ComReg understands that such a process is not currently in place in Ireland, and this lack of verification creates a clear avenue for scammers to obtain Irish numbers which can be used to commit fraud. ComReg strongly recommends that relevant operators should implement a verification process similar to that identified in Japan as part of its process of issuing Skype numbers (or alternatives) to end users.

76. The IMDA in Singapore requires operators to maintain a register containing records of their IP telephony subscribers[15], with the information ready to be made available for inspection by authorised Singapore government agencies. The records are required to contain the information shown in Figure 4.

[14] The name given to the identity document issued to citizens and residents in Japan

[15] https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/licensing/licenses/ipteltcs.pdf

	IP telephony subscriber registration requirements – Singapore
	• Name
	• Identity Number (as applicable, NRIC[1] number, FIN[2], passport number of the subscriber and business registration number of the company for corporate customer)
	• Billing address / Service address (where applicable)
	• Contact information (landline number, mobile number, or email address)
	• Service period
	• Service ID
	• Assigned client IP address and user ID/user name (where applicable)
	• Equipment ID (where applicable)

Note 1: National registration identity card, received by every Singapore citizen and permanent resident.

Note 2: Foreign identification number (FIN) is a unique identification number issued to foreigners who are working, studying, or residing in Singapore.

Figure 4: IP telephony subscriber registration requirements – Singapore [Source: IMDA, 2018]

77. Before recording the information referred to in Figure 4, operators are required to:

- where the subscriber is located in Singapore, require the production of the subscriber's identity card issued, passport or employment pass and keep a copy of such evidence of identity; or
- where the subscriber is not located in Singapore, use best efforts to verify the identity of the subscriber through appropriate documents that are recognised by the authorised establishments in the country of purchase.

78. It is also interesting to note that, in September 2023, the FCC issued an order that imposes additional requirements on VoIP providers.[16] This order includes a revision to existing rules requiring VoIP providers to certify that numbers allocated to them will not knowingly be used to transmit, encourage, assist, or facilitate illegal robocalls, illegal spoofing, or fraud, in violation of robocall, spoofing, and deceptive telemarketing obligations. While this is not a direct KYC obligation, it may prove sufficient to incentivise VoIP providers to complete more extensive checks on new customers.

3.11 Organisational awareness and support at senior level

79. Implementing effective KYC procedures can be challenging if not completed in a holistic manner. Operators are therefore encouraged to develop KYC checks and processes which take account of end-to-end workflows and

[16] https://docs.fcc.gov/public/attachments/FCC-23-75A1.pdf

existing practices to increase process effectiveness and improve the customer experience.

80. However, KYC procedures and processes are only as effective as the employees implementing them. ComReg therefore also strongly encourages operators to implement regular training and awareness programs to ensure that relevant individuals within the organisation are well-informed about KYC requirements and potential changes introduced as a result of the ever-changing fraud landscape.

81. KYC is also not a one-time process. Operators should aspire to foster a KYC culture across all of its relevant sales and operations teams, where individuals understand and value its importance.

82. Achieving a KYC culture requires commitment from senior leadership. To this end, operators should consider allocating to a director or senior manager overall responsibility within the organisation for the establishment and maintenance of effective KYC systems and controls. This individual might also be tasked with producing regular reports for senior management covering, amongst other things, suspected fraud, or misuse incidents; the status of KYC related projects and training; and the status of action(s) taken in response to recommendations raised in previous reports. The same individual should also be encouraged to collaborate with industry peers to share insights on the latest incidents and the effectiveness of emerging tools and solutions (see Section 4.3 below).

3.12 Collaboration and shared responsibility

83. The shared nature of communications networks, and the associated misuse of these networks by those seeking to perform scams facilitated by calls and texts, makes collaboration amongst operators, ComReg and other stakeholders critical to success.

84. ComReg values the very important work already undertaken by the Nuisance Communications Industry Taskforce (NCIT) to combat scams and other unsolicited communications.

85. ComReg may, in the future, consider further best practices in KYC. ComReg strongly encourages further ongoing collaboration between operators and other organisations to help tackle the problem of scams, including by sharing data where appropriate. We also encourage operators to continue to share information when appropriate to prevent scams or other misuse.

