An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Combatting scam calls and texts

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

Consultation

Reference: ComReg 23/52

Date: 16/06/2023

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

Additional Information

Approval

Legal Disclaimer

This Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Commission for Communications Regulation is not bound by it, nor does it necessarily set out the Commission's final or definitive position on particular matters. To the extent that there might be any inconsistency between the contents of this document and the due exercise by it of its functions and powers, and the carrying out by it of its duties and the achievement of relevant objectives under law, such contents are without prejudice to the legal position of the Commission for Communications Regulation. Inappropriate reliance ought not therefore to be placed on the contents of this document.

Content

Section Page

Annex

Section Page

List of Tables and Figures

Table — Page

Figure — Page

Executive Summary

Introduction and background

1.1 Nuisance communications or scam calls and texts refers to a range of unwanted, unsolicited communications that have the clear intent to defraud by misleading the receiver, so that they unknowingly provide sensitive personal and financial information. Scams are a blight on society and cause significant financial and economic damage to all sectors of society including consumers, business, and public bodies. They 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.

1.2 Telecoms end-users, civil society, and governments are increasingly concerned about this issue, and urgent action is required by all stakeholders to help combat this now daily scourge. To this end, this consultation proposes the mandating of certain specific interventions by ComReg to combat scam calls and texts.

1.3 Recent years have seen us become increasingly reliant on fixed and mobile networks to communicate with one another. We spend approximately **15 billion minutes every year** talking to family, friends, colleagues and businesses, while also sending around **2.5 billion SMS text messages** per annum. While new communications channels have emerged, consumers' use of Voice and SMS remains high and continues to facilitate consumer and business communications. Such services are also critical to the delivery of important public and social services. This was ably demonstrated during the Covid-19 period where services were progressively delivered through calls and SMS texts - an extra 1.5 billion call minutes a year were received due to Covid-19.

1.4 Lately however, fraudsters, internationally but also domestically, have turned to using these networks to target anyone with a phone, and this has seen scam calls and text fraud increase substantially. Cloud security specialists have calculated that 2022 had the highest percentage of mobile phishing encounter rates ever - with over 30% of users exposed every quarter. **Ireland, as an English-speaking country** with a developed economy, is disproportionately targeted compared with our EU neighbours. Our dependence on telecoms technology is now being exploited by criminals, who often use social engineering type attacks with the intention of illegally acquiring personal and financial information, ultimately to abet financial fraud.

1.5 There is now evidence that chatbots are being used to remove grammatical and spelling errors, which until now have often been a hallmark of SMS smishing. More broadly, experts have sounded a warning on Artificial Intelligence ("AI") as it becomes increasingly sophisticated and harder to detect. AI can now

generate photorealistic images and convincingly replicate people's voices, further broadening the threat landscape.

Importance of trust and why it's being lost

1.6 People need to trust that those contacting them are genuine; otherwise, avoidance will result in legitimate and potentially important calls and texts going unanswered. People answer calls and read text messages in the anticipation that the caller or sender is someone they know or with a legitimate reason to contact them, or a business providing services of value to them (for example banking and postal delivery). Until recently, we trusted that the calls and text messages we received were genuine. Irish numbers and Sender IDs should provide consumers with information they value (e.g., geographic location/ name organisation) which increases the chance of answering a call or reading a text.

1.7 Unfortunately, fraudsters have taken advantage of our trust in telecommunications. As a result, there has been an increasing prevalence of scam calls and texts with fraudsters routinely impersonating a range of business and government agencies, including public health and law enforcement. Such scams make consumers wary of answering calls and reading text messages, thereby seriously diminishing the ability of genuine callers or senders to deliver services.

1.8 Scam calls and texts inevitably reduce the trust consumers place in those services. Understandably, many Irish consumers no longer trust the number displayed on their phone when it rings, or the identification on their text message, because of previous bad experiences. A Behaviour & Attitudes ("B&A") Survey commissioned by ComReg for this consultation offers a disturbing picture of how trust in calls and texts has deteriorated. For example:

- **Around half of consumers** now require some confirmation of the legitimacy from the caller or sender of a text or they will cease the voice or text exchange.
- Over **40% of consumers that use SMS services**[1] **have lost trust** in these communications and increasingly pay less attention to them. **One in four** consumers pay no attention at all to SMS messages that they receive.

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

1.9 Absent intervention, trust will continue to decline threatening the very use of telecommunications services and the networks that provide them. This also has serious consequences for the delivery of public services. The HSE and An Garda Síochána, among others, have outlined to ComReg the serious repercussions that this lack of trust in calls and texts brings, increasing incidence of missed health appointments and the diversion of scarce public service resources to deal with the repercussions.

Harm to consumers

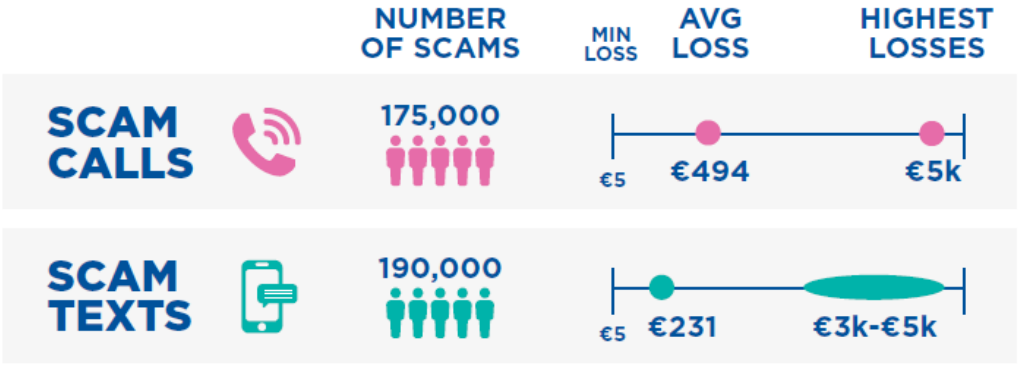
1.10 To determine the extent of the problem and identify what regulatory measures may be necessary, ComReg commissioned Europe Economics to estimate the extent of the harm and to assess appropriate interventions. The frequency of Nuisance Communications in Ireland is stark. **Over 90 per cent of adults in Ireland have received a scam call** to their mobile phone in the last year, while **84 per cent have received some form of scam text**. The most impersonated organisations are banks along with postal and courier services but followed closely by the HSE and other public bodies.

1.11 The statistics published by the Central Statistics Office ("CSO") are dependent on the provision of data by An Garda Síochána. However, long standing evidence suggests that scams of this type are grossly underreported to police authorities. This occurs for a multitude of reasons, including that consumers feel too embarrassed to report the crime, amounts taken are relatively small, or simply not knowing who to contact.

1.12 The research commissioned by ComReg provides the first insight into the **likely number of people defrauded** due to Nuisance Communications. It is estimated that there were **approximately 365,000 cases of fraudulent scams** in Ireland over the last 12 months. While financial fraud affects all demographics, **young people under 25 years account are by far the most impacted group, accounting for 40% of all fraud cases.**

1.13 Not every instance of fraud is the same, with the financial harm ranging from small to relatively large amounts, however the soaring number of cases is a cause of concern. It is estimated that **175,000 people** were defrauded after receiving scam calls with a median loss of around €200, while **190,000 people** lost around €100 after receiving scam texts.

Figure 1: Financial Fraud from scam calls and texts



1.14 However, the harm due to scam calls and texts is not just limited to direct financial fraud, there are also significant impacts upon people's wellbeing and emotional state. It is estimated that scam calls and texts in the last year were responsible for up to:

- **89 million annoying/irritating** communications; and
- **31 million distressing** communications.

1.15 Scams can take a steep emotional toll on people, and research commissioned by ComReg shows that scams impact individuals' health and well-being, regardless of whether they have experienced financial loss or not. Constant scam attempts can increase stress levels and negatively impact people's mental health which is even more insidious when the fraudsters target those most vulnerable who are often older, lonely and/or managing an illness. Older people also show significantly higher levels of concern about being scammed, and this instils fear and anxiety about engaging in calls where the number or service is unfamiliar to them.

Harm to business and public bodies

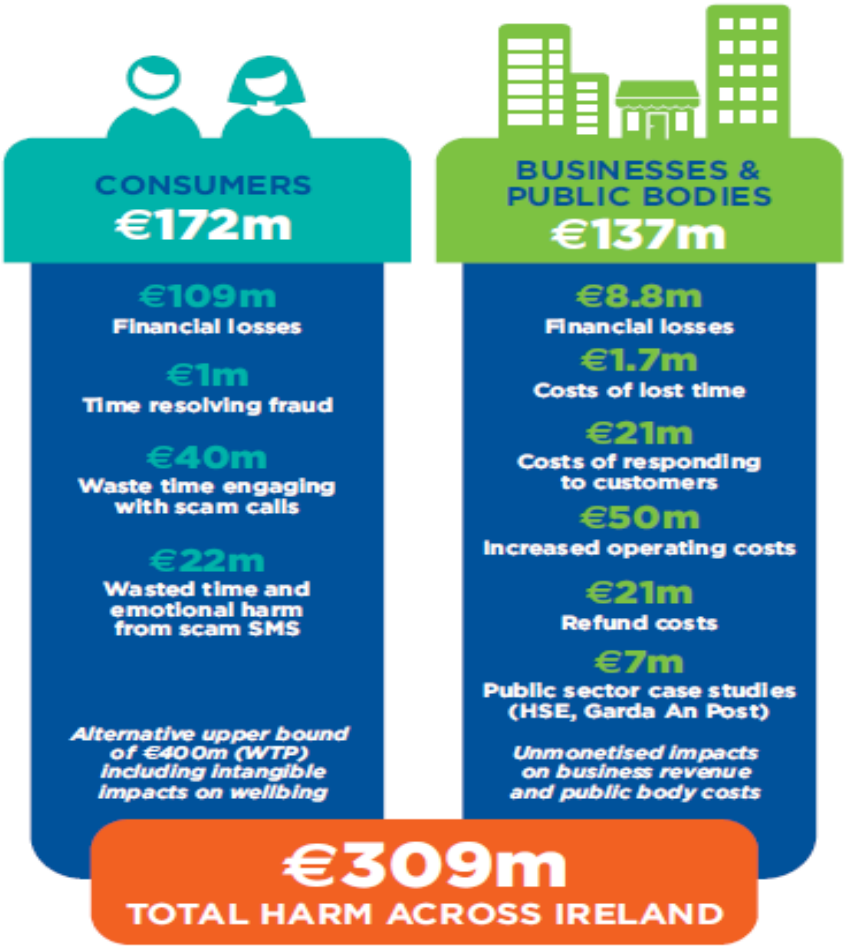
1.16 Of course, there is also significant harm caused to businesses by nuisance communications. Firms use voice and text communications to generate revenues of approximately €48 billion every year but scam calls and texts pollute the channels used by business to communicate with consumers.

I. It is estimated that **over 5,000 businesses have been the victim of fraud after receiving scam calls and texts in the past year,** amounting to **over €8.8 million in the past year alone**.

II. The time and resources spent resolving customer problems and responding to customer queries **is estimated to be €21 million last year**.

III. **Approximately one in three businesses have implemented scam-prevention measures** (for example new software/programmes, staff training, moving to alternatives etc)**, with costs estimated at €50 million last year**.

Figure 2: Economic and social harm from calls and texts in 2022



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

What action can regulators and policy makers take to combat fraudsters?

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

because some organisations who rely heavily on telecommunications, for example in the financial and logistics sectors, appear to have yet to grasp the fundamental role that they too can play in ensuring the integrity of their end-to-end delivery paths.

1.19 What is undeniable is that more action is needed to protect consumers, both now and in the future as fraudsters adapt to regulatory measures. **Two out of three adults state that regulatory intervention would increase their trust in calls and texts** which provides a sound basis for restoring trust by implementing effective regulatory intervention. In that regard, ComReg has identified several technical and regulatory interventions which should significantly impact the volume and effectiveness of scams that reach Irish consumers.

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

1.21 The purpose of this consultation therefore is to determine what package of interventions best reduces and mitigates the harm caused by scam calls and texts. ComReg is proposing a package of Voice and SMS interventions which it considers would best deal with the ongoing scourge of nuisance communications at this time. Real-world experience of these interventions in other countries is encouraging and provides convincing evidence of their effectiveness with significant declines in the rates of scam calls and texts following their introduction. This package should therefore significantly reduce, though not fully eliminate scams and their harm, not least because fraudsters will continually try to circumvent any interventions imposed by ComReg.

Voice Interventions

1.22 ComReg is proposing **five measures** to reduce harm and restore trust in voice communications. It is proposed that the first four measures would be put in place **within six months** of ComReg's final Decision and are designed to address obvious vulnerabilities and reduce fraud in an expedited fashion.

a) **A Do Not Originate ("DNO") list** refers to phone numbers which are never used for outgoing calls. For example, certain banks provide numbers for consumers to contact them, but they never contact a consumer using the same number. Consequently, any calls that appear

to come from these numbers are spoofed and therefore should be automatically blocked.

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

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

d) **Fixed CLI Call blocking** operates in the same way as mobile CLI call blocking but blocks nuisance calls that are spoofing Geographic Numbers (e.g., 01, 061) and/or the non-geographic numbers that businesses use (e.g., 0818).

1.23 These initial interventions should help reduce nuisance calls, however of themselves they will not be enough to combat scam calls which can still originate from valid numbers within Ireland rather than abroad (e.g., primarily using pre-pay phones). Further, scams are likely to become increasingly sophisticated as scammers adapt to the initial interventions. Therefore, ComReg also proposes to introduce a **Voice Firewall** over a period of 18 months.

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

SMS interventions

1.25 ComReg proposes two interventions to reduce the harms associated with scam SMS messages.

a) ComReg would establish a **Sender ID Registry** which would allow businesses to register their Sender ID. Telecommunications providers would then block any message bearing a Sender ID from any source other

than in the registry. In this way, fraudsters would be unable to pose as legitimate businesses to mislead consumers.

b) A **SMS Scam Filter**[2] that operates like the spam filters that are applied to email inboxes by detecting and blocking harmful links or content that encourages you to click on the link and then install malware or enter personal information, that is used in turn to commit fraud using that consumer's details.

1.26 The SMS Scam Filter is an essential measure to prevent criminals from attempting to defraud Irish customers because, like the voice firewall, it is a dynamic intervention that reacts to the latest scams. A fully effective SMS Scam Filter requires anti-scam software to scan the content and location data of an SMS to identify potentially suspicious or malicious content (e.g., fraudulent URLs). Such an intervention requires a legislative basis.

1.27 ComReg is fully engaged with its parent department, the Department of the Environment, Climate and Communications ("DECC") in driving this issue forward. Within the European Union, equivalent legislation is already in place in Belgium, and is proposed to be implemented in Poland. Ireland is also part of the *anglosphere* and as such is markedly more susceptible to text-based scams using the English language than its European counterparts. As the drawbridge is being raised in countries such as the United States, United Kingdom, Canada and Australia, it is crucial that Ireland follows suit as any torpidity on its part would leave Irish citizens even more exposed to fraud.

1.28 The continuing absence of a SMS Scam Filter would run the risk of undermining interventions to reduce nuisance communications because fraudsters will simply target Ireland, and SMS communications, if effective interventions are introduced for Voice, but not for SMS. Any package of interventions must be cognisant of the ability of fraudsters to readily switch across scams, platforms, and territories. Appropriate legislation is essential to this end as without it, ComReg nor the operators can do little else to stymie the spread of text-based fraud.

Cost and benefits of interventions

[2] SMS content scanning is a capability that is necessary to enable the eventual, and desirable, deployment of a SMS Firewall by Irish mobile operators. A SMS Firewall defends mobile networks against all SMS-based messaging attacks and provides full protection and control over all messaging on the network. All messages are routed through the firewall, analysed, classified and where necessary blocked. Without SMS content scanning, only a rudimentary evaluation of SMS is possible.

1.29 The relatively modest costs of these interventions will primarily be borne by the telecoms operators that implement them. However, as some operators have readily acknowledged, interventions to curtail scam calls and texts should increase trust in those services, safeguarding operators' long run commercial interests by being able to offer services and networks worthy of consumers' continued trust. As their continuing commitment to ComReg's NCIT attests, operators are very aware of the damage fraudulent calls and texts can do to their business and reputation. Nevertheless, the B&A survey shows that **only 16% of consumers think that operators have done enough to protect them from scam calls and texts.**

1.30 Speedily implementing these interventions provides operators with a prime opportunity to further demonstrate their commitment to protecting consumers from criminals and ensuring that the services they provide can be trusted. ComReg also notes that some operators have defended their recently announced annual price increases (first increase commenced in April 2023) based on generating revenues to finance investment in the upgrade of networks and services. It is inconceivable that such upgrades would not include measures to protect their customers from criminals who are committing fraud using the very same services provided over their networks.

1.31 Finally, ComReg notes that analysis conducted by Europe Economics shows that the overall benefit of the package of interventions implemented would be in the order of **€1.5 billion** over the next seven years**.** In summary, the benefits to society for each euro spent on the interventions is substantial and highlights the importance of implementing them all in a timely manner. When combined, ComReg's proposed interventions should bring **€50 euros in economic and social benefit for every €1 spent securing networks.**

Next Steps

1.32 ComReg invites views from interested parties on all aspects of this Consultation over the next 6 weeks, before 5pm on 28 July 2023. Recognising the breadth of issues covered in this consultation, ComReg has given an additional two weeks over the normal four weeks identified in ComReg's Consultation Procedures[3].

1.33 Following receipt and consideration of submissions in response to this document, and other relevant material, including the Europe Economics Report, ComReg intends to publish a response to consultation and final decision for Nuisance Communications in Q4 2023.

[3] See ComReg Document 11/34

Chapter 1

1 Introduction

1.1 Background and Purpose

1.1 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.

1.2 In its Electronic Communications Strategy Statement for 2023 to 2025 (Document 22/109)[4], ComReg set out its intention to undertake a number of tasks in relation to nuisance communications, not limited to:

a) a gap analysis to identify further measures that may be taken, including more dynamic interventions.

b) proactive monitoring of trends in nuisance communications both in Ireland and abroad;

c) formalising inter-operator and cross-sector cooperation and coordination;

d) identifying actions for industry and ComReg to raise consumer awareness of scams;

e) ultimately, developing an overarching long-term national strategy to combat nuisance communications; and

f) contributing to international regulatory initiatives to promote an international approach, as appropriate.

1.3 In September 2022, ComReg published an Information Notice (Document 22/77[5]), which was an Update on the work of the Nuisance Communications Industry Taskforce, which committed to a policy consultation on potential actions ComReg, and operators may take to combat Nuisance Communications (see Section 2.6 below), noting that:

"*The NCIT has been working at pace to tackle the scourge of nuisance*

[4] ComReg 22/109: Electronic Communications: Draft Strategy Statement 2023-2025 see https://www.comreg.ie/media/2022/12/ComReg-22109a.pdf
[5] ComReg 22/77: Nuisance Communications - Update on the Nuisance Communications Industry Taskforce see https://www.comreg.ie/publication/nuisance-communications-update-on-the-nuisance-communications-industry-taskforce

communications. Appropriate regulatory underpinning has not been overlooked however, and to that end ComReg aims to launch a major policy consultation in early 2023."

1.4 Nuisance Communications are a multi-faceted problem that require a multi-faceted response. In essence, scams are the result of fraudsters using networks to contact and deceive consumers. Any national strategy to combat scams should encompass actions to a) trace, catch and prosecute fraudsters, b) secure electronic communication networks and c) increase consumer awareness of scams[6].

1.5 ComReg considers interventions that prevent fraudsters using networks and numbers to reach Irish consumers are critical, as networks and numbers are both regulated and the bottleneck through which scams travel – this is the focus of this consultation and ComReg's work in this area. Notwithstanding, ComReg considers that its work could help inform the work of the Department of Justice's Advisory Council against Economic Crime and Corruption[7] which is tasked with developing a national strategy to combat economic crime including fraud.

1.6 Accordingly, this Consultation aims to consider and identify what technical interventions are required to combat Nuisance Communications[8] and reduce the economic and societal harm caused to Irish consumers, businesses and society, in accordance with ComReg's statutory functions and objectives and duties. The Consultation addresses:

a) The economic and societal harm caused by Nuisance Communications;

b) The potential interventions that may be undertaken to remedy this harm, including the technical specifications of each of the interventions.

c) The potential cost and benefits of implementing a package of interventions and which form part of relevant to ComReg's preferred policy options;

[6] Indeed, the UK government recently indicated that it will adopt this approach in its recent plan to combat fraud ""*Economic crime Plan 2*"" Link "*The forthcoming Fraud Strategy will set out how the government will cut fraud… Through the new Strategy we will: • Pursue fraudsters, disrupting their activities and bringing them to justice more often and quicker* • ***Block frauds at source by dramatically reducing the number of fraud and scam communications that get through to the public*** • *Empower people to recognise, avoid and report frauds and equip them to deal easily and appropriately with frauds that do get through.*""

[7] Department of Justice "*Review of structures and strategies to prevent, investigate and penalise economic crime and corruption - Report of the Review Group*" Link

[8] This refers to scam calls and SMS made over public networks. Other mediums for scams such as emails or number independent communications platforms (e.g., emails or Over-the-Top applications) are outside the scope of this particular Consultation.

d) ComReg's assessment of the potential interventions against ComReg's statutory objectives in a number of draft Regulatory Impact Assessments ("RIAs"); and

e) The Draft Decision Instruments for the preferred package of interventions.

1.7 ComReg is also consulting on its Draft Technical and Functional specifications for each intervention, which outline ComReg expectations for the implementation of each intervention. These are only available upon request to relevant undertakings that would be involved in their implementation – please contact marketframeworkconsult@comreg.ie to request a copy[9].

1.8 Further, this Consultation contains Draft updates to the Numbering Conditions of Use and Application Process document ("Draft updated Numbering Conditions") (23/52d)[10] which ComReg is minded to adopt in order to enable the preferred package of interventions and combat scams more generally.

1.9 This Consultation is accompanied by an Information Notice which provides and overview and summary of key components of this plan ("Consultation Overview") (Document 23/52e)

1.2 Information gathering

1.10 ComReg commissioned Behaviour & Attitudes[11] to conduct consumer ("B&A Consumer Survey") (Document 23/52b) and business surveys ("B&A Business Survey") (Document 23/52c) to better understand the prevalence and impact of Nuisance Communications on Irish consumers and businesses.

1.11 ComReg also commissioned Europe Economics[12] (Document 23/52a) (the "Europe Economics Report") to assist in estimating the harm from Nuisance Communication to the Irish economy and society and to conduct a cost benefit analysis of the potential interventions to reduce this harm. The Europe Economics Report was informed by information gathered from various sources, including:

a) The B&A Consumer Survey and the B&A Business Survey;

b) Interviews conducted by Europe Economics and ComReg with civil society stakeholders (the "Stakeholder Interviews"), including:

[9] Please mark the email FAO Donnacha Hennessy.
[10] These are proposed updates to the existing *ComReg 15/136R3 -* Numbering Conditions of Use and Application Process
[11] 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.
[12] 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.

- impersonated businesses (e.g., Irish retail banks, An Post);
- impersonated government agencies (e.g., HSE); and
- agencies involved in law enforcement (the National Economic Crime Bureau of an Garda Síochána, Europol) and the Central Statistics Office ("CSO") to discuss methodological issues in recording fraud in Ireland.

c) Interviews conducted with industry stakeholders such as MNOs, security specialists and vendors of security solutions;

d) Interviews conducted by ComReg with fellow National Regulatory Authorities ("NRAs"), as well as the responses received from 19 NRAs to a Request for Information ("RFI") sent by ComReg in December 2022 to members of the Independent Regulators Group[13] ("IRG") (the "IRG RFI"); and

e) Information and metrics provided by members of the NCIT.

1.12 ComReg seeks and welcomes the views of interested parties on all aspects its preliminary findings set out herein which will be used to inform ComReg's future development of a strategy to combat Nuisance Communications.

1.3 Structure of this document

1.13 The remainder of this document is structured as follows:

- **Chapter 2:** Background information
- **Chapter 3:** Economic and social harms from Nuisance Communications
- **Chapter 4:** The potential technical interventions to combat Nuisance Communications
- **Chapter 5:** Draft Regulatory Impact Assessments
- **Chapter 6:** Updating the Numbering Conditions
- **Chapter 7:** Draft Decisions Instruments
- **Chapter 8:** Making a submission and the next steps
- **Annex 1:** Econometric analysis of victims of fraud

[13] The Independent Regulators Group is a group of European National Telecommunications Regulatory Authorities that functions as a forum for exchange of best practices and discussions on regulatory challenges in communications between NRAs.

- **Annex 2:** Provides information on ComReg's Legal Framework and Statutory Objectives.

Chapter 2

2 Background

2.1 In this Chapter, ComReg sets out some relevant background information to ComReg's assessment of the harm due to nuisance communications and the potential interventions that could reduce same, including information on the following:

- The importance of Voice and SMS communications;
- The importance of Irish telephone numbers;
- What are Nuisance Communications;
- Fraudsters and scams;
- The recent increase in scam calls and texts;
- ComReg's work to date; and
- The work of other NRAs.

2.1 The importance of Voice calls and SMS to Irish society

2.2 Telecommunications services are essential to our everyday lives and allow us to keep in touch with our family and friends while engaging with businesses for goods and services. Voice calls and SMS are unique among calling and messaging services in that they are universally installed and activated on mobile devices by default, unlike alternatives which are reliant upon a consumer downloading the application to their device (e.g., WhatsApp etc).

2.3 Irish businesses rely upon Voice and SMS texts for conducting their sales and business operations (with only 13% of Irish companies reporting no use of either technology). Firms that use voice and text communications as part of their revenue generating strategies earn revenue of approximately €48 billion through the use of these services, and scam communications puts this in jeopardy by making it more difficult for organisations and consumers to communicate with one another.[14]

Voice calls

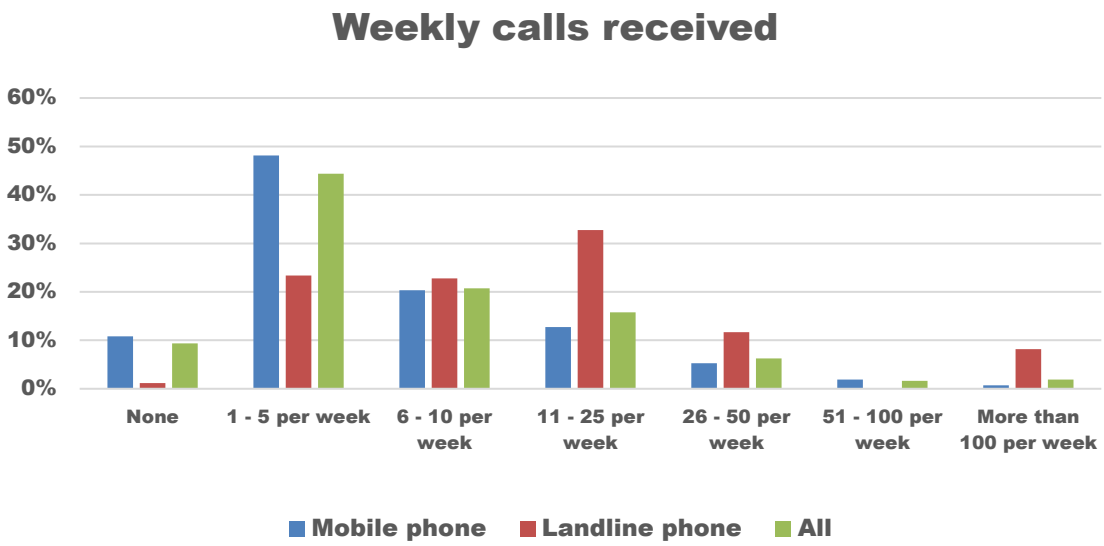
2.4 A Voice Call is a connection over a telephone network between the called party and the calling party that enables people to hold conversations and communicate information in real time. This makes Voice Calls an instantaneous

[14] See Europe Economics Report – Page 54.

means of transmitting information between people, critical to the daily life of many consumers and organisations.

2.5 There are approximately 6.9 million voice capable subscriptions[15]. Over the past year, Irish mobile and fixed networks carried over 14.6 billion Voice minutes. As illustrated in Figure 3, on average mobile users receive 10 calls per week.

Figure 3: Weekly voice calls received by mobile or landline, Q4 2022



Source: ComReg analysis of B&A Consumer Survey[16]

2.6 Voice services are also critical to delivery of important public and social services. This was ably demonstrated during the Covid-19 period where services were increasingly required through calls and text message (e.g., an extra 1.5 billion minutes a year were received due to Covid-19). While new communications channels have emerged, consumers use of Voice and SMS remains high and continues to facilitate consumer and business communications. Voice services are critical to Irish businesses, with 84% reporting using Voice calls for their business operations, 72% to contact other business, 58% to facilitate communication between staff and 56% to connect with end-customers[17].

Short Messaging Service

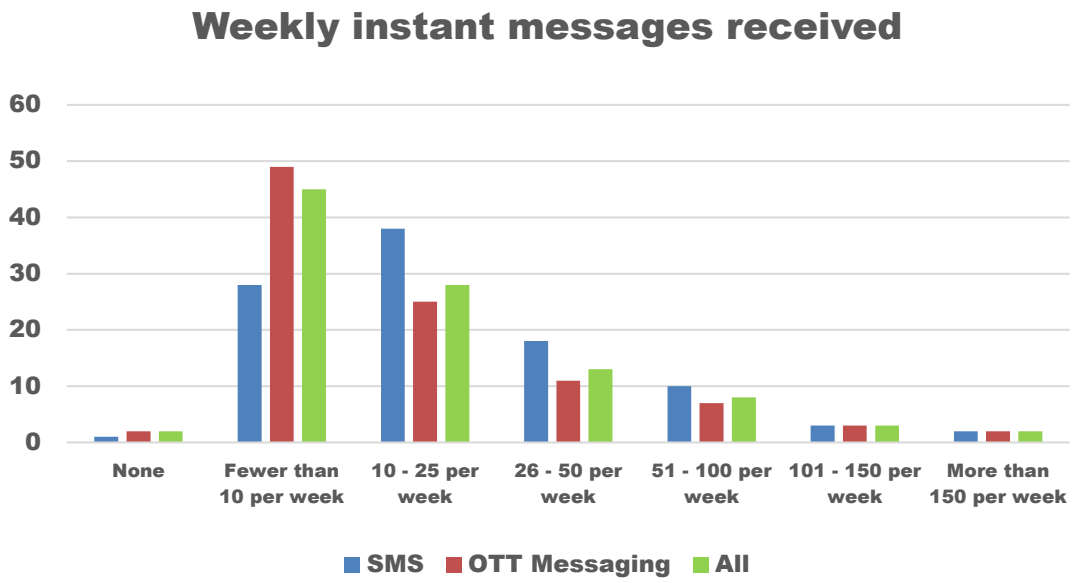
2.7 Short Messaging Service ("SMS") is a text messaging service component of all mobile phone networks. SMS uses standardised communication protocols that let mobile devices exchange short text messages. SMS rolled out commercially

[15] ComReg QKDR data for Q2 2023. Using the traditional Voice networks - this excludes other devices (e.g., laptops) which may receive Voice calls transmitted using VOIP.
[16] Q3 "*Approximately how many calls do you receive on your mobile phone per week?*" and Q4a "*What is the main way in which you make and receive calls, by mobile or landline?*"
[17] B&A Business Survey, slide 9.

as part of 2G mobile networks and became hugely popular worldwide as a method of text communication and transmitting information to mobile devices.

2.8 There are approximately 5.7 million subscriptions for consumer devices capable of receiving a SMS[18]. Notwithstanding the success of other messaging apps, significant volumes of SMS are still sent and received every quarter, with 2.5 billion texts being sent in the 12 months to Q2 2022. While many consumers now use OTT messaging applications, such as WhatsApp, as their primary means of P2P messaging, 22% of Irish consumer still rely primarily on SMS[19] with higher rates of use for older people (65+)[20]. On average, consumers receive approximately 25 texts a week.

Figure 4: Weekly instant messages received by preferred channel, Q4 2022



Source: ComReg analysis of B&A Consumer Survey data[21]

2.9 SMS remains an important means of communication for certain cohorts of the population in particular as it is generally considered to be the only truly universal messaging service, not relying on both parties to have downloaded an OTT app. As a result, SMS continues to be an important method of communications between businesses and their customers ("B2C"). While P2P communications have moved to OTT applications over time, the importance of SMS to B2C has if anything increased, with the majority of Irish:

[18] As of Q2 2023. Using the traditional Voice networks - this excludes other devices (e.g., laptops) which may receive Voice calls transmitted using VOIP.
[19] B&A Consumer Survey Slide 9
[20] Europe Economics Report, Figure 4.13
[21] B&A Consumer Survey - Q.4b "*Approximately how many text messages do you receive per week?*" and Q.5 "*Main way of sending and receiving instant messages?*"

a) businesses reporting some use of SMS (65%), to either contact other business (35%), communicate between staff (45%) or connect with end-customers (36%)[22]; and

b) consumers reporting some use of SMS for some B2C activity (66%) (e.g., reminders for appointments)[23].

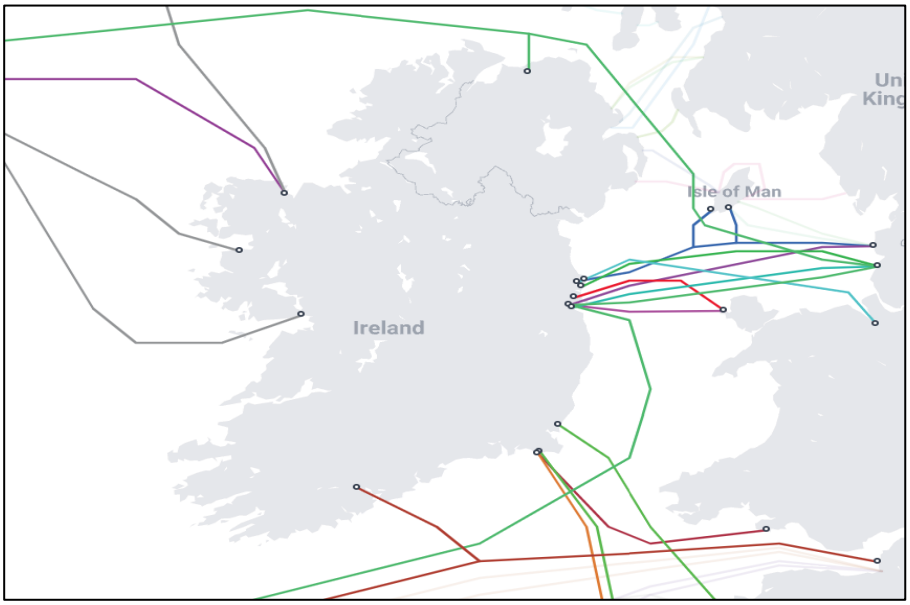
2.10 SMS is not only used for the purpose notifying consumers of offers or appointment offers, but also increasingly for new uses such as customer authentication or verification for of services (e.g., Know Your Customer ("KYC")[24] for a new app, two-factor authentication ("2FA") for financial transactions). In contrast with P2P, for B2C SMS can complement (rather than substitute) many OTT applications, being used to facilitate consumer sign up or verification. (i.e., SMS is used for verifications of OTT applications).

Transit of international traffic

2.11 Operators originate voice calls and SMS on fixed or mobile networks before sending the call or text toward its intended recipient. Calls and texts that both originate and terminate in the state are handed over directly between domestic operators, in many cases without ever leaving the state. However, a significant share of calls or texts reaching Irish consumers originate abroad and must be delivered to domestic operators by foreign operators via one of a small number of international gateways (ingress), typically after being carried via a submarine cable terminating on the Island of Ireland (see Figure 5**Figure 5** below). Operators that provide this service for Voice calls are known as International Gateway Operators ("IGOs") [25]. Although accounting for a small share of overall Voice Calls (approximately 8% by minutes[26]), it is understood that the bulk of scam calls originate abroad and reach Irish consumers via these channels (although ComReg understands from An Garda Síochána that scam calls originating in Ireland are increasing).

[22] B&A Business Survey, Slide 9.
[23] B&A Consumer Survey
[24] Know Your Customer is the often-mandatory process of identifying and verifying a customer's identity, for example when opening a bank account and periodically over time.
[25] ComReg has identified 14 IGOs from an information request issued in January 2023 to the companies on the numbering list. All IGOs originate traffic and are therefore a subset of the 30 known Fixed line and mobile Originating Operators.
[26] IGO RFI

Figure 5: Submarine cables connecting to the Island of Ireland



Source: Submarinecablemap.com

2.2 The importance of Irish telephone numbers

2.12 Telephone numbers are an integral part of both fixed and mobile electronic communications networks and services worldwide. Numbers are critical to the routing of Voice calls and SMS and also convey information which consumers may find useful (e.g., geographic location), enabling consumers to understand of the source and authenticity of incoming Voice calls or SMS.

2.13 The trust Irish consumers have in Irish numbers influences the likelihood of consumers and businesses making and receiving calls, and thereby the benefits of ECS and ECN itself. However, this trust has been exploited by fraudsters who now use the numbering platform to perpetuate fraud on consumers. Until the late 20th century, when the vast majority of voice telecommunications consisted of fixed telephony, each telephone number routed calls to a unique subscriber address, with geographic relevance identifiable within each subscriber number. Today such numbers, known as **Geographic Numbers** ("GNs"), are still linked to a particular geographic region that is identifiable from the area code (e.g. '01' for Dublin, '061' for Limerick)[27].

2.14 But, because of the growth in mobile telecommunications and other telephony services, further number ranges such as Mobile Numbers and non-geographic numbers (NGNs) have been introduced.

[27] There are 50 Area Codes (excluding the 048 code for Northern Ireland). Within these Area Codes there are Minimum Numbering Areas (MNAs). There are 106 MNAs in Ireland. See https://www.comreg.ie/industry/licensing/numbering/area-code-maps-2/

- a NGN is a type of telephone number that is not linked to a particular geographic location identifiable from the number i.e., a NGN does not identify the call termination point. ComReg has consulted extensively on NGNs[28] and introduced measures to address the cost of using such numbers and to tackle confusion among consumers about the differences between the numbers. There are now only two Non-Geographic Number ("NGN") ranges, 1800 Freephone and 0818 Standard Rate.

- Mobile Numbers are numbers assigned to the use of Mobile telephony services, primarily for P2P communications (e.g., 083, 085, 086, 087 and 089). Mobile Numbers do not contain geographic information of any significance, other than to indicate that the SIM was provided in Ireland. Nevertheless, Irish consumers likely recognise such numbers as relating to a resident of Ireland. Mobile Numbers have taken on additional importance in recent years, with the increased use of SMS for 2FA, as a means of customer identification.