86. In some instances, it may be appropriate to share intelligence with other sectors. For example, Singapore has a joint strategy for anti-money

laundering (AML) across telecommunications, banking and other industries which uses its national database / identification to verify customers' information, and, in October 2023, the Monetary Authority of Singapore (MAS) and the IMDA published a joint consultation paper proposing a Shared Responsibility Framework (SRF) for phishing scams. The SRF assigns financial institutions and telecommunication companies' relevant duties to mitigate phishing scams and requires payouts to affected scam victims where these duties are breached.

87. The proposed framework aims to strengthen the direct accountability of financial institutions and operators to consumers. It sets out discrete and well-defined duties for institutions and operators to mitigate the risk of consumers falling prey to phishing scams. Breaches of these duties, such as a failure to send outgoing transaction notification(s) to consumers in the case of financial institutions, and a failure to implement a scam filter in the case of operators, would be the starting point for determining the party to be held responsible for losses under the framework. It therefore incentivises financial institutions and operators to strictly uphold the desired standards of anti-scam controls.

88. In the same vein, faced by an increasing threat of industrial-scale fraud, telecommunications providers and the UK Government signed the Telecommunications Fraud Sector Charter[17], a voluntary agreement to improve counter-fraud efforts, in October 2021. Under the charter, providers have agreed to tackle fraud through a multi-point action plan. The telecommunications providers have committed to, inter alia:

- identify and implement techniques to block scam calls and share data on the source of these calls across the sector[18]
- identify and implement techniques to block smishing texts[19]
- work with banks to strengthen authentication checks at the point a device contract is applied for and at the point a customer requests to move their number to a new provider (to tackle SIM swap and Mobile Number Portability (MNP) fraud).

[17] https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter

[18] Data sharing to combat fraud and scams, will be supported by specific case studies which will be provided to the UK Information Commissioner's Office (ICO) for potential inclusion in its data sharing hub.

[19] Providers will share reported URLs and phone numbers suspected to be linked with smishing with the UK National Cyber Security Centre (NCSC) and UK National Fraud Intelligence Bureau (NFIB). Providers will seek to restrict access to URLs confirmed by the NCSC as used for smishing in accordance with legal and regulatory obligations.

3.13 The future of KYC

89. Businesses and financial institutions are increasingly implementing technology-backed identity verification solutions. Biometrics, machine learning, artificial intelligence (AI), and optical character recognition (OCR) are among the tools that are transforming how businesses verify customers.

90. Recent research indicates that eKYC verification solutions are now beginning to eclipse conventional KYC practices. For example, a recent study from Juniper Research predicts that the number of digital identity verification checks will surpass 70 billion in 2024, growing 16% over the previous year[20].

91. Automation and artificial intelligence are the driving forces behind digital KYC verification and enhanced automation, together with an increasing adoption of AI, and these are expected to improve KYC practices in coming years, further streamlining customer verification and onboarding journeys.

92. With the increasing availability of highly customisable verification solutions utilising automation technologies, telecommunications operators, like many other businesses across a variety of industries will have an improved capability to fight fraud, meet compliance and onboard legitimate customers.

[20] https://www.juniperresearch.com/press/digital-identity-verification-checks-to-pass/

4 Best practice KYC guidance

4.1 Purpose of this guidance

93. This guidance sets out the "Know Your Customer", or KYC, steps ComReg expects operators (mobile network operators, mobile virtual network operators, fixed operators, and cloud service providers) to adopt when providing phone numbers to consumers and businesses. Many of the measures are based on practices that some operators already have in place, and ComReg views the guidance as consolidating and sharing best practice.

94. The guidance is part of ComReg's ongoing work to disrupt scam calls and texts and will assist operators in ensuring compliance with the Numbering Conditions of Use and Application Process (ComReg 15/136R4) ("Numbering Conditions").

95. If operators have robust processes in place to manage access to valid numbers, particularly preventing access to those who intend to misuse them, and then respond appropriately when number misuse is reported, this will benefit not only the operator but consumers, business, public bodies, and other organisations who rely on their services.