2.15 **Calling Line Identification**[29] ("CLI") Caller ID or CLI, provides the receiving end of a call with a number for the calling phone. CLI is often used to identify the caller or the geographic location from which a call originated, or to enable saved contact names for known numbers to appear on the recipient device. Companies such as those with call centres can often choose a CLI for their outbound calls so that the telephone number used enhances the ability of the call recipient to identify the company trying to contact them (e.g., the customer of a bank may already have the telephone number being used as the CLI stored in their phone address under their bank name)

2.16 Similarly, for SMS a sender may supplant the mobile number with alphanumeric text, known as a **Sender ID**[30]. This is typically done by businesses/organisations to facilitate recognition of their text messages by consumers, who are unlikely to recognise or memorise the business's entire mobile number. For example, for most mobile users the Sender ID is their phone number, while a business or organisation may choose to display its trading name instead of its phone number (e.g. "An Post", "BOI").

2.3 What are Nuisance Communications

2.17 The daily use of electronic communications networks and services is exploited by criminals, who use social engineering type attacks, with the intention of

[28] Non-Geographic Numbers | Commission for Communications Regulation (comreg.ie)
[29] Calling Line Identification (CLI) is the number presented or displayed by the party making a telephone call to the recipient of that call.
[30] Note that the term Sender ID in this document generally refers to the case where an alphanumeric business name is used rather than a phone number.

illegally acquiring personal consumer information, ultimately to abet financial fraud (though a wide array of other harms are caused by it – see Chapter 3). Such scams can take many forms, however in each case the fraudster aims to secure a financial payoff from either taking over a consumer account or tricking a consumer into making one or more payments to the fraudster. Such practices include[31]:

- **Vishing** – a phone call designed to get you to share personal information and financial details, such as account numbers and passwords. A seemingly genuine number is displayed to gain your trust and encourage you to share information. The vishing attempt may sound robotic (see Robocall below).

- **Smishing** – a SMS message designed to gain your trust and encourage you to share information) and is where text messages are sent to trick you into clicking on a malicious attachment or link.

- **Wangiri** – short calls or faked missed calls prompt you to call back an international number. The call-back provides financial benefit for the fraudster often at the expense of the caller.

- **Tech Support Scam Calls** – calls where a fraudster claims to offer a technical support service. The fraudster typically attempts to get consumers to allow remote access to their computer. After remote access is gained, the fraudster attempts to gain your trust to pay for supposed "support" services, steal your credit card account information or to persuade you to log in to your online banking account.

- **Robocall –** calls generated automatically, where you hear a recorded message that often sounds as if it was a robot listing options that, if selected, would connect you to the fraudster

2.18 Recent scam calls and texts have also involved "spoofing", whereby the fraudsters impersonate a legitimate Irish business or organisation by presenting their name or number or pretend to be based in Ireland by presenting an Irish number. This greatly increases the effectiveness of scams by misleading consumers as to the identity of the originator of the call or SMS text. There are two main spoofing practices.

- **CLI Spoofing** where the CLI (Caller ID) has been faked by a fraudster and appears to be a call from a genuine number or business. In effect, it appears that an incoming call is coming from a local number that is already known and trusted to the receiver.

[31] See Chapter 4 of the Europe Economics Report for further details.

- **Sender ID Spoofing** occurs when the number or name as displayed on a recipient device's screen has been faked by a fraudster and appears to be a SMS from a genuine business or organisation. In effect, it appears that an incoming SMS is coming from a local business or organisation that is already known and trusted.

2.4 Fraudsters and scams

The stages of a scam

2.19 Almost all scams are comprised of four key stages, whereby a fraudster will:

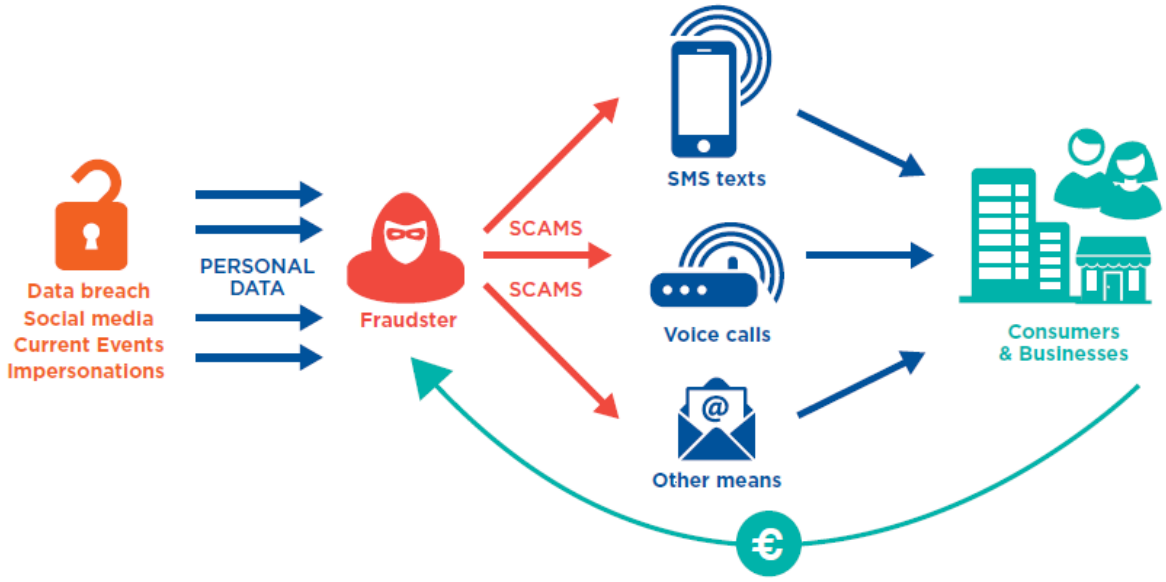
1. **Conspire** – The fraudsters plan their scam, after gathering information on their targets and devising a suitable premise.
2. **Connect** – The fraudsters then connect with the target(s) via communication channels such as Voice call or SMS.
3. **Convince** - The fraudsters then, through conversation or the content of the message, convinces the target of the need to make a payment or provide their personal information.
4. **Close** - Finally, the victim either makes the payment or provides their personal information, after which the fraudster will secure or conduct the payment and terminate the connection.

Figure 6: The four stages of a scam

Fraudsters use telecommunication networks to commit fraud

2.20 Fraudsters utilise public, international ECS networks to contact consumers in Ireland and other countries by SMS and Voice calls. Scam operations are typically operated by criminal groups which can commit scam calls and SMS both within the same country and from other countries. International fraudsters often target wealthier countries, in particular those with more common, widely shared languages such as English. Hence, fraudsters have the ability to contact consumers to elicit information and/or payments from a consumer to complete their fraud. Without such networks, fraudsters would be limited in how many potential victims they can reach.

Figure 7: How fraudsters use telecommunication networks to commit fraud



2.21 Fraudsters can use consumers own genuine information to persuade them of the authenticity of the scam (e.g., using the targets own name, showing a consumer the last 4 digits of their bank account). In this way, weak network security and data breaches fuel scams. Fraudsters often use lists of personal information in combination with phone numbers that have been obtained through various means, such as

- buying them from illicit data brokers;
- extracting them from malware-infected devices;
- stealing them from other companies in data leaks; and

- increasingly, obtaining or complementing such information with information on potential victims garnered via social media. Using such sites, fraudsters can identify and impersonate the friends, family or colleagues of victims using information or images posted online[32].

2.22 Scam call operations often use large call centres or automated dialling systems to place a large number of calls to potential victims. Once a victim answers the call, the fraudster will typically use a script to try to trick them into providing personal information or sending money. The fraudsters may ask for sensitive information such as Personal Public Service ("PPS") number, credit card information, or bank account numbers, ask the victim to send money through wire transfer, gift card or via cryptocurrency, or even request remote access to the victim's computer. Once they have obtained this information or money, they will often quickly disappear and use it for fraudulent activities.

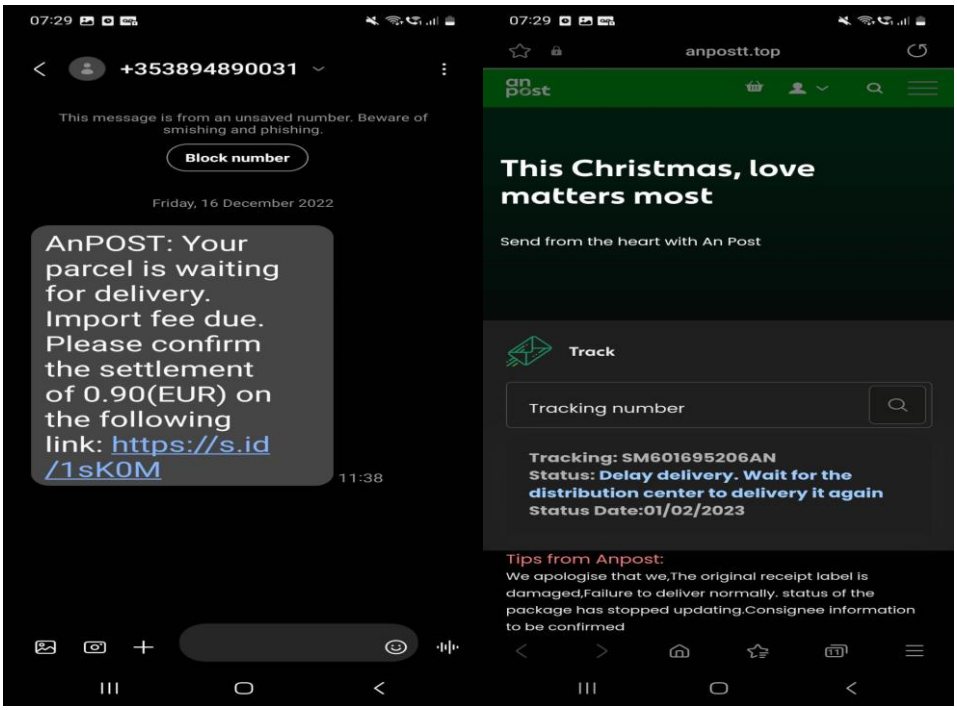
2.23 Scam call centres are often based in countries with relatively low labour costs and a large pool of skilled English-speaking workers (e.g., India) in order to target wealthy English-speaking countries. There are reports of centres with hundreds of staff operating 24/7, generating tens of thousands of calls daily. This is crucial to many scam calls given the low success rate for scams, with the consumer survey indicating there are up to 3 successful scams per 1,000 received[33]. While many scam calls have originated from abroad in the past, ComReg understands from An Garda Siochana that over past 12 months a greater share of reported scam calls appear to originate within the State (primarily through the use of pre-pay burner phones).

2.24 Scam SMS operations will send text messages to many potential victims at once. Fraudsters may use SIM banks[34] to store and manage a large number of SIM cards, each with a different phone number[35]. They can then use these SIM cards to send a large number of text messages to potential victims. Fraudsters often operate from a moving vehicle to avoid detection and triangulation of their location by MNOs and law enforcement agencies[36].

[32] DublinLive.com 21st March 2023 "*Expert warns of WhatsApp 'family emergency' scam targeting users across Ireland*" Link
[33] This is based on scam calls and resulting fraud as reported to the Consumer survey. ComReg considers that underreporting of scam calls is more likely than fraud, and therefore this figure should be considered as an upper bound on scam effectiveness.
[34] A SIM bank is used to store and manage a large number of SIM cards in a single location.
[35] Using different numbers can make it more difficult for victims to block or for authorities to trace fraudsters.
[36] Commsrisk.com, 20 March 2023 "*Sixth Suspect Arrested for Massive Paris IMSI-Catcher SMS Scam*" Link

2.25 The text message may appear to be from a legitimate source, such as a bank, government agency, or a well-known company. The scam may request the recipient to provide either personal information or payment details in response. Alternatively, the message may ask the victim to click on a link, which leads to a fake website or app that looks like a legitimate one asking them to enter their personal information, as shown in Figure 8Figure 8 below. Once the victim enters their personal information into the website, the fraudsters can use it for fraudulent activities.

Figure 8: Example of a scam text impersonating An Post and accompanying website, 16th December 2022



2.26 A single 64 port SIM bank (see Figure 9Figure 9), available online for between €700-€800 and can generate 640,000 scams texts for less than €1,000 per month – as multiple MNOs offer SIM-only mobile plans offer up to 10,000 texts messages per month, for as little as €14.99. A fraudster could well recoup these and other costs (e.g., fake website development) with even a low success rate, noting that the consumers survey indicates there are up to 4 successful scams per 1,000 received.

Figure 9: Example of a SIM Bank

Source: Advert for a 64 port SIM Bank on sale at AliExpress.

Incentives for criminals to perpetuate scams

2.27 Fraudsters have an incentive to perpetuate scams wherever the revenues generated by a scamming operation exceeds its costs. The profitability of scam calls and texts is determined by a number of factors, including: the number of victims targeted; the success rate of the scam; the amount of money each victim is scammed out of; the cost of running the scam; and the likelihood of facing sanctions.[37]

2.28 Although the success rate is highly critical to the profitability of a scam, most scams require only a small percentage of the recipients to fall for the scam to achieve profitability. The required success rate of scams is highly variable, with different types of scams needing different levels of success to achieve profitability. For example, a scam that involves tricking victims into providing personal information or wiring money may require far lower success rates to achieve profitability than a fake delivery charge scam where the sums scammed could be much smaller, albeit such scams are often directed at emptying bank accounts as opposed to collecting small sums for purported delivery costs.

2.29 To increase the success rate, fraudsters use a number of tactics to gain the trust of their victims, which may include:

- impersonating well-known business or government agencies;
- impersonating family members or friends;
- using the user's personal information gathered through a data leak or via social media to gain trust;

[37] Fraudsters likely factor in the risk of being caught and facing prosecution or penalty into their expected value of launching a scam. Given the difficulty in tracing fraudsters, many fraudsters likely consider the risk of facing sanction low.

- capitalising on current events which may require a refund, fee or social transfer or submitting personal information (e.g., Revenue at the end the tax year[38], An Post at Christmas); and

- using fear tactics or injecting a false urgency, such as claiming that there is an emergency the consumer must address.

2.30 Fraudsters react remarkably quickly to current events to maximise their effectiveness. On 8 July 2023, Rogers (one of Canada's largest telecoms companies), experienced a failure lasting approximately 15 hours. The following day, fraudsters were reported as having launched successful campaigns exploiting this network outage, claiming to offer credits to affected customers in lieu of the downtime[39]. Fraudsters tendency to exploit current events, combined with successful scams being copied by fraudsters at home and abroad results in scams coming in waves.

Fraudsters are an enduring threat to consumers and business

2.31 Each evolution in the use of ECS and smartphones to communicate, make payments and/or share personal information presents new opportunities to fraudsters. Indeed, the recent increase in scams appears to coincide with the increased use of online payments, shopping and banking, during the COVID-19 pandemic, which has created opportunities for fraudsters to steal data and money from unsuspecting users by SMS texts and Voice calls. Past waves of scams have similarly made use of evolutions in consumer purchasing behaviour (e.g., PRS scams exploiting SMS subscription services).

2.32 ComReg's proposed approach should constrain the ability of fraudsters to reach consumers and to impersonate trusted organisations and contacts. However, fraudsters will not run out of opportunities and events to capitalise on and data leaks feed and exacerbate scams. Data leaks can occur without warning, and immediately expose a large number of consumers at once to highly targeted scams[40]. Notably, the Irish wave of scams coincided with the leak of the user data including the mobile numbers of over 500 million Facebook users[41], containing over 1.3 million Irish users[42]. Therefore, any package of measures proposed by ComReg must include a *dynamic* component which can tackle nuisance communications in real time and take account of economic and societal developments.

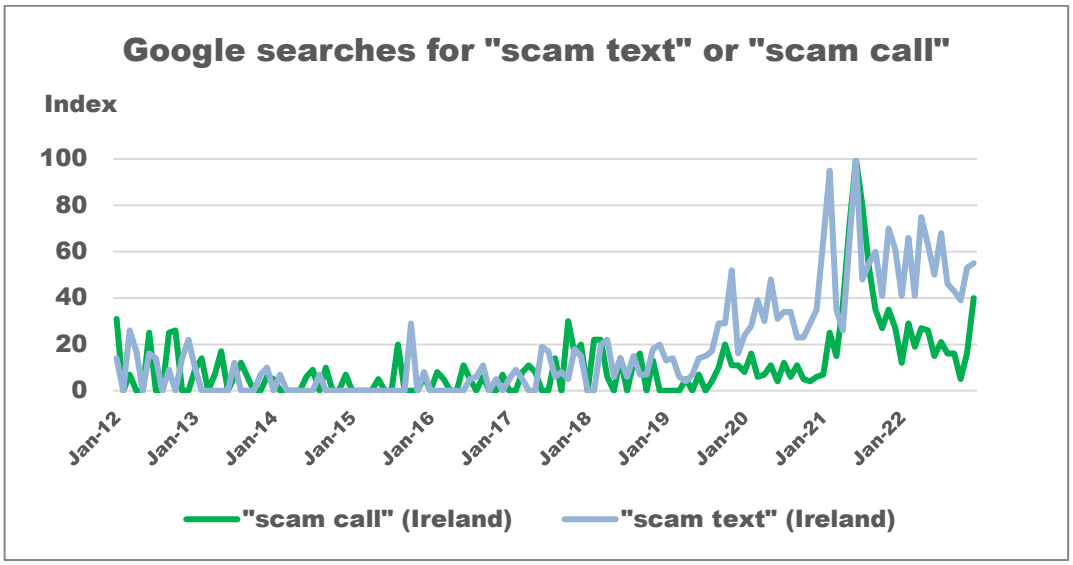
[38] Revenue.ie "*Warning: Latest SMS (text message) scam*" Link
[39] CBA.ca July 10, 2022 "*Rogers warns of text scams 'claiming to offer credits' in wake of service outage*" Link
[40] The Optus hack in Australia resulted in the theft of personal information belonging to 9.8 million customers, including names, birth dates, physical and email addresses, and phone numbers. This information was subsequently used by fraudsters to attempt fraud. Link
[41] Cybernews.com, 27 September 2022 "*Facebook data leak: you should be on the lookout for scams*" Link
[42] Independent.ie "Meta fined €265m in Facebook data-scraping case that exposed millions of mobile phone numbers" Link

2.5 The recent increase in scam calls and texts

2.33 In late 2020, ComReg identified a serious risk of harm to consumers arising from an increase in the volume of Nuisance Communications. In particular, there was an increased number of consumer queries regarding scam calls and texts and media reports of same. There is little debate whether there has been an increase in the incidence of scams call and texts – almost every mobile user can personally attest to this. ComReg's survey data indicates that 91% and 84% of Irish consumers have received a scam call or text in the past 12 months alone.[43]

2.34 However, it can be difficult to quantify the scale of the increase because no data is gathered on the incidence of SMS and Voice scams over time. Nevertheless, scam prevalence can be indirectly inferred from consumers own behaviour, namely online searches regarding scam calls and texts.[44] **Figure 10** Figure 10 below shows the relative frequency of searches for "scam texts" or "*scam calls*", which indicate that the number of SMS and Voice scams experienced by Irish consumers increased substantially from early 2020 onwards and peaked in 2021, when consumers searched scams approximately 10 times more than occurred between 2012-2019. This remains elevated and increasing in Q4 2022.

Figure 10: Relative frequency of Google searches for scam calls or texts in Ireland, 2012-2022

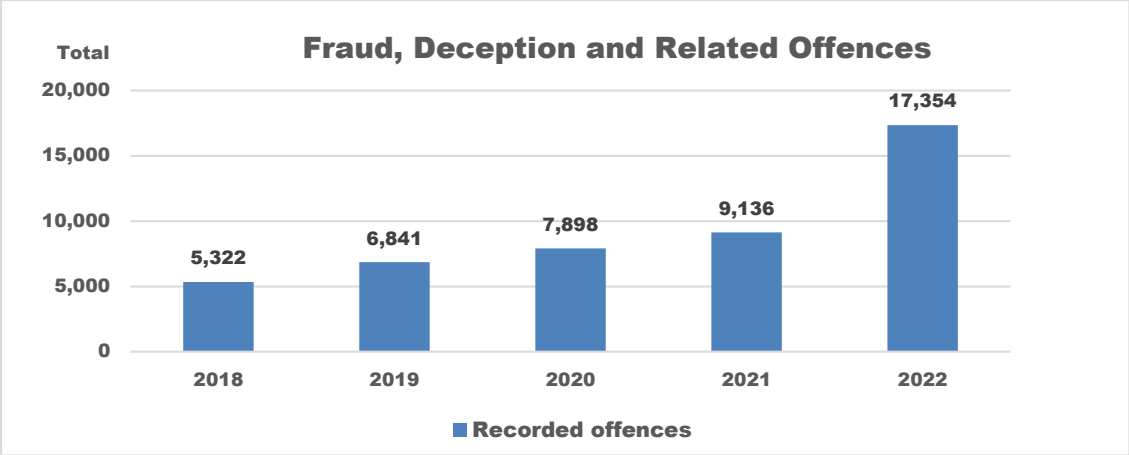


Source: ComReg analysis of data from Google Trends[45]

[43] B&A Consumer Survey, slides 14 and 21.
[44] While not a direct measure of scam prevalence, such data can be a proxy for the increase in scam calls and texts experienced by Irish consumers because consumers will likely search for news regarding scams upon receipt of suspicious calls or texts. Consistent with this, the terms most commonly searched alongside "*scam call*" and "*scam text*" are the names of organisations that fraudsters frequently impersonate (e.g., B.o.I, AIB, An Post, DHL, HSE)
[45] Google Trends is a website by Google that provides data on the popularity of top search queries in Google Search across various regions and languages.

2.35 This prevalence of scam calls and SMS texts had led to a rise in the incidence of fraud, as shown by the latest annual data on fraud published by the CSO, shown in Figure 11 below[46]. While the data does not solely relate to fraud conducted via scam calls or texts, the CSO notes that the 90% year-on-year increase in 2021 was "*largely driven by unauthorised transactions and attempts to obtain personal or banking information online or by phone*."[47] This analysis is echoed by the work of FraudSMART[48] which in 2021[49] observed that 72% of those surveyed stated that fraudsters have contacted them over the phone and 32% said they had been contacted via text message (see Chapter 3 for further details on the prevalence of fraud).

Figure 11: Recorded fraud related offences, as of 2018-2022 (annualised to Q1)



Source: CSO crime statistics

2.36 ComReg notes that reported annual fraud has declined in 2022, which is unsurprising as quarterly CSO data showed fraud falling in recent quarters.[50] It should be noted that all figures for fraud published in both the ComReg, and Europe Economics report relate to fraud in 2022 - the year with lower fraud[51]. While any decline in fraud is heartening, as scam prevalence remains high, the decline in fraud likely results from a decline in trust, which is a key harm from such scams.

[46] It should be noted that all CSO data on crime is released under reservation.
[47] Please see the CSO's latest statistical release on crime in Ireland "Recorded Crime Q1 2022" accessible here
[48] FraudSMART is a fraud awareness initiative developed by Banking & Payments Federation Ireland. Launched in October 2017, the campaign aims to raise consumer and business awareness of the latest financial fraud activity and trends and provide simple and impartial advice on how best they can protect themselves and their resources.
[49] See FraudSMART-Monitor-Oct21.pdf. Survey of 1,000 adults, July 2021, Coyne Research.
[50] This is corroborated by An Garda Siochana's provisional crime data for 2022 (published March 2023) showing that fraud overall had fallen since 2021 by 32%, driven by a 48% decline in Phishing/Vishing/Smishing type fraud. For more information, please see the press release by An Garda Siochana "*Provisional Crime Statistics 2022 - 2nd March 2023*" Link
[51] Being conducted in October/November 2022. Respondents were asked regarding their experience of scams and fraud in the prior 12 months.

2.6 ComReg's work to date

The present wave of Nuisance Communications

2.37 Upon identifying Nuisance Communications as an emerging threat to Irish consumers, businesses, and trust in public ECS networks, ComReg reviewed the issue to assess the best means for ComReg to combat Nuisance Communications. On 17 December 2021, ComReg published an Information Notice as ComReg Document 21/129[52] outlining its intention to form NCIT.

2.38 The NCIT comprises 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 NCIT membership consists of ComReg and the following operators (in alphabetical order): Blueface, BT Ireland, Colt, eir, Imagine Communications, Intellicom (DigitalWell), Magnet, Sky Ireland, Tesco Mobile, Three, Twilio, Verizon, Viatel, Virgin Media, Vodafone and Voxbone[53].

2.39 The NCIT meets every month and has now met on 17 occasions. In between each of these meetings, ComReg engages bilaterally with each of the operators to facilitate the development of the technical specifications and discuss progress on the implementation of certain interventions, including checking progress with respect to each operators plans and roadmaps for implementation of relevant interventions.

2.40 In September 2022, ComReg published an Information Notice (ComReg 22/77[54]), which provided an update on the work of the NCIT, including the progression of a number of interventions.

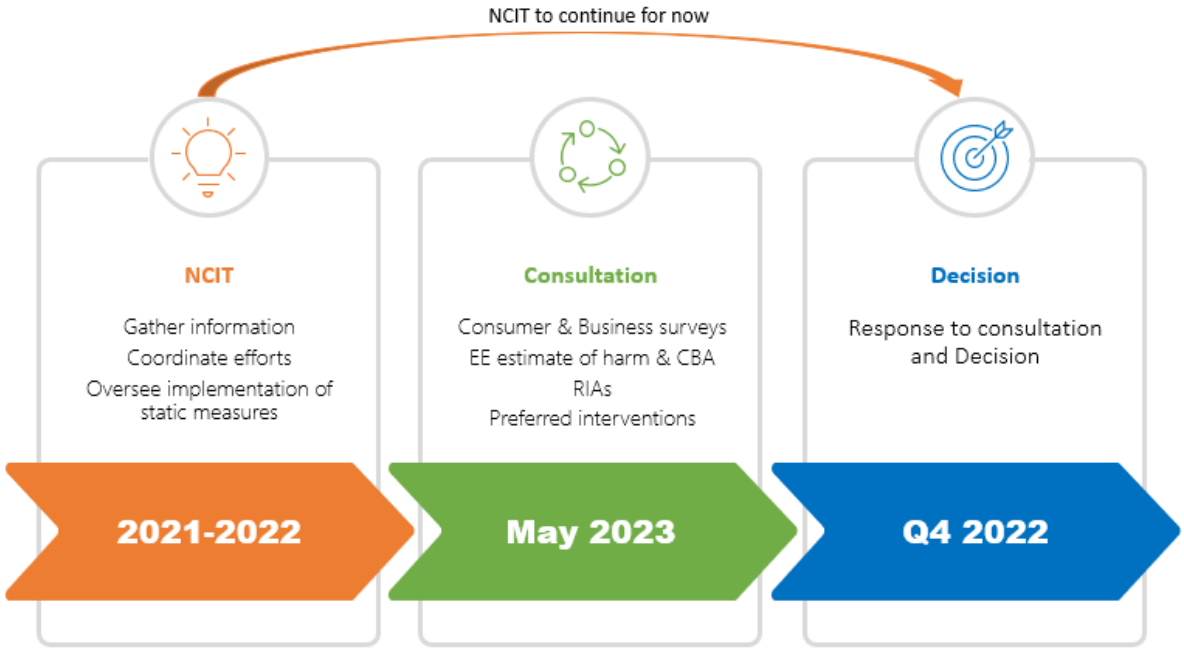
- Following a trial conducted in September 2022, DNO has now been launched[55] with a DNO list and a Protected Numbers list to block outbound calls from trusted numbers or calls from unallocated numbers.
- The activation of the Irish fixed CLI intervention on international calls was targeted by NCIT to be completed by the Irish international gateway operators by 31 March. To date six of fourteen international gateway operators have activated the intervention.

[52] ComReg 21/129
[53] Since the completion of its 6-month report, Voxbone has sought membership of the NCIT. Recently acquired by Bandwidth: https://www.bandwidth.com/newsroom/voxbone-joins-the-bandwidth-family/
[54] ComReg 22/77: Nuisance Communications - Update on the Nuisance Communications Industry Taskforce see https://www.comreg.ie/publication/nuisance-communications-update-on-the-nuisance-communications-industry-taskforce
[55] https://www.comreg.ie/industry/licensing/numbering/do-not-originate-list/

- The activation of the Irish mobile CLI intervention on international calls is targeted by NCIT to be completed by the Irish international gateway and mobile operators at latest 30 September 2023[56].

2.41 This consultation is proposing to codify a number of interventions proposed through the NCIT and will also consider other interventions that may complement these measures. In this way, the consultation forms a continuation and extension of the efforts of the NCIT, which will run for at least the duration of its current terms of reference.

Figure 12: Envisaged project timeline



Past work to combat Nuisance Communications

2.42 It should be noted that ComReg has dealt with instances of Nuisance Communications in the past.

- In 2004, ComReg issued Decision Notice D13/04 "Protecting Phone Users from Internet Dialler Scam"[57]. This direction imposed obligations on Internet Service Providers and providers of publicly available telephone services. The measures imposed sought both to raise awareness of the issue and to protect consumers from Internet Dialler Scams.
- In 2010, following the transfer of responsibility for the regulation of premium rate services (PRS) from the Regulator of Premium Rate

[56] Both interventions would block calls originating from abroad presenting with Irish CLIs – one for blocking calls with spoofed Fixed line CLIs and a second for blocking calls with spoofed Mobile CLIs.
[57] For more information, please see ComReg 04/117

Telecommunications Services Limited ("RegTel") to ComReg, ComReg re-published the code of practice that had been prepared and published by RegTel on 1 October, 2008[58]. This was aimed at eliminating the prevalence of scams using premium rate services in the State.[59]

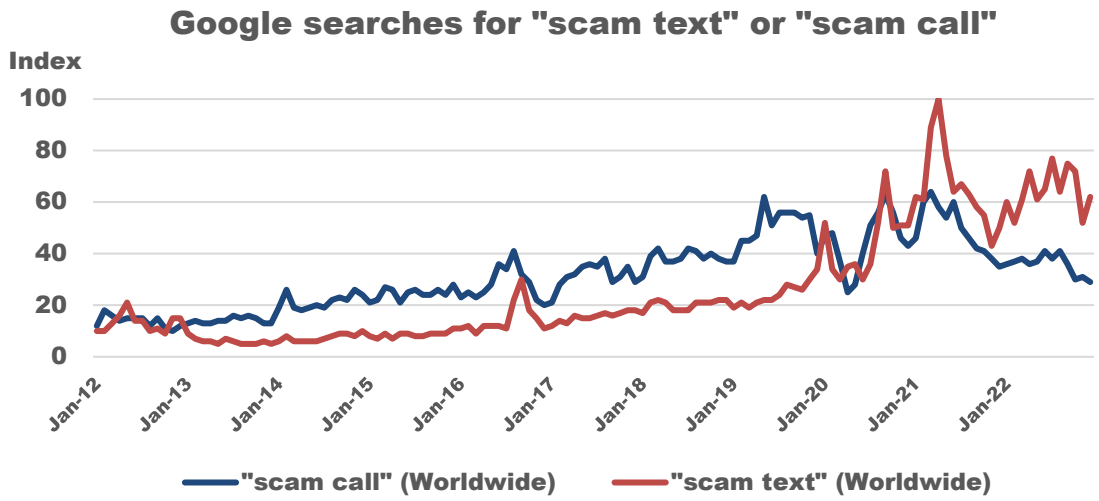
- In 2009[60], 2010,[61] and 2014[62], ComReg took steps to raise awareness among businesses of the issue of fraudsters hacking businesses telephone systems/exchanges, known as PBXs (Private Branch eXchange), which could result in the company concerned having to pay for the calls that are made by the hackers ("PBX hacking").
- In 2017, ComReg published advice to consumers on how to avoid being scammed in the midst of a wave of WanGiri scam calls originating from abroad[63].
- In 2023, ComReg secured a guilty plea in Dublin District Court against Kaleyra UK Ltd, a premium service aggregator, in relation to breaches of Communications Regulation Act, whereby fraudsters signed up consumers to monthly payments using Premium Rate Services[64].

2.7 The work of other NRAs

2.43 Nuisance Communications is a global scourge which is not unique to Ireland. Both international media reports and Google search data indicate that many other countries experienced similar increases in Nuisance Communications in the past 24-36 months.

[58] ComReg 10/54. Link
[59] In accordance with Section 15(7) of the Act continues and is the code of practice to be observed by providers of specified PRS, until a code of practice replacing it is prepared and published by the Commission.
[60] ComReg 09/41. Link
[61] ComReg 10/83. Link
[62] ComReg 14/123. Link
[63] The original advice has now been replaced with the following updated guidance here.
[64] ComReg 23/18. Link

Figure 13: Relative frequency of Google searches for scam calls or texts worldwide, 2012-2022



Source: ComReg analysis of Google Trends data

2.44 It is therefore unsurprising that NRAs across Europe are now beginning to take action to prevent nuisance communications.

2.45 ComReg has directly engaged with other NRAs to share information and experiences and received 19 responses from NRAs to a questionnaire it issued to members of the Independent Regulatory Group ("IRG") (the "IRG RFI"), to understand what actions other jurisdictions are taking to deal with this serious issue. The NRAs ComReg has engaged with includes:

a) Australian Communications and Media Authority (ACMA)

b) Belgian Institute for Postal services & Telecommunications (BIPT)

c) Canadian Radio-Television & Telecommunications Commission (CRTC)

d) Finland - Transport and Communications Agency (Traficom)

e) Germany – Bundesnetzagentur (BNetzA)

f) Italy – Autorita per le Garanzie nelle Comunicazioni (AGCOM)

g) Singapore – Infocomm Media Development Authority (IMDA)

h) UK – The Office of Communications (OFCOM)

2.46 Many European NRAs report a large increase in Nuisance Communications in their jurisdictions over the past 24 months[65] with most considering what actions to take to combat scams. Certain NRAs have already taken certain actions, for example, Belgium and Poland have or are enacting legislation to enable SMS

[65] Response to the IRG RFI

content scanning while in the Finnish NRA is working with Finnish telecommunications operators to find ways to prevent mobile CLI spoofing.[66] In very few countries have MNOs taken the initiative in the absence of regulatory intervention, although there are notable exceptions in Anglosphere countries.[67]

2.47 It is hoped that this Consultation can provide useful information to regulators, other relevant agencies and policymakers both in Ireland and abroad.

[66] Traficom looks for ways to block international scam calls | Traficom
[67] The regions where English is natively spoken by the majority of the population often termed "the Anglosphere".

Chapter 3

3 Economic and Societal Harm from Nuisance Communications

3.1 This Chapter examines the economic and social harms that arise due to nuisance communications in Ireland. In order to propose suitable interventions, it is first necessary to understand the multifaceted effects of scam calls and texts on our society. In particular, estimates of harm assist ComReg in determining whether the proposed interventions are proportionate and effective in reducing and mitigating the harms to consumers and businesses. This Chapter is therefore a necessary precursor to the policy issues in each of the draft RIAs that follow in Chapter 5.

3.2 There have been various international estimates of the harm caused by nuisance communications. However, these are of a very general nature[68] and neither ComReg nor Europe Economics are aware of any estimates which are based on seeking direct insight and evidence from consumers and businesses about how they have been harmed. The estimates of Europe Economics therefore break new ground by providing new and robust estimates of harm that has been informed by a wide variety of sources including:

1. **Consumer Survey:** B&A conducted a survey of over 1,200 consumers to understand the prevalence and harm caused by scam calls and texts.
2. **Business Survey:** B&A also conducted a survey of over 800 representative businesses in Ireland to understand the harm from scams to their operations.
3. **Interviews with relevant stakeholders:** ComReg and Europe Economics conducted interviews with businesses and public sector bodies that had particular insight into the harm caused by nuisance communications and to provision of critical services (e.g., Ireland's key retail banks, An Post, the HSE, the CSO and An Garda Síochána).
4. **Europe Economics estimates of the harms:** Europe Economics designed a bespoke empirical model to estimate all quantifiable harms. This model used as inputs data from both the consumer and

[68] For example, the FCC estimated benefits of at least $3 billion from eliminating illegal scam robocalls. That estimate assumed a benefit of ten cents per call and multiplied it across an estimated figure of 30 billion illegal scam robocalls per year, derived from third-party data. https://docs.fcc.gov/public/attachments/DOC-362932A1.pdf

business surveys, key stakeholder interviews, and desk-based research.

5. **Econometric research on scam victims:** ComReg has conducted research into the demographic determinants of scam victimhood and payments using the consumer survey data, contained in Annex 2.

6. **Analysis of media reports of scam calls and texts:** ComReg monitors print and online media to identify the scams targeting Irish consumers.

3.3 This Chapter also serves as a repository of key findings of ComReg's research which should be of use to a wide array of policymakers, enforcements agencies and businesses and notably in relation to raising awareness of scams among most at-risk consumers[69], implementing measures to catch fraudsters[70] or legislating to enable the full benefit of certain technical interventions[71].

3.4 The remainder of this Chapter is laid out as follows.

- Section 3.1 details the prevalence of the different types of scams experienced by consumers and business in Ireland.
- Section 3.2 provides a summary of the approach used by Europe Economics to estimate the various harms.
- Sections 3.3, 3.4 and 3.5 provide estimates of the harm to consumers, businesses and other bodies (e.g., public bodies and operators etc) respectively.
- Section 3.6 provides a summary of the overall estimates of the harm to Irish society.

3.1 Prevalence of scam calls and texts in Ireland

Scam calls

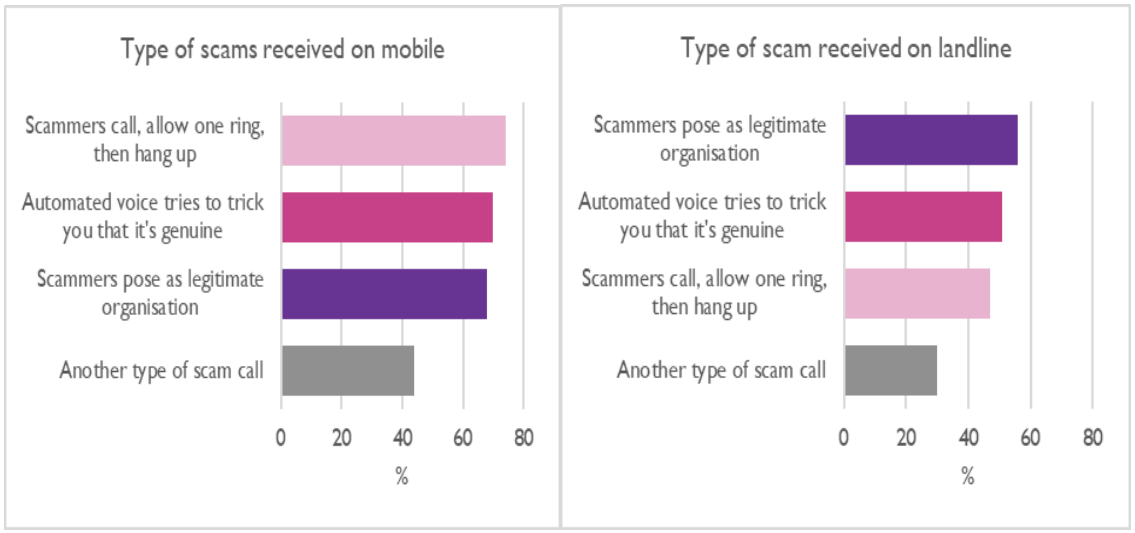
3.5 The B&A Consumer Survey investigated the prevalence and type of scams that consumers have encountered in the past 12 months. There is a high prevalence of scam calls in Ireland with approximately 91% and 74% of Irish mobile and landline consumers having received scam calls in the past 12 months[72]. This implies that 3.5 million Irish consumers[73] have received 59 million scam calls in

[69] ComReg's econometric research on scam victimhood and payments can enable consumer awareness campaigns to target at-risk consumers.
[70] This includes for example the use of call tracing to aid in the prosecution of international fraudsters.
[71] For example, legislation is required to fully enable the SMS Scam Filter, discussed in Chapter 4
[72] B&A Consumer Survey Slide 14.
[73] Europe Economics Report, page 103.

2022 alone[74] (18 scam calls per subscriber a year). This points to an average of approximately **161,000 scam calls being received each and every day.**

3.6 The B&A Consumer Survey shows a variety of different scams across mobile and landline platforms. The most prevalent types of scams are Wangiri Calls (one ring and hang up), automated voice calls, and calls posing as a legitimate organisation. While Wangiri Calls appear most often, there is a high prevalence of other types of scams across both mobile and fixed platforms, demonstrating that fraudsters rely on multiple scam types in parallel rather than any one particular scam type at any one time; indeed a scam can involve the interplay of different approaches (for example a mixture of vishing and smishing) in order to dupe the unsuspecting consumer.

Figure 14: Types of scam calls received by mobile and landline users



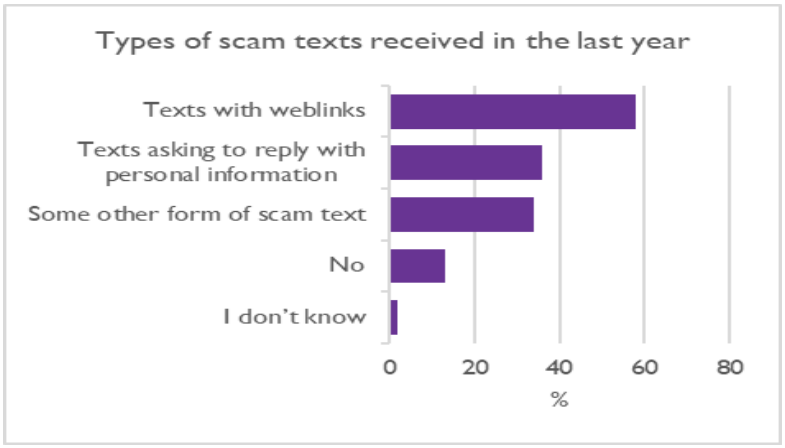
Source: Europe Economics analysis of consumer survey data

Scam texts

3.7 Approximately 84% of Irish consumers report having received any type of scam text in the past 12 months[75]. On average, Irish consumers receive 15 scam texts a year. This implies that 3.2 million Irish consumers[76] received over 47 million scam SMS messages in 2022 alone[77]. As shown in Figure 15 below**Figure 15**, most scam texts include a hyperlink and are the most prevalent means of scamming customers. This equates to an average of **approximately 129,000 scam texts being received each and every day.**

[74] Europe Economics Report, page 37.
[75] B&A Consumer Survey Slide 21.
[76] Europe Economics Report, page 103.
[77] Europe Economics Report, page 38.

Figure 15: Types of scam texts received by mobile users



Source: Europe Economics analysis of consumer survey data

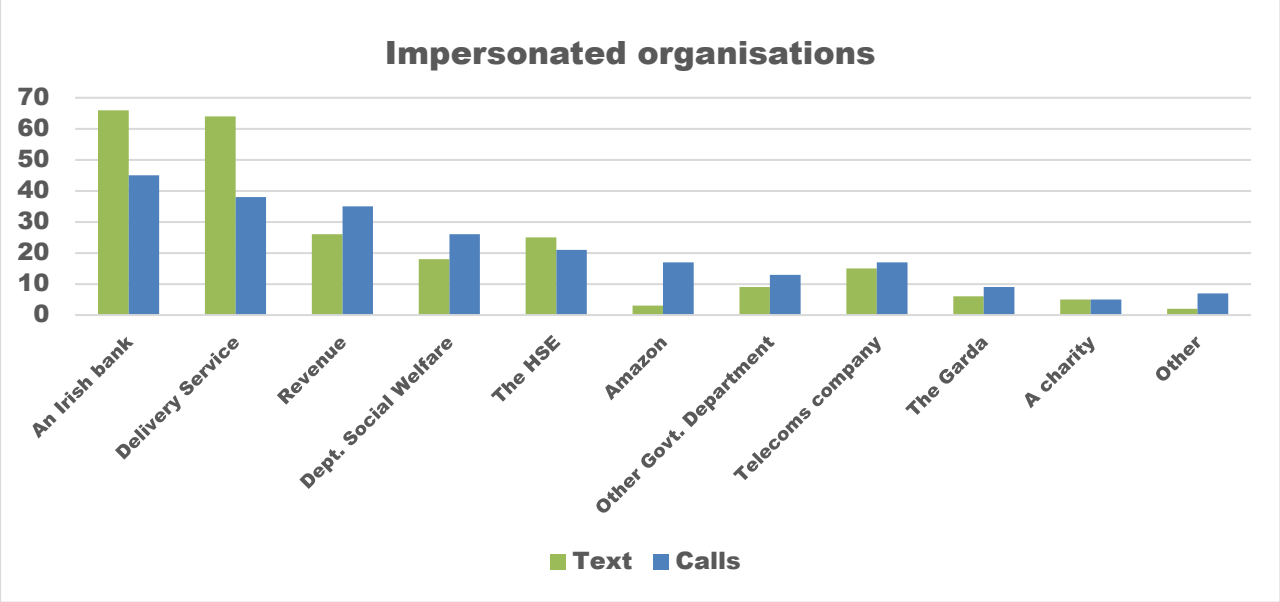
Which organisations are being impersonated?

3.8 Scams frequently involve impersonation, with the majority of recipients of scam calls (74%) and texts (89%) report having received scams impersonating a legitimate organisation[78].

3.9 Recipients of scams involving impersonation most commonly report having received scams from Irish banks, delivery service providers and government agencies (Revenue, Dept. of Social Welfare, HSE) as shown in Figure 16. While there is a considerable overlap between the types of business and organisations impersonated by scam calls and texts, fraudsters more likely to impersonate government agencies using calls, and banks and delivery service companies using SMS.

[78] Consumer Survey Q.27a and Q.27b & Q.10a and Q.10b.

Figure 16: Reporting of different organisations by recipients of scams involving impersonation



Source: Consumer Survey Q.27b (n=911) & Q.10b

3.10 Overall, over half of Irish consumers report receiving a scam call or text impersonating a government department, with this rising to up to seven in ten if An Post is included. This indicates that as many as 2.5 million Irish people may have received a scam call or SMS impersonating a government agency.

3.11 ComReg staff have also been actively monitoring print, broadcast, online and social media to be informed as to the latest scams being operated in the Irish market. ComReg includes a list of scams[79] identified in Table 1**Table 1** below. Again, this shows that fraudsters rely on multiple different types of scams often operating in parallel. Moreover, fraudsters have developed new scams over time. In particular:

- Delivery services, Revenue and the Department of social welfare were the most impersonated in-early 2020 at the beginning of the Covid-19 lockdown;
- The HSE and retail banks were impersonated throughout 2020 and 2021, with more agencies being targeted in 2022 (an Garda Siochana, Credit unions); and
- Fraudsters have now moved onto targeting users of other number-based platforms (e.g., Revolut, WhatsApp) and smaller companies (e.g., eFlow, Credit Unions, recruitment agencies) in 2022 and 2023.

[79] This is not intended as an exhaustive list of media mentions, merely a list of mentions of distinct waves of scams that appear to use SMS or Voice. It should be noted that no scam forwarding service (e.g., "Text 7726") exists at present in Ireland.

Table 1: Selection of scam waves, January 2020 - March 2023

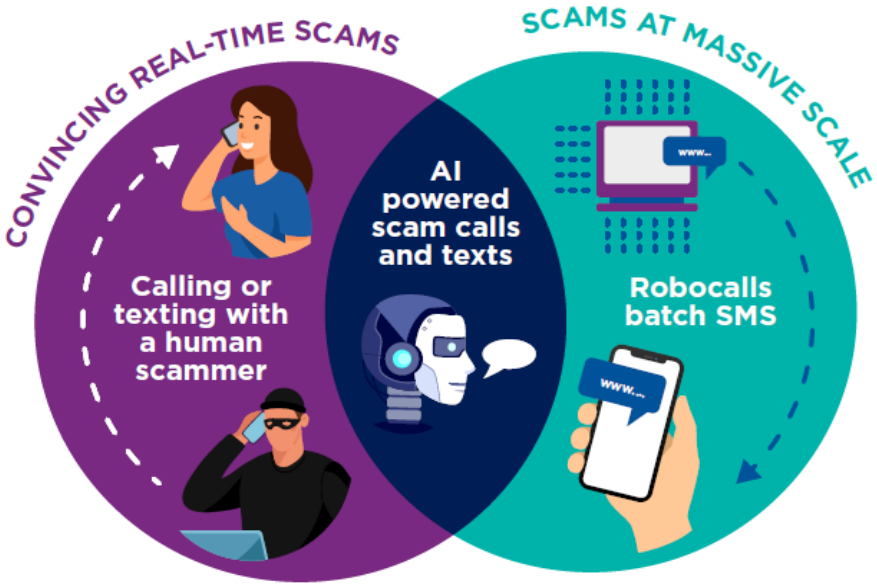
Year	Month	Body Impersonated	Scam
2020	January	Amazon	Prime Scam (Wave 1)
	March	DSP	PUP SMS scam
		An Post	Delivery scam
	April	Netflix	Netflix Scam
	May	Revenue	Revenue Tax Refund
	July	DSP	PUP SMS scam
	June	DSP	Welfare SMS (Wave 1)
		Revenue	Revenue SMS (Wave 1)
	July	HSE	Contact Tracing SMS
		Revenue	Revenue Tax Refund
		AIB	AIB Smishing (ATM card)
	August	BOI	BOI Smishing
		DSP	Welfare SMS (Wave 2)
	December	Customs	Customs SMS
		An Post	Delivery SMS
		Revenue	Revenue SMS (Wave 2)
2021	January	Customs	Customs SMS
		HSE	Vaccine appt. SMS scam
		DSP	PUP SMS scam
		KBC	KBC Fraud services scam
	March	Gardaí	Gardai Confidential Line Spoofing
	April	DSP	DSP Hotline
			Welfare SMS (Wave 3)
		FluBot	FluBot (Delivery Scam)
		Amazon	Prime Scam (Wave 2)
		Gardaí	Imminent Arrest Scam
		Customs	Customs SMS
		HSE	Covid Test SMS
	May	HSE	HSE Cyber Attack
			Medical appt. scam
	June	FluBot	FluBot (Delivery Scam)
	July	Gardaí/DSP	Imminent arrest SMS
			Compromised PPS SMS
		PTSB	PTSB Smishing
		DSP	"Neighbour spoofing" Calls
		HSE	Vaccine appt. SMS scam
	August	Eir	Eir broadband fix
		KBC/Ulster	KBC/Ulster Bank exit
	October	HSE	HSE Cyber Attack
2022	March	Banks	Crypto scam
		P2P via WhatsApp	“Hi Mam” WhatsApp scam
	April	AIB	Taxi scam (ATM card)
		Revolut & AIB	Smishing scam
	May	Various	Money laundering
	July	BOI	BOI Smishing and Phishing
	August	BPFI	Bank Smishing
		P2P via WhatsApp	Irish language romance scam
		An Post	Delivery SMS
	September	P2P via WhatsApp	Investment scams
	October	Banks/Gardaí	Money mules
	November	BOI	Combined call and text scam
		P2P via WhatsApp	“Wrong number” scam
	December	P2P via WhatsApp	'Hi Mum' WhatsApp scam (Wave 2)
		Amazon	Amazon Phishing
2023	January	P2P via WhatsApp	Blackmail (intimate photos)
		Revolut	Revolut phishing scam
		Revolut & AIB	Revolut vishing
		Revolut	Revolut Smishing
	February	Various credit unions	Credit Union Phishing Scam
		eFlow	M50 toll payment
		DECC & ESB	Electricity benefit
		PTSB	PTSB Smishing (Wave 2)
	March	P2P	Grandparent Scam
		Recruitment agencies	Hays Recruitment scam
		P2P via WhatsApp	Family emergency
		Garda (GNECB)	Garda calling in relation to fraud
		P2P via WhatsApp	Account takeover via 2FA SMS to target users contacts
		Department of Justice	Call from Immigration Service Delivery

3.12 ComReg also follows international reporting on scams because many scams that originate abroad, particularly in the Anglosphere, will ultimately be copied by fraudsters targeting or operating in the Irish market. For example, the recent wave of road tolling scams via text message began in Australia in the summer of 2022 and had moved to Ireland by the Spring of 2023. Similarly, the Hays recruitment scam was initially focussed on Hays Australian branch in January of this year before spreading to the U.K and Ireland in March.[80]

3.1.1 Scams of the future: AI powered scams

3.13 Concerningly, emerging evidence indicates that fraudsters abroad are using advanced AI based software to perpetuate scams. AI based scams could combine the relative strengths of human and automated scams (e.g., robocalls); being able to both generate convincing speech or text in real time and perpetuate such scams at a massive scale (given the reduced need for personnel)[81]. Alternatively, such scams could be highly targeted (given their increased effectiveness) and thereby avoid the usual suspicious patterns of call origination, making detection more difficult.

Figure 17: The unique harm from AI based scams



3.14 In that light, we note that there are growing reports of:

[80] Recruitment Scam Alert | Hays
[81] For example, robocalls can reach many consumers but rely on recorded messages, whereas scam callers are more convincing but can only make one call at a time.

a) AI based voice-mimicry software is being used to imitate the voice of business associates or even family members in distress[82] as well as commit identity fraud[83]. Recent cases in Australia, the USA, and Canada indicate that such scam calls may soon arrive in Ireland. A large share of Irish consumers could be targets for impersonation by voice-mimicry software, given the ubiquity of video content publicly available on social media.

b) AI based chatbots, such as ChatGPT, enabling fraudsters to automate instant messaging apps that conduct convincing conversations in real time via text or email, at massive scale[84]. Indeed, this risk was recently highlighted by Europol in a report titled "*ChatGPT: The impact of Large Language Models on Law Enforcement*"" published in in March 2023:

> *"ChatGPT's ability to draft highly authentic texts on the basis of a user prompt makes it an extremely useful tool for phishing purposes. Where many basic phishing scams were previously more easily detectable due to obvious grammatical and spelling mistakes, it is now possible to impersonate an organisation or individual in a highly realistic manner even with only a basic grasp of the English language…..ChatGPT may therefore offer criminals new opportunities, especially for crimes involving social engineering, given its abilities to respond to messages in context and adopt a specific writing style…*
>
> *To date, these types of deceptive communications have been something criminals would have to produce on their own. In the case of mass-produced campaigns, targets of these types of crime would often be able to identify the inauthentic nature of a message due to obvious spelling or grammar mistakes or its vague or inaccurate content.* ***With the help of LLMs, these types of phishing and online fraud can be created faster, much more authentically, and at significantly increased scale***."[85]

[82] For example, see Business Insider 6th March 2023 "A couple in Canada were reportedly scammed out of $21,000 after getting a call from an AI-generated voice pretending to be their son" Link and Dailymail.co.uk 31 March 2023 "Scammers cloned VOICE of Houston man with AI and conned his parents out of $5K by claiming he'd been in car accident - mom forced to postpone cancer treatment as a result" Link

[83] For example, the Guardian "AI can fool voice recognition used to verify identity by Centrelink and Australian tax office" 16th March 2023 Link

[84] See for example The Strait Times online 12th March 2023 "*Broken English no longer a sign of scams as crooks tap AI bots like ChatGPT: Experts*" and 14th March 2023 ABC7 news online "*Thieves can use ChatGPT to write convincing scam messages with human-like language, experts warn*".

[85] Europol ChatGPT "The impact of Large Language Models on Law Enforcement"

3.15 Next-generation AI based scam calls and texts should be expected to reach Ireland and increase with time as the underlying technology becomes more widely available (e.g., software like ChatGPT from OpenAI for text generation, or VoiceLab from Elevenlabs for voice cloning[86]). Such scams could be harmful where combined with CLI Spoofing or Sender ID spoofing (e.g., using a company's number and mimicking the voice of staff) or even in the absence of spoofing (e.g., impersonating a family member in distress).

3.16 Regulating or even banning[87] AI-based software and applications alone cannot be expected to mitigate the risk of AI-based software being used to scam Irish or indeed European consumers. The cost of developing such software has declined rapidly in recent years[88], and therefore regulation will not prevent such software being developed. In the face of barriers to development in certain jurisdictions, development of AI-based software will likely shift to more permissive jurisdictions. Fraudsters should be expected to deploy such software in the EU regardless of the legality. Fraudsters may even train their own models on datasets of past scams and illustrative scripts.

3.17 Next generation, AI based scams may increasingly rely on content gathered from social media to fuel scams. Fraudsters may use video content or posts from social media to imitate the voice, speech and/or image of an individual in real time[89]. In Europe alone, tens of millions of users could be at targets for impersonation, given the widespread use of social media – exposing a far higher number of friends and family to being potential victims.

3.1.2 Demographics most susceptible to financial losses

3.18 ComReg has conducted an econometric analysis of the B&A Consumer Survey data[90] in order to better understand the people most susceptible to financial fraud. ComReg has found that younger consumers, in particular those under 25, are much more likely to report having been scammed in the past 12 months[91]. In particular, respondents between the ages of 16-25 and 26-35, were far more likely (14 and 3 times respectively) to report having lost money as a result of a scam call or text, relative to older users.

3.19 This aligns with other recent research that shows that while all age groups suffer financial losses, it is younger people who are disproportionately impacted. For

[86] https://beta.elevenlabs.io/.
[87] BBC News 1 April 2023 "ChatGPT banned in Italy over privacy concerns" Link
[88] ARK Investment Management LLC, 2023 "BIG IDEAS 2023" Link
[89] CBC News "How scammers likely used artificial intelligence to con Newfoundland seniors out of $200K" Link
[90] Econometrics is an application of statistical methods to economic data in order to give empirical content to economic relationships. In short, econometric techniques can be used to examine the correlation between two variables, controlling for other variables.
[91] In particular respondents between the ages of 16-25 and 26-35, were 14 and 3 times more likely to report having lost money as a result of a scam call or text, relative to older users.

example:

a) Recent Research by Permanent TSB found that victims are more likely to be young (under 45, particularly Millennials) living in Dublin or urban areas.[92]

b) In the UK, younger people were significantly more likely to be victims of fraud with those aged 20 to 39 accounting for 39% of all reports to Action Fraud.

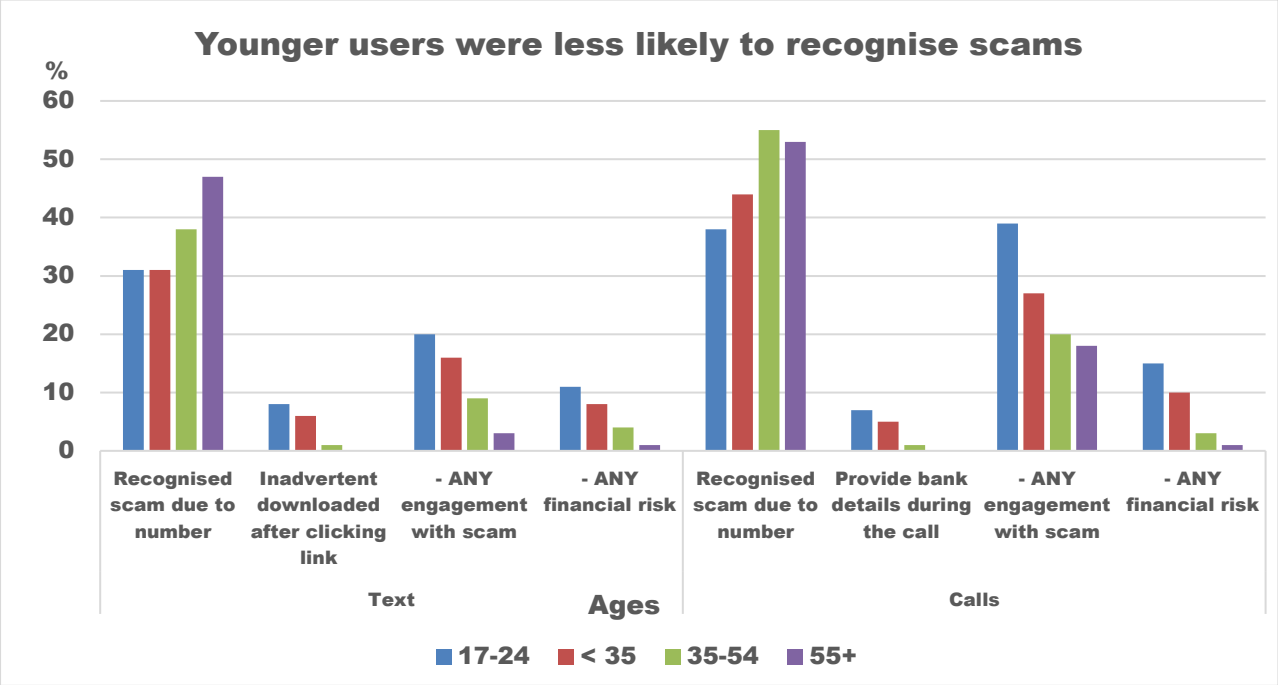
c) Recent research by Barclays band found that 21–30-year-olds being fifteen times more likely to be a victim compared with those aged over 70[93].

3.20 This does not appear to result from fraudsters specifically targeting younger consumers, rather that they are more likely to fall for a scam, potentially as younger consumers make greater use of mobile payments and online purchases. The Barclays research provides some insight into the reasons that make young people more susceptible to scams. Around 40% of this cohort reveal they rarely read the T&Cs, and a third admit to shopping with a brand they haven't heard of if they appear to be offering a good deal. This finding is supported by evidence regarding consumer behaviour following receipt of scam, shown in Figure 18Figure 18 below, which shows that younger consumers were less likely to recognise scams. This has implications for organisations aiming to reduce the effectiveness of scams and incidence of fraud, as discussed in Annex 1.

3.21 However, as noted below, older people are more likely to be concerned or very concerned about scam texts (81%)[94] and therefore are more likely to be victims of emotional and mental distress even where they do not suffer a direct financial loss.

[92] PermanentTSB.ie 23 November 2023 "*Reflecting Ireland: An insight into consumer behavioural change in Ireland – Fraud*" Link
[93] Barclays 14 June 2022 "*Young people warned to be vigilant this summer as Barclays data reveals 21-30 year olds are most at risk of scams*" Link
[94] B&A Consumer Survey, slide 13.

Figure 18: Scam recipients' reactions to a scam calls and texts, by age



Source: B&A Consumer survey, Questions 28 & 11[95]. The percentages above are for users that received a scam call or text applies to the (160 of the total sample of 176 (c.90%)).

3.2 Identifying and estimating the harm from scam calls and texts

3.22 Europe Economics approach to estimating the harms from scam calls and texts combines evidence from public data sources, stakeholder interviews and results from the B&A Consumer and the B&A Business Surveys with extrapolation to the relevant Irish population and business demographics. Europe Economics has deployed three approaches to estimating harms.

I. **Bottom-up cost modelling** which involves estimating the harm to a stakeholder group by summing up all individually estimated harms, derived from the surveys including losses from fraud, the monetary value of time spent resolving scams; or the monetary value of time spent engaging with scam calls or texts.

II. **Willingness-to-Pay** calculations which estimates the harm to a stakeholder group by asking the group (in the Consumer or Business survey) how much they would be willing to pay to avoid all scams. Three complementary categories of WTP questions were asked in order to provide added robustness to the estimates and avoid the double counting of harms. The WTP values are then extrapolated to the

[95] Q.28 When you received scam texts on your mobile phone in the past year, did you do any of the following? Q6a/Q6b Yes

business and consumer population using CSO consumer and business demographic data.

III. **Case studies** provide examples of harm that were not captured above given their bespoke nature. Europe Economics presents several cases studies of harms caused to public bodies, particularly those that rely on calls and text to deliver important pubic and social services.

3.23 For the purpose of this section, ComReg presents the final estimates or range of estimates provided by Europe Economics with the more detailed analyses contained within the Europe Economics Report. Although Europe Economics has endeavoured to gather as much information as possible, it will be apparent to the reader that some harms are inescapably difficult to estimate with any reasonable margin of certainty, given the data available or lack of certainty regarding future market trends. Therefore, Europe Economics estimates of harm are necessarily conservative estimates because many harms are not quantifiable.

3.24 For further information on the methodologies deployed by Europe Economic, please see the Appendices to the Europe Economics Report.

3.3 Harm to Irish consumers

3.25 ComReg assess the impact of scams on Irish consumers under the following headings.

i. The financial losses from fraud, including the costs of resolving cases;

ii. Emotional harm and wasted time (which could have been used more productively); and

iii. Loss of trust in voice and SMS communications.

i. Financial losses from fraud

3.26 The majority of scams do not succeed, and the vast majority of recipients of scam calls or texts will not be defrauded. Although borne by only a small share of consumers[96], financial losses are the largest and most evident harm suffered by consumers. It is estimated that there were approximately 365,000 cases of direct financial losses in Ireland over the last 12 months[97] with 175,000 people defrauded after receiving scam calls and 190,000 people defrauded after receiving a scam text[98]. This equates to an average of approximately 1,000

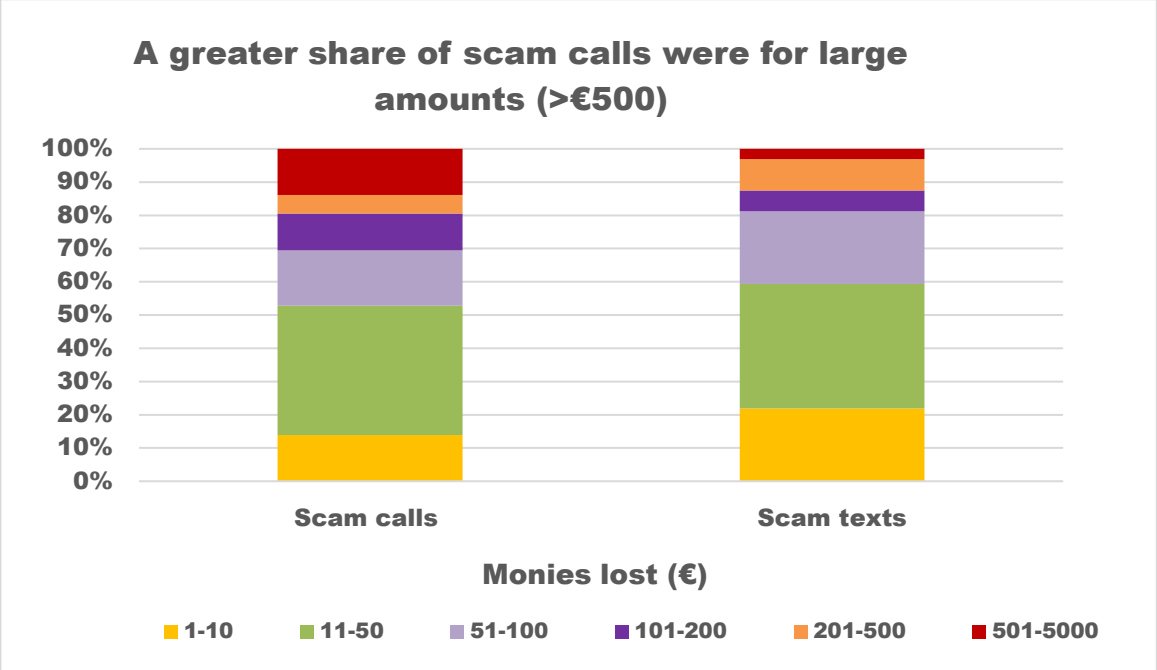
[96] However, scams also affect other groups, with young consumers under 25 years of age more likely to experience financial loss as a result of a scam call or text.
[97] Approximately, 5% and 6% of Irish consumers lost money in the last 12 months as a result of a scam call or text respectively
[98] Europe Economics Report, Page 5

cases of fraud each day because of scam calls and SMS texts.

3.27 The losses observed in the consumer survey range from €5 to €5,000, with scam calls accounting for a higher share of large scams (e.g., >€500). This broad range is to be expected given how the amount defrauded varies significantly across individual instances of fraud (e.g., subscription scams, one-off payment, emptying a current account[99]). Notably, the median loss is around €50 for both scam calls and texts, while the average is somewhat higher for scam calls than texts, from €230 to €490 respectively. This aligns with other research which shows that most (but not all) fraud attempts typically involve amounts in the low to mid hundreds of euros, for example:

- Permanent TSB found that people are more likely to experience fraud attempts seeking to take less than €500 rather than larger amounts.[100]
- European Commission also shows that the magnitude of financial losses varied markedly and depending on the type of fraud experienced, with 46% for amounts less than €50 and around 85% for amounts less than €500.[101]

Figure 19: Shares of scam calls and texts, by monies lost



Source: ComReg analysis of survey data. This excludes the approximately one in three victims that could not recall the amount lost

[99] Numerous media accounts indicate a high prevalence of direct payments or account takeover. Although, less well covered by media reports, there is evidence that many fraudsters attempt to sign consumers up to subscription payments. This may be desirable from the perspective of a fraudster as such payments are less likely to arouse suspicion and accrue over time.
[100] Permanent TSB "Under 45s more likely than older people to fall victim to financial fraud, according to Permanent TSB's latest Reflecting Ireland consumer research" Published on 23 November 2022 Link
[101] European Commission,2020,'The Scams and Fraud survey' Link

3.28 Depending on the financial status of the victims such sums of money can have devastating impacts. For example, recent CSO data shows that 20% of households are now short of money to cover their expenses every month[102]. Amounts of €100 or less could be highly detrimental in such cases. Further, younger people (15 – 29) who are most impacted by fraud have the lowest average incomes.[103] This aligns with recent European Commission research[104] which showed that the financially vulnerable might be particularly at risk. The survey illustrates that the probability of experiencing a financial loss due to a scam or fraud (amongst those who experienced such a fraud) is 12 percentage points higher for someone in a financially difficult situation compared to someone whose financial situation is more straightforward. Recent research by Ofcom regarding online scams found that while one in five suffered a loss of greater than €1,000, losses below €100 were the more frequent (42%)[105].

3.29 However, large financial losses also occur, with thousands of people likely to have been defrauded for amounts of over €1,000 through scam calls and texts. These are significant amounts regardless of individual income levels and can wipe out entire savings in some cases.

Quantified financial loss

3.30 In total, Europe Economics estimates that Irish consumers suffered financial losses of €109 million to scam calls and SMS (with €75 million from calls and €35 million from texts).[106]

Table 2: Economics estimates of consumer harm from fraud (€ million)

Scam type	Gross Loss	Net loss	Cost of resolution	Total
Scam Calls	86	75	0.8	76
Scam Texts	44	35	0.2	35
Total	130	109	1	110

Source: Europe Economics analysis.

Comparison to previous estimates of fraud

3.31 The estimate of approximately 365,000 victims of fraud significantly exceeds previous estimates of reported fraudulent crime by a considerable amount. For

[102] CSO "Pulse Survey: Our Lives, Our Money - October to November 2022" Link
[103] CSO "Earnings Analysis using Administrative Data Sources 2020" Link
[104] European Commission,2020, *'The Scams and Fraud survey'*, page 45
[105] Yonder "Online Scams & Fraud Research 2022 Executive Summary Report" page 19
[106] Europe Economics estimate the total amounts scammed at approximately €141 million (€90 million from scam calls and €51 million from scam texts). The total amount lost by consumers is lower because victims recover some of the monies lost. This depends on the specific circumstances of the scam and the actions taken by the consumer. Once this and the value of time lost to such actions is included the total financial loss is €119.1m.

example, the CSO Recorded Crime shows that there were approximately 12,000 Fraud, Deception & Related offences recorded on An Garda Síochána's PULSE database in the year 2022. However, this is to be expected as the B&A Consumer Survey is the first attempt to survey a representative sample of the Irish population to estimate the prevalence of scam calls and texts. Long standing evidence suggests that scams of this type are severely underreported to police authorities.[107]

3.32 We can see this ably demonstrated in the UK where Office of National Statistics ("ONS") measures the prevalence of crime based on a survey (not dissimilar to ComReg's) and can be compared to actual reported offences. Indeed, the ONS note that the survey is the most reliable indicator for the more common types of crime experienced by the general population. The ONS report around 3.8 million instances of fraud[108] - by contrast, Action Fraud (the UK public-facing national fraud and cybercrime reporting centre) reported 326,753 reported offences – i.e., 92% of such fraud are not reported.

3.33 This occurs for a multitude of reasons, including that consumers feel too embarrassed to report the crime, amounts taken are relatively small, or simply those defrauded do not know who to contact. As we have observed, the majority of cases are for amounts of less than €100 and victims may decide it is simply not worth reporting such cases.

ii. Wasted time and emotional harm

3.34 The majority of recipients of scam calls or texts do not suffer any financial loss. However, the surveys show that there are other impacts that cause harm to consumers while also distorting the efficient and effective functioning of the numbering platform. Europe Economics estimates that approximately 3.5 and 3.2 million consumers are at the very least inconvenienced by scam calls or texts (but do not suffer a direct financial loss).

3.35 Consumers have reported a variety of different non-financial harms. Prior to estimating the harm associated with this category, ComReg first describes the harm associated with wasted time and emotional harm.

Wasted time

3.36 Scams waste time which could have been spent on activities that consumers value. As described by Europe Economics, consumers incur an opportunity cost when they receive and engage with scam calls and texts as these actions consume time and resources that could otherwise be allocated to other things.

[107] The Psychology of Fraud, Persuasion and Scam Techniques: Understanding What Makes Us Vulnerable; Routledge, December 2020
[108] Crime in England and Wales - Office for National Statistics (ons.gov.uk)

Scam calls and texts received during working hours take time out of a productive activity that, in aggregate, could be costly to the economy; while those received out of work hours takes away valuable leisure time. The B&A Consumer Survey shows that consumers spent around 2 million hours[109] dealing with scam calls in the 12 months preceding November 2022.

Emotional harm

3.37 Falling victim to scams and fraud can have significant negative impacts on mental health and wellbeing with victims typically reporting significantly higher levels of anxiety and lower levels of happiness. Long standing research[110] shows the additional hidden harms that victims of financial fraud face and these can have a steep emotional toll. Successful scams can be traumatic for their victims, in particular following the loss of a substantial sum of their monies but not exclusively so. This can be seen in the experience of one Irish man after losing an unspecified amount:

> "*Just sat there staring at my life savings account which had been absolutely drained…. Went home. Sat down on the couch. Looked at my account again. Called the family. Fighting back the tears*"[111].

3.38 Research[112][113][114] shows that scams can impact the health and well-being of individuals, irrespective of whether they have experienced financial loss or not. Constant scam attempts can increase stress levels and harmfully impact people's mental health which is even more insidious when the fraudsters target those most vulnerable who are often older, lonely and/or managing an illness. It is therefore unsurprising that 70% of Irish consumers reported being concerned about either texts or calls[115]. Given the large volume of such calls and texts, and their negative toll on consumers, the overall emotional burden is likely to be high.

3.39 The B&A Consumer Survey demonstrates how harmful even unsuccessful scams can be to consumers. The majority of consumers that received a scam

[109] Europe Economics Report page 106. As a robustness check Europe Economics separately estimated the value of lost time. Europe Economics estimated the cost of lost time to scam calls as €40 million using the estimated value of an hour produced by the Department of Transport combined with the time lost to scam calls.
[110] For full discussion, See Chapter 4, Button, M and Cassandra, C,' The impact of fraud upon victims, 2017, Routledge
[111] Irishmirror.ie 30 August 2023 "*Irishman 'fighting back tears' warns others after latest AIB scam 'raided' life savings*" Link
[112] After reviewing 16 research papers and datasets from across the world and from UK police, Which? UK found victims suffer personal harm from fraud regardless of whether they lost money or were reimbursed. Devastating emotional impact of online scams must force government action - Which? News
[113] Bailey, J (2021) et al showed that scams impact individuals in terms of health and well-being, irrespective of whether they have experienced financial loss, and trigger implementation of strategies intended to avoid being defrauded. Older adults and "scams": evidence from the Mass Observation Archive Bailey, Jan; Taylor, Louise; Kingston, Paul; Watts, Geoffrey. The Journal of Adult Protection; Brighton Vol. 23, Iss. 1, (2021): 57-69
[114] Gordon and Buchannan (2013) observed that anxiety could be triggered independently of actually being defrauded; simply being aware scams exist may incite fear of being defrauded.
[115] B&A Consumer Survey, Slide 12

call (85%) or a scam text (81%) found such communications were an annoying inconvenience. More troublingly, nearly one in three (29%) found such communications were distressing. Europe Economics estimate that that there was a total of 89 million calls or texts that were annoying/irritating and 31 million scam calls or texts that were distressing in the last 12 months[116].

Quantified harm

3.40 Europe Economics estimates that the total inconvenience of scams (which would include both the value of time lost to calls and the emotional distress caused by scam texts)[117] at €62 million. The full methodology is outlined in Appendices of the Europe Economics Report.

Total consumer harm from scam calls and texts

3.41 The total estimated impacts[118] on consumer harm are summarised in Table 3Table 3 below – this consists of the sum of the financial loss and the costs of wasted time and emotional harm.

Table 3: Europe Economics estimates of consumer harm (€ million)[119]

Quantified Harm	Scam Calls	Scam Texts	Total
Financial Losses from fraud	75	35	109
Wasted time and emotional harm	41	22	63
Total Harm	116	57	172

Figures may not sum due to rounding

iii. Loss of trust in voice and SMS communications

3.42 People need to trust that people contacting them are genuine, otherwise call avoidance would result in legitimate calls and texts going unanswered. Consumers want to answer calls and read text messages in the anticipation that the caller or sender is someone they know or with a reason to contact them, or a business providing services of value to them (e.g., banking and parcel delivery). This trust underpins the use of Voice calls and SMS and the benefits Irish consumers and businesses derive from these networks[120]. Any such loss of trust could result in large consumer harm, were it to undermine the benefits of SMS and Voice set out in Sections 2.1 and 2.2. Further, the loss of trust is higher among younger groups that are more susceptible to such scams and scam victims – this will lead to precipitous decline in use of the numbering

[116] Europe Economics Report page 46.
[117] Using a bespoke backward-looking WTP model. See the Annex for further details.
[118] Other impacts not estimated include increased phone bills etc.
[119] Europe Economics Report page 49.
[120] See the CLI Blocking RIA and Sender ID Ria for more information on the trust in numbers and SenderIDs.