4.2 Scope of the guidance

96. ComReg's guidance is set out in four sections:

- Due diligence checks before assigning telephone numbers (Section 4.3)
- Ongoing compliance and assessment of risk (Section 4.4)
- Responding to incidents of number misuse (Section 4.5)
- Continued review and evaluation of processes (Section 4.6)

97. In using this guidance, operators are required to ensure their continuing compliance with obligations under relevant data protection and other applicable legislation.[21]

[21] Such as for instance in relation to Anti-Money Laundering, and legislation that combats fraud.

4.3 Due diligence checks

Risk-based assessment

98. Operators are expected to establish the legitimacy of those requesting phone numbers to protect consumers from fraud, to safeguard the reputation of the operator and the broader industry, and to ensure that prompt action may be taken in the event of any problems.

99. Before assigning numbers to customers, operators should therefore take reasonable steps to understand the customers who have requested numbers, and the risk of number misuse.

100. The types of checks and level of scrutiny may vary across different types of customers. For example, a relatively lower level of scrutiny may be appropriate for an existing customer with whom the operator already has a relationship, is familiar with the customer's intended use of and need for numbers, and already holds relevant information.

101. However, the assignment of numbers will encompass a much broader range of customers, including new customers. In assessing the likelihood of number misuse, ComReg expects that all operators will need to undertake further checks to best understand the customer's request. The exact nature of these checks will depend on the customer and the request being made, but operators are expected to undertake the following KYC checks, as a minimum, before assigning telephone numbers to customers (see Figure 5).

KYC checks for individual customers	KYC checks for organisation / business customers
• Customer name	• Contact name
• Customer address (including Eircode)	• Organisation / business names (registered name and trading name)
• Contact email	• Registered office address (including Eircode)
• Contact telephone number	• Business address (if different from registered office address)
	• Contact email
	• Contact telephone number

Figure 5: Minimum KYC checks before the provision of phone numbers

102. Some KYC checks are necessary to ensure that the Numbering Conditions are not breached. For example, particular attention is needed when assigning Irish geographic numbers. Section 4.1(2) of the Numbering Conditions sets out that "*A Geographic number shall only be assigned to an end-user whose residence/business premises is physically located within the designated minimum numbering area (MNA) for that geographic number*". Therefore, operators, including Cloud Service Providers, are required to establish and verify the location of their customers before providing geographic numbers to

customers. The practice of a customer self-declaration of location is insufficient and does not meet this requirement. Evidence of location must be sought by and provided to the operator, e.g. operator to verify a customer's utility bill as evidence of address.

103. In addition, in the case of Non-Geographic Numbers (NGNs) (1800 Freephone and 0818 Standard Rate), operators are expected to request the customer business information set out in sections 4.3 and 4.4 of ComReg 15/136R4 before providing NGNs to customers.

104. When conducting checks, an operator may identify information that could indicate a high-risk customer. Examples of potential indicators are shown in Figure 6 below.

Indicators of potentially high-risk customers
• Incorrect or incomplete information (such as address information)[1]
• For cloud-based telephony providers, not using an Irish IP address or the use of a virtual private network (VPN)
• Signing up outside of business hours (bad actors may try to access telecoms resource outside of business hours to circumvent checks)
• Name, address, IP address, or other information matching a disabled or dormant account with the operator
• The same email address being used to request multiple number assignments
• For purported business customers, use of a generic non-business email address

Note 1: Including instances where address information does not correspond to Eircode

Figure 6: Indicators of potentially high-risk customers

105. It is important to note that, on their own, each of the indicators highlighted in Figure 6 may not identify a potentially high-risk customer, but a combination of the indicators might highlight a potential risk[22].

106. Where potentially high-risk customers are identified, operators should undertake further checks, such as:

- reviewing whether any complaints have been received about phone numbers already allocated to the customer; or
- checking for any unusual activity involving previously allocated phone numbers, e.g. high volumes of calls/texts, particularly where the calls are short or often dropped, or texts are sent over a short period of time.

[22] In the future it may also be appropriate for operators to check against relevant centralised databases, such as the shared fraud database, proposed by the Banking and Payments Federation Ireland (BPFI), intended for banks to share real-time information on fraud cases and other criminal activity with authorities and other banks

107. ComReg expects operators to only provide phone numbers to customers that they are satisfied have met the relevant KYC checks.