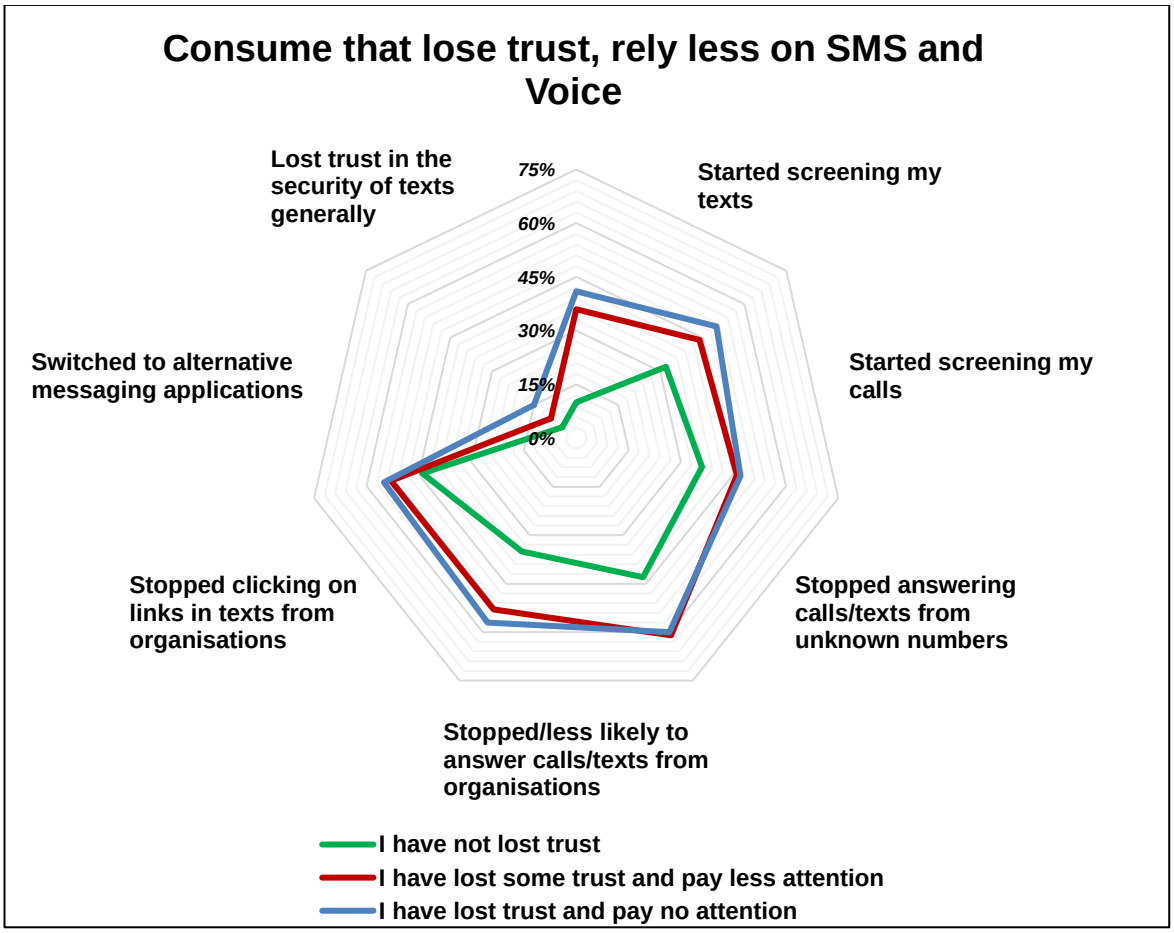
platform over time if measures are not implemented to address lack of trust.

3.43 The B&A Consumer Survey found concerning signs of scams reducing consumers trust in voice and text communications. For example:

- Around half of consumers now require some confirmation of the legitimacy off the caller/sender.
- Over 40% of consumers that use SMS services[121] have lost trust in these communications and pay less attention to them[122].

3.44 The B&A Consumer survey reveals that consumer have become increasingly distrusting of the calls and texts they receive. As illustrated in Figure 20Figure 20, consumers that have already lost trust due to scam calls and texts are more likely to show reduced use or reliance on SMS or Voice subsequently (i.e., screening calls/texts, stop answering unknown calls/texts etc).

Figure 20: Reduction in trust and use of Voice/SMS, among users



[121] Such services include information/reminders about health appointments, banking and utility bill.
[122] One in four consumers claim to pay no attention to SMS as a result of their unpleasant experiences with scam texts.

Source: ComReg analysis of B&A consumer data.[123]

3.45 This all points to a reduced utility of Voice calls and SMS for senders and users alike as many legitimate calls/texts now go unanswered/unread. Indeed, a sizable minority of survey respondents reported a loss of trust in texts and have switched to alternative messaging applications (e.g., WhatsApp) because in their experience calls and texts over the telephone numbering platform have become untrustworthy.

3.46 The evidence suggests that this usually occurs not because consumers prefer alternative applications or because it views these alternatives as being essentially equivalent to one another. Instead, such migration usually occurs because the consumer decides that the harms and nuisance associated with using calls and/or texts are so high that they avoid using voice and SMS altogether or insofar as possible. It stands to reason that if the telephone numbering platform operated more effectively then consumers would have no need to migrate to alternative means.

3.47 Europe Economics estimates that the lost benefit to consumers due to lack of trust could be as high as **€230 million per annum**[124]. This is not included in the total quantified harm above given these are second order impacts and difficult to estimate with certainty. Nevertheless, this is considered further under the "Impacts on consumers" within each of the Draft RIAs in Chapter 5.

3.4 Harm to Irish businesses

3.48 Businesses may suffer losses from a reduction in sales because of a degradation of consumer trust in SMS and Voice. The B&A Business Survey highlights the high degree to which businesses rely upon SMS and Voice for B2C communications. This includes advertising and sales, and ComReg notes that:

a) More than half of businesses (56 per cent) use mobile calls or texts for one part of their communication strategy;[125] and

b) Among these firms, on average 10 per cent of revenue was supported by telecommunications (e.g., calls or texts for reminders) in the past year

[123] This uses data gathered in response to Q.38 "*In relation to your awareness of scam call and texts, has any of the following happened?*" and Q.40c "*If so, has your experience of scam calls and texts affected your trust in communications from the organisations that provide the aforementioned services?*" where QQ.40c was asked only to consumers that reported using SMS or Voice calls.
[124] Europe Economics Report page 44
[125] Business survey. Q.19(a) Does your business use mobile calls (text) for any of the following parts of its telecommunication strategy?

3.49 Combining these statistics with the CSO data available on Irish business profiles, Europe Economics estimates that €48bn in revenue is supported by calls and texts, which is exposed to the impact of nuisance communications.[126]

3.50 The B&A Business Survey also found a small share of businesses believed they had lost some revenues as a result of scam calls and texts reducing consumers' confidence in their B2C communications, with over a third of businesses reporting having lost between 2.5%-5%. Based on this and CSO data on average business, Europe Economics note a potential loss in revenue of €2.4 billion annually due to scam calls and texts.

3.51 ComReg assesses the impact of nuisance communications on Irish businesses under the following headings.

i. Financial losses from fraud.

ii. Wasted time dealing with nuisance communications; and

iii. Increased operating costs due to mitigating harm from fraud attempts.

i. Financial losses from fraud

3.52 Fraudsters regularly impersonate Irish businesses (e.g., banks and delivery services) in order to establish trust with the caller before attempting to obtain personal, banking or security information with the intention to commit fraud. This has consequences for the businesses being imitated which are discussed below (e.g., communicating with customers, mitigation measures etc.).

3.53 Approximately 10% of businesses (or around 30,000 firms) have been the victim fraud through call/texts in the preceding 12 months, accounting for circa 15% of total business fraud. Europe Economics estimate that around 5,000 businesses suffered a financial loss in 2022, losing around €1,707 on average (which is broadly in line with the average loss of €1,400 reported by Fraudsmart).[127] Furthermore, where a business is the victim of financial fraud, time is spent engaging with scams and dealing with the fallout of same. Dealing with attempts to defraud a business is a costly use of valuable staff time, imposing a high opportunity cost on affected businesses.

3.54 Europe Economics estimate the total financial loss to businesses in Ireland to be €10.5 million in the last 12 months (€8.8m from direct financial loss and €1.7m spent by businesses engaging directly with scams).

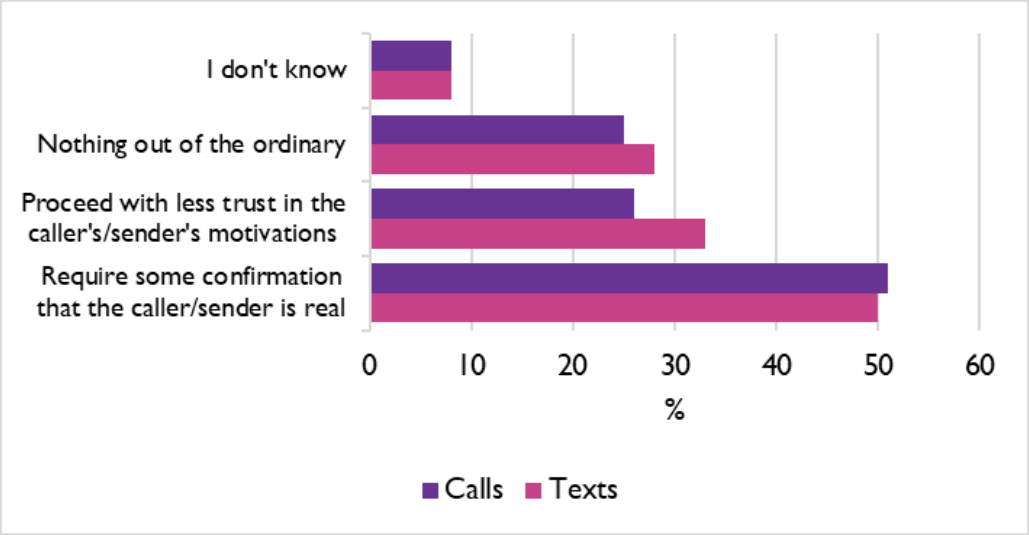
ii. Cost of wasted time dealing with scams

[126] CSO, Enterprises in 'total business economy', 2020, Average turnover, uplifted to 2021 prices.
[127] FraudSMART (2022). 'Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud'

3.55 Business spends time and resources dealing with consumer queries and complaints where their customers are the target or victims of the scam. Consumers reach out to businesses to report potential scams and or seek resolution where losses have been incurred.

3.56 Businesses also spend a significant amount of time and resources convincing consumers their communications are in fact genuine given the reduced trust in SMS and Voice calls. Half of consumers now require additional information to authenticate the caller or sender (e.g., what is the call about, is it a follow up call or is the issue something I am aware of etc). This is unsurprising given the prevalence of scams impersonating legitimate organisations. This decreases the utility and efficiency of answered calls and texts.

Figure 21: Impact of scam texts on trust of B2C communications specifically



Source: Europe Economics analysis of consumer survey data

3.57 Europe Economics estimates the value of this time lost to be approximately €21m in the last year alone (based on the mean time spent on resolving customer problems caused by impersonation attempts).

iii. Increased operating costs

3.58 Scam calls and SMS may raise the operating costs of affected businesses in a number of ways.

- First, businesses reported incurring costs through a failure to communicate with consumers as a result of scam calls or texts, which may inhibit business's ability to schedule appointments or receive payments. Europe Economics estimates the harm from this additional expenditure at €28m in the last year, using the average cost reported by businesses that experienced this cost (€1,997). This harm may increase over time given that the need to reassure consumers of the

veracity of a business's communications may intensify the longer scams persist at such high levels.

- Second, businesses reported incurring costs to mitigate the harm from scam calls and texts. Europe Economics estimates the harm from this additional expenditure at €50 million in the last year, using the average cost reported by businesses as having been incurred to implement scam-prevention measures.

- Third, organisations such as banks may incur costs from dealing with fraudulent payments. Consumers my recover some of the monies lost through fraud through scam calls and texts. In some cases, this may be the result of a successfully cancelling a payment[128], in other cases, it may be because of organisations themselves refunding affected parties. Europe Economics estimates that this harm could be as high as €23 million in the past year, based on the monies reported as having been recovered by respondents to the B&A Consumer Survey.

Conclusion on the harms to businesses from scam calls and texts

3.59 Europe Economics estimates **a total harm to business of €132.5 million** from scam calls and texts over the last 12 months as shown in Table 4.

Table 4: Summary of quantified harms to businesses (€m)

Quantified Harm	Total
Financial Losses from fraud	10.5
Time and resource spent dealing customer experience of scams	21
Cost of scam prevention measures	50
Cost of not engaging with customers	28
Cost of refunding customers	21
Total Harm	130.5

3.5 Harm to other organisations

Public Bodies

[128] For example, consumers cancelling a cheque after sending by post.

3.60 Government departments (e.g., Dept. of Social Welfare), public agencies (e.g., HSE, An Garda Siochana) and regulators (e.g., ComReg) suffer many harms as a direct consequence of scams. To understand these harms, Europe Economics conducted interviews with a number of bodies, to understand and where possible estimate the cost of the harms. The purpose of this section is to provide a snapshot of the potential harm to public facing bodies – because it only estimates harm for selected agencies the overall harm estimate is inevitably highly conservative.

3.61 Scam calls and texts reduce consumers trust in SMS and Voice calls, which are used by many public bodies to provide information, schedule appointments or otherwise communicate with Irish citizens. Scam calls and texts may therefore raise the operating cost of public bodies which may invest in alternative communication channels and/or anti-cyber security measures or software. This arises given the key role SMS and Voice as means of near universal B2C communications.

3.62 For example, consumers may simply ignore texts purporting to be sent by public bodies, which may result in missed appointments or information regarding critical services. This harm is likely to be most acute precisely when such communications are most vital, as fraudsters often target notable events (e.g., Covid-19 scams, An Post Christmas scams). In this way, fraudsters may exacerbate the impact of negative events on consumers, frustrating the effort of public bodies to ameliorate the effect of various events or crises.

3.63 Given the time available, Europe Economics interviewed a select number of agencies, which are considered especially likely to suffer harm as a result of scam calls. Based on information provided in the stakeholder interviews, Europe Economics has estimated several costs[129] to key public bodies, which are:

a) **HSE –** Europe Economics have estimated the cost to the HSE of scams calls and texts from a greater number of missed appointments and the cost of certain cyber security measures[130].

b) **An Garda Síochána –** From discussions with An Garda Síochána, it appears the additional cost of staff to handle scam calls and texts.

c) **An Post –** As an example of the measures undertaken by An Post, a direct-to-consumer campaign.

[129] This is non-exhaustive, and merely represents the harms which were quantifiable given the available information.
[130] This relates only to a specific share of the HSE's total expenditure to tackle cybersecurity.

3.64 The harm estimated that a portion of the harms suffered by these few agencies alone amounts to around €7 million. It should be noted that each body suffers further harms which were not readily quantifiable given data availability or inherent uncertainty, and the interviews covered only a fraction of potentially affected public bodies. Accordingly, the likely cost of the total harm to public bodies is probably many multiples of this identified cost. Unlike for consumers and businesses, it is not possible to estimate total harm by extrapolating the harm experienced by surveying a representative sample, given the uniqueness of the harms suffered by different public bodies (which are themselves unique).

Harm to operators

3.65 Operators may also suffer a range of harms too[131], including but not limited to:

- Potential revenue reductions from a reduced use of SMS and/or Voice;
- Cost of carrying fraudsters traffic which may be unpaid;
- Opportunity cost of time spent handling complaints; and
- Cost of configuring network to handle peaks associated with waves of scam calls or texts.

3.66 However, unlike other stakeholders, operators may potentially benefit from scams by earning revenues from "*poison traffic*" arising from scam calls or texts. Given the data available, Europe Economics has not estimated the direct harms to operators. At this juncture, ComReg assumes that operators are not net-beneficiaries of scam traffic though further assessment of this may be conducted in the future.

3.67 ComReg considers that an operators business case for investment in the proposed interventions should be made given the harm arising to operators' consumers and long-term commercial interests. In the long-run, scam calls and texts could negatively impact the revenues generated by operators from providing Voice and SMS services, and from the networks over which such services are transmitted. As noted by Europe Economics[132]:

> "*Operators were clearly aware of the potential impacts of scam calls and texts on the communications they facilitate. One MNO, in particular, noted that interventions to curtail fraudulent communications could increase trust in mobile numbers, and suggested that there was scope for operators to benefit commercially from being able to offer networks of trust. The operators were also clearly aware of damage scam calls and texts*

[131] This section covers harms from scam calls and texts to operators. Notably the cost of interventions are borne by operators and this is handled separately in the RIAs.
[132] Europe Economics Report, page 31.

can do to organisations' reputations, and hence also the trust consumers have in the communications they send."[133]

3.68 Notably, the key harm suffered by operators relates to second order effects of scam (e.g., reduced use by consumers of Voice/SMS) and not direct harms, such as financial loss. This highlights an asymmetry in the incidence of harm; while consumers and businesses are suffering today, operators may not suffer for a time and bear only a fraction of the total social cost of harms for now. In essence, while operators suffer harm, the cost of unprotected networks is primarily being borne by Irish consumers and businesses.

3.6 Overall economic and societal harm from scam calls and texts

3.69 Unsurprisingly given the diversity of harms and the large number of impacted parties, the overall harm from scam calls and texts is substantial. Europe Economics conservatively estimates that scam calls and texts resulted in harm of over €300 million in the 12 months to November 2022 as shown in Table 5. As noted earlier, **this a conservative estimate, being limited to only those harms that were quantifiable given the data available.**

Table 5: Summary of all harms quantified by Europe Economics (€m)

Quantified Harm	Total
Harm to consumers	172
Harm to business	130.5
Public Body (Case Studies)	7
Total Harm	**309**

Figures may not sum due to rounding

3.70 ComReg discuss the implications arising from this harm in each of its draft RIAs that follow in Chapter 5.

133 Operators are clearly concerned with how consumer perceptions can damage reputation and revenue growth. For example, Eir in its latest set of published accounts observed in relation to Risks Related to Our Business and Industry that *If we are unable to maintain a favourable brand image or maintain a positive customer experience, we may be unable to retain existing and/or attract new customers, leading to loss of market share and revenue*." eir_Q4-22_results_report.pdf – p20.

Chapter 4

4 The potential technical interventions to combat Nuisance Communications

4.1 Introduction

4.1 This Chapter identifies and describes the potential interventions that are available to ComReg in combating Nuisance Communications. The main output from this Chapter is to identify a list of interventions to be assessed in one or more draft RIAs that follow in Chapter 5. In that regard, this Chapter forms the basis of Section 5.2.2 ("Identifying Regulatory Options") and Step 2 of ComReg's RIA Guidelines.

4.2 In order to ensure that all potential interventions are appropriately considered, ComReg provides a full list and description of all technical interventions that are available to ComReg and have been considered in other jurisdictions and/or proposed by stakeholders in the NCIT and/or over the course of stakeholder interviews. Table 6 Table 6 provides a high-level summary of the interventions available to ComReg, the source of the interventions and the intended impacts.

Table 6: Long list of interventions and their intended impact

Technology	Interventions	Source	Intended Impact
Voice (6)	1. Do Not Originate	NCIT	Prevents Voice calls from certain assigned numbers, from originating in, or being carried into the State.
	2. Protected Numbers	NCIT	Prevents Voice calls from all unassigned numbers, from originating in, or being carried into the State.
	3. Fixed CLI call Blocking	NCIT	Prevents Voice calls from abroad using Irish fixed numbers, from being carried into the State.
	4. Mobile CLI call Blocking	NCIT	Prevents Voice calls from abroad using Irish mobile numbers (except for roamers), from being carried into the State.
	5. Voice Firewall	Discussion with other NRAs	Screens and blocks Voice calls from terminating on public ECS networks.
	6. Stir/Shaken	Discussion with NRAs	Authenticates Voice calls at the point of origination and termination.
SMS (5)	1. Shortening the Chain	NCIT	Limit the number of "hops" in SMS journey to a known, limited number of trusted 'hops' and blocks SMS for those Sender IDs coming other sources.
	2. ID Ban	Discussion with NRAs	Blocks SMS with SMS senderID from terminating on public Mobile networks in the State.
	3. ID Registry – Full or partial	Discussion with NRAs	Permits only SMS from registered Sender IDs using verified paths to terminate on public mobile networks.
	4. O-D verification	Discussion with industrial stakeholders	Terminates only SMS with Sender ID, when authenticated by the recipient network via a passcode database.

	5. Content Filter	NCIT	Blocks or labels SMS containing suspect content from any source including mobile phones, terminating on public Mobile Networks.

4.3 Not all interventions listed in Table 6 are necessarily appropriate for consideration in the draft RIAs. ComReg notes that any intervention that is not technically feasible, effective and/or cannot be implemented in a timely manner could not be considered a valid regulatory option in a draft RIA because it would not be able to reduce or mitigate the harms as outlined in Chapter 3. Further, even where an intervention is technically feasible and effective, its implementation over an extended period could result in the harms to society continuing over that period (where other interventions could have been more effective in reducing the harm in the short term).

4.4 Any interventions that are technically feasible/effective and implementable over a timely period can be assessed in the draft RIAs as regulatory options against ComReg's broader statutory objectives and duties including the obligation to promote competition. ComReg also notes that the impact on stakeholders arising from each intervention is assessed separately in the 'Impact on Stakeholders' for each draft RIA below.

4.5 With that in mind, ComReg assesses each of the interventions as follows.

I. **First**, ComReg provides a description and illustration of each intervention including how it could reduce the harm caused by Nuisance Communications ("Description");

II. **Second**, ComReg assesses whether the proposed intervention is technically feasible and effective in relation its intended purpose ("Technical feasibility and effectiveness"); and

III. **Third**, ComReg assesses whether the intervention is implementable over a reasonable period[134] ("Timelines")

4.2 Potential Voice Interventions

1. Do Not Originate & 2. Protected Numbers

I. Description

1. Do Not Originate

[134] ComReg notes that these timelines are associated with a greenfield deployment and some interventions may have already been implemented voluntarily by some operators. It is in part due to the slow implementation of these interventions by some operators (through the auspices of the NCIT) that ComReg is now mandating these measures over the proposed timelines.

4.6 Many organisations have telephone numbers that are never used for making outgoing calls to customers. These are usually phone numbers that consumers call for service information such as a customer care line (e.g., banking, credit cards etc.). Using CLI spoofing, fraudsters can make calls that appear to originate from these "inbound-only" numbers to trick consumers into answering the calls. Operators may block calls from these numbers to prevent fraudsters impersonating legitimate businesses. This creates no difficulty for the business concerned as the numbers in question are not used for making outbound calls. A list of such "inbound-only" numbers is called a Do-Not-Originate or DNO list.

2. Protected Numbers

4.7 PN numbers are numbers that have not been assigned by ComReg to operators, which should therefore not originate calls. Using CLI spoofing, fraudsters may make calls that appear to originate from these Irish numbers to trick consumers into answering the calls. To combat such scam calls, operators can block any calls supposedly originating from these numbers. This creates no difficulties in the delivery of services because there are no services currently being provided via these numbers.

II. Technical feasibility and effectiveness

4.8 DNO and PN lists and their feasibility are assessed together because both aim to address spoofing of numbers which should not originate calls. The general feedback from operators is that these interventions are not overly complex to implement.

4.9 In relation to technical feasibility, a DNO trial[135] conducted by ComReg and a small number of telecoms[136] operators (September 2022) demonstrated the technical feasibility and effectiveness of the DNO and PN lists with operators successful in blocking calls that are provided on both the DNO and PN lists. The trial also tested ComReg's administration of the DNO list by preparing the application process and encouraging organisations to apply for the addition of suitable numbers to that list[137].

4.10 Several of the trial operators had also implemented blocking of numbers on the PN list during this time. The trial tested the capability of operators to block calls on the lists and this was effective in demonstrating the technical feasibility of the interventions. ComReg and industry agreed to a wider implementation of DNO, which has already been launched and no issues with technical feasibility have been raised to date. Currently 15 NCIT operators have implemented DNO

[135] ComReg notes that a trial is possible to as this intervention does not require upfront investment costs from operators.
[136] The five operators who took part implemented the initial DNO list of 17 numbers.
[137] This initial list, which comprised numbers from several organisations, was prepared with the assistance of the Banking and Payments Federation of Ireland ("BPFI").

and PN and report that the interventions are working well.

4.11 In relation to effectiveness, all NCIT members have agreed that the interventions based on the DNO and PN lists should be effective in tackling nuisance communications. Indeed, these interventions have already proved very useful, with thousands of calls presenting as coming from numbers on the trial DNO List blocked. ComReg notes that this intervention is already in use and proving effective in Belgium, Australia[138], UK[139] & USA[140] as a means by which to reduce nuisance communications.

4.12 ComReg published an Information Notice regarding DNO (ComReg 22/86)[141], a Guidance Note and Application Form (ComReg 22/86a)[142], and a dedicated webpage[143] where further information is available. The implementation of the PN list is analogous to the DNO list and several of the trial operators have also implemented blocking of numbers on the PN list.

4.13 Therefore, ComReg is of the preliminary view that the DNO/PN intervention is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

4.14 ComReg is of the preliminary view that the DNO and PN intervention can be implemented within 6 months of any final Decision. This preliminary view is informed by:

- Discussions with industry stakeholders in the NCIT which indicates that that this requires a simple manual updated to operators' systems.
- It is currently implemented by the majority of NCIT members, with remaining NCIT members expected to complete in due course.
- The successful trial of this intervention was completed within a 6-month period; and
- A number of NCIT members have implemented this intervention in less than 3 months.

4.15 Therefore, ComReg is of the preliminary view that the implementation of the DNO and PN intervention within six months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow.

[138] https://www.acma.gov.au/sites/default/files/2019-11/Combating-Scams-summary-report.DOCX
[139] Tackling scam calls and texts: Ofcom's role and approach
[140] FCC Acts to Stop International Robocall Scams | Federal Communications Commission
[141] https://www.comreg.ie/publication-download/nuisance-communications-launch-of-do-not-originate-protocol
[142] https://www.comreg.ie/publication-download/do-not-originate-list-guidance-note-for-organisations-and-application-form
[143] http://www.comreg.ie/dno

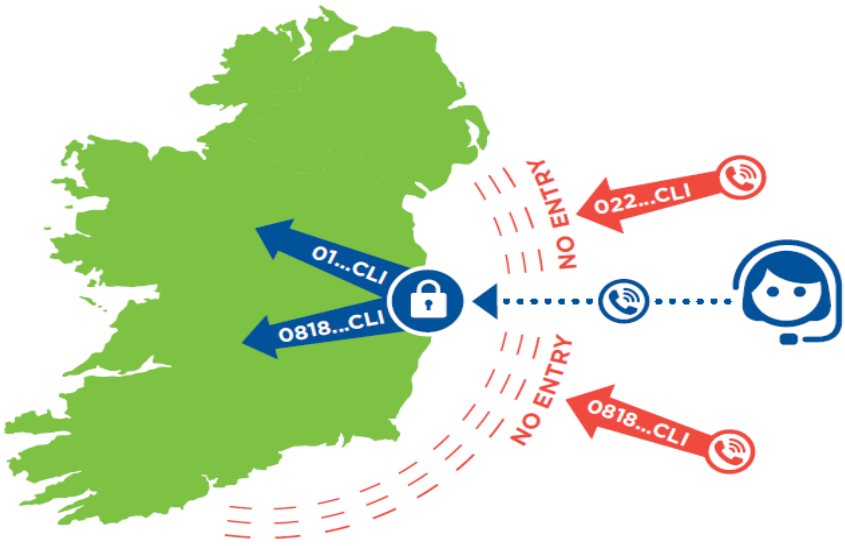
3. Fixed CLI Call Blocking

I. Description

4.16 Currently, IGOs allow Voice calls with Irish Fixed CLIs[144] into the State from abroad. Using CLI spoofing to disguise their identity and exploit the trust Irish consumers place in Irish GNs and NGNs, fraudsters based overseas can make calls appear to originate from Ireland. Operators could block calls presenting these numbers as CLIs (i.e., spoofed CLIs) to prevent fraudsters impersonating legitimate Irish organisations. This is known as Fixed CLI Call Blocking.

4.17 There are a small number of legitimate use cases for an Irish Fixed CLI originating outside the State (for example an overseas call centre). This however can be facilitated by use of a dedicated and secure connection, known as a "*long line"*.[145] The 'long line' PSTN call origination measure was agreed by NCIT members as part of its Fixed CLI specification and is an intervention that is to be implemented as soon as possible in anticipation of the implementation of the call blocking measure being discussed here. Any lack of progress on this intervention will put Irish telephone users at serious risk from fraudsters while undermining the integrity of the PSTN voice service.

Figure 22: Fixed CLI Call Blocking and long-lining



II. Technical feasibility and effectiveness

4.18 In relation to the technical feasibility, the specifications for this intervention have

[144] Irish Fixed CLIs refers to CLI presenting all Irish number except mobile (e.g., GN and NGNs).
[145] Long-line means the implementation by an undertaking of a dedicated SIP or alternative trunk type to serve an end-user to ensure that calls from that end-user originate on the Irish PSTN.

been operator led and determined in collaboration with other NCIT members. The specifications have been completed and the network designs required for the Fixed CLI call blocking intervention commenced in Q3 2022. The testing and deployment of the intervention in the individual operator networks followed by 'go-live' commenced in Q1 2023[146]. Seven operators have activated the measure in their networks. ComReg published an Information Notice regarding DNO (ComReg 23/47)[147], where further information is available. ComReg's functional requirements specification for the intervention is available upon request to relevant operators.

4.19 In relation to effectiveness, NCIT members have agreed that this intervention should prove effective in reducing nuisance communications by identifying and blocking nuisance calls stemming from international networks and presenting with Irish fixed CLIs. Calls originating from overseas which are using an Irish fixed Calling Line Identification (CLI) as a Presentation Number shall always be blocked on International Gateways. Calls from overseas platforms such as call centres that use Irish fixed CLIs may continue to so with a direct private customer connection from such platforms to the Irish telephone network (*longline*). This intervention is likely to be effective by preventing fraudsters from spoofing Irish Fixed CLIs and allowing such calls to made to Irish consumers and businesses who may perceive that a call is from a legitimate source and are thus more likely to answer it.

4.20 Therefore, ComReg is of the preliminary view that the Fixed CLI call blocking intervention is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

4.21 ComReg is of the preliminary view that the Fixed CLI intervention can be implemented within 6 months of any final decision. This preliminary view is informed by the following:

- Based on information provided at the NCIT, ComReg understands that the blocking requires a simple manual updated to operators' systems. Operators have suggested that it would take six months to have this intervention fully operational in their networks (subject to organisation prioritisation).
- Discussions with industry stakeholders in the NCIT who indicated that that this intervention can be based on existing technologies deployed by network operators (e.g., Session Border Controllers).

[146] This assumes that each involved operator continues to give very high priority to the implementation of the intervention in their networks.
[147] https://www.comreg.ie/publication/tackling-nuisance-communications-cli-call-blocking-update

- Operators have already been making progress on implementing this intervention through the auspices of the NCIT and 7 operators have already implemented the Fixed CLI intervention. This also accounts for the time operators may need to implement the "long-lining" solution for extraterritorial use of Irish fixed numbers, such as by call centres.

4.22 Therefore, ComReg is of the preliminary view that the implementation of the Fixed CLI intervention within six months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow this section.

4. Mobile CLI Call Blocking

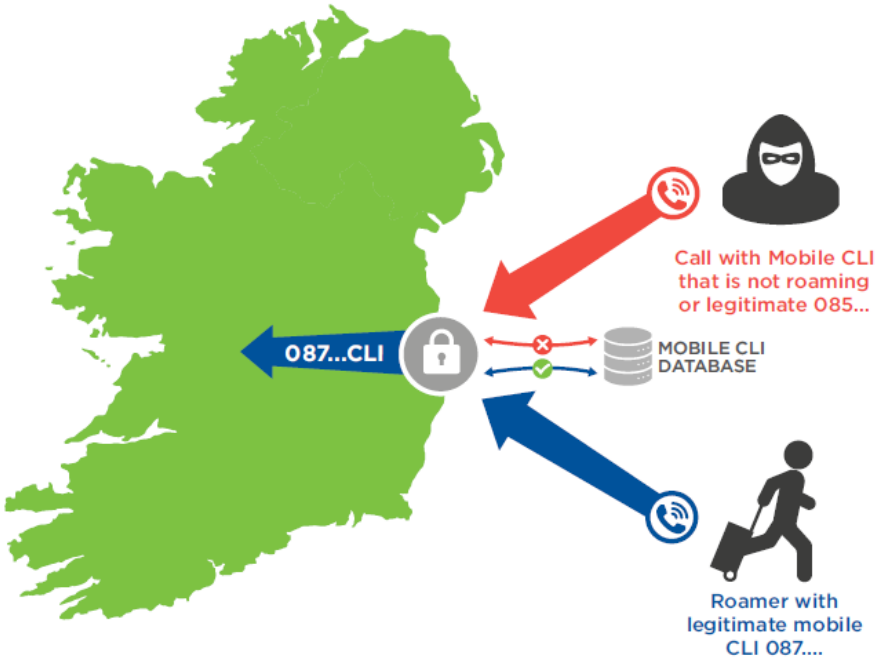
I. Description

4.23 Currently, IGOs allow any Voice calls with Irish Mobile CLIs[148] into the State. Using CLI spoofing, fraudsters based abroad can make calls that appear to originate from Irish mobile numbers. IGOs may block calls presenting these numbers as CLIs, to prevent fraudsters impersonating legitimate Irish mobile numbers. This is known as Mobile CLI Call Blocking.

4.24 There are limited legitimate use cases for a call originating abroad to present an Irish Mobile CLI. For example, in the case of calls from Irish mobile users abroad ("outbound roaming") or for calls from Irish mobile or fixed line users to non-Irish mobile users who are in Ireland ("inbound roaming") where the call is routed via the inbound roamers home network into the state using an Irish Mobile Number assigned ("Mobile Station Roaming Number") by Irish MNOs to those roamers on a temporary basis.

[148] Irish Mobile CLIs refers to CLI presenting all Irish mobile number (e.g., 087, 083 ranges).

Figure 23: Mobile CLI Call Blocking



II. Technical feasibility and effectiveness

4.25 In relation to technical feasibility, two issues regarding the implementation of mobile CLI have been evaluated by NCIT.

4.26 **First**, the 'roamer check' aspect of the intervention is based on the 'MAP' signalling protocol which is part of the SS7 protocol stack and widely in use in mobile networks. For this intervention, it is used to implement the 'roamer check' capability from the Irish international gateway network operator to the serving Irish mobile network operator (as per the telephone number indicated in the CLI of the call). The 'MAP' signalling protocol approach for the roamer check is part of Phase 1.

4.27 However, based on NCIT and associated discussions with operators, it is understood that the MAP signalling protocol is not available on all the Irish networks, particularly in the case of some of the smaller international gateway operators. Such operators would need international voice calls presenting with Irish Mobile CLIs, to use the services of an Irish operator that has fully implemented roamer check.

4.28 The intervention will in the future include an industry 'proxy server' approach accessible by a protocol other than MAP. This server would also contain Mobile Number Portability ('MNP') data which would be needed to determine the serving network for the mobile CLI which being checked for its roaming status. This approach, if availed of by smaller international gateway operators, would

remove the need for such operators to use the services of another operator in the manner described at 4.27 above. Rather, incoming calls could be validated by using the 'proxy server' once the international gateway operator receiving the call sends a validation request to the proxy server in respect of such calls. ComReg notes that this approach has been implemented in Finland for the same purpose[149].

4.29 **Second**, mobile voice calls are delivered using various technology standards (e.g., 2G/3G and 4G (i.e., VoLTE) and the current NCIT technical specification only caters for mobile roamers on 2G/3G networks which are currently used to deliver the vast majority of mobile voice calls). However, the intervention must also cater for an anticipated growth in VoLTE roaming over the coming years.

4.30 In order to address the issues raised above – this intervention would be implemented in two phases

- Phase 1 would require all IGOs to implement the Mobile CLI call blocking intervention. Each IGO would undertake the roamer check from its own international ingress point[150] and therefore avoid blocking calls from legitimate roamers. Those IGO's who due to technical limitations of their current networks are unable to use the MAP protocol-based roamer check would in this phase use the services an Irish operator who has fully implemented roamer check.
- Phase 2 would require an industry roaming proxy server to include a non-MAP signalling protocol for IGOs to perform roamer check. In addition to the proxy server aspect this phase would also address the requirement to apply 'roamer check' for VoLTE roamers.

4.31 A technical specification for Phase 1 of this intervention was developed by the NCIT operators. ComReg is satisfied that this intervention is technically feasible. It is anticipated that testing and deployment of the intervention in the operator networks (international gateway and mobile network operators) would proceed over the coming months. Activation of this intervention by the relevant operators has been targeted by NCIT to be achieved by at latest 30 September 2023[151].

4.32 Mobile CLI call Blocking covering Phase 1 has an agreed technical specification developed by the NCIT members. ComReg's functional requirements specification for the intervention, covering both Phase 1 and Phase 2, is

[149] EN Recommendation to Telecommunications Operators on Detecting and Preventing Caller ID Spoofing.pdf (kyberturvallisuuskeskus.fi)
[150] Failure to apply screening for one operator will impact Nuisance calls for all fixed and mobile users in the Irish network. Fraudsters will learn this vulnerability quickly and will move to exploit it.
[151] This assumes that each involved operator gives very high priority to the implementation of the intervention in their networks.

available upon request to relevant operators. This specification includes the proposed network architecture for the Phase 2 roaming proxy server.

4.33 In relation to effectiveness, NCIT members agree that this intervention should be effective in tackling nuisance communications by identifying and blocking nuisance calls stemming from international networks and presenting with Irish mobile CLIs. Fixed and mobile operators in Ireland would implement a roaming status check for all calls they receive that present with mobile CLIs. Those calls with CLIs which are not actually roaming would be blocked. This intervention would be effective because Irish Mobile CLIs would not be received on calls from abroad unless the call is from a legitimate Irish roamer. Similar measures have already been introduced in other EU countries.[152]

III. Timelines

4.34 Mobile CLI Intervention is divided into two phases and the timelines are assessed across these phases.

4.35 ComReg is of the preliminary view that Phase 1 of the Mobile CLI Call Blocking intervention can be implemented within 6 months of any final decision for the following reasons:

- The current technical specification (v1) was agreed by NCIT at the beginning of August 2022 at which point relevant operators indicated that it would take one year to have this intervention fully operational in their networks (subject to prioritisation within each operator organisation).
- The target deadline set by NCIT is that this intervention is implemented by all relevant operators no later than 30 September 2023.
- Relevant operators have been making some progress on their preparations to activate this intervention and ComReg has continually urged these operators to ensure priority is given within their organisations in meeting this timeline.