Specific measures for eSIMs and cloud based telephony

108. ComReg recognises that some number services may present particular KYC-related challenges for operators, including eSIMs (particularly prepaid mobile) and cloud telephony. For this reason, ComReg strongly encourages operators, where applicable, to adopt the specific measures outlined as follows.

eSIMs

109. MSPs are advised to implement eKYC solutions to ensure information relevant to all customers using eSIMs (particularly prepaid mobile) is gathered and recorded appropriately. In relation, ComReg advises MSPs, where possible, to implement the following minimum measures in their eKYC solutions to identify and verify a subscriber's identity:

Minimum measures expected of a eKYC solution supporting eSIM provisioning process
• Customer name should be provided by the subscriber
• Customer address should be provided by the subscriber
• A photograph of an official ID document[1] should be provided by the subscriber that can be electronically analysed by the operator and verified for authenticity
• A live photograph (selfie) portrait should be taken by the subscriber on a smartphone, suitable for biometric template extraction, which can then be compared electronically by the operator with the portrait in the official ID document

Note 1: An official ID document is considered to be a valid passport, driving licence, or Public Services Card (PSC)

Figure 7: Minimum measures expected of eKYC solution

110. MSPs are also expected to remain informed of the security risks and challenges presented by the use of eSIMs[23], and regularly audit their eKYC measures to safeguard the eSIM provisioning process and mitigate fraud. Operators are also asked to be cognisant of the guidance on Over-The-Air (OTA) provisioning provided in ComReg's strategy to promote OTA provisioning[24].

[23] For example, see https://www.enisa.europa.eu/publications/countering-sim-swapping, and https://www.enisa.europa.eu/publications/embedded-sim-ecosystem-security-risks-and-measures
[24] https://www.comreg.ie/media/2022/06/ComReg-2248a.pdf

Cloud-based telephony

111. Cloud Service Providers and operators providing Internet-based voice communication services, sometimes referred to as cloud-based telephony services, are expected to implement sufficient KYC checks to ensure that geographic numbers are assigned only to customers located in the relevant minimum numbering area (MNA)[25] by verifying the customer's identity and address.

112. ComReg expects such validation to be achieved through the use of an appropriate eKYC solution capable of supporting the measures as set out in Figure 7.

Managing due diligence checks

113. Operators are expected to document the KYC checks they complete before assigning Irish telephone numbers to customers. Operators should have appropriate governance measures in place to ensure that due diligence checks are carried out as intended and that risk assessments are recorded.

114. Operators should consider designating overall responsibility within the organisation for the establishment and maintenance of effective KYC systems and controls to a specific member of their management team.

115. This individual would be tasked with producing regular reports for their organisation covering, inter alia, suspected fraud or number misuse incidents; the status of KYC related projects and training; and the status of action(s) taken in response to recommendations raised in previous reports and/or by ComReg. The same individual should also collaborate with industry peers to share insights on the latest incidents and the effectiveness of emerging tools and solutions.

116. Operators should also consider training requirements relevant to the best practice set out in this guidance for all individuals involved in the process of assigning phone numbers to customers.

4.4 Ongoing compliance and assessment of risk

117. Operators are expected to have measures in place to reassess the risk of phone number misuse after numbers have been assigned, and to address non-compliant behaviour. This can be achieved through clear contract information and ongoing compliance checks, outlined as follows:

[25] See ComReg 15/136R4: Numbering Conditions of Use and Application Process

Contract information

118. To help ensure ongoing compliance following assignment of phone numbers, operators should set out clearly in wholesale and reseller contracts that numbers must be used in compliance with the Numbering Conditions.[26]

119. In particular, CSPs and operators providing cloud-based telephony services should ensure that contracts with their customers clearly articulate that a geographic number shall only be assigned to an end-user whose residence/business premises is physically located within the designated MNA for that geographic number.

Ongoing compliance

120. Operators are expected to monitor the level of risk posed by their customers, and regularly monitor for the potential misuse of numbers. Such monitoring should be tailored to each customer and the level of potential risk that may have been identified.

121. When monitoring for number misuse, operators should consider routinely testing and/or monitoring specific risks associated with a particular customer. For example, operators may wish to check the source IP Address[27], volume and duration of outbound calls generated by numbers assigned to customers and/or the volume of outbound texts sent during certain time intervals and apply a holistic view to determining appropriate use.

122. The frequency of testing should be aligned to the level of risk associated with each customer. For example, a low-risk customer with no history of number misuse will likely require less frequent monitoring than a potentially high-risk customer.

123. Operators are expected to review their risk assessments on an ongoing basis and update them in response to significant changes. Such changes may include:

- the operator receiving complaints about the customer's use of assigned numbers which may indicate a change in the level of risk posed, and
- changes to the customer's behaviour such as the customer refusing to engage with the operator, being obstructive and/or reluctant to provide information.

[26] ComReg 15/136R4: Numbering Conditions of Use and Application Process

[27] While ComReg is aware that IP addresses are not necessarily tied to a given location a cloud provider could implement checks on the originating IP to detect obvious abuse.

4.5 Responding to incidents of number misuse

124. Operators are expected to deal with number misuse incidents quickly and proactively by addressing non-complaint behaviour and investigating incidents of suspected number misuse in a timely manner, as follows:

Addressing non-compliant behaviour

125. Operators are expected to have robust procedures in place to address non-compliant behaviour by its customers. Where there is suspected number misuse, e.g., a large volume of texts originating from a mobile phone number during a short period of time, operators should first engage with the customer to understand the nature of the traffic in question and consider whether it is a problem and how best to resolve it. This may involve increased monitoring or, where appropriate, the suspension or withdrawal of numbers assigned to the customer.

Investigating and reporting incidents of suspected number misuse

126. Operators are expected to develop and maintain processes for handling complaints related to potential and actual misuse of phone numbers. This is expected to include maintaining a record of any investigations, outcomes and action taken in relation to such misuse.

127. Operators should ensure that appropriate action is taken to investigate and resolve incidents of suspected misuse in a timely manner, taking into consideration the severity and urgency of the issue. Consumers and organisations should be able to notify operators quickly and easily of suspected number misuse incidents.

128. As the first point of contact for consumers, telecoms operators are expected to investigate and handle number misuse complaints from their customers. Operators should designate a person/point of contact and clearly communicate how to report suspected misuse e.g., by email or phone call to a dedicated phone number. Complainants should also be made aware of the outcome of any misuse investigation/incident as soon as possible.

129. Operators should, as far as reasonably possible, prevent any further potential misuse once they have been informed or have identified a potential concern.

130. To prevent any further harm to consumers, operators should take appropriate action which may include temporarily blocking numbers or customer accounts, suspending services, or withdrawing numbers. Action taken should be proportionate to the evidence the operator has received and the potential risk posed.

131. Operators are expected to also provide support and information to any affected consumers, and cooperate as appropriate with ComReg, law enforcement and other relevant organisations, including other telecoms operators.

4.6 Continued review and evaluation of processes

132. The tactics employed by bad actors will continuously change; scam calls and texts are proving very lucrative for fraudsters at the expense of the good name of the telecommunications industry and the financial cost of its customers. ComReg therefore expects operators to keep up to date with industry developments and regularly review their KYC processes to ensure they remain robust and relevant. This should include updating processes to incorporate lessons learned from previous incidents of number misuse.

4.7 Conclusion

133. The importance of restoring and protecting trust in telephone numbers cannot be understated. ComReg advises all operators, including cloud service providers, to ensure that KYC checks are built into all stages of number provision processes. Strong KYC will discourage fraudsters from getting access to and misusing Irish phone numbers to the detriment of consumers in Ireland.

134. ComReg anticipates and appreciates operators' assistance and vigilance in this matter. ComReg will keep KYC practices under review and, if needed, may explore introducing mandatory KYC checks, if KYC practices do not improve and the level of scam calls and texts persist across society as a result.

5 Comments

135. ComReg welcomes comments on this document. Please submit comments by email to kyc@comreg.ie by 5.30pm on Wednesday 1 May 2024. ComReg will then publish a final version of this document.