4.36 ComReg is also of the preliminary view that Phase 2 of the Mobile CLI Intervention can be implemented within 2 years of any final decision for the following reasons.

- Phase 2 would require the setup of an industry roaming proxy server to include a non-MAP signalling protocol for IGOs to perform the roamer check. In addition to the proxy server aspect, Phase 2 would

[152] Bundesnetzagentur - Press - Improved protection against telephone number manipulation as from 1 December

address the requirement of applying 'roamer check' for VoLTE roamers. This requires some time, given the inevitable complexity of implementing a new platform and the related inter-operator process.

- ComReg observes that VoLTE still accounts for a small minority of voice calls made. The more widespread rollout of VoLTE is at least 2 years away (noting that radio spectrum recently released by ComReg as part of its Multi Band Spectrum Award ("MBSA2")[153] contains rollout licence conditions of 2 years in respect of VoLTE)[154][155].
- Based on the Finnish example 24 months appears an appropriate amount of time for implementation

4.37 Therefore, ComReg is of the preliminary view that the implementation of the Mobile CLI intervention within six months (Phase 1) and within two years (Phase 2) of a ComReg Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the RIAs which follow this section.

5. Voice Firewall

I. Description

4.38 Voice firewalls are designed with advanced real time call data analytics using Machine Learning and Artificial Intelligent techniques to detect and act upon unusual patterns of call signalling data, traffic volumes etc. The deployment of voice firewall interventions by Irish operators can be expected to significantly enhance and extend the range of protections afforded to Irish telephone users beyond what is provided for by the current 'static' CLI spoofing focussed interventions.

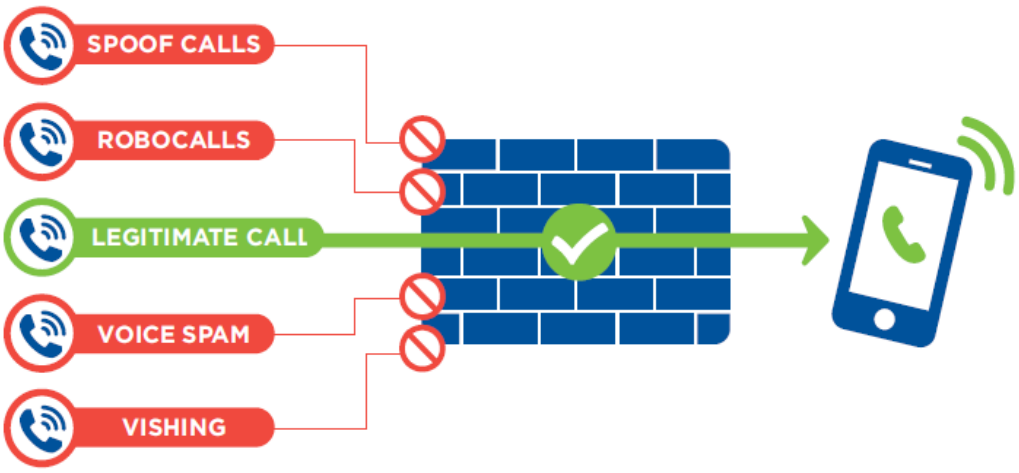
4.39 As part of the NCIT process, ComReg and the NCIT identified voice firewalls as a potential means of dynamically combatting scam calls, noting that fraudsters would over time find new means to execute scams and new pathways to contact Irish consumers.

[153] See Multi Band Spectrum Award 2022 (MBSA2) | Commission for Communications Regulation (comreg.ie)

[154] Schedule 1, Part 4, Section 6: Quality of Service (QoS) Obligations, 4 The "VoLTE Availability" Obligation, Licence Condition (1) *"(1) Where the Licensee has deployed LTE technology in any of the bands in which it holds rights of use under this Licence and also offers a mobile voice service to consumers using those bands, the Licensee shall:(a) enable VoLTE technology on its network and on its Base Stations which use those bands within 1 year; (b) make a VoLTE service available to its end users (including MVNO end users) that have a VoLTE-enabled handset within 1 year; and (c) deploy and maintain VoLTE across 50% of its LTE Base Stations which use those bands within 1 year and across 100% of such Base Stations within 2 years."*

[155] ComReg notes that some operators would likely have implemented VoLTE in advance of other operators and may need to implement this aspect of Mobile CLI much sooner.

Figure 24: A Voice Firewall



II. Technical feasibility and effectiveness

4.40 Voice firewalls are technically feasible with various different types having already been introduced by MNOs abroad (e.g., Norway[156], Spain[157] and UK[158]). Voice firewalls are also readily implementable noting that multiple security solutions providers provide not only Voice Firewall software, but also installation and training. ComReg's functional requirements specification for the intervention is available upon request to relevant operators. ComReg notes that this work stream is not as advanced as other proposals discussed in NCIT as part of the NCIT layered approach to implementing interventions[159]. In that regard, ComReg proposes to provide extended timelines (see below) to allow for the intervention implemented.

4.41 In relation to effectiveness, voice firewalls actively monitor network traffic and block malicious/scam calls depending on the rules configured within the firewall[160]. Voice firewall solutions use different sets of protocol information elements which leads to different types of scam filters. However, firewalls typically use a form of AI to review calls with advanced real time call data analytics using machine learning to detect and act upon unusual patterns of call

[156] Hiya News: Telenor Norway Deploys Hiya to Stop New Wave of Fraud Calls Targeting Norwegians
[157] https://blog.hiya.com/masmovil-pepephone-hiya-in-the-spanish-market
[158] https://newsroom.ee.co.uk/ee-takes-a-stand-against-scammers-with-latest-international-call-blocking-technology/
[159] It was decided to park the voice firewall intervention work for 12 months to focus on developing the DNO, LTPN, Fixed and mobile CLI interventions.
[160] In the context of a Voice firewall, a type 1 error (sometimes referred to as a 'false positive') occurs when the firewall mistakenly blocks a legitimate call, while a type 2 error (sometimes referred to as a 'false negative') occurs when the firewall fails to block a scam call. To minimize both type 1 and type 2 errors, Voice firewalls often use a combination of filtering techniques, which analyse various aspects of the call, such as the sender, content, and behaviour, to determine whether it is legitimate or scam/fraudulent. By continuously updating their filtering rules and algorithms, Voice firewalls can improve their accuracy and reduce the occurrence of both type 1 and type 2 errors.

signalling data, traffic volumes etc. ComReg notes the recent experience of EE in the UK which blocked as many as 11 million scam calls in a little over a month, following the introduction of an artificial intelligence-based Voice Firewall in July 2022[161].

4.42 Therefore, ComReg is of the preliminary view that the Voice Firewall intervention is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

4.43 ComReg is of the preliminary view that Voice Firewalls can be implemented within one year of any final decision, for the following reasons:

- The timeline from Vendors suggests that, once procured, the installation takes no more than 6-9 months; and
- Voice firewalls appear readily implementable noting that multiple security solutions providers provide not only Voice Firewall software, but also installation and training.

4.44 However, consistent with its layered approach to interventions as specified at the NCIT an additional 6 months would be provided such that Voice Firewalls should be implemented within 18 months of any final decision. This is also in recognition of the fact that overlapping resources will be required to implement both the static interventions (as outlined above) and the Voice Firewall.

4.45 Therefore, ComReg is of the preliminary view that the implementation of the Voice Firewall intervention within 18 months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow this Chapter.

6. Stir/Shaken

I. Description

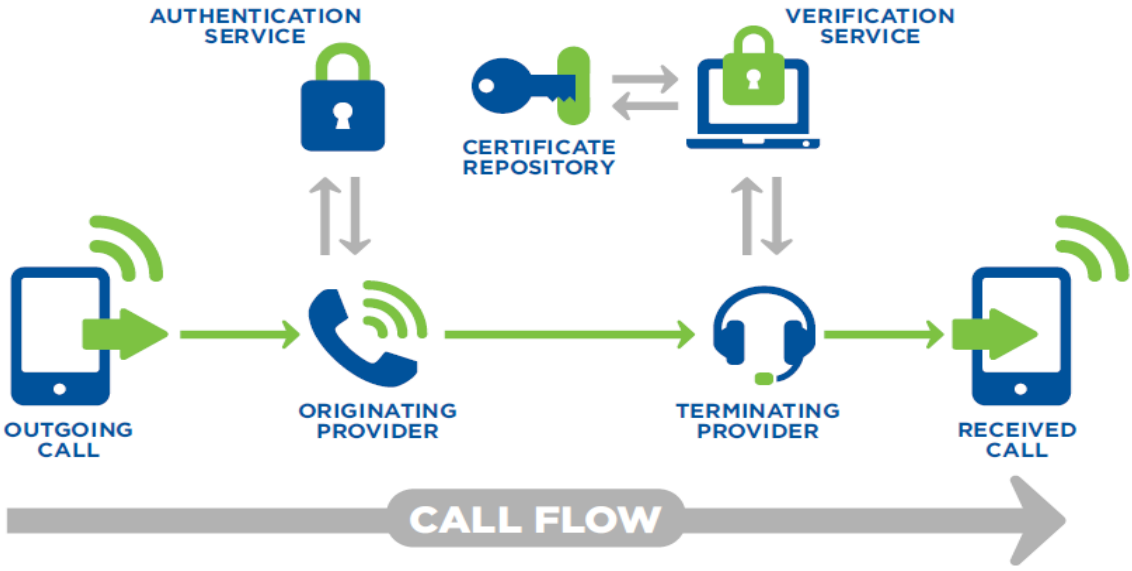
4.46 Currently, Voice calls are not authenticated as legitimate at origination. Therefore, fraudsters can originate calls which may terminate on Irish networks, ultimately reaching Irish consumers. Without a process of verification at source, operators cannot block Voice calls based on the source of origination alone given its unreliability.

4.47 In recognition of the CLI spoofing problem and the absence of end-to-end validation of the CLI, the Internet Engineering Task Force ("IETF") [162] has defined a technology architecture based on extensions to the Session Initiation

[161] Ibid
[162] https://datatracker.ietf.org/doc/html/rfc7340

Protocol[163] ("SIP") for call validation, called Secure Telephone Identity Revisited ("STIR"). This is implemented with the Signature-based Handling of Asserted information using toKENs ("SHAKEN") to form the STIR/SHAKEN scheme. STIR/SHAKEN could be a potential long term global solution for CLI validation. In summary, under STIR, phone numbers are 'attested' and 'signed' at call origination and 'verified' at call termination. The terminating network can then block or label the call as suspicious.

Figure 25: STIR/SHAKEN



II. Technical feasibility and effectiveness

4.48 STIR/SHAKEN has been in place US and has since evolved and been adopted in both Canada and France. Indeed, the efficacy of the technologies used for call authentication" in the STIR/SHAKEN framework was very recently assessed by the United States Federal Communications Commission ("FCC") (December 2022) which concluded that the framework is "*effective at authenticating caller ID information and identifying illegally spoofed calls, and we anticipate its effectiveness would increase as STIR/SHAKEN implementation becomes more widespread*". [164] Furthermore, it was noted that while there was concern that providers may be applying its technical requirements inconsistently. "*There is general agreement in the record, however, that when applied as designed, the technology used in the STIR/SHAKEN framework effectively allows providers to identify calls with illegally spoofed caller ID information.* Therefore, if implemented correctly and

[163] Session Initiation Protocol (SIP) is a signalling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. SIP is used for signalling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol (IP) networks as well as mobile phone calling over LTE (VoLTE).

[164] Triennial Report on the Efficacy of STIR/SHAKEN | Federal Communications Commission (fcc.gov)

on a widespread basis, STIRSHAKEN would be technically feasible in Ireland.

4.49 However, due to the underlying technology, STIR/SHAKEN's caller ID authentication standards can only work on IP-based phone networks[165]. Because a non-IP approach has yet to be determined the above evaluation could not include feasibility of STIR/SHAKEN for non-IP networks. ComReg notes that the FCC has launched an inquiry to examine potential call authentication solutions for non-IP networks, including the nexus between non-IP caller ID authentication and the IP transition generally.[166] Given the substantial use of non-IP networks in Ireland currently – the use of STIRSHAKEN absent a solution for non-IP based networks would mean that STIRSHAKEN may be technically feasible but it is not viable at this point given the extent of legacy non-IP technologies in Irish networks. However, ComReg would continue to monitor progress on a solution for non-IP based networks and update its view in line with last available information.

4.50 In relation to effectiveness, implementation of caller ID authentication technology using the STIR/SHAKEN standards should reduce illegal spoofing and help operators identify calls with illegally spoofed caller ID information before those calls reach their subscribers. STIR/SHAKEN allows voice service providers to verify that the caller ID information transmitted with a call matches the caller's number.[167] Its widespread implementation aims to reduce the effectiveness of illegal spoofing and allow operators to identify calls with illegally spoofed caller ID information before those calls reach their subscribers.

4.51 However, its effectiveness is dependent on widespread rollout across all operators and over an appropriate period which is discussed further below. For example, in the US where it has been implemented since 2021[168] consumers received an extraordinary 34.9 billion unwanted robocalls over the first half of 2022, but only 8% of this volume originated from the top-seven US carriers (AT&T, Lumen, Charter, Comcast, T-Mobile, US cellular and Verizon), each of which have implemented the STIR/SHAKEN framework. [169]The framework has yet to be implemented by smaller operators who account for much of the remaining unwanted calls originating in the US, but all are required to do so by

[165] Non-IP networks do not have the capability to maintain this type of digital information on calls, therefore the STIR/SHAKEN verification information, including who generated the call, is not available on those networks.
[166] See Call Authentication Trust Anchor, WC Docket No. 17-97, Notice of Inquiry, FCC 22-81, at 17-21, paras. 37-42 (rel. Oct. 28, 2022) (Non-IP Authentication Notice of Inquiry).
FCC Seeks to Fill Challenging Gap in STIR/SHAKEN Robocall Defenses | Federal Communications Commission
[167] In summary, under STIR, phone numbers are 'attested' and 'signed' at call origination and 'verified' at call termination. STIR/SHAKEN allows voice service providers to verify that the caller ID information transmitted with a particular call matches the caller's number. If a call fails verification, there is high likelihood it is maliciously spoofed, and such information can be shared with the caller, or the call can be blocked.
[168] Both the Canadian Radio-television and Telecommunications Commission ("CRTC") and the Federal Communications Commission ("FCC") in the United States required operator use of the protocols by June 30, 2021 Combating Spoofed Robocalls with Caller ID Authentication | Federal Communications Commission (fcc.gov)
[169] Robocall Investigation Report | TNS (tnsi.com)

June 30, 2023.

4.52 Furthermore, given that many of the nuisance calls in Ireland are generated offshore, there would be little value currently in implementing these standards in Ireland on its own unless it became a globally adopted approach or the balance of nuisance communications swung heavily toward onshore generation. Consequently, its effectiveness will depend on its use globally. Given that many of the nuisance calls in Ireland are generated offshore, there would be little value currently in implementing these standards in Ireland on its own unless it became a globally adopted approach or the balance of nuisance communications swung heavily toward onshore generation.

4.53 In order to tackle the large number of nuisance calls originating and terminating outside North America, the FCC issued an order in May[170] that requires each gateway provider to submit a certification and mitigation plan to the Robocall Mitigation Database[171]. The order also requires gateway providers to authenticate calls with US NANP numbers in the caller ID field by June 30, 2023[172]. However, it remains to be seen how effective such an approach will be in practice. Again, ComReg will monitor developments in this regard.

4.54 Implementing a STIR/SHAKEN type intervention would require the input and cooperation of other countries at least on a quasi-global scale. Such input and cooperation would need to be carried out at least at a European level, most likely by the Conference of Postal and Telecommunications Administrations ("CEPT"), so as to encompass all of Europe and would thus require the commitment of many nation states[173], European and beyond, and far more than the two that have done so in North America[174]. Bearing in mind the immaturity of implementation of any of these standards globally and the uncertainty surrounding which approach is likely to win out, ComReg considers this potential intervention can only be considered a longer term one at this point, notwithstanding its indubitable potential to be a long-term global solution for CLI validation[175] and the rapidly evolving macroenvironment. ComReg may need to revisit the use of STIRSHAKEN, particularly if the other proposed interventions

[170] https://docs.fcc.gov/public/attachments/DOC-383499A1.pdf
[171] The FCC maintains a Robocall Mitigation Database in which voice providers are required to "certify whether and to what extent they have implemented the STIR/SHAKEN caller ID authentication framework." Phone companies must reject any calls from voice service providers that are not listed in the database, and the FCC can issue fines to providers that don't file certifications.
[172] In effect, the FCC expands the prohibition to include calls from not only foreign originating voice service providers but also foreign intermediate providers. Therefore, once effective, domestic providers may only accept calls carrying U.S. NANP numbers sent directly from foreign-originating or intermediate providers that are listed in the Database.
[173] The French decision of 2019 [15] also evokes STIR/SHAKEN as a long-term solution. In order to test it, ARCEP has already introduced specific ranges (for geographic, mobile and non-geographic numbers) which are dedicated to authenticated numbers. In July 2020, France adopted legislation requiring French service providers to implement a call authentication solution protecting their customers from various types of telephony-based fraud by July 2023
[174] In 2021, Canada's telecommunication regulator, the CRTC, mandated the use of caller ID authentication (IP voice calls only) using the STIR/SHAKEN protocol that the FCC already applies in the US to block robocalls .
[175] It is likely that all European operators wishing to terminate calls, where both the called party number and the calling party number are US numbers would have to implement STIR/SHAKEN at some point.

referenced in this consultation fail to deliver in a timely and effective fashion.

III. Timelines

4.55 The proposed implementation timelines are not considered further given the technical feasibility issues highlighted above.

4.56 In light of the above assessment, ComReg is of the preliminary view that STIR/SHAKEN is not a valid regulatory option for the purpose of this consultation and consequently is not considered further at this time.

4.3 Potential SMS Interventions

7. Shortening the chain

I. Description

4.57 Currently, many organisations that contact their customers via SMS, use a Sender ID to enhance the recognition and credibility of their SMS messages. Using Sender ID spoofing, fraudsters can send messages that appear to originate from legitimate businesses to deceive consumers into following the instruction contained within the message and providing financial or personal information.

4.58 SMS are not authenticated as legitimate at origination and are often rerouted internationally through one or more cloud/aggregator networks before arriving at the terminating network. Terminating networks therefore cannot block or screen Sender ID, without further information on their origination or pathway. Therefore, fraudsters can originate SMS using misleading Sender ID which may terminate on Irish networks, ultimately reaching Irish consumers.

4.59 From initial responses garnered from relevant companies, the banks (and it appears, other SMS clients such as delivery companies) appear to rely on a number of business communication providers, who in turn depend on an unknown (and potentially varying) number of aggregators ‘hops’ to deliver an SMS message to the end user. SMS messages which traverse several providers has an increased exposure to potential interception by threat actors, thereby compromising the privacy of the message.

4.60 ComReg and the NCIT initially proposed to reduce such risk by limiting the use of particularly sensitive Sender IDs to certain paths, an approach known as “shortening the chain”. This amounts to ensuring that the pathways for key Sender IDs are secure and would not carry SMS with false or misleading Sender ID. Further, limiting these messages to defined routes would enable the MNOs to filter spoofed messages arriving on other routes. ComReg and the NCIT agreed to progress this measure for key companies with Sender IDs most

susceptible to impersonation by fraudsters. While the members of the NCIT (all ECS providers) agreed this was technically feasible, the success of this measure ultimately depends on engagement and action by the relevant businesses.

II. Technical feasibility and effectiveness

4.61 This intervention would require businesses (e.g., financial institutions) to work with their messaging providers to 'shorten the chain', ensuring messages are delivered over a short, fixed route. MNOs can then block messages bearing these sender IDs over other routes (i.e., distinguishing the scam messages from the genuine). This initial filtering has the potential to be very effective in blocking many of the most harmful scam messages and should notably address scams based on spoofed SenderIDs, at least in the case of the particularly sensitive SenderIDs (e.g., Banks).

4.62 Members of the NCIT agreed this was technically feasible and could potentially be achieved with a bank's existing messaging provider, or it might involve a change of messaging provider, or even a direct connection from a banks' systems to one or more MNO networks. However, the success of this measure depends on engagement and action by the relevant businesses (e.g., banks/delivery companies). To help achieve this, and at the request of MNO NCIT members, ComReg has contacted the financial institutions, via the BPFI, seeking information on the routes that their SMS messages might take and suggesting that they could look to 'shorten the chain' to enable the MNOs to block scam messages from other sources

4.63 However, progress on this intervention can be best described as underwhelming, with delays in the confirmation of key Sender IDs by target companies. Based on the responses received from the target companies to its letter of 1 June 2022 and subsequent meetings, ComReg has formed the view that the companies were not prepared or willing to undertake the work necessary to "shorten the chain"[176]. It might be the case that such companies do not fully understand the SMS services they have come to rely upon for their critical business operations and therefore assume little to no responsibility for the integrity of the end-to-end delivery path; to their mind the matter has been outsourced.

[176] In ComReg's view these responses did not fully address the questions asked and did not constitute a willingness to 'shorten the chain' as requested. One response claimed that the chain has already been shortened according to its messaging provider which ComReg considered to not be credible given that provider's position regarding the approach of shortening the chain in the NCIT and in bilateral meetings. ComReg continued to apply pressure via engagement with the Central Bank of Ireland which resulted in a round of meetings with the three largest (remaining) retail banks – BOI, AIB and Permanent TSB. During the meetings with the banks, ComReg put forward the case that it is impossible to secure the bank's sender IDs with the current A2P messaging market structure; that the MNOs stood ready to block messages from unapproved sources; and that ComReg are available to advise on the dialog between the banks and their messaging providers if desired.

4.64 In light of the disappointing level of engagement, it is unlikely that this intervention would be effective as ComReg cannot mandate business to 'shorten the chain' and the effectiveness of this intervention cannot be achieved without the committed voluntary assistance of Sender ID users.

4.65 In light of the above assessment, ComReg is of the preliminary view that the 'shortening the chain' intervention is not a valid regulatory option for the purpose of this consultation and is not considered further in this consultation.

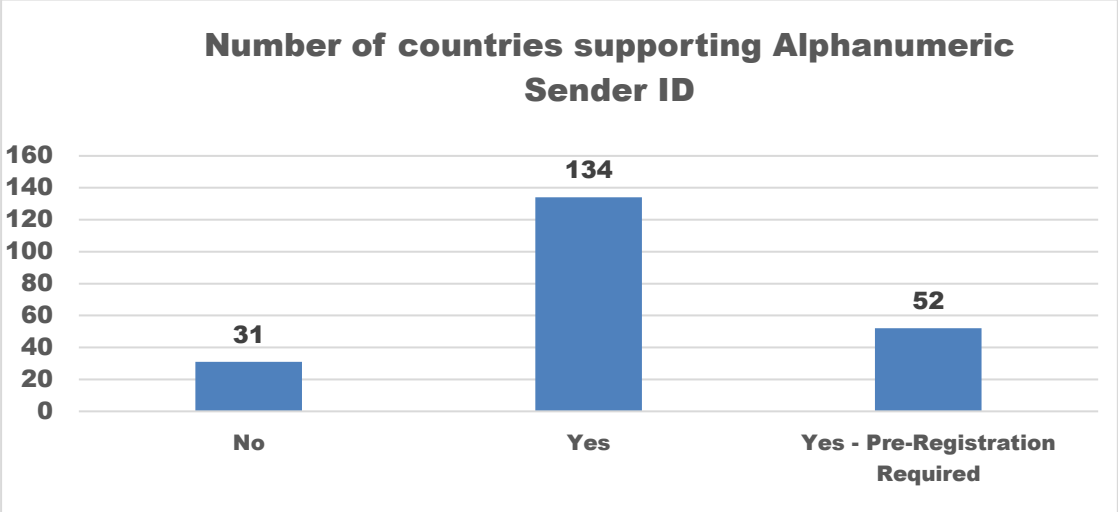
Interventions 8 - 10 – The regulation of Sender ID

4.66 The following three proposed interventions (i.e., 8, 9 and 10) all concern regulating the use of SMS originating addresses including Sender ID, which is one means of tackling Sender ID spoofing.[177] In summary, a regulator can require operators to block all SMS carrying Sender IDs, or only those that are unregistered or do not conform to certain rules. This is not a novel approach and has been implemented to various degrees in other jurisdictions.

4.67 In total, it appears that over one in three countries regulate Sender ID to some extent, with data from Twilio[178] covering over 200 countries indicating that while Sender ID is permitted in the majority of countries (62%), a significant minority of countries require pre-registration (24%) or do not permit Sender IDs (14%) such as the USA and Canada. Twilio report that this number is increasing over time as "*In many countries, regulatory bodies are increasingly filtering illegitimate A2P SMS use cases to curb unwanted messaging*."[179] Indeed, ComReg is aware that both Agcom and the ACMA are currently consulting on similar measures.

[177] SMS using a Sender ID are not necessarily authenticated in any way (neither at point of origination in spoofing cases nor along its "route"), facilitating fraud using Sender ID Spoofing.
[178] Twilio website "I*nternational support for Alphanumeric Sender ID*" https://support.twilio.com/hc/en-us/articles/223133767-International-support-for-Alphanumeric-Sender-ID
[179] Ibid

Figure 26: International support for Alphanumeric Sender ID



Source: Twilio[180]

4.68 ComReg now examines a number of different interventions which work by requiring MSPs (Mobile Service Providers) to block SMS spoofing Irish mobile numbers or carrying Sender ID deemed invalid, which are to block all:

- SMS with Sender ID ("Sender ID Ban")
- SMS with Sender IDs which are not pre-registered ("Sender ID Registry")
- SMS with ID which cannot be verified by code verification ("SMS OD Verification")

8. Sender ID Ban

I. Description of interventions

4.69 The most straightforward means of preventing Sender ID spoofing is to require mobile operators to block SMS messages containing any alphanumeric SenderID.

II. Technical feasibility and effectiveness

4.70 This approach involves blocking all SMS messages bearing any Sender ID. This is technically feasible because operators would block all Sender IDs in the same way as it would block Sender IDs not on a SMS Registry.

4.71 This approach would be effective because it would block all SMS

[180] ComReg assumes this information is accurate, and accepts the information as described by Twilio on its website – Link "*Alphanumeric-Sender-ID-for-Twilio-Programmable-SMS*". Twilio link to the data underlying the Table stating "*Which Countries Support Alphanumeric Sender IDs? You can find out which countries support Alphanumeric Sender IDs on this page*."

communications using Sender IDs (only the originating numbers would be displayed). In this way, fraudsters would be unable to pose as legitimate businesses by contacting consumers using Sender IDs.

III. Timelines

4.72 ComReg is of the preliminary view that the Sender ID Ban can be implemented within 3 months of any final Decision. This preliminary view is informed by:

- Discussions with industry stakeholders in the NCIT indicates that blocking SMS with Sender IDs could be implemented relatively straightforwardly with time mainly required to provide businesses notice that Sender IDs would no longer be available as a means to communicate; and
- The need for some amount of time to allow for the usual change management processes/practices within an operator environment.

4.73 Therefore, ComReg is of the preliminary view that the Sender ID Registry is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow this section.

9. Sender ID Registry – Full or partial

I. Description

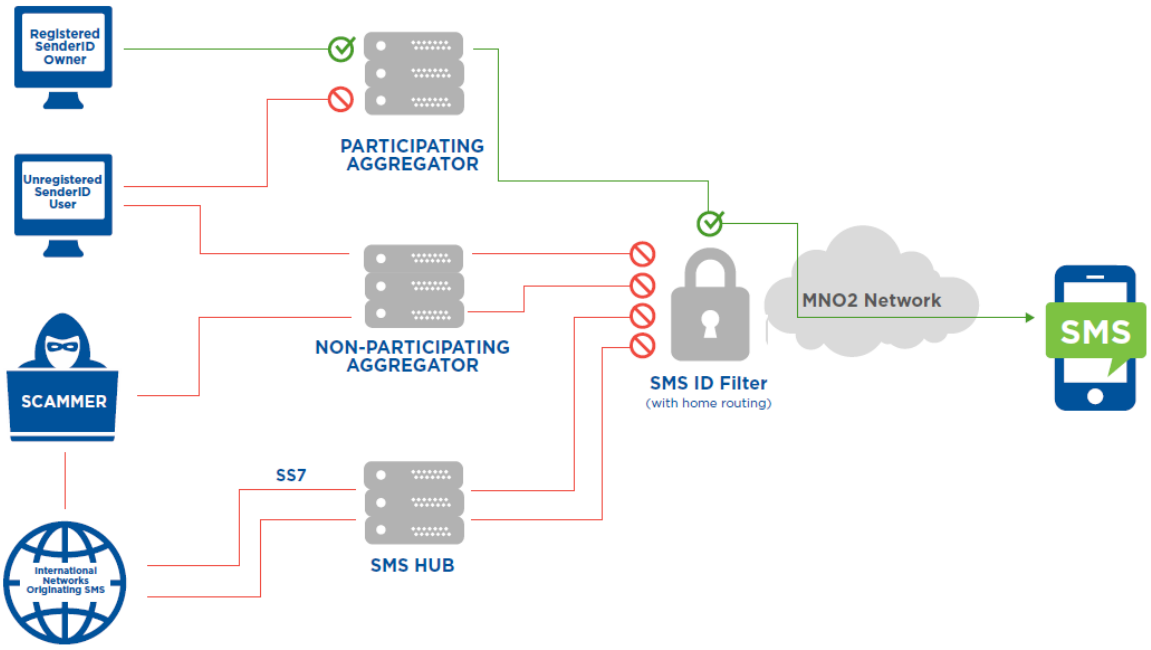
4.74 Sender ID may also be protected by securing the pathways by which SMS are transmitted. This involves requiring senders and aggregators that send or carry messages containing any alphanumeric Sender ID ("Participating Aggregators") to follow a set of rules or a code of practice which requires that they register their Sender ID with ComReg or a registry operator and thereby authenticate the source of such messages. The MSPs[181] are then responsible for blocking any message bearing that Sender ID or potentially any unregistered Sender ID from any other source. To clarify, this includes blocking SMS that are spoofing Irish mobile numbers instead of using invalid Sender ID. This blocking is required to ensure the effectiveness of the Sender ID Registry and reduce the avenues for scammers for impersonating businesses/organisations or individuals. Absent such blocking scammers would move scams based on Sender ID to scams based on spoofing of Irish mobile numbers using SMS, significantly reducing the effectiveness of the Sender ID Registry.

4.75 A registry may be "full", encompassing all potential Sender IDs or "partial" whereby only the most important Sender IDs are covered. A key design parameter for any partial registry is whether SMS messages with unregistered

[181] For the avoidance of doubt, all participating MSPs are responsible for blocking all SMS containing a Sender ID that are not compliant with the technical specification.

Sender IDs are permitted or blocked automatically. Alternatively, such messages could be labelled, so as to inform consumers of the unverified source[182].

Figure 27: Full Sender ID Registry



II. Technical feasibility and effectiveness

4.76 The technical feasibility of this intervention concerns (i) the setting up and running of the registry by ComReg including the secure authentication of Sender ID owners (ii) the implementation of filtering functionality and relevant MNO connections by the Participating Aggregators and (iii) the technical requirement for operators to block any message spoofing Irish mobile numbers or bearing a sender ID from any source other than approved Participating Aggregators connections according to the registry.

- In relation to (i), while the set-up and running costs associated with the SMS Registry are non-trivial (discussed below), there are no technical barriers preventing its implementation. Both full and partial SMS are technically feasible and have already been implemented in

[182] The IMDA adopted this approach for its implementation period of its full registry to facilitate the transition.

other jurisdictions. For example, ComReg notes that a SMS registry has been introduced in Italy[183], Singapore[184] and the Czech Republic.

- In relation to (ii), most aggregators operate in the global market and have implemented similar or identical functionality in other jurisdictions.
- In relation to (iii), blocking any message spoofing Irish mobile numbers or not on an authenticated list is straightforward for operators to implement and no technical issues should arise in its implementation.

4.77 In relation to its effectiveness, this intervention would be effective at reducing nuisance communications by requiring aggregators to register their Sender IDs to ensure that only legitimate businesses or organisations can use Sender IDs to send SMS to mobile users. For example, since the establishment of the Singapore Sender ID Registry ("SSIR") in March 2022:

- There has been a 64% reduction in scams through SMS from Q4 2021 to Q2 2022.
- Scam cases perpetrated via SMS now account for around 8% of scam reports in Q2 2022, down from 10% in 2021.[185]

4.78 It is no longer a voluntary regime, where organisations that wish to protect their Sender IDs ("Protected Sender IDs") could register with the SSIR. The full registration requirement took effect in Singapore on 31 January 2023 which will further increase its effectiveness by including all organisations that use Sender IDs.

4.79 Therefore, ComReg is of the preliminary view that the SMS Registry is likely to be technically feasible and effective at reducing nuisance communications.

III. Timelines

4.80 While introducing a Sender ID registry takes considerable work on the part of the regulator (full or partial), ComReg is of the preliminary view that a partial or full Sender ID registry could be implemented within 12 months and 24 months of any final Decision. This preliminary view is informed by:

[183] The rule requires that the senders of bulk SMS messages register their Sender ID with AGCOM, the Italian Communications Authority, as per AGCOM Resolution No. 42/13/CIR NRA entitled: Rules for Testing of Indicators for Alphanumeric identification of the Subject in the caller SMS/MMS used for Messaging Services. A Sender ID cannot be used if it has not been registered on AGCOM's database. https://alias.agcom.it/docs/guida_registrazione_alias.pdf
[184] https://www.sgnic.sg/smsregistry/overview
[185] Full Sender ID Registration to be required by January 2023 - Infocomm Media Development Authority (imda.gov.sg)

- Discussions with industry stakeholders and the IMDA that indicate that while introducing a Sender ID registry takes considerable work on the part of the regulator (full or partial) it is implementable within a reasonable timeframe, from 6 months in the case of a partial registry to 18-24 months in the case of a full registry.
- In relation to the full registry, 24 months accounts for the need for time to allow for are a number of parallel workstreams required to make SMS ID registry which are for:
    - ComReg – 6-12 months approvals, before implementation which could take another 12 months
    - MNOs & participating aggregators - 6-12 months to set up system and conduct testing etc.
- The only benchmark for a full registry is Singapore, which suggest 18 months is possible. The 24 months can be combined with a phase-in period – roughly 6 months before deadline – when SMS with unregistered IDs would be flagged as “likely spam”.

4.81 Therefore, ComReg is of the preliminary view that the Sender ID Registry is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow this section.

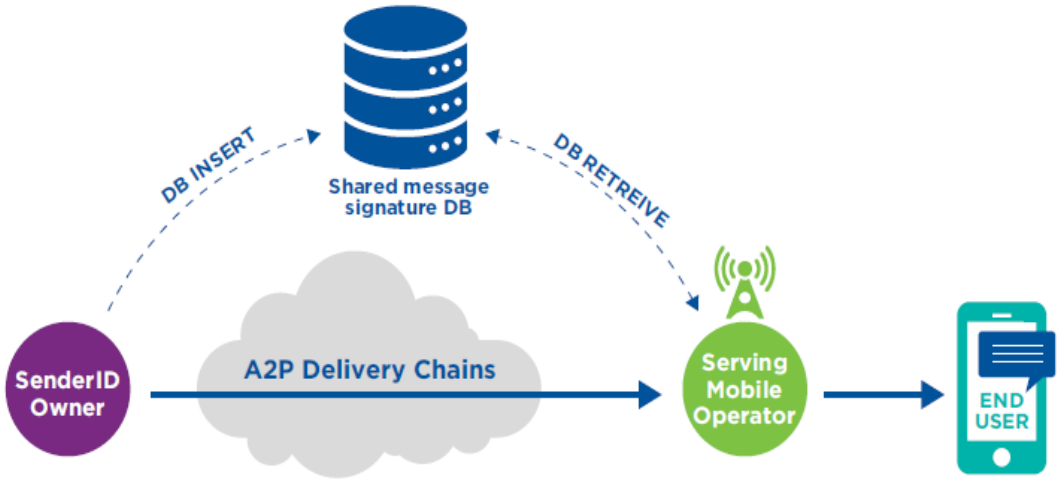
10. SMS Origin-Destination verification

I. Description

4.82 One means of securing Sender ID would be through use of message verification codes. This solution would involve requiring aggregators, (the originator of an SMS bearing a protected SenderID) to publish to a shared cloud-based database with a unique signature of the message, using a unique identifier known as a “hash value”, before sending it down an unmodified, un-shortened delivery chain. A hash value is a very large number that’s calculated through an algorithm, and that is associated with a particular piece of data (in this case some combination of the Originating Address, Destination Address and text message content). If the data is altered in any way, and the hash is recalculated, the resulting hash will be completely different. The concept of hashing is a cornerstone of IT security and is often used in digital forensic investigations to verify the authenticity of digital evidence for example.

4.83 Once the message arrives at the MNO for delivery, its signature would be freshly re-calculated and checked against the shared database. Only unmodified messages from sources with write-access to the shared database would pass this check, thereby allowing other messages to be discarded by the MNO before delivery.

Figure 28: SMS Origination-Destination verification



II. Technical feasibility and effectiveness

4.84 Several solution providers, and Italian NRA AGCOM have posited this concept which is sometimes informally (and very loosely) referred to as “STIR/SHAKEN for SMS”. However, this solution appears solely theoretical at present, as ComReg is unaware of any network applying this in a real-world setting. Therefore, it requires further studies to confirm its practicality and process design, and no existing implementations based on this approach exist today. ComReg is therefore of the preliminary view that it is prudent not to consider SMS Origin-Destination verification at this juncture but will continue to monitor its development.

4.85 In light of the above assessment, ComReg is of the preliminary view that SMS Origination-Destination verification is not a valid regulatory option for the purpose of this consultation and consequently is not considered further at this time.

11. SMS Scam Filter

I. Description

4.86 A SMS Scam Filter involves the use of advanced real time data analytics using Machine Learning and Artificial Intelligent techniques to detect and act upon unusual patterns of content or hyperlinks in SMS messages. The deployment of SMS Scam Filter by Irish operators can be expected to significantly enhance and extend the range of protections afforded to Irish mobile telephone users beyond what is provided for by any other interventions focussed on ‘static’

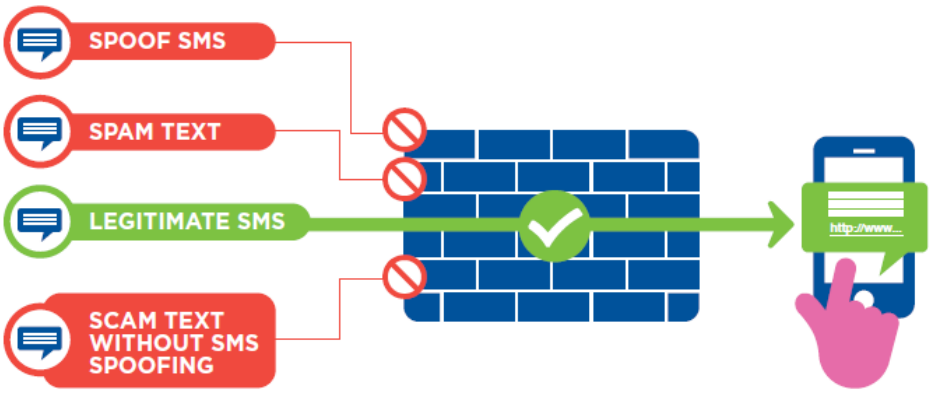
Sender ID Spoofing[186]. As part of the NCIT process, ComReg and the NCIT identified SMS Scam Filters as a potential means of dynamically combatting scam texts, noting that fraudsters would over time find new means to execute scams and new pathways to contact Irish consumers.

4.87 The SMS Scam Filter scans the contents of the SMS by automatically scanning all text messages and filters those that are likely to contain malicious content. Absent this approach only a rudimentary evaluation of SMS is possible, and any such evaluation is inherently limited (e.g., the metadata). This data provides a far more limited indication of the nature of message content, being unable to identify let alone examine URLs and other signs of a scam.

4.88 Any attempt to filter scams without content scanning is unlikely to be accurate and therefore effective in combatting scam. Indeed, numerous scam texts present in Ireland today may be far less likely to be identified and blocked absent content scanning (e.g., P2P scams such as the "Hi Mum" scam). Moreover, any filtering which excluded content scanning would be easily overcome by fraudsters, as it would not identify suspicious contents and URLs that are highly indicative of a scam.

4.89 For these reasons, content scanning is essential to enable the eventual deployment of a what could be termed a "SMS firewall", whereby all SMS messages routed to Irish consumers are analysed, classified and blocked where deemed likely to be scam. Therefore, throughout this Consultation, where ComReg refers to a SMS Scam Filter, this involves the use of content scanning.

Figure 29: Graphical representation of SMS Scam Filter



[186] In the context of SMS Scam Filter, a type 1 error (sometimes referred to as a 'false positive') occurs when the firewall mistakenly blocks a legitimate text, while a type 2 error (sometimes referred to as a 'false negative') occurs when the SMS Scam Filter fails to block a scam text. To minimize both type 1 and type 2 errors, SMS Scam Filters use a combination of filtering techniques, which analyse various aspects of the message, such as the sender, content, behaviour, and most importantly the message content to determine whether it is legitimate or scam/fraudulent. However, by continuously updating their filtering rules and algorithms, a SMS Scam Filter can improve their accuracy and reduce the occurrence of both type 1 and type 2 errors.

II. Technical feasibility and effectiveness

4.90 SMS Scam Filters have been implemented by numerous operators and are readily available noting that multiple security solutions providers provide relevant software, installation, and training services. Under this intervention, the mobile operators would deploy an anti-scam filtering capability to scan for indicators of SMS scam and harmful content in real time on new or pre-existing SMS Scam Filters. The overall aim of this approach is to prevent the spread of malware via SMS by adding advanced SMS Scam Filter capabilities to the messaging domain.

4.91 Discussions with market players indicate that SMS Scam Filters are effective in blocking scam texts. SMS Scam Filters have been highly effective in other countries also which have seen a significant decline in the rates of scam texts. For example:

- Vodafone UK reported that daily average volumes of scam texts fell by 76% in December compared to May, with over 45 million phishing messages blocked since the end of August 2021.[187]
- Everything EveryWhere (EE) in the UK, blocking as many as two hundred million scam texts in a year, following the introduction of an artificial intelligence based "anti-scam filter" in 2021[188].
- In April 2022, Telstra in Australia[189] introduced the technology and had blocked over 185 million scam text messages in the three months to July[190] and 225 million to December – around 775 malicious texts blocked every minute[191].
- In 2019, Optus deployed an SMS Scam Filter to combat the rise of SMS scams. Between 1 December 2020 and 31 March 2022, Optus blocked more than 232 million scam calls and now block an average of ten million texts every month.[192]
- Singtel, Starhub, and M1 in Singapore have implemented anti-scam filtering solutions in their networks from end-October 2022.

4.92 Therefore, ComReg is of the preliminary view that a SMS Scam Filter is likely

[187] https://www.vodafone.co.uk/newscentre/news/vodafone-hammers-christmas-fraudsters-with-spam-reduction-december-2021
[188] https://newsroom.ee.co.uk/ee-takes-a-stand-against-scammers-with-latest-international-call-blocking-technology/
[189] Australian operators must "make best efforts to identify, trace, block and otherwise disrupt scam calls and scam SMS" messages, the new rules mandate, noting tell-tale signs of scams including blocked or invalid caller line identification (CLI) numbers, calls that don't present call-back details to the destination network, and CLIs that don't correspond to the range allocated to a particular carrier.
https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf
[190] 185 million malicious texts blocked and counting (telstra.com.au)
[191] https://exchange.telstra.com.au/tag/scams/
[192] https://www.optus.com.au/connected/leaders-insights/optus-fight-against-fraud

to be technically feasible and effective at reducing nuisance communications.

4.93 ComReg notes that the SMS Scam Filter can be implemented in a number of ways. It could require operators to implement a SMS Scam Filter by requiring operators to apply a SMS Scam Filter to all SMS for:

- All mobile consumers by default ("All-in");
- All mobile consumers, except where the consumer wishes not to avail of the service (i.e., the consumer "Opt-out"). This could, for example, include automatic enrolment, wherein a notification SMS would be sent to mobile users, with a an opt-out option at the end stating (e.g., "Send STOP to unsubscribe")
- All mobile consumers, that indicate their wish to avail of the service (i.e., the consumer "Opt-In"). This could, for example, be achieved by a notification SMS offering the service being sent to mobile users, with an Opt-In option at the end stating (e.g., "Send YES to subscribe").

4.94 However, the imposition of the SMS Scam Filter as an "All in" or an "Opt-Out" introduces potential legal issues on the protections of end user rights in relation to interception and data protection as provided in the ePrivacy directive and the GDPR. It is ComReg's understanding that a change to the current legislation to allow for the SMS Scam Filter is necessary. ComReg has been in constructive and detailed meetings with the Department of the Environment, Climate and Communications in relation to these issues and the matter is currently under consideration.

4.95 ComReg welcome views from Interested Parties on how the SMS Scam Filter could be implemented and, in particular, views on whether it should be implemented as an All In, Opt-Out or an Opt-In as described above.

III. Timelines

4.96 ComReg is of the preliminary view that SMS Scam Filter can be implemented within one year of any final decision, for the following reasons:

- This is a standard timeline for the implementation of a new platform
- Operators have indicated to ComReg that it would take a year to have this intervention fully operational in their networks.
- The timeline from Vendors suggests that, once procured, the installation takes no more than 6-9 months; and
- SMS Scam Filters appear readily implementable noting that multiple security solutions providers provide not only the software, but also installation and training.

4.97 Therefore, ComReg is of the preliminary view that the implementation of the SMS Scam Filter intervention within 12 months of any Decision is a valid regulatory option for the purpose of this consultation and should be considered in one or more of the draft RIAs which follow this section.

Conclusion.

4.98 Given the above, ComReg notes that there are eight valid regulatory options (summarised below) that are technically feasible and would likely be effective in reducing nuisance communications. These will next be assessed in the draft RIAs against ComReg's broader statutory objectives and duties including the obligation to promote competition and protect consumers.

Table 7: Suitable interventions

	Interventions
1.	DNO
2.	PN
3.	Fixed CLI Call Blocking
4.	Mobile CLI Call Blocking
5.	Voice Firewall
6.	Sender ID Blocking
8.	SMS Registry
9.	SMS Scam Filter

Chapter 5

5 Draft Regulatory Impact Assessments

5.1 Building on its earlier considerations, ComReg next considers which interventions among those discussed in Chapter 43.4 can combat Nuisance Communications and reduce the economic and social harm being experienced by users of telecommunications services in Ireland outlined in Chapter 3.

5.2 This Chapter sets out ComReg's four draft RIAs which assess the various interventions, as well as an assessment of the combined effect of the preferred interventions across all RIAs.

- First, ComReg assesses a number of matters common to all RIAs in order to identify the relevant policy issue, regulatory options and stakeholders.
- Second, within each individual draft RIA, ComReg then assesses the various regulatory options to determine ComReg's preferred combination of interventions having regard to the impact on stakeholders, competition, and consumers.

5.3 Finally, ComReg assesses the preferred interventions from each of the RIAs (the "Overall Preferred Option") against ComReg's statutory remit, including relevant functions, objectives, duties and principles which are outlined in Annex 2.

5.1 RIA Framework

5.4 In general terms, a RIA is an analysis of the likely effect of a proposed new regulation or regulatory change, and, indeed, of whether regulation is necessary at all. A RIA should help identify the most effective and least burdensome regulatory option and should seek to establish whether a proposed regulation or regulatory change is likely to achieve the desired objectives, having considered relevant alternatives and the impacts on stakeholders. In conducting a RIA, the aim is to ensure that all proposed measures are appropriate, effective, proportionate and justified.

5.5 A RIA should help identify the most effective and least burdensome regulatory option and should seek to establish whether a proposed regulation or regulatory change is likely to achieve the desired objectives, having considered relevant alternatives and the impacts on stakeholders. In conducting a RIA, the aim is to ensure that all proposed measures are appropriate, effective, proportionate and justified. RIA's will be finalised in the final Decision having taken into account

responses to this Consultation.

5.1.1 Structure of the RIAs

5.6 As set out in ComReg's RIA Guidelines[193], there are five steps in a RIA. These are:

a) Step 1: describe the policy issue and identify the objectives;

b) Step 2: identify and describe the regulatory options;

c) Step 3: determine the likely impacts on stakeholders;

d) Step 4: determine the likely impacts on competition; and

e) Step 5: assess the likely impacts and choose the best option.

5.7 A RIA typically assesses each of the five analytical steps consecutively before concluding on its preferred option. The draft RIAs in this consultation follow a similar structure, however, the inclusion of eight potential interventions across both voice and SMS poses a challenge because many of the possible interventions are not mutually exclusive, are complementary or target the same overarching policy issues. Further, as these interventions apply in many cases to the same operators, any combination of interventions could potentially result in cumulative effects. Therefore, a number of steps will be conducted jointly across all RIAs.

5.8 Considering the above and to allow for the appropriate assessment of the interventions, while avoiding any duplication of analysis in the following sections, ComReg first, identifies the overarching policy issues and objectives to be addressed across all draft RIAs, noting each of the individual RIAs may have separate policy issues and objectives. (i.e., Step 1). Then ComReg determines the draft RIAs that will be required and the associated regulatory Options (i.e., Step 2 of the RIA process) and identifies the industry stakeholders (i.e., Step 3 of the RIA).

5.9 ComReg has adopted the following structure in relation to Step 3 and Step 4 – the impact on consumers is considered first, followed by the impact on stakeholders and consumers. This order does not reflect any assessment of the relative importance of these issues – however much of the impact on industry stakeholders (e.g., use of voice calls) and competition (e.g., distortions to competition) derive from consumers likely reaction to scam calls and texts.

[193] See Document 07/56a – Guidelines on ComReg's approach to Regulatory Impact Assessment – August 2007.

5.10 Of themselves, the RIA Guidelines and the RIA Ministerial Policy Direction provide little guidance on how much weight should be given to the positions and views of each stakeholder group (i.e., Step 3 of the RIA process), or the impact on competition (i.e., Step 4 of the RIA process). Accordingly, ComReg has been guided by its statutory objectives which it is obliged to seek to achieve when exercising its functions.

5.11 Finally, ComReg assesses the extent to which the Overall Preferred Option regulatory measure would, if implemented, be likely to achieve one or more of ComReg's statutory objectives in the exercise of its related statutory function or functions (Step 5) across all interventions from the individual draft RIAs. ComReg will assess any cumulative effects of interventions on their proportionality, competition, and consumers.

Competition and consumers

5.12 The focus of Step 4 is to assess the impact on competition of the various regulatory options available to ComReg. In that regard, ComReg notes that it has various statutory functions, objectives and duties which are relevant to the issue of competition. These are set out at Annex 2.

5.13 As outlined below, there are different elements to competition that are relevant in determining the impact of any of the preferred options. These include:

a) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality[194] ("Impact on consumers").

b) Encouraging efficient use and ensuring the effective management of numbering resources[195] ("Efficiency use of numbers");

c) ensuring that there is no distortion or restriction of competition in the electronic communications sector[196] ("Promoting competition"); and

d) Promoting efficient investment and innovation in new and enhanced infrastructures[197] ("Efficient Investment").

5.14 The 'Impact on Competition' assessment, arising from each of the regulatory options, is assessed within each RIA under the headings provided in (b) to (d) above. In doing so, ComReg notes that it previously set out its assessment of the impact of the Options on each of the stakeholders and consumers earlier in each RIA and does not repeat the assessment and instead ComReg refers to

[194] Section 12(2)(a)(i) of the Communications Regulation Act 2002, as amended, and see too Regulation 4(3)(d) of S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022.
[195] Section 12(2)(a)(iv) of the Communications Regulation Act 2002, as amended. .
[196] Section 12(2)(a)(ii) of the Communications Regulation Act 2002, as amended.
[197] Regulation 4(5)(d) of S.I. No. 444 of 2022. See too Regulation 4(3)(b) of S.I. No. 444 of 2022.

the relevant aspects of same in completing its assessment.

5.15 Telephone numbers are a finite resource with many different services and users, and the management of these numbers involves the careful consideration of a broad range of factors (e.g., administrative, regulatory, social, economic, and technical) with a view to ensuring that telephone numbers are optimally and efficiently used. Broadly speaking, the efficient use of numbers cannot be consistent with widespread harm to consumers and business arising from their use.

5.16 Further, it can be generally assumed that what is good for competition is good for consumers. This is because increased competition between operators brings benefits to their customers in terms of price, choice and quality of services. In that regard, options that are good for competition above are likely to be good for consumers.

5.2 The Draft RIAs (Joint steps 1-3)

5.2.1 The policy issues & the objectives (Joint Step 1)

Policy issues

5.17 While separate policy issues are discussed at the outset of each individual RIA, ComReg has identified two broad policy issues that are relevant to all draft RIAs conducted in this consultation:

1. Reduce the harm[198] to consumers and businesses from Nuisance Communications ("Economical and Societal Harm"); and
2. Restore and protect trust in ECS Networks and telephone numbers.

5.18 The overarching policy issues for all draft RIAs is to implement those technical interventions that best achieve these two objectives, having regard to ComReg's statutory framework and associated objectives and the particular facts and circumstances of the technical interventions. Any additional policy issues are discussed at the outset of each draft RIA.

1. Economic and Societal Harm

5.19 Given the tendency (but not exclusively) for scams to come in waves, as fraudsters opportunistically take advantage of opportunities or data leaks, ComReg considers that Irish consumers and businesses are susceptible to unpredictable and potentially increasing spikes in fraud and/or inconvenience. ComReg considers that absent interventions to combat Nuisance Communications there could be large and persistent harm to consumers and

[198] As described in detail in Chapter 3.

businesses.

5.20 Chapter 3 describes in detail the economic and societal cost associated with Nuisance Communications. These are not repeated here, however the preferred interventions would be those that best mitigate or reduce such costs. With that in mind, each draft RIA contains different interventions and therefore may impact different scam types and/or harms among those listed above. In each draft RIA, ComReg will highlight what specific harms an option would target and the benefits arising from each of the option.

2. Trust in ECS Networks

5.21 Nuisance communications may cause consumers to lose trust in numbers through attempts to commit fraud thereby undermining the benefits of ECS services to Irish consumers, businesses and wider society. ComReg sets out below how Nuisance Communications can damage trust and reduce the effectiveness of the numbering platform in the delivery services to consumers.

5.22 Nuisance communications create a number of distinct effects that threaten the efficient and effective functioning of the Numbering platform, including:

- uncertainty caused by a previous scam call experience may infect a consumers' beliefs across all calls regardless of who is calling (Contagion effect);
- such problems may reduce the volume of calls made and received over the numbering platform (Call reduction);
- a reduction in the use of services through numbers by consumers would eventually reduce the incentives for Service Providers ("SPs") to continue to provide services over the numbering platform (Feedback effect); and
- there may be additional issues of equity for some services used by vulnerable groups (i.e., some services that would normally be provided over voice or SMS may move to alternative platforms not readily available to all social groups) (Social effect).

5.23 ComReg considers these issues below in assessing consumer harm.

Contagion effect

5.24 ECS networks are public platforms enabling any user in the world with signal or a line to connect with any other user almost instantaneously. The openness and convenience of such networks has underpinned their rise and there has been a transformational impact on society. This underpins the benefits or Voice and SMS as a means or two-way communications for consumers and businesses,

and SMS as a means of broadcast information for businesses.

5.25 However, consumers may not wish to receive calls given the problems associated with fraud and scams. Indeed, The B&A Consumer Survey reveals that many consumers use their devices primarily to communicate with people and business that are local or known to them. A single bad experience of nuisance communications may lead a consumer to expect that other calls unknown to them may be scam related.

Call/SMS Reduction effect

5.26 ComReg considers that the high incidence of nuisance communications reduces the usefulness of the numbering platform to consumers and supresses the volume of calls and texts, leading to a loss of consumer surplus. Where consumers lose trust in numbers, and in Irish ECS more broadly, this can cause consumers to not answer calls and not read SMS messages, inevitably leading to a greater non-response rate. A greater non-response rate in turn could undermine the usefulness of Voice and SMS as a means of communication to consumers, ultimately leading to a greatly reduced use as a means of communication. Indeed, the B&A Business Survey found that nuisance communications are leading to missed appointments and lost business for Irish businesses. In short, trust is being lost in electronic communications services, and this is in turn impacting consumers and the economy at large.

Feedback effect

5.27 Scam calls and texts and the ensuing reluctance of many consumers to properly engage with voice calls and texts acts as a disincentive for businesses offering services through these means and this, in turn, leads to a reduced and/or lower quality range of telephony/text services which callers may require (e.g., fewer consumer help lines, fewer businesses using SMS to remind consumers of appointments). If the value of providing these services through calls and texts to SPs is diminished, then this may affect the quality of service provided over the platforms.

Social effects

5.28 There may be additional issues with regard to accessing some services over the numbering platform in that nuisance communications could have a particularly negative impact on some more vulnerable consumers for whom voice calls and/or texts provide important access to essential services (e.g., paying bills) or social services (e.g., healthcare, social security). For certain classes of more vulnerable consumers, including some elderly persons or persons with disabilities, voice-based telephony services are essential when travelling to a physical location is difficult; often these are the groups that are

most vulnerable to nuisance communications.

5.29 Given the frequency of nuisance communications and the damaging effects on public confidence in the integrity and trustworthiness of electronic communications, it is apparent that absent interventions to combat Nuisance Communications and restore consumers trust in Networks, trust in Voice and SMS services and consequently ECS networks could be harmed irreparably.

Objectives

5.30 ComReg is undertaking this series of draft RIAs having regard to its statutory objectives which are summarised in Annex 2. These RIAs also have regard to the fact that ComReg is required to take all reasonable measures which are aimed at achieving its prescribed statutory objectives while such measures must also be proportionate to those objectives. ComReg also notes that, in achieving its objectives, its ultimate aim is to choose regulatory measures which maximise the benefits for consumers in terms of choice and quality.

5.31 Having identified the policy issues and objectives, as outlined earlier, ComReg identifies the regulatory options and the RIAs required to assess those options.

5.2.2 Identifying Regulatory Options (Joint Step 2)

5.32 Chapter 4 lists and describes the various interventions that are potentially available to ComReg in addressing its overarching policy issues and objectives.

5.33 ComReg identified eleven potential interventions and following an assessment of the technical feasibility and effectiveness and timelines for implementation, eight interventions were identified for assessment in one or more draft RIAs. Table 8 summarises the assessment conducted in Chapter 5.

Table 8: Assessment of long list of potential interventions

Interventions	Suitable?	Assessment
Do Not Originate	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Protected Numbers	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Fixed CLI Call Blocking	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Mobile CLI Call Blocking	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. Already agreed by NCIT members.
Voice Firewall	**Yes**	Technically feasible, as evidenced by its implementation by many MNOs. Many “off the shelf” solutions are available and are reported as being effective.
Stir/Shaken	**No**	Technically feasible, as shown by implementation in other jurisdictions. However, STIR/SHAKEN is unsuitable at present as • success depends on effective deployment in all countries; • few countries have implemented it; • there is no coordinated plan for its broad implementation • is relatively expensive relative to alternative interventions.

Shortening the chain	**No**	Technically feasible, as agreed by the NCIT. However, shortening the chain has proven challenging to implement due to high reliance on companies such as financial institutions which appear unable or unwilling to undertake necessary actions. As the success is entirely dependent on these companies, ComReg is not minded to pursue this intervention further.
Sender ID Ban	**Yes**	Technically feasible and would prevent Sender ID spoofing.
Sender ID Registry – Full or partial	**Yes**	Technically feasible, as evidenced by its implementation by other NRAs, notably in Singapore. The complexity and burden of intervention rests primarily with ComReg.
SMS Origin-Destination verification	**No**	Relies upon a hypothetical process which does not yet exist in practice. While this appears technically feasible, no examples exist in practice to confirm its feasibility and/or effectiveness. Would require a long lead in time to allow consideration (further research, feasibility studies, proof of concept etc.).
SMS Scam Filter	**Yes**	Technically feasible, as evidenced by its implementation in other jurisdictions. ID scanning was already agreed by NCIT members. Many "off the shelf" solutions are available and are reported as being effective. However, this requires a legislative change by the Irish Government, similar to that in Belgium and Poland, so that it can be implemented. ComReg is not the legislator but has engaged with its parent department DECC to this end. As previously discussed, this is considered in spite of the fact that any D.I may require legislation, and ComReg may therefore not propose a Draft DI at this stage.

5.2.3 Grouping the interventions into draft RIAs and regulatory options

5.34 The inclusion of nine potential interventions poses a challenge because some of the interventions are mutually exclusive while others are interdependent. It is therefore necessary to group interventions and assess across one or more different draft RIAs. Within each draft RIA ComReg must then determine what interventions constitute separate Regulatory Options and how those options relate to one another. In doing so, ComReg considers not only economic, but practical matters, such as the implementation of the interventions. Where Options naturally build upon one another, it may be most appropriate to assess the cumulative impact of Options beginning with the minimal viable set of interventions, assessing further interventions as additional Options (essentially a "layered" assessment).

5.35 Key to this analysis is the impact of interventions on one another's effectiveness. The ability of fraudsters to switch between scams exploiting different vulnerabilities and 'gaps' leads to complementarities between interventions plugging those 'gaps. Therefore, interventions that plug gaps which are substitutable from the perspective of a fraudster are therefore complementary. In effect, such interventions support one another, as only if both interventions are enacted is any benefit achieved. Otherwise, fraudsters merely reroute their scams to reach Irish consumers exploiting other 'gaps'.

5.36 With that in mind, ComReg assesses the eight regulatory options in the following way (illustrated in Figure 30 below).

I. Firstly, interventions are divided between those targeting SMS and Voice scams. These interventions target a specific communications technology and are independent of each other (i.e., an SMS intervention does not directly target a scam conducted over only a voice call and vice-a-versa) and, while multi-channel scams have been reported at some level, the majority of fraudsters are currently thought to face some barriers to switching between technologies.

II. Secondly, the SMS interventions are assessed as follows.

- Sender ID Blocking and the SMS Registry relate to regulating the use of Sender IDs and can be considered together in the draft '**Sender ID' RIA**. Only one preferred option is available because the interventions are substitutes for one another. (i.e., a SMS Registry and Sender ID Block cannot be implemented together.)
- The SMS Scam Filter is complementary to the Sender ID interventions and targets all SMS communications regardless of the format (i.e., whether an SMS has a Sender ID or otherwise). This intervention is therefore considered separately in the draft '**SMS Scam Filter' RIA.**

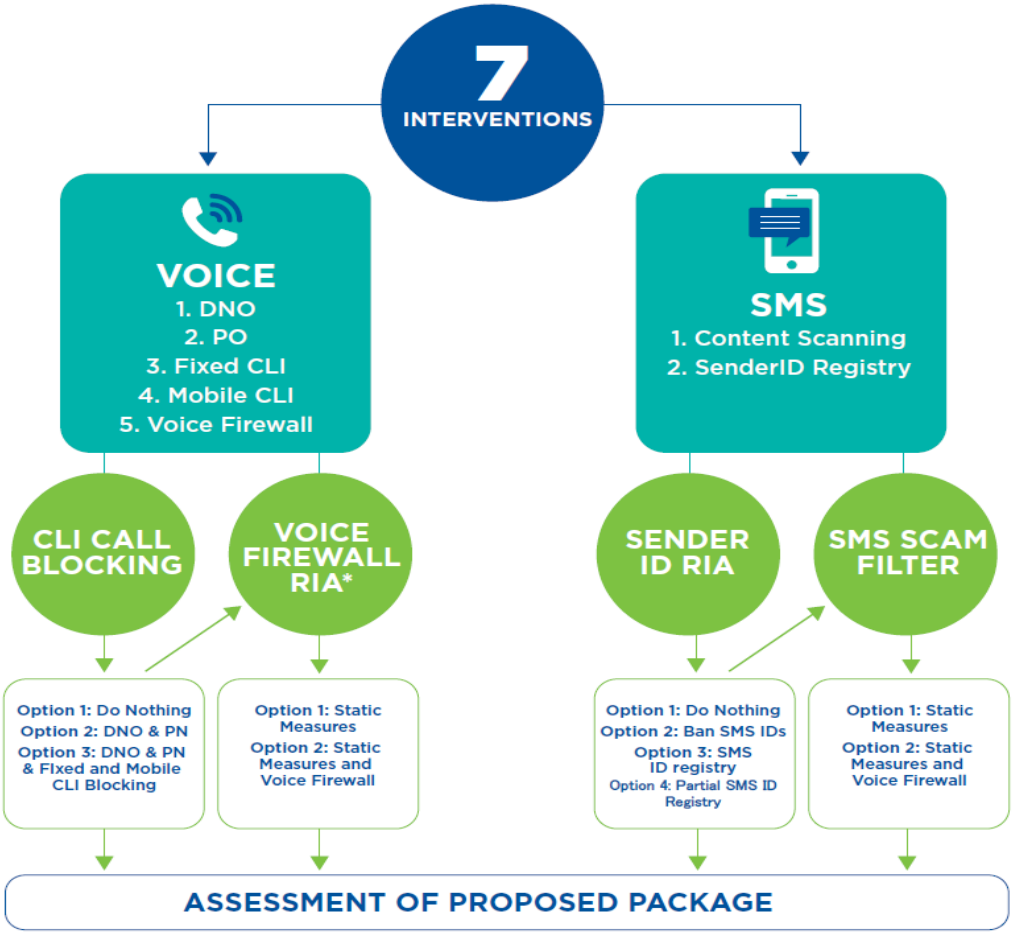
III. Thirdly, the voice interventions are assessed as follows.

- All voice interventions besides the voice firewall relate to blocking the use of certain numbers and closing gaps in networks that fraudsters may target and switch between and are considered together in the draft **'CLI Call Blocking' RIA**. These interventions are complementary and therefore ComReg's overall preferred option may consist of one or more options. Within this draft RIA, the DNO and PN are assessed jointly, given the advanced state of implementation by operators. Similarly, Fixed and Mobile CLI Call Blocking are assessed jointly, given neither have been fully implemented to date and both are likely highly substitutable from the perspective of an international fraudster, which could merely switch from spoofing of fixed to mobile CLIs or vice versa in the face of one but not both interventions.
- The Voice Firewall is complementary to the other Voice interventions and targets all Voice calls. While the Voice

Firewall may overlap to some degree[199] with other voice interventions, it targets scams through a different mechanism and achieves distinct benefits. This intervention is therefore considered separately in the draft '**Voice Firewall' RIA.**[200]

5.37 These four draft RIAs are assessed in the remainder of this Chapter.

Figure 30: The assessment of the proposed interventions as regulatory options across the four RIAs



5.38 Having identified the overarching policy issues and objectives above the remainder of this Chapter is divided between the four draft RIAs.

Implications of the Preferred Options on each RIA

[199] For example, a Voice Firewall could block scam calls prevented by DNO, Protected Numbers, and Fixed CLI Blocking interventions.

[200] In theory, SMS and Voice firewalls may prevent some scams prevented by the other interventions. However, firewalls would also block scams not targeted by static measures. Firewalls may therefore substitute or complement static interventions, depending which effect dominates. Which effect dominates depends on a number of factors such as whether any overlap in prevented scams is significant, whether the firewall would block all scams covered by static measures, and on how many further scams the firewall would block.

5.39 The draft RIAs herein are not in any particular order and the issues they address can overlap. If an option in one draft RIA has or may have implications for any option in the other draft RIA, then this is considered.

5.2.4 Identification of stakeholders (Joint Step 3)

Identification of stakeholders

5.40 The focus of Step 3 is to assess the impact of the various regulatory options on stakeholders. A precursor to the subsequent steps in the draft RIA, therefore, is to identify the relevant stakeholders.

5.41 Stakeholders consist of three main groups:

- Consumers, which for the purposes of this draft RIA, relates primarily to residential consumers and businesses (the impact on consumers is assessed within each RIA under "*Impact on Consumers*");
- Impersonated businesses (e.g., An Post, DHL, AIB, BOI, PTSB, eFlow) and impersonated or otherwise affected Government agencies (e.g., HSE or An Garda Siochana); and
- Industry stakeholders (the impact on stakeholders is assessed within each RIA under "*Impact on Stakeholders*").

5.42 There are several key industry stakeholders in relation to the matters considered in this Chapter, namely operators that:

1. Originate Voice traffic[201];
2. Terminate Voice traffic[202];
3. Transit inbound traffic via an International Gateway[203];
4. Terminate SMS traffic[204];
5. SMS aggregators[205]; and
6. Other operators (resellers, including MVNOs).

Determining which providers each intervention must apply

5.43 The effectiveness of an intervention is a function of the operators that implement it – (i.e., if all operators implement each intervention, full coverage of effectiveness would be provided). However, it may not be proportionate to

[201] Operators that originate Voice calls capable of connecting with public networks.
[202] Operators that terminate Voice calls capable of connecting with public networks.
[203] Operators that carry Voice calls from international PSTNs into the State.
[204] Operators that terminate SMS on public mobile networks.
[205] SMS aggregators that carry SMS traffic that terminates on public mobile networks in the State.

impose certain regulatory options and the associated costs on smaller operators with a small base of customers. In other cases, 100% coverage is required in order to prevent any gaps than might undermine the implementation of the interventions (s) on a national basis.

5.44 In this section, the interventions are assessed to determine which operators would be required to implement each of the interventions should one or more form part of ComReg's preferred option(s). This assessment is undertaken in three parts.

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

II. **Second,** ComReg assesses how to apply the interventions in a manner that achieves the greatest coverage while being proportionate in their implementation.

III. **Third,** ComReg provides information on the number and type of operators that would be required to implement each intervention.

I. Which interventions require 100% coverage such that the intervention would apply to all relevant operators.

5.45 The implications for each type of traffic and intervention are shown in Table 9 Table 9 below. A key point is that complete coverage is required for any intervention targeting call origination or international transit. Any 'gap', or uncovered operator that handles this traffic could potentially undermine the entire intervention as fraudsters would likely exploit that 'gap' to potentially reach all Irish consumers. Indeed, this may happen even without conscious switching by the fraudster due to inter-operator agreements on automatic call rerouting. Therefore, it is critical that interventions targeting call origination or international transit (i.e., DNO/PN, Fixed and Mobile CLI) be applied to all operators that service this traffic.

Table 9: Coverage required to ensure each interventions effectiveness

Traffic Type	Intervention	Applies to operators that...	Coverage required for effectiveness
Origination	**DNO & PN**	Originate Voice calls capable of connecting with public networks	**Complete coverage** - a single gap can be used to reach many Irish consumers. Exacerbated by "least-cost routing".
International	**DNO & PN Fixed & Mobile CLI Call Blocking**	International Gateway Operators (IGOs)	**Complete coverage** - a single gap can be used to reach many Irish consumers. Exacerbated by automatic call re-routing agreements
Termination	**Voice Firewall**	Terminate voice calls on public networks	**Near complete coverage –** a single gap only allows for scams to reach a limited number of subscribers on

			its own network. (e.g., covering 90% of subs protects 90% of subs).
	Sender ID Ban **Sender ID Registry** **SMS Content Scanning**	Terminate SMS on public networks	**Near complete coverage –** as a single operator only allows for scams to reach subscribers on its own network. (e.g., covering 90% of subs protects 90% of subs).

II. What approach best provides the greatest coverage for all remaining interventions.

5.46 The remaining interventions all concern terminating traffic (or combinations of originating and terminating traffic) and that such interventions (i.e., all SMS interventions and the Voice Firewall) may:

- be implemented by placing the obligation on either the service providers (e.g., MVNO and/or MNO) or the network operator itself (e.g., MNO); and
- achieve broadly the same effect by applying such interventions on all operators or only the largest, as such interventions are effective in proportion to its coverage (i.e., the number of consumers that receive its protection) because fraudsters cannot find an alternative network to connect to a consumer's device and thereby reach that consumer.

5.47 ComReg considers this further below.

Network Operators

5.48 ComReg proposes to place the responsibility primarily on the network operators to ensure that all relevant traffic (including third party traffic e.g., MVNOs) terminating on its network has been subject to each of the relevant interventions outlined above if adopted (i.e., Voice Firewall, Sender ID Ban, Sender ID Registry, SMS Scam Filter), where technically feasible.

5.49 ComReg understands that this is only technically feasible where the network operator operates the core network elements on behalf of these virtual operators. For example, a network operator is capable of applying a Voice Firewall to the traffic of those resellers or virtual operators that rely upon it for their core of their network (e.g., in the case of a MVNO this refers to Gateway Mobile Switching Centre (GMSC) or Home Location Register (HLR)). A network is not required to implement the intervention on behalf of Virtual operators with independent core network or provided by third parties.

Virtual Network Operators with independent core network

5.50 A number of virtual operators do not rely upon their host network operators[206] for core network services, instead relying on third party service providers.[207]. These virtual operators would also be required to apply these interventions to the traffic[208] (subject to reaching the subscriber cut-off, see below).

Smaller networks or operators

5.51 There are many public Voice network operators across both fixed and mobile in Ireland, of varying sizes, as shown below.

Figure 31: Voice capable subscriptions and lines on public networks, at a wholesale level [✂...✂]

Source: ComReg data on mobile subscribers[209] and fixed voice lines

5.52 ComReg considers that requiring all such networks to implement these measures may be disproportionate, provide little additional benefit while imposing a large cost on smaller firms, potentially distorting competition. ComReg is therefore of the preliminary view that it would be appropriate to provide a threshold for the mandate of these interventions to account for the smaller fixed networks providing Voice services that would otherwise be included.

[206] In the case of MVNOs, the host network is the provider of RAN services.
[207] Specifically, ComReg understands from discussions with operators that [✂…✂].
[208] In the case of MSPs, full MVNOs have their own network-switching infrastructure and negotiate their own interconnect agreements and generate revenues not only from outgoing traffic, but also for incoming traffic. Therefore, distinguishing these operators from 'lighter' MVNOs without any core elements is appropriate.
[209] Fixed Voice is measured using lines, both residential and non-residential, as a proxy for subscribers as this is the most appropriate data available. ComReg considers this a conservative estimate of end-users for landlines, noting that the true number of users may be higher in the case of non-residential lines. This data is the best data available to ComReg for attributing landlines at a wholesale level. ComReg will update this data where an operator can demonstrate with adequate evidence that a sufficient number of attributable Fixed Voice Lines on their network are either a) inactive or b) account for a negligible share of Fixed Voice.

5.53 ComReg considers that a cut-off of 5% of relevant subscriptions (roughly 270,000 subscribers for SMS and 330,000 subscribers and lines for Voice[210]) appears appropriate as this covers most Voice subscriptions including landlines while not covering overly small networks, noting the figures in Figure 31 above. In this way, the interventions would only apply to MSPs that are above the 5% threshold. ComReg is satisfied that this approach is proportionate as it only includes sufficiently large operators, while ensuring the majority of consumers benefit from the protection of Voice Firewall.

Table 10: The coverage achieved and impacted companies for different cut-offs

Technology	Cut-off (subs/lines)	Affected Companies	Coverage Achieved[211]
SMS Scam Filter & SenderID Registry	>5% (>270,000)	MNOs	94% subscribers and 97% of SMS traffic
	>1% (>54,000)	MNOs and [✂…]	100% of subscribers and SMS traffic
Voice Firewall	5% (>330,000)	MNOs (incl. Fixed Voice), Virgin (incl Fixed Voice)	94% of Voice subscribers • **Mobile** – 97% of subscribers • **Fixed** – 83% of subscribers
	>1% (>66,000)	MNOs (incl. Eircom and Vodafone Fixed Voice), and [✂….]	98% of Voice subscribers • **Mobile** -99 % of subscribers • **Fixed** -95% of subscribers

Source: ComReg data on mobile subscribers[212] and fixed voice lines[213]. Preferred approach highlighted in yellow.

5.54 In relation to virtual operators that are not captured above (either directly or via their host network), ComReg notes that there remains scope for these entities to implement such interventions voluntarily (e.g., voice firewall). ComReg has had discussions with a number of vendors which suggests that there are a variety of business models available.

5.55 ComReg considers this approach appropriate and proportionate for the following reasons.

I. The costs imposed on network operators from implementing these interventions (e.g., voice firewall) on behalf of its virtual operators that do not own their own core infrastructure is likely to be small and limited to the higher throughput that would result from servicing the

[210] These figures are rounded to the nearest multiple of 10,000 for convenience. These figures are based on subscriptions that are attributable at a wholesale level. The effect on the cut-off of alternative available data (QKDR) for each data is marginal (<15,000 subscribers at the 5% cut-off). No firms are affected by this, noting that all operators that exceed the higher cut-off by over 100,000 subscriptions/lines. ComReg will repeat and update this analysis in the Response to Consultation.

[211] This table present coverage in terms of subscribers not traffic, as information on traffic is not readily available at a network level for Fixed. ComReg considers this a conservative but appropriate approach as while mobile generates more traffic any device that could be answered may be used to reach an end-user. This includes the subscribers of [✂…] as ComReg understands from discussions with both [✂…✂] core network in the next [✂…✂] months. Should this migration not proceed this MVNO would be treated as a separate entity and therefore [✂…].

[212] This is mobile subscriptions excl. MBB and M2M.

[213] Fixed Voice is measured using lines, both residential and non-residential, as a proxy for subscribers as this is the most appropriate data available. ComReg considers this a conservative estimate of end-users for landlines, noting that the true number of users may be higher in the case of non-residential lines.

virtual operators' traffic. For example, MVNOs traffic accounts for less than 11% of all mobile traffic (and no more than 7% for any one operator) - given the likely economies of scale associated with operating any of the interventions targeting terminating traffic, the marginal costs of servicing a virtual operators traffic (on the same core) are likely to be small and less than what would be the case if such virtual operators had to implement such an intervention themselves. It is therefore appropriate that the host operator bears the costs associated with this traffic. ComReg also considers that implementing these interventions at a network level better protects a wider range of consumers in the most proportionate manner because networks necessarily carry a greater level of subscribers and traffic than service providers.

II. Extending the obligation on network operators to include all virtual operators regardless of their network infrastructure would likely impose disproportionate costs on the network operators (e.g., MNOs) and is unlikely to be proportionate. The network architecture associated with virtual operators that build their own core elements (including network-switching infrastructure) is different to those that do not own any core network infrastructure (i.e., network operator operates the core on its behalf), and traffic cannot be serviced in the same way without imposing additional costs on network operators. In any event, such an approach would create obvious issues for the virtual operator retaining the independence of its core network (if an MNO for example was filtering traffic on its core network) and the advantages that such architecture brings. Such an approach would also not promote infrastructure-based competition in line with ComReg's statutory objectives.

III. The thresholds discussed above prevents this measure from being disproportionately costly to smaller network and virtual network operators.

5.56 ComReg considers that potentially applying a Voice Firewall, a SMS Scam Filter and Sender ID registry only to networks with at least 5% of all Voice capable subscriptions or SMS subscribers respectively would achieve significant benefits and ensure that such a measure is applied in the least onerous manner. Based on this threshold, the SMS Scam Filter and Sender ID Registry would apply to Three, Vodafone and Eir (incl. Eircom). The Voice Firewall would also apply to these operators but would additionally include Virgin (incl. UPC). ComReg estimates that such measures would cover:

- 94% of SMS subscriptions and 97% of SMS traffic on public networks; and

- approximately 94% of Voice subscriptions on public networks covering approximately
    - 97% voice capable mobile subscriptions; and
    - 83% of voice capable landlines lines

III. To which firms would each intervention apply?

5.57 Given the above, ComReg now summarises what interventions would potentially apply to whom.

5.58 Not all operators carry all types of traffic (e.g., SMS or Voice), therefore which operators an intervention applies to depends primarily on the type of traffic carried on its network. To identify what firms carry the relevant traffic, ComReg has analysed the following datasets:

- The Electronic Register Of Authorised Undertakings ("ERAU")[214];
- The Telephone Numbering database[215]; and
- The QKDR database[216].

5.59 ComReg has combined these datasets to identify what firms each intervention is likely to apply to - the results of which are summarised in Table 11 below. This has in turn informed Europe Economics' assessment of the aggregator and average cost of interventions to industry stakeholders contained within the RIAs.

Table 11: Identifying the companies to which each intervention applies

Technology	Interventions	Identified firms
Voice	DNO List & PN List	**Originators of Voice traffic: approximately** • 30 firms identified from the Numbering database **IGOs (subset of above)** • 14 identified (from the IGO RFI)
	Fixed & Mobile CLI Call Blocking	**IGOs:** • 14 identified(from the IGO RFI)
	Voice Firewall	**Network with >5% of Voice-capable subscriptions and lines on public networks:** • Three, Vodafone, Eir (incl. Eircom), Virgin (incl. its Fixed Voice)
SMS	Sender ID Ban	**Filtering by MSPs** **Network with >5% of SMS subscriptions on public networks:** • Three, Vodafone and Eir **SMS aggregators** • All participating aggregators
	ID Registry *partial or full*	
	Content Scanning	**Network with >5% of SMS subscriptions on public networks:** • Three, Vodafone and Eir

[214] The ERAU is a register which captures all providers of ECS services, managed by ComReg.
[215] The numbering database contains information on all operators assigned telephone numbers by ComReg.
[216] The QKDR compiles data provided to ComReg by ECS with a turnover of over €500,000.

5.3 Draft CLI Call Blocking RIA

5.3.1 Policy Issues

5.60 ComReg previously noted that the two overarching policy issues relevant to all draft RIAs are:

i. being to reduce the harm to consumers and businesses from scam calls; and

ii. protecting and renewing trust in ECS Networks and Services.

5.61 ComReg is mindful of these policy issues in determining its preferred option. The remainder of this section further defines these main policy issues as they relate to this draft RIA in order to appropriately assess the available regulatory options.

5.62 Overseas fraudsters often use inexpensive and readily available technology to present calls with maliciously spoofed Irish CLIs to display a number more familiar or recognisable to the person receiving the call. The numbers which fraudsters use to defraud people include:

- Mobile numbers where consumers may recognise the mobile prefix (086) (085) and assume someone (whether for business or social purposes) who is not on their contacts is trying to reach them.
- Geographic numbers (e.g., 061 for Limerick, 043 for Longford) where consumers may recognise their local numbers and assume a person or business is trying to contact them from a fixed line number.
- Non-geographic numbers (e.g., 1800 or 0818) where consumers assume that a business (e.g., bank or credit card company) is trying to contact them using a freephone or 0818 number.

5.63 Both domestic and overseas fraudsters may present calls with maliciously spoofed fixed or mobile CLIs to display a number of a trusted or well-known organisation to the person receiving the call. The numbers that fraudsters often use includes the in-bound only numbers of:

- Irish companies (e.g., banks)
- Irish government agencies (e.g., Department of Social Welfare)
- Postal and delivery service providers (e.g., An Post)
- Other legitimate organisations (e.g., NGOs)

5.64 Consumers have a high level of awareness of these numbers[217] and fraudsters take advantage of this by spoofing such numbers which makes it more likely that the call would be answered. This can result in significant harms to consumers either through fraud taking place and/or through annoyance or distress from receiving calls (See Chapter 3). The ensuing unpleasant experiences can in turn lead to Irish consumers no longer trusting the number displayed on their phone when it rings.

5.65 The spoofing of numbers primarily stems from international networks which present as an Irish mobile or fixed CLI (e.g., appear as a valid mobile or geographic range). There are also some numbers which should not appear as a CLI because they are either unassigned to any operator or are outbound calls from trusted numbers which are used for inbound calls only (e.g., a bank's non-geographic number).

5.66 With that in mind, the main policy issue associated with this draft RIA is to reduce the harm from scam calls on consumers and trust in ECN by:

I. identifying and blocking calls originating from international networks and presenting with Irish CLIs; and

II. identifying and blocking calls which should not appear as a CLI to consumers (regardless of where they are originated) because they are either unallocated or inbound only numbers.

5.67 The above two policy questions are related noting that the preferred option could comprise one or more of the available options.

5.3.2 Regulatory Options (Steps 1 & 2)

5.68 As outlined in Section 5.2.2 5.2.2, the available interventions for the purpose of this RIA are:

- **Option 1** – No new regulatory measure(s).
  - This approach would maintain the status quo position with no intervention(s) proposed by ComReg.
- **Option 2** – Implement the DNO and PN intervention.
  - This approach would implement DNO and PN intervention as outlined in the technical specification.
- **Option 3** – Implement Fixed and Mobile CLI Call Blocking in addition to DNO and PN.

[217] See Document 21/82b and Document 17/70b

- This approach would implement DNO, PN, Fixed and Mobile CLI Call Blocking as outlined in the technical specifications. Fixed and Mobile CLI Call Blocking are assessed together because the implementation of one but not the other could not achieve the stated policy objectives for both fixed and mobile calls.

5.3.3 Impact on industry stakeholders, consumers, and competition (Steps 3 & 4)

I. Impact on consumers

5.69 This section provides information on the impacts on consumers arising from the regulatory options outlined above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the direct impacts on consumers arising from the regulatory option is assessed (e.g., the reduction in harm due to fraud and time lost to scam calls etc); and

II. Second, other relevant impacts (e.g., impact on trust) arising from the implementation of the regulatory options are assessed.

Option 1: Do Nothing

I. Direct impacts

5.70 Under Option 1, each of the harms from scam calls detailed in Chapter 3 are likely to remain high. There are numerous factors that could cause this harm to increase (such as fraudsters increasing the rate of scams, or it is becoming more difficult to perpetrate scams in other jurisdictions and relatively easier in Ireland) or decrease because consumers adapt their behaviour towards scams and become less susceptible to fraud)[218].

5.71 However, fraudsters are dynamic and adapt their tactics with new forms of scams emerging over time. ComReg notes that the harm is more likely to increase as the fraudsters become ever more sophisticated even where consumers adapt to older scams[219]. Further, as noted earlier, other English-speaking countries are already implementing various interventions (e.g., CLI Call Blocking and voice firewalls) and fraudsters would inevitably direct more scams towards unprotected Irish consumers under this Option.

[218] Europe Economics have estimated how this harm could potentially develop, depending on which factors dominate.
[219] For example, Cyber attackers are diversifying their tactics and finding new ways of scamming customers. As outlined in: HP Wolf Security Threat Insights Report Q4 2022 | HP Wolf Security

5.72 As described in Chapter 3[220], Europe Economics estimates that the current level of harm to Irish consumers and businesses arising from scam calls is approximately €187 million per annum[221]. Therefore, under Option 1 the harm to society is likely to remain substantial and at least at these levels but probably greater.

II. Other Impacts

Trust in voice calls

5.73 There is strong evidence to suggest that until recently Irish consumers had a high degree of trust in Numbers. For example, in relation to Geographic Numbers, consumers had relied to a large degree on the information provided by the number (e.g., the geographic area and the CLIs which consumers see upon receipt of a call). In 2021 (ComReg 21/28b[222]) (the "GN Survey"), B&A found that Irish consumers understood and desired geographic numbers to provide information on the geographic location of the call. For example:

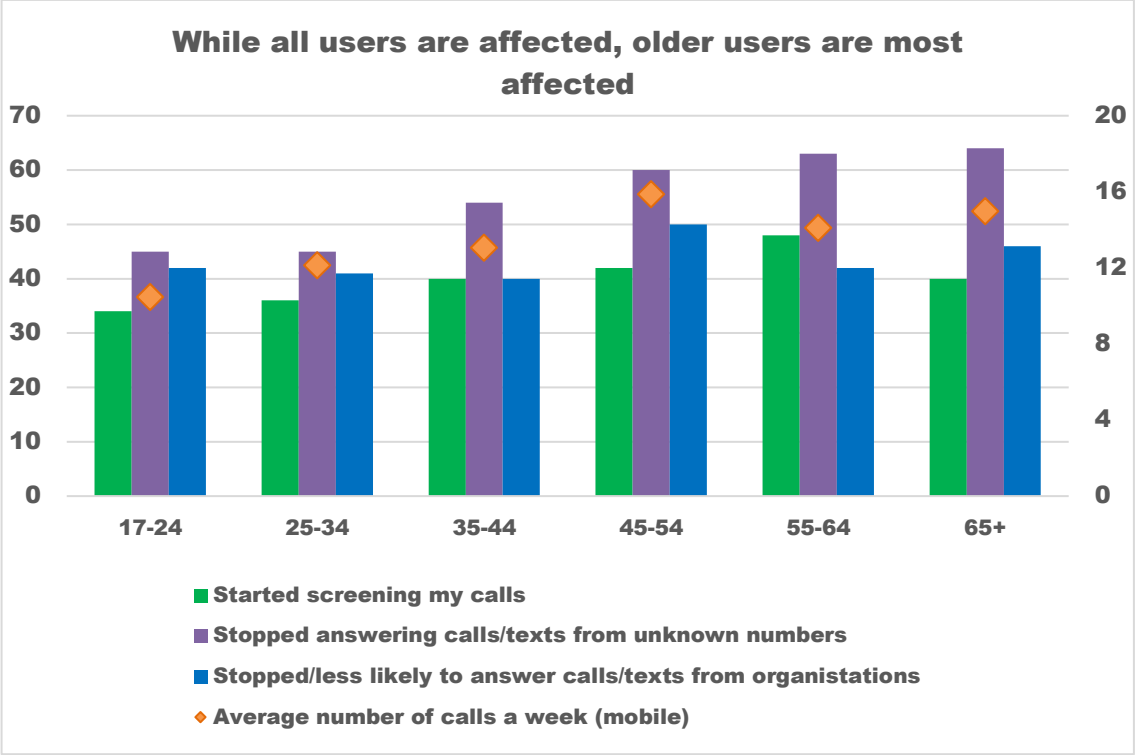
- 83% of Irish consumers know their local area code[223].
- 81% of Irish consumers are satisfied that a household or business must have a physical presence in an area to avail of its area code
- 74% of Irish consumers consider it important to know the geographic location of the number when they are called[224]
- 72% of Irish consumers trust that a call with an Irish CLI is from the geographic location associated with that number[225]
- Around 60% of Irish consumers will answer a call from an Irish CLI that is not a regular contact, if it has geographic number[226]. This makes voice calls a reliable means of contacting the majority of Irish consumers, which is valuable to businesses that need to contact consumers for their business.

5.74 Scam calls have markedly degraded the trust consumers place in the authenticity of Voice calls from consumers and organisations. Many consumers have stopped answering or screening calls, or otherwise reducing their use of Voice calls as illustrated in Figure 32. This is particularly true of older users,

[220] See also Section 4.4 – 4.6 of the Europe Economics Report.
[221] Comprising €116 million (consumers) and €71 million (businesses)
[222] B&A "*Geographic Numbering Survey: Quantitative report*" Link
[223] In response to the Question 8 "*Do you know the Area Code associated with Geographic Numbers in your area (i.e. your local area code)?*"
[224] In response to the Question 13 "*When receiving a call, how important is it to know the geographic location of a number calling you (i.e. where the caller is calling from)?*"
[225] In response to the Question 19 "*To what extent do you agree or disagree with the following statement (I trust that the caller is making the call from the Geographic location associated with the number)*"
[226] In response to the Question 16 "*How likely are you to answer a call from a Geographic Number that is not one of your regular contacts*?"

who happen to be more dependent on Voice calls.

Figure 32: Loss of trust in calls as a result of scams, by age[227]



Source: ComReg analysis of data from the B&A Consumer Survey

5.75 As outlined above, nuisance communications create a number of distinct effects that reduce trust and threaten the efficient and effective functioning of the numbering platform. ComReg now assesses each of these effects (i.e., contagion, call reduction, feedback, and social effects) with respect to voice calls under Option 1. ComReg notes that this section is also relevant to the draft SMS Scam Filter RIA which follows this RIA.

Contagion

5.76 Contagion refers to the uncertainty caused by the prevalence of scam calls and/or a previous scam call experience which may infect a consumers' beliefs across all calls regardless of who is calling. Under Option 1, it is likely that contagion would spread as consumers become increasingly suspicious about the calls they receive. As Chapter 3 outlines, there are already a number of clear examples of contagion across the numbering platform. For example:

[227] In relation to Question 40c "*Has your experience of scam calls and texts affected your trust in communications from the organisations that provide the aforementioned services?"* and Question 38 "*In relation to your awareness of scam calls and texts, has any of the following happened?"* Average number of calls is displayed on the right axis.

- 70% of consumers are concerned or very concerned about scam calls.[228] Those who have experienced a financial loss have a heightened level of being 'very concerned'.
- 60% of businesses are concerned or very concerned about scam calls[229], with businesses that use mobile numbers to communicate also showing higher levels of concern**.**

5.77 ComReg is of the preliminary view that the numbering platform already suffers from contagion and that this would likely increase under Option 1.

Call reduction

5.78 Call reduction refers to reductions in the volume of calls made and received over the numbering platform due to contagion. Contagion is causing consumers to accept less calls due to the fear of being scammed. Notably, consumers are now not accepting calls from people they may know or from business or public bodies providing services that consumers would ordinarily be interested in (e.g., deliveries, hospital appointments etc). This is because fraudsters primarily impersonate organisations that a consumer would likely be interested in. This reduces the volume of calls received over the numbering platform as consumers decide to answer less and less calls. For example:

- 56% of consumers have stopped answering calls from unknown numbers due to the prevalence of scam calls[230]; and
- 43% stopped answering calls/texts that may be from businesses or government agency[231] due to the prevalence of scam calls.

5.79 ComReg is of the preliminary view that there is clear evidence that nuisance communications are supressing the volume of voice calls to the detriment of consumers and businesses.

Feedback effect

5.80 The feedback effect refers to the reduced incentives for people and organisations to use voice calls because of the reduction in people answering calls. Businesses may decide not to provide services over the numbering platform because of the low answer rate (i.e., the call reduction creates a feedback effect). Businesses and consumers would reduce their reliance on Voice calls given the level of harm being borne by Irish consumers and businesses. In particular, businesses are likely to switch to alternative means of contacting consumers even though their preference may be to contact

[228] B&A Consumer Survey, Slide 12
[229] B&A Business Survey, slide 11
[230] B&A Consumer Survey, slide 31
[231] B&A Consumer Survey, slide 31

consumers using voice calls on public networks. For example, 39% of businesses have already made changes to how they communicate with consumers.[232]

5.81 These changes often avoid the use of public phone networks and rely more on an alternative means of communications (e.g., email, secure messages, online portal etc.).[233] Notably, 23% of consumers already ignore calls purporting to be from organisations due to scam calls. While only a small share of consumers has moved to alternative instant messaging platforms as a result of scams to date, this figure is likely to grow as the harms persist and such consumers may not transition back to traditional voice.

5.82 Critically, any movement to alternative platforms would have arisen due to nuisance communications and the misuse of the numbering platform rather than any underlying preference for those alternatives. The numbering platform needs to compete with alternative ways of delivering services to some or all users, such as web-based messaging, and social media; however, such choices should be made neutrally, rather than because the numbering platform has been compromised in some manner. Any move to alternatives should ensue from informed decisions made by consumers and businesses, rather than being the result of having to deal with nuisance communications, as is currently the case.

5.83 ComReg is of the preliminary view that there is clear evidence of a feedback effect with organisations particularly affected as they consider moving to alternative ways of contacting consumers.

Social effect

5.84 The social effect arises in cases where some services that would normally be provided over voice switch to alternative platforms (due to prevalence of nuisance communications) that are not readily available to some social groups. People's reluctance to engage with voice calls due to fear of being scammed could have a particularly negative impact on vulnerable consumers for whom voice services provide important access to essential services (e.g., healthcare, social security). The social effects of reduced voice calls resulting from call avoidance can be very detrimental for those who may be dependent on one or more social services.

5.85 For example, older people are more likely to be affected by people and organisations (in particular) moving to alternatives because older people use these alternative services at a much lower rate. The use made by over 65s make of alternative voice-calling platforms (e.g., WhatsApp, video calls, social

[232] B&A Business Survey, slide 23.
[233] B&A Business Survey, slide 23.

media) is three times lower than the average person and up to 6 times lower compared to younger groups. The over 65s are also the only group currently using voice calls primarily over the phone. They use voice calls three times as much as other alternatives to voice (e.g., video calls, VOIP calls etc).

5.86 Older people are also more likely to be concerned or very concerned about scam calls (84%)[234] and are the most likely to stop answering unknown calls, with 64% of over 65s not answering unknown numbers[235]. Many organisational numbers are unlikely to be known to older people (or consumers generally for that matter) and the most commonly impersonated organisations are those which older people are most likely to require (e.g., banks, HSE, delivery companies and other public bodies).

5.87 For example, several banks have outlined to ComReg the potentially serious repercussions of this lack in trust in calls such as being unable to assist older customers with issues relating to their account through alternative means (e.g., online or chat). Similarly, a 75-year-old person who primarily relies on voice communications may be greatly impacted if he/she is less contactable by their healthcare providers. Indeed, ComReg has evidence from the HSE of such situations arising in practice. The HSE has outlined to ComReg the potentially serious repercussions of this lack of trust in calls (See Chapter 3). It is for such reasons that the possible impacts of reduced trust on more vulnerable consumers must be carefully considered.

5.88 ComReg is of the preliminary view that that nuisance communications are having detrimental social impacts.

5.89 Overall, consumers are therefore unlikely to prefer Option 1 because it would perpetuate the harm caused by nuisance communications and would be highly unlikely to restore any trust to the numbering platform.

Option 2: DNO and PN

I. Direct impacts

5.90 Under Option 2, the DNO and PN would directly reduce the harm from scam calls in two ways.

- First, Option 2 stops fraudsters spoofing business numbers that are not used for inbound calls by preventing consumers receiving calls from such numbers. ComReg understands from an Garda Síochána that this constitutes a small, but material share of total scam calls. (i.e., while the volume of calls to such numbers are small, they are likely to be more

[234] B&A Consumer Survey responses to Q.5a "*How concerned are you about … Scam Calls*"
[235] B&A Consumer Survey, slide 32

effective at scamming than other numbers because consumers are more likely to recognise them).

- Second, Option 2 stops fraudsters spoofing numbers that have not yet been assigned and reduces the range of numbers that are available to be spoofed. Option 2 also reduces the effectiveness of scams by removing the use of numbers that can be used for impersonating businesses. For example, fraudsters have spoofed unassigned non-geographic numbers in order to give the appearance of coming from a business or from the Dublin area (which has high consumer recognition).

5.91 Europe Economics notes there is considerable evidence on the effectiveness of the DNO and PN from international case studies (summarised earlier in Chapter 4). Further, information provided by a large IGO that has implemented DNO, PN and CLI Call Blocking shows that scam calls using CLI Spoofing of legitimate businesses appears to account for a small share of all scams calls in Ireland[236]. Europe Economics estimates that under Option 2 the net present value of the incremental reduction in harm would be €20 million over seven years, or roughly €3 million per annum.[237]

II. Other Impacts

Trust in voice calls

5.92 Option 2 would improve the trust consumers place in voice calls relative to the status quo under Option 1. While appearing to account for just a small share of all scam calls, ComReg notes that calls impersonating key businesses and organisations are very likely to undermine the trust of consumers in business communications. For example, consumers are unlikely to know that some organisations only use certain numbers for inbound calls only and would never contact a consumer using that same number. Consumers may check a number online to see whether a number belongs to a particular organisation and be more likely to answer and engage as a result. DNO should assist in restoring some trust in voice calls because these numbers are an easy target for fraudsters to spoof given that they are actively being used for inbound calls. PN should also be expected to protect the trust of consumers by reducing the number of calls using unassigned Irish numbers.

5.93 This option is likely to reduce each of the effects assessed under Option 1 (e.g., contagion, feedback social effect) but only to a limited extent because consumers would still receive scam calls from other sources. However, it is likely to reduce the feedback effect because organisations would be less likely

[236] This is based on calls blocked by the IGO from its implementation of DNO, PN and Fixed and Mobile CLI Blocking over a 5 month period.
[237] See Tables 9.9 and 9.11 the Europe Economics Report.

to move to alternative platforms because their number would not be spoofed if placed on the DNO list. This would also have the effect of reducing the social effects because organisations may be less likely to switch to alternative platforms that some demographics (e.g., older people) are less accustomed. By protecting the important numbers that businesses use, a DNO list can enable businesses and organisations to secure their own numbers. This can protect the use of voice for business communications. ComReg would hope that the current enrolment increases once DNO awareness increases[238].

5.94 ComReg is of the preliminary view that consumers would likely prefer Option 2 to Option 1. However, consumers would also likely prefer additional protections beyond the use of DNO/PN because nuisance communications appear in a variety of different forms and are likely to continue to occur under Option 2.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

I. Direct Impacts

5.95 Under Option 3, Mobile and Fixed CLI Call Blocking would reduce the harm from scam calls by preventing overseas fraudsters from spoofing Irish numbers. Europe Economics notes that there is strong evidence demonstrating the effectiveness of both Fixed and Mobile CLI Call Blocking interventions from international case studies and also from discussions with early adopter operators in Ireland. Further, information provided by An Garda Síochána and a large IGO that implemented DNO, PN and Fixed and Mobile CLI Call Blocking suggests that CLI Spoofing accounts for the majority of identifiable scam calls experienced in Ireland in recent months[239].

5.96 In relation to its implementation in Ireland Europe Economics notes that:

> *"Approximately 88 per cent of all call minutes in Ireland are accounted for by mobiles, and there are 3.6 times more mobile international/roaming minutes than the total number of fixed international outgoing minutes.[240] This intervention is therefore likely to be especially effective at limiting the risk of fraud caused by CLI spoofing scams in general"*

5.97 Accordingly, Europe Economics considers that Fixed and Mobile CLI Call Blocking should prevent a large share (90%) of current scams. Europe Economics estimates that under Option 3, the net present value of the reduction

[238] In the UK, where DNO has been in effect for a number of years, the DNO list covers over 12,000 numbers which are not used for outbound calls. On a pro-rata basis, this could imply that when completed Ireland's DNO could contain as many as 1,000 numbers.
[239] This is based on calls blocked by the IGO from its implementation of DNO, PN and Fixed and Mobile CLI Blocking over a 5 month period.
[240] Europe Economics analysis of ComReg data. Source: Fixed Line Statistics and Mobile Statistics, Total Fixed International Outgoing Minutes (000's) and Mobile International/Roaming Minutes (000's), Q2 2022 [online].

in harm could be as high as €900 million over seven years, or roughly €129 million per annum.[241] This is an upper bound for the impact of the static voice interventions, as it assumes no adaptation by fraudsters.

Table 12: Reduction in harms under Option 1-3, relative to status quo

Option	Benefits to Irish society relative to status quo (Option 1)
Option 1 (No regulatory measures)	-
Option 2 (DNO&PN)	Over 7 year – €21 Million Annually - €3 Million
Option 3 (DNO&PN, Fixed and Mobile CLI Call Blocking)	Over 7 year – €900 Million Annually - €129 Million

II. Other Impacts

Trust in voice calls

5.98 Option 3 would block calls that originate from abroad and are spoofing Irish numbers. Because most scam calls currently arise due to Fixed and Mobile CLI spoofing, it would better protect Irish numbers compared to Option 1 and Option 2. Consumers would be able to know that Irish numbers appearing on their caller ID are calls originating within Ireland. While caution would still need to be exercised, as scams do and will continue to originate in Ireland, consumers would be able to rule out the possibility that these calls are coming from abroad. This would be a notable improvement on the current case where some consumers ignore the geographic information provided by the caller ID because they suspect it is a scam from abroad. This option is likely to reduce each of the effects (e.g., contagion, feedback etc) assessed under Option 1 and be particularly effective at reducing contagion as the largest source of scam calls would be reduced. Therefore, consumers are likely to prefer Option 3.

Conclusion on impacts on consumers

5.99 Based on the assessment above, ComReg is of the preliminary view that consumers are unlikely to prefer Option 1 because the large harms on consumers would continue to occur or worsen as other countries, particularly those in the Anglosphere, take preventative steps. While Option 3 is preferred to Option 2, consumers are also likely to value Option 2 and the implementation of the PN/DNO Lists. Option 3 could in some respects negate the need for a PN/DNO list over time – however, scams can and do originate in Ireland also and a PN/DNO list would provide a necessary protection against scams that

[241] See Table 9.9 and 9.11 of the Europe Economics Report. The present-value of the value of the harm is the sum of the incremental values for DNO, PN, Fixed CLI Blocking, Mobile CLI Blocking.

impersonate important businesses or social services.

5.100 Therefore, consumers and businesses are likely to prefer a combination of Option 2 and Option 3 because, in combination, they offer the greatest potential for a reduction in the harm from scam calls and best safeguard the trust in and use of Voice calls and Irish numbers more generally.

II. Impact on industry stakeholders

5.101 For the purposes of this draft RIA the relevant industry stakeholders, among those outlined in Section 5.2.2, are considered to be operators that:

1. originate Voice traffic;
2. terminate Voice traffic;
3. transit traffic via an International Gateway; and
4. provide other services (resellers, including MVNOs).

5.102 This section provides information on the impacts on such industry stakeholders arising from the potential adoption of the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this regard:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

5.103 Several operators have made progress in implementing fixed and mobile CLI Call Blocking, with some associated financial costs having already been incurred. Nevertheless, for the clarity and purpose of this assessment, ComReg assumes that no costs have been incurred to date[242]. This practical approach considers the maximum impact of each option and assumes all costs lie ahead of the operators. (i.e., a greenfield approach.)

Option 1: No regulatory intervention

I. Financial impacts

5.104 Option 1 would not impose any financial costs on any of the operators.

II. Other Impacts

[242] Under the status quo, operators may choose not to incur costs by electing not to undertake any technical measures to combat scams. Indeed, certain operators have informed ComReg that they would await a regulatory requirement before undertaking further work on technical specifications in this RIA.

5.105 Under this option, the harms to operators (e.g., commercial benefits from being able to offer networks of trust etc) would continue to occur and the scope for operators to benefit commercially from being able to offer networks of trust would be reduced because the present level of scam calls is diminishing trust in voice calls and Irish numbers which in turn reduces the use of Voice services. Operator reputations would also continue to be damaged as scams proliferate across society negatively impacting the revenues generated by operators from providing Voice services. For example, only 16% of consumers think that operators have done enough to protect them from nuisance communications[243].

5.106 Therefore, operators are likely to prefer interventions that reduce the rate of scam calls and are unlikely to prefer Option 1.

Option 2: DNO and PN

I. Financial impacts

5.107 Under Option 2, the DNO and PN list would be applied by fixed line and mobile originating operators on all originating voice traffic. ComReg estimates that there are approximately thirty such operators[244] and each would incur some expense arising from the implementation of this option. Europe Economics has estimated both the one-off costs (e.g., implementing the initial list) and on-going costs (e.g., updating the list periodically) of the DNO/PN per operator as follows.

- A one-off cost of approximately €33,000 in the year of implementation; and
- On-going OPEX costs of approximately €3,000 per annum[245].

5.108 The costs referred to above only concern those operators which have yet to implement the intervention in full or in part. Several operators have made significant progress in implementing DNO and PN and thus would likely prefer Option 2 to Option 1 because it would offer better protection for their customers with little additional costs. Overall, ComReg considers that few if any operators would prefer Option 1 over Option 2 given the improved customer outcomes that would be achieved at minimal cost.

II. Other Impacts

5.109 The sustained level of scam calls impersonating businesses threatens the continued use of voice calls. Option 2 would safeguard trust to some extent in business numbers and the use of voice calls for businesses which should benefit the long-term commercial interests of Voice operators.

[243] B&A Consumer Survey, slide 42.
[244] Based on the number of operators in receipt of numbers directly from ComReg. the numbering conditions.
[245] See Table 9.3 of the Europe Economics Report.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

I. Financial impacts

5.110 Mobile and Fixed CLI Call Blocking are applied on transiting traffic and therefore the cost of this intervention is borne by IGOs. Roughly half of the operators impacted under Option 2 (e.g., non-IGOs) are unaffected by Option 3. ComReg assumes that such operators would prefer Option 3 given the improved consumer outcomes that would likely result. ComReg now focuses on the IGOs that are affected by Option 3.

5.111 ComReg estimates that there are 14 IGOs based on its request for information[246]. Furthermore, it should be noted that over [✂…✂] % of traffic is carried by 6 operators, which are [✂…✂] (the "Big 6 IGOs"). The value and distribution of costs differ between Fixed and Mobile CLI Call Blocking. For example:

- Fixed CLI Call Blocking is borne by all IGOs who must block calls using Irish CLIs originating abroad and facilitate *'long-lining'*[247] by operators. Europe Economics estimates the one-off cost of this at approximately €46,000, based primarily on the cost of testing the blocking capability of the intervention[248].

- By contrast, the cost of Mobile CLI Call Blocking would be borne primarily by the larger IGOs. Europe Economics estimates this cost at approximately €350,000 for each of the [✂…] with an on-going cost of €60,000[249] who are anticipated to apply blocking on behalf of smaller IGOs[250].

5.112 Smaller IGOs could be exposed to higher costs if larger IGOs were unwilling to "scrub" international traffic on behalf of smaller IGOs. At present, ComReg is aware that some larger IGOs are offering to apply this intervention to the traffic carried by smaller IGOs (subject to commercial agreements). From NCIT discussions and bilateral discussions, ComReg understands that in particular [✂…✂] are willing to offer such a service and play a proactive role in protecting Irish consumers from international fraudsters[251]. Such an approach would be welcome as it would benefit smaller IGOs in protecting end-users. In fact , larger

[246] All IGOs originate traffic and are therefore a subset of the 30 known Fixed line and mobile Originating Operators.
[247] As described in Chapter 4.
[248] See Table 9.3 of the Europe Economics Report.
[249] See Table 9.3 of the Europe Economics Report.
[250] Either after traffic has been handed over to [✂...], or by "passing over" traffic for blocking before having it returned. Any payments for such services amount to a transfer of costs between IGOs and are therefore excluded for present purposes.
[251] For the purpose of estimation of cost Europe Economics has estimated that the three MNOs and one IGO, BT, implement the Mobile CLI Blocking on behalf of smaller IGOs

IGOs should have an interest in providing such a service given that any exceptions would create a 'gap' and potentially undermine their own investment.

5.113 Operators that have already implemented Fixed and/or Mobile CLI Call Blocking would prefer Option 3. Indeed, the investments already made in implementing this intervention would be weakened if other operators failed to do so because fraudsters would likely exploit that 'gap' to reach Irish consumers, including the customers of operators that have already implemented the intervention. To maximise their return on investment such operators would prefer if Option 3 applied to all relevant operators. In relation to those operators that have not implemented this option – the knowledge of knowing that this intervention has been implemented by other operators already provides some assurance that a return on their investment would be earned soon after implementation. This intervention also provides a higher degree of protection for customers at a relatively low cost.

5.114 It is difficult to foretell whether IGOs would prefer Option 2 or Option 3, given the trade-off between cost and customer protection. Option 3 would provide better customer protection, but would also impose a greater cost, in particular on the three MNOs and BT, as outlined in Table 13 below. BT, Three, Vodafone and Eir may prefer Option 2 over Option 3, if motivated by cost alone, but may prefer Option 3 if they prioritise consumer protection. ComReg assumes that other IGOs would likely prefer Option 3 to Option 2, given the small incremental costs that would be borne under Option 3 (again, noting that some operators are already implementing these interventions)

5.115 All the operators identified above would appear able to afford these measures, with annual revenues far in excess of one-off costs. Furthermore, and for context, the Big 6 IGOs collectively earned in excess of €[✂…✂] million in 2022[252] from providing this transit service to third parties (noting that a number transit traffic for their own networks).

Table 13: One-off costs per stakeholder for each Option, relative to status quo

Option	Originating Operators (excl. IGOs)	Smaller IGOs	Key IGOs
Option 1 (Do nothing)	-	-	-
Option 2 (DNO&PN)	€33,000	€33,000	€33,000
Option 3 (DNO&PN, Fixed and Mobile CLI call Blocking)	€33,000	€79,000	€435,000 (€935,000 incl. VoLTE)

[252] IGO RFI.

II. Other Impacts

5.116 The same impacts described under Option 1 would apply here – however Option 3 would better reduce the harms from nuisance communications (e.g., fraud and emotional harm) and best protect trust in the numbers that are used to deliver telecommunications services. Therefore, Option 3 would also best protect the long-term commercial interests of providers of voice services as trust underpins the use of Voice services.

Conclusion on impact on industry stakeholders

5.117 Based on its assessment, ComReg is of the preliminary view that Option 2 and Option 3 are likely to be preferred by most stakeholders, particularly those that have already implemented this intervention. However, cost conscious operators particularly those smaller IGOs (which collectively account for less than [✂…✂]% of transited traffic) are less likely to prefer Option 3, partly because they may have to rely on larger IGOs to implement this intervention on their behalf for it to be most cost-effective.

III. Impact on competition

5.118 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the statutory objectives as they relate to competition, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the promotion of competition and the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on efficient investment arising from the regulatory option is assessed.

Option 1: No regulatory intervention

5.119 ComReg notes that the assessment provided under this option is also relevant to the draft 'Voice Firewall' RIA because it provides an appropriate benchmark with which to measure the effectiveness of that intervention regardless of the preferred option in this draft RIA. (i.e., this is the status quo absent any intervention at all).

Efficient use of numbers

5.120 Against the objective of ensuring the efficient and effective use of numbers for the benefit of consumers, it is evident under Option 1 that the numbering resource is not being used efficiently or effectively and that this is resulting in observable and significant consumer harm. A situation where 51 million annoying and 17 million distressing scam calls are made to consumers each and every year, and approximately 500 consumers a day are being defrauded by scam calls, is clearly not consistent with the efficient and effective use of the numbering platform and also constitutes the misuse of numbers.

5.121 As noted above, numerous scam calls exploit the lack of protection afforded to Irish numbers at present, with fraudsters using CLI spoofing to impersonate Irish businesses and government agencies. In this way, telephony numbers are being used to perpetuate fraud and undermine ECS networks. The status quo is therefore not consistent with the efficient use of numbers noting that this constitutes misuse. If scam calls continue at their current rate, consumers may adapt by not answering voice calls at all, thereby further undermining the legitimate use of Irish numbers.

5.122 Finally, it is clear that operators under Option 1 do not have processes in place to reduce access to valid numbers by those who intend to misuse them. The misuse of the numbering resource is likely to continue and multiply in Ireland under Option 1 as fraudsters become more sophisticated and other English-speaking countries put in place interventions of their own. ComReg discusses how operators could improve their number assignment processes through Know Your Customer measures in Chapter 6.

Promoting Competition

5.123 Competition is not currently providing adequate levels of protection to consumers from the harm caused by nuisance communications. The current high prevalence of nuisance communications is distorting competition because it affects all operators in the same way. Competitive discipline may be muted if operators expect there to be a good chance that rivals are experiencing similar problems. There has been little attempt by operators to differentiate themselves from rivals by making investments in consumer protection measures that would reduce the nuisance communications arising on their networks. Consumers would likely switch to alternative operators if nuisance communications could be avoided by doing so – however, operators have not distinguished themselves from rivals in any serious way or not at all in most cases. This stifles the competitive process because consumers have little incentives to switch between operators if there are no differences between them in relation to protecting against nuisance communications. This is particularly relevant in light of the serious harm caused to consumers as identified in Chapter 3.

5.124 The lack of protection against nuisance communications arises for a number of reasons.

- First, the incentives to provide protections are not sufficiently high because the majority of the harm/damage of scams are not borne by operators themselves but rather are being borne by their customers, be they consumers or businesses (i.e., €187 Million p/a)[253]. As noted by Europe Economics, without such an incentive, the level of investment by operators is likely to be less than socially optimal, as much of the cost of scam calls represents an "externality" to operators (e.g., not being borne by either contracting party) from the narrow perspective of cost.

- Second, operators are likely concerned that such investments, even if they were made, would prove inefficient if other operators did not replicate similar interventions.[254] Absent regulation, operators may underinvest in interventions whose effectiveness relies upon the coordinated implementation by many other operators. Otherwise, any such investment might prove inefficient. Hence, industry-wide interventions may ultimately be required in order properly address some aspects of nuisance communications.

- Third, the current lack of investment may also be borne from the fact that operators may be unconvinced that competing for customers on the basis of protection against nuisance communications would cause sufficient switching to justify relevant investments. Absent this competitive pressure, operators face little incentive to invest in scam protection in the short run. For example;

    - Competition in mobile markets is multifaceted and involves more than just price – however, adding an additional facet to competition would increase the informational load that consumers must bear when making a product decision. Research conducted by the ESRI Price Lab found that consumers are unable to make good purchasing decisions when descriptions of products force them to think about too many things at once[255]

    - Consumers would not be able to directly observe the actual level

[253] Europe Economics Report page 63.
[254] This is true of a number of the interventions being considered in the Consultation, including:
- DNO and PN - which relies upon implementation by all originating operators and IGOs.
- Fixed and Mobile CLI Blocking – which relies upon implementation by all originating operators and IGOs.
- Mobile CLI Blocking – which also relies upon the implementation of supporting inter-operator processes (i.e., MAP protocol and Share Solution).

[255] Lunn, Pete et al, 2016, PRICE Lab: An Investigation of Consumers' Capabilities with Complex Products, ESRI.

or effectiveness of protection offered by operators' ex-ante, and choice could easily become distorted by perceived rather than actual level of protections afforded by an operator. Consumers may experience the same level of scam calls after switching having compromised on other aspects of competition.

- Fourth, there may be an understanding to maintain the status quo so as to avoid making network investments, such as might be needed to reduce nuisance communications. Such arrangements might be fairly easy to maintain given the small number of network operators and the comparative ease with which one network operator can monitor any significant investment in interventions by a rival operator. In effect, there could be an understanding to delay investments to save additional network costs.

5.125 Given the incomplete consumer information, negative externalities, and coordination failures outlined above, it would appear that competition has not provided sufficient incentives to protect consumers, leading to a market failure and socially suboptimal levels of investment in measures to tackle scam calls. If networks are not timely in offering sufficient protections, despite the significant harm caused by these communications, it would suggest a competitive failure that requires regulatory intervention. Clearly identifiable harms (as evidenced in Chapter 3) for important services (e.g., voice and SMS) should be addressed in a well-functioning competitive market over an appropriate period. However, that is clearly not the case with respect to nuisance communications in Ireland.

5.126 That is not to say operators would not undertake any investment but rather that the level of investment necessary to protect consumers is insufficient. There are measures that operators can take independently, and some overseas operators have been proactive in implementing measures that significantly reduce the threat in their countries. Indeed, there are examples of operators attempting to distinguish their voice service from rivals as most protected from scams (e.g., EE in the UK and Telenor in Norway). However, this represents only a handful of examples internationally despite the worldwide plague of scam calls.

5.127 Furthermore, this option does not promote infrastructure-based competition between voice calls and other VOIP based platforms (e.g., WhatsApp) for a number of reasons including:

- Consumers and businesses may no longer see Voice calls as a viable option given the preponderance of nuisance communications which reduces reliance on the numbering platform.

- Consumers and businesses may move to alternative messaging platforms, despite preferring SMS at present[256] (e.g., OTT for P2P[257] and B2C[258]) ; and

- Declining use of SMS may lead to reduced investment and further reduce competition between providers of SMS services and alternative instant messaging platforms[259].

5.128 More generally, the declining use of voice calls owing to nuisance communications under Option 1 distorts the incentives that providers of voice services (e.g., fixed and mobile network operators) have to compete and invest in their networks and services thereby reducing infrastructure-based competition. For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform. Businesses may switch to alternative technologies to provide such services, that are inferior for serving these specific consumer and business needs at present (e.g., OTT delivery of VOIP for P2P, or apps, email or push notification for B2C[260]) but may have the notable advantage of not suffering from nuisance communications to the same extent as traditional voice calls. This would also greatly reduce the competition between Voice communications and alternative networks for P2P and B2C communications, as Voice calls decline in utility. As operators will know, once consumers and businesses switch to alternative means these switching decisions tend to be for a long period or permanent.

Efficient investment

5.129 Under Option 1 there is a risk that the investments already made voluntarily by some operators would become inefficient. For example, investments by some operators who have already implemented or begun implementing Fixed or Mobile CLI interventions (or would do so in the future under this Option) could become inefficient if other operators do not make concurrent investments. As previously noted, any operator that has yet to take appropriate steps potentially undermines other operator's investment as fraudsters would likely exploit that

[256] These can be considered inferior in the sense that at present consumers and businesses choose voice for certain services, revealing a current preference for Voice calls as a means of communications for those services.
[257] Which is subject to more QoS issues due to latency and potentially less trusted due to a lack of numbers. Notably during the pandemic Irish mobile consumers returned to fixed and mobile voice calls for P2P communications.
[258] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish GN.
[259] For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform.
[260] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish GN.

‘gap’ to reach all consumers including those that made an investment.

5.130 Further, under Option 1, operators would face lower incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications (i.e., 2018/2019) may now become inefficient because such investments were made on the basis of an effectively functioning numbering platform. This may also reduce the incentive for future investments if operators are of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

Option 2: DNO and PN

Efficient use of numbers

5.131 Under Option 2, the DNO and PN should reduce the present misuse of Irish numbers and result in a more efficient use of numbers compared to Option 1 given that the numbers used by businesses and included in the DNO and PN lists would only be used for valid purposes. The DNO and PN List should also decrease the volume and effectiveness of scams impersonating Irish businesses and government agencies while also reducing the susceptibility of consumers to fall for scams by removing numbers of particular importance and credibility (e.g., banks).

5.132 This more efficient use of numbers however would only apply to those numbers on the DNO and PN lists and its impact, while positive, would be limited given the many other avenues used by fraudsters to commit fraud.

Promoting competition

5.133 Under Option 2, DNO and PN should reduce both scam calls and the resulting fraud. In particular, the DNO should improve trust and thereby consumers use of such numbers. This would increase the use of numbers more generally by consumers to contact businesses relative to Option 1. In this way the DNO and PN can help preserve the use of voice communication by business to communicate with consumers, thereby protecting the incentive for operators to compete to provide such services to businesses and also compete on issues such as quality of service for those services.

5.134 Furthermore, reducing the level of scams impersonating businesses may also increase consumers’ confidence in answering calls from businesses, potentially reducing the share of legitimate calls that go unanswered and improving the efficiency of businesses that contact consumers by Voice call.

5.135 However, because Option 2 only extends to numbers on the DNO/PN lists, its ability to promote competition and reduce the existing distortions to competition

as outlined under Option 1 is clearly restricted to this specific use.

Efficient Investment

5.136 Option 2 better protects the investments that have already been made in voice services compared to Option 1 because it better preserves the use of and demand for voice calls. Absent the protection provided by Option 2, service providers and businesses that use certain numbers to allow consumers to contact them may need to invest in alternative communications channels to contact consumers. Such behaviour could result in existing investment becoming inefficient such that those investments would never have been made had operators been aware of the damage nuisance communications would inflict on the numbering platform. Therefore, Option 2 is less likely to result in inefficient investments compared to Option 1.

Option 3: DNO, PN, Mobile and Fixed CLI Call Blocking

Efficient use of numbers

5.137 Under Option 3, Mobile and Fixed CLI Call Blocking should further reduce the effectiveness of scams impersonating both businesses and government agencies relative to Option 1 and 2. This is because these interventions reduce scams through the avenue currently most used by fraudsters (i.e., CLO spoofing). In particular, it would prevent scam calls being spoofed from abroad using Irish GNs, NGNs or MNs (which are popular with fraudsters at present). Further, it would prevent scam calls originating from the numbers of businesses or agencies which have not been included on the DNO or by entities currently unaware of the DNO under Option 1. Fixed and Mobile CLI Call Blocking should greatly reduce the present misuse of Irish numbers better ensuring that where numbers are used, they are used more efficiently than is currently the case.

5.138 Therefore, Option 3 would better promote the efficient use of numbers than Option 1 or Option 2.

Promoting competition

5.139 Option 3 should reduce the distortions to competition outlined under Option 1 because all originating operators would be required to put in place the Mobile and Fixed CLI intervention and this would close the main avenue (spoofing numbers) through which scam calls are currently made in Ireland. Operators would then compete on the basis that such calls would be blocked rather than under Option 1 where competition failed to deliver the same protections that could be reasonably expected to arise in an effectively functioning market.

5.140 Furthermore, if this intervention is applied to all originating operators, it would not lead to any competitive distortions such that only some operators and their

associated consumers would benefit from the intervention. By imposing a common, minimum standard for consumer protection across all operators, Option 3 is less distortionary to competition than relying on operators implementing solutions of their own accord. As outlined above, if left to competitive forces alone there is reason to believe that Mobile and Fixed CLI Call Blocking would not be implemented across industry as operators face a collective action problem.

5.141 Option 3 also represents a reinforcement of all the benefits provided under Option 2 because it strengthens the benefits of DNO/PN by extending its protection to all inbound international voice traffic and improves trust in numbers relative to Option 1 or 2 given that otherwise such numbers would be unprotected by DNO and only partially covered by PN. This should capture further scam calls targeting businesses not captured by DNO (e.g., nearest neighbour).

5.142 Finally, Option 3 would also improve trust in numbers and thereby enhance the likelihood of consumers answering calls from unknown Irish mobile numbers. In this way, Option 3 can help preserve the use of voice communication to provide services between Irish consumers and therefore protects the incentive for MNOs to compete to provide such services to businesses, and relatedly to compete on issues like the QoS for those services.

5.143 Therefore Option 3 would better promote competition that either Options 1 or Option 2.

Efficient Investment

5.144 Under Option 3, the addition of Fixed and Mobile CLI Call Blocking should bring the greatest reduction in inefficient investment resulting from scam calls and CLI spoofing. In particular, Option 3 removes the risk that that investments by some operators who have already implemented or begun implementing Fixed or Mobile CLI interventions (or would do so in the future under this Option) could become inefficient. As we have noted, any uncovered operator potentially undermines an operator's investment as fraudsters would likely exploit that 'gap' to reach all consumers including those that made an investment. In summary, Option 3 would best promote efficient investment and innovation in new and enhanced infrastructures by facilitating MNOs to make investments in the knowledge other MNOs would be subject to the same consumer protection measures.

5.145 Further, under Option 3 operators would face better incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications, and which were made on the basis of an effectively

functioning numbering platform would also be better protected under this option. This option would also increase the incentives for future investments if operators were of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

5.146 By best promoting the use of and demand for Voice calls for P2P and B2C communication, Option 3 benefits operators that may otherwise need to invest in alternative communications channels in order to contact consumers. Absent this protection, service providers and businesses may need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient as it would be driven not by unmet need but by a degradation of existing voice network's ability to continue to meet the existing need for such services. Therefore, Option 3 is less distortionary to investment than Option 2.

Conclusion on impact on competition

5.147 Based on the assessment above, ComReg is of the preliminary view that a combination of Option 2 and Option 3 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

5.148 The above assessment and the accompanying Europe Economics Report demonstrate that there is significant consumer and societal harm present under Option 1. On the other hand, Option 2 and Option 3 address the policy issues described at the outset of this RIA by identifying and blocking calls stemming from international networks and presenting with Irish CLIs and identifying and blocking calls which should never appear as a CLI in the first place. This would promote competition and the more effective functioning of the numbering platform. Therefore, ComReg is of the preliminary view that, on balance, Option 2 and Option 3 are the preferred option in terms of its impact on stakeholders, competition and consumers. These interventions are referred to as the 'static interventions' in the subsequent draft RIAs in this consultation.

5.149 It should be noted this preliminary view only concerns the policy issues described at the outset of this draft RIA. (e.g., identifying and blocking calls stemming from international networks and presenting with Irish CLIs etc). This preferred option may not be sufficient to address all scam calls, and this is discussed further in the draft 'Voice Firewall' RIA which follows.

5.4 Draft Voice Firewall RIA

5.4.1 Policy Issues

5.150 In Section 5.2.1, ComReg noted that the two overarching policy issues relevant to all draft RIAs are:

i. to reduce the harm to consumers and businesses from scam calls; and

ii. to protect and renew trust in ECS Networks and Services.

5.151 The remainder of this subsection further defines these main policy issues as they relate to this draft RIA in order to appropriately assess the available regulatory options. With that in mind, ComReg notes that this draft RIA builds on the previous draft CLI Blocking RIA, where the main policy issue was, among other things, to reduce harm by identifying and blocking calls making illegitimate use of Irish CLIs from international networks. While the preferred option appropriately addresses that policy issue, it does not address all nuisance voice communications and readers will obviously appreciate that it may become less effective over time depending on how fraudsters react to its implementation.

5.152 In that regard, there are three areas of scam voice calls that are not addressed by the preferred option in the draft CLI Blocking RIA, and which are of relevance to this draft RIA.

- **First**, scam calls that originate in Ireland are unaffected by Fixed or Mobile CLI Call blocking but there is increasing evidence that scams are also originating in Ireland – primarily through the use of pre-pay burner phones. It is also possible that fraudsters could exploit other unknown or unidentified vulnerabilities in network that have not already been identified.
- **Second**, fraudsters from abroad do not always use CLI spoofing of Irish numbers and on occasion use their own numbers from where the scam originates or spoof the numbers of a foreign country trusted by Irish consumers (e.g., certain scams have used +44, the UK's dialling code). Such scams can travel by what is ostensibly legitimate traffic and cannot simply be blocked on the basis of the CLI and route alone.
- **Third**, future scams may well become more sophisticated as the Fixed and Mobile CLI Call Blocking takes effect. Any call a consumer might receive from whatever location could potentially be a scam call. Blocking such traffic requires an assessment of characteristics of the traffic itself, and not merely whether the route matches the CLI.

5.153 With that in mind, the main policy issue associated with this draft Voice Firewall RIA is to reduce the harm from scam calls and protect and renew trust in ECN by identifying and blocking scam calls regardless of how and where they originate and with an emphasis on scams that would not be blocked under the static interventions (i.e., DNO/PN Lists and/or Fixed and Mobile CLI Call Blocking).

5.4.2 Regulatory Options (Steps 1 & 2)

5.154 The available interventions for the purpose of this draft RIA (and previously discussed in Chapter 3) are as follows.

- **Option 1 –** No Voice Firewall – Preferred Option from the draft 'Voice CLI' RIA' only
  - No additional interventions to the Preferred Option outlined in the draft 'CLI Blocking RIA ', which is to implement the DNO, PN and Mobile and Fixed CLI Call Blocking as stated in the technical specification.
- **Option 2** – Implement a Voice Firewall (in addition to the Preferred Option from the draft 'Voice CLI' RIA')
  - This approach would implement the Voice firewall, alongside the DNO, PN and Mobile and Fixed CLI Call Blocking as stated in the technical specifications.

5.4.3 Impact on industry stakeholders, competition and consumers (Steps 3 & 4)

I. Impact on consumers

5.155 This section provides information on the impacts on consumers arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the direct benefits to consumers arising from the regulatory option are assessed (i.e., reduction in time lost to scam calls and monies to fraud); and

II. Second, other relevant impacts arising from the implementation of the regulatory is assessed (i.e., trust in numbers, use of Voice calls etc.).

I. Direct impacts

Option 1

5.156 The static voice interventions should significantly reduce the number of scam calls and fraud. Europe Economics estimate that these interventions could reduce the value of the present harm to consumers and businesses by approximately €900 million over a 7 year period[261]. However as noted above, these interventions would not prevent all scam calls being made or received and there are three areas that would not be addressed under Option 1

5.157 In relation to I, currently the bulk of scam calls originate abroad and reach Irish consumers via these channels. However, ComReg understands from An Garda Síochána that scam calls originating in Ireland are increasing- primarily through the use of pre-pay burner phones. These cannot be easily identified and blocked because they use valid Irish SIMs to perpetuate fraud. These types of scams are likely to increase significantly under Option 1 because fraudsters will recognise that the static interventions are focussed on stemming calls from international networks and presenting with Irish CLIs etc. Scams using valid SIMs (whether in Ireland or abroad) would not be captured by this intervention.

5.158 In relation to II (scams using valid CLI from abroad)[262] primarily use Wangiri calls (a Japanese word, literally means one ring and cut). Fraudsters will use international numbers to dial users in other countries and immediately disconnect the calls. The scam lies in the hope that they will be called back, and the unassuming caller will then be routed to a premium rate number, overseas, and billed a large sum of cash to listen to a pre-recorded message. These types of calls have been used in Ireland previously by taking advantage of peoples trust in Geographic Numbers. For example, in Mayo, people received Wangiri calls which appeared to come from a local number because the numbers '94' (the prefix to all landline telephones number in the Castlebar district) - appeared on screen but were instead fraudsters from Tunisia.[263]

5.159 Other related scams from abroad include impersonating banks and government agencies without CLI spoofing and instead spoofing using the prefix +44). Scams using the UK international code +44 are particularly prominent in Ireland as many people typically have family and friends based in the UK and may be more likely to answer compared to other international codes. These scams would continue to occur under Option 1 because there is no intervention that

[261] See Table 9.9 and 9.11 of the Europe Economics Report.
[262] For example, calls that appear with an international dialling code (e.g., +44),
[263] Mayo being targeted today by 'Wangiri' phone fraudsters | Connaught Telegraph (con-telegraph.ie)

would protect against them.

5.160 In relation to III (more sophisticated scams), there is a high likelihood of scam calls becoming significantly more sophisticated through criminal's use of advanced AI technologies such as ChatGPT and Microsoft's Vall-E (a tool that converts text to speech)[264]. Emerging evidence suggests that fraudsters abroad are using these technologies to imitate the voice of businesses or family members in distress in order to commit fraud[265]. These scams can combine the relative strengths of different AI tools such as voice mimicry and Chat GPT to generate convincing speech or text in real time and perpetuate such scams on a large scale[266].

5.161 Family emergency calls have already been initiated in the United States and Canada where money is requested based on a voice mimicking a family member[267][268]. Such a call could come from someone who sounds just like a friend or family member but is actually a fraudster using a clone of their voice. Using a short sample of anyone's voice, this technology can accurately convert written sentences into convincing sounding audio. A sample of anyone's voice can be obtained[269] and used to impersonate that person and can appear highly credible.

5.162 It is inevitable that these types of scams will arrive on Irish shores and can be expected to have a higher rate of fraud compared to the current wave of scams. A large share of Irish consumers could be targets for impersonation by voice-mimicry software, given the ubiquity of video content publicly available on social media. Next-generation AI based scam calls should be expected to reach Ireland and increase with time as the underlying technology becomes more widely available (e.g., software like VoiceLab for calls[270]).

5.163 Therefore, a significant amount of scam calls and associated harm will inevitably remain following the implementation of the static interventions. Moreover, the present volume and prevalence of such scam calls would likely increase with time, as domestic and international fraudsters adapt their operations to circumvent the static interventions. Therefore, while effective and beneficial, the

[264] Vall-E is not yet available to the public, but other companies, like Resemble AI and ElevenLabs, make similar tools that are.
[265] For example, AI based voice recognition has been used to verify identity by Centrelink and Australian tax office. AI can fool voice recognition used to verify identity by Centrelink and Australian tax office | Artificial intelligence (AI) | The Guardian
[266] For example, robocalls can reach many consumers but rely on recorded messages, whereas scam callers are more convincing but can only make one call at a time.
[267] Scammers use AI to enhance their family emergency schemes | Consumer Advice (ftc.gov)
[268] For example, a couple in Canada were reportedly scammed out of $21,000 after getting a call from an AI-generated voice pretending to be their son" 6th March 2023 Link
[269] This can be obtained through a number of means by ringing a person and recording them for a very short period or obtaining it through social media or recoding in public.
[270] https://beta.elevenlabs.io/.

impact of the static interventions should be expected to degrade over time.

5.164 Therefore, consumers are highly unlikely to prefer Option 1.

Option 2

5.165 The static interventions only target scam calls arriving from a specific route (i.e., fixed and mobile CLI spoofing target scam calls from abroad that spoof Irish numbers). However, the voice firewall is a dynamic intervention that is designed to intercept scam calls regardless of how or where they originate. In this way, voice firewalls do not directly target each of the gaps outlined above, rather these gaps are captured through an assessment of each inbound call made to an individual caller. In this way, the voice firewall would complement the static interventions by covering over avenues that fraudsters use.

5.166 As noted by Europe Economics, "*In the longer term (after a year) the voice firewall could be implemented, which would enhance the benefits of the other interventions by adding a more dynamic element. As scammers become confronted by the blocks on their activities caused by those interventions in the shorter term, they will likely evolve their methods to maintain access to the pool of potential victims in Ireland. A voice firewall has the potential, in the longer term, to help combat the problems more dynamically and address scam calls that get around the previous interventions*".[271]

5.167 While voice firewalls do not target specific gaps directly, it is likely that it would reduce the scams described above because voice firewalls logs, monitors (e.g., the route taken to arrive onto the network), and controls all inbound voice network activity regardless of where the call originates (i.e., not just international traffic) which should reduce the rate of scam calls. Furthermore, behavioural analysis in firewalls uses both AI and ML to conduct advanced data analytics to predict potential attacks and to identify patterns. Such technologies allow operators to analyse and monitor network traffic and activity for signs of suspicious or malicious behaviour, and to remediate the threats. The data subject to these analytics depends on the firewall provider but typically includes:

- Information and logs that the firewall gathers locally, and scams assessed by the firewall in other countries, including pre-created watch lists.
- phone call characteristics (e.g., numbers that are making a large number of calls) and number owner details.
- previous call histories and recipient reports of fraud.
- network probes strategically positioned across the globe

[271] Europe Economics Report, p75.

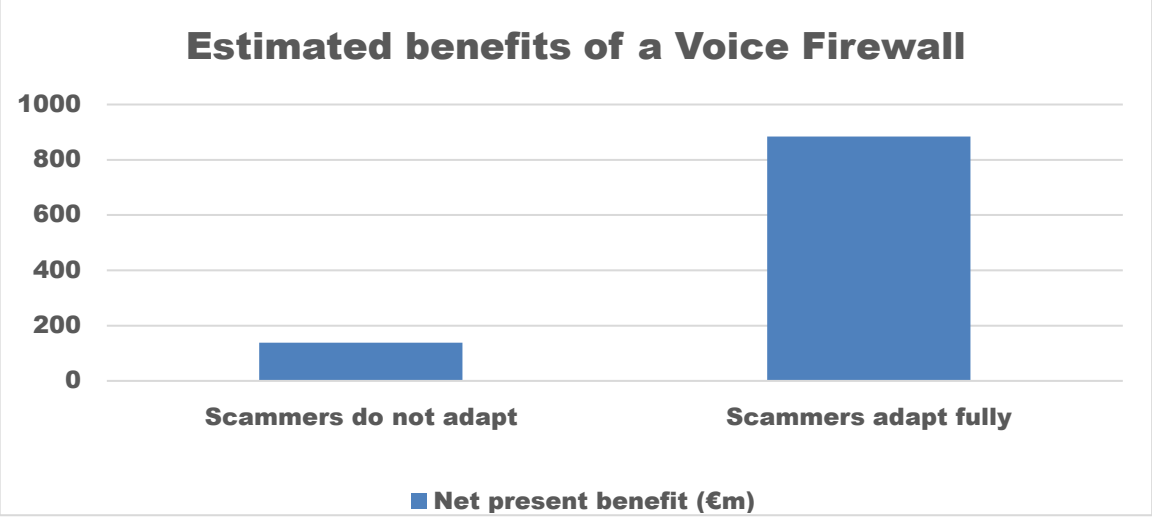
- Intelligence gathered from law enforcement agencies.

5.168 The importance of the Voice Firewall grows as fraudsters adapt to the static interventions by either sidestepping (e.g., scam calls without CLI spoofing, originating scams within Ireland, bringing Irish SIM cards abroad) or overcoming them (e.g., impersonating businesses not on the DNO). The Voice Firewall would provide annual benefits of €152m over 7 years in addition to the static voice interventions even where fraudsters do not adapt because they offer protection that simply cannot be provided by the static interventions (e.g., against scams originating in Ireland etc).

5.169 It should be noted that the importance of the Voice firewall would increase as fraudsters adapt to ComReg's static interventions, rising to €892m where fraudsters fully adapt. The exact benefits of the voice firewall would depend on the reaction of fraudsters to the static interventions – however it is highly likely to be closer to €892m in the longer run given how sophisticated scams are expected to become in the future. Depending on how fraudsters adapt to the static interventions, the Voice firewall represents a healthy social return on investment of between €15- €89 for every €1 spent**.**

5.170 Therefore, consumers are likely to prefer Option 2 and the introduction of a Voice Firewall.

Figure 33: Impact voice firewall in addition to the static voice interventions, for different levels of fraudster adaptation



II. Other Impacts

Trust in voice calls

Option 1

5.171 Option 1 would improve the trust of consumers in Voice calls, relative to the status quo where no regulatory measures would be implemented. The static voice interventions should reduce the prevalence of scam calls and the number of scam calls received by consumers, in particular those using CLI spoofing. Option 1 would therefore protect the trust consumers place in key numbers relative to status quo. However, the impact is likely to be temporary as fraudsters can be expected to adapt to the implementation of the static interventions. There is no reason to think that consumers would trust voice calls more in the long run because a subset of those communications (i.e., spoofed numbers from abroad) are blocked. In effect each of the effects outlined above (e.g., contagion, feedback etc) would continue reducing trust in the numbering platform in the longer run.

Option 2

5.172 Under Option 2, the combination of a Voice firewall and the static voice measures would provide the greatest protection to Irish consumers, by both blocking scam calls making illegitimate use of CLIs but also by blocking suspicious voice traffic originating in potentially legitimate uses. Absent the static voice measures, some of those nuisance calls may end up being received by consumers because, while effective, the voice firewall cannot provide full protection all of the time due to the rapid evolution of nuisance calls[272]. Furthermore, to the extent that the static interventions would restore trust, this would only be in the short term and before fraudsters could adapt to the implementation of the Fixed and Mobile CLI Call Blocking. As noted by Europe Economics "*the ability to adapt to evolving threats from scammers gives this intervention the potential to improve consumer and business trust in voice communication in the longer term. Knowing that a voice firewall is in place to respond to CLI spoofing and potentially other forms of threats could imbue call receivers with trust that the calls they receive are legitimate*"[273]

5.173 As this regulatory option would block the most scam calls, ComReg considers that it would be most likely to restore trust in Voice calls, particularly in the short run. As previously noted, two out of three adults state that regulatory

[272] Absent the static measures, fraudsters would likely continue to spoof Irish numbers, given the importance of such numbers to Irish consumers. As a Voice Firewall assesses many millions of calls, even a with high degree of accuracy a large number of scam calls would not be blocked and still reach consumers. Even were only a small share of attempted scam calls using CLI spoofing to reach consumers, this is still a large number of scam calls. Therefore, absent the static interventions, a Voice Firewall is unlikely to protect trust fully as fraudsters would likely continue to spoof Irish numbers.
[273] Europe Economics Report, page 73

intervention would increase their trust in calls and texts, rising to 9 out of 10 once adults that are unsure of its effect are excluded[274].

5.174 Consequently, Option 2 and the combination of the static interventions and the voice firewall would result in the greatest reduction in scam calls, while protecting the use of Irish numbers. Therefore, Option 2 would best safeguard the trust in Voice calls and Irish numbers and is likely to offer the best defence, thereby promoting the continued use of Voice by Irish consumers and businesses.

Conclusion on impacts on consumers

5.175 Based on its assessment, ComReg is of the preliminary view that Option 2 is likely to be preferred by consumers and businesses as it offers the greatest reduction in the harm from scam calls and best safeguards the trust in and use of voice calls and Irish numbers more generally.

II. Impact on industry stakeholders

5.176 As this draft RIA relates solely to Voice interventions, the relevant industry stakeholders, among those outlined in Section 5.2.4, are operators that:

a) Originate Voice traffic;

b) Terminate Voice traffic;

c) Transit traffic via an International Gateway; and

d) Other operators (resellers, including MVNOs).

5.177 This section provides information on the impacts on industry stakeholders arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

Option 1: No voice firewall, preferred option in CLI Call Blocking RIA only.

[274] Q.45 "*If regulatory interventions were made to block scam calls and texts, to what extent would this impact the level of trust you have in calls and texts you receive in the future?*". 27% of respondents answered that they were "Unsure of the impact" of such regulatory actions on their trust in calls and texts. Upon implementation, such consumers trust either would or would not be affected, therefore we consider the estimated of consumers whose trust will be positively impacted to be a lower bound estimate.

I. Financial impacts

5.178 Under Option 1, no financial costs would be incurred by operators other than those already incurred through the implementation of the DNO, PN lists and both Fixed and Mobile CLI Call Blocking.

II. Other Impacts

5.179 The benefits to operators in terms of the protecting their consumers and commercial interests from this option are as previously outlined above. However, as 5.171some level of scam calls should be expected to remain and negatively impact trust and use of Voice calls these scams would continue to threaten operators' long-term commercial interests.

Option 2: Voice Firewall and preferred option from the 'CLI Blocking RIA'

I. Financial impacts

5.180 A Voice firewall is applied on terminating voice traffic and therefore the cost of this intervention is borne by terminating operators. The requirement to implement a Voice Firewall would apply to Eir, Three, Vodafone and Virgin. To inform ComReg's assessment, Europe Economics has estimated both the one-off costs (e.g., the cost of software purchase and installation) and on-going cost (e.g., on-going cost of software) of Voice Firewall per operator.

5.181 Under Option 2, most operators would pay the same as under Option 1 as only operators required to implement a Voice firewall would pay more. However, Option 2 would impose an additional cost on Eir, Three and Vodafone and Virgin, as shown in Table 14 below.

Table 14: One-off costs per stakeholder for each Option, relative to status quo

Intervention costs	Originating Operators	Small IGOs	Large IGO [275]	Virgin[276]	MNOs
Option 1 DNO&PN, Fixed and Mobile CLI call Blocking	€33,000	€79,000	€935,000	€79,000	€935,000
Option 2 DNO&PN, CLI Call Blocking & Voice Firewall	€33,000	€79,000	€935,000	€1.2 Million	€2.1 Million

[275] This is the IGO assumed to implement Mobile CLI V1 and bear its full cost.
[276] Virgin is in the unique position of having >5% voice capable subs but not bearing the higher cost of Mobile CLI Call Blocking.

II. Other Impacts

5.182 Under Option 3, the harms outlined from scam calls we outlined in Chapter 3 would be most reduced, thereby best protecting trust in Voice calls and Irish numbers .

Conclusion on impact on industry stakeholders

5.183 Based on its assessment, some operators may be of the view that the implementation of voice firewall is unnecessary given its additional costs. Conversely, however, operators may also prefer Option 2 given the additional protections provided by that option, including improved consumer outcomes for Voice calls, thereby safeguarding their long run commercial interests.

5.184 In particular, such operators may value the future-proofed protections provided by the voice firewall with regard to scam prevalence. Indeed, the UK MNO EE has implemented a voice firewall and relayed its benefits to consumers. While cost-conscious MNOs may prefer Option 2, ComReg suspects few would be so blinkered as to prioritise costs in the short term over the continued use of Voice services in the long run – not to mention the higher rate of consumer fraud and harm.

III. Impact on competition

5.185 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the relevant statutory objectives on competition, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on the efficient investment arising from the regulatory option is assessed.

Option 1: No Voice Firewall, preferred option in CLI Blocking RIA only.

Efficient use of numbers

5.186 Implementing the static interventions would represent a significant improvement in terms of the efficient use of numbers. However, such interventions on their own would not prevent all scam calls being made and certain scam calls would continue to be made through other routes. In particular, ComReg notes that scams could still occur through (i) calls that originate in Ireland and (ii) through the use of Irish SIMs abroad. The use of these numbers to commit fraud could not be considered efficient and would remain a misuse of Irish numbers. Therefore, while Option 1 would increase efficiency due to the implementation of static interventions the impact would be limited to calls that originate over those routes.

Promotion of competition

5.187 The static interventions would promote competition but only insofar as identifying and blocking calls stemming from international networks and then presenting with Irish CLIs or by identifying and blocking calls which should never appear as a CLI because the numbers are either unassigned or are inbound only numbers. Importantly, these interventions would be highly unlikely to promote competition in the long run given that the effectiveness of the static interventions can be reasonably expected to wane as scams become more sophisticated. Consequently, the distortions to competition previously identified above would continue to exist in the long run. Furthermore, even in the short run, where the static interventions would have the greatest impact on promoting competition, scam calls would continue to be made using other routes as we have discussed.

Efficient Investment

5.188 The static interventions would encourage efficient investment in ECS because all relevant operators would be required to implement those interventions and therefore there would be no ‘gaps’ to be exploited by fraudsters. Notably however, and unlike the fixed and mobile CLI interventions, the effectiveness of the voice firewall in reducing nuisance communications is not dependent on implementation by other operators. In effect, an operator implementing a firewall would reap the full benefit of that investment independent regardless of other operator decisions.

5.189 However, Option 2 would promote efficient investment and innovation in new and enhanced infrastructures because the investment made in the firewall would be forward looking and there is a high degree of likelihood that the firewall would provide protection against scams in the future – scams that would otherwise have occurred. Therefore, there is a lower risk that any investments made in a voice firewall would become inefficient. Further, its speedy implementation would prevent operators from having to make further future investments to address the damage caused by nuisance communications. This

may be particularly acute for Voice services for B2C which has a more diverse and specialised ecosystem (e.g., the operators serving the call centres serving Irish businesses).

Option 2: Voice Firewall and preferred option from the 'CLI Blocking RIA'

Efficient use of numbers

5.190 Given the investment made by the industry in the work of the NCIT, ComReg is satisfied that the 'static' interventions are robust and powerful. However, on their own they are unlikely to offer sufficient protection because there are other avenues, as we have discussed earlier, that fraudsters could use Under Option 2. The combination of a Voice firewall and the static interventions would provide the greatest protection to Irish numbers, by both blocking scam calls that are clearly making illegitimate use of CLIs but also by blocking suspicious voice traffic originating in potentially legitimate uses. In this way, it is less likely that numbers would be used inefficiently.

5.191 In particular, the voice scam calls that originate in Ireland are unaffected by Fixed or Mobile CLI Call Blocking but there is growing evidence that scams are originating in Ireland. These particular cases of fraud directly use Irish numbers so the use of a voice firewall is particularly important as otherwise such scam calls would not be interrupted. Further, because the voice firewall provides protection against future scams it better promotes long run efficiency effects. Therefore, Option 3 clearly best promotes the efficient use of numbers, by minimising their misuse and promoting their legitimate use.

Promoting competition

5.192 Option 3 would maximise benefits to consumers by appropriately and proportionately addressing significant consumer harms (as evidenced in Chapter 3) for clearly important services. Option 2 would complement the static interventions in reducing the rate of nuisance communications. Option 2 would also play an important role in reducing any competitive distortions by mandating measures that that one would expect to be provided in a well-functioning competitive market over an appropriate period.

5.193 Because the static interventions can only target specific sources of scams, the addition of the voice firewall would importantly broaden the scope of consumer protection to better cover current scams. Further, it is unlikely that the static interventions of themselves would protect long run competition because it is highly likely that scams would evolve in response to the static interventions. Indeed, absent the implementation of the voice firewall it is highly likely that further regulatory interventions would be required in the short-term as scams inevitably become more sophisticated.

5.194 Finally, under Option 2 there remains a high degree of flexibility in terms of how the voice firewall is implemented by operators and the features and functionality it would use. There are a variety of different types of firewalls that can be implemented, and the technical specifications afford operators a degree of discretion over how this is done. Competition may even drive protection beyond the levels envisaged by ComReg thereby underpinning the role of competition in driving benefits for consumers. This provides assurance that there is little risk of the obligation itself creating unintended distortions or imposing due costs.

Efficient Investment

5.195 A Voice Firewall would act as a strong complement to the static interventions in promoting efficient investment, by reducing potential distortions to competition and the misuse of numbers. Option 2 would encourage efficient investment and innovation in new and enhanced infrastructures by encouraging the rollout of voice firewalls to protect consumers, promoting innovation and ensuring the efficient use and effective management of the national numbering resource. Such investments would be efficient because there is a clear requirement for these interventions given the harms outline in Chapter 3 and it is highly likely that such technologies would be implemented at some point by some operators in the future. However, the implementation of this infrastructure now would address the current ongoing harm to both consumers and operators. Option 3 best prevents inefficient investment by protecting the current and future investment in current Voice services and networks, and the use of Irish numbers.

Conclusion on impact on competition

5.196 In light of the above, ComReg is of the preliminary view that Option 2 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

5.197 The above assessment, together with the Europe Economics Report, demonstrate that there is currently a significant consumer and societal harm present due to nuisance communications. While the static interventions are effective for their intended purpose, there are other forms of scams that would still occur. Under Option 2, the Voice Firewall would complement the static interventions and provide additional and proportionate consumer protection measures. Option 2 clearly address the policy issues described at the outset of this draft RIA because a voice firewall would reduce the rate of scam calls generally but would also address scam calls that originate in Ireland as well as scams through valid non-Irish numbers from abroad. It would also provide protection against future more sophisticated scams designed to circumvent the

static interventions as fraudsters make increased use of AI and ML technologies.

5.198 Therefore, ComReg is of the preliminary view that Option 2 is the preferable option.

5.5 Draft Sender ID RIA

5.5.1 Policy Issues

5.199 In Section 5.2.1, ComReg noted that the two overarching policy issues relevant to all draft RIAs are

i. being to reduce the harm to consumers and businesses from scam calls; and

ii. to protect and renew trust in ECS Networks and Services.

5.200 ComReg is mindful of these policy issues in determining its preferred option. The remainder of this subsection further considers these main policy issues as they relate to this draft RIA in order to appropriately assess the available regulatory options.

5.201 Fraudsters, be they overseas or here in Ireland use relatively inexpensive and readily available technology to send SMS with maliciously spoofed Sender IDs to impersonate an individual or trusted businesses/organisation. Such businesses/organisations include:

- Irish companies (e.g., banks or delivery services)
- Irish government agencies (e.g., Department of Social Welfare)
- Other legitimate organisations (e.g., NGOs)

5.202 Consumers have a high level of awareness of these organisations and fraudsters take advantage of this by impersonating them by means of a fake Sender ID. This makes it more likely that the consumer will read and comply with the instructions contained within the SMS. This can result in significant harms to consumers either through fraud and/or through annoyance or distress at receiving such SMS (See Chapter 3). The ensuing objectionable experiences can in turn lead to Irish consumers no longer being able to trust the Sender ID displayed on their SMS messages.

5.203 Unfortunately, there is significant incidence of impersonation through scam text messages. ComReg understands from An Garda Síochána that this constitutes a major share of total SMS fraud. ComReg's research reveals that around 9 in 10 consumers claim a legitimate organisation was impersonated, with the most prevalent organisations impersonated being banks, followed by postal services (An Post), Revenue and the HSE.[277] For organisations, this level of impersonation is impacting mainly organisations with a large consumer base and who would typically have a regular requirement for them. On average, 3 in

[277] B&A Consumer Survey, slide 37.

4 businesses claim to spend around 25 hours resolving scam texts in the past year – though rates are significantly higher depending on the organisations affected. More pertinently, the scamming reduces trust consumers have in SMS and consequently are less willing to engage with SMS.

5.204 With that in mind, the main policy issue associated with this draft RIA is to reduce the harm to consumers arising from scam SMS using spoofed Sender ID that impersonate organisations.

5.5.2 Regulatory Options (Steps 1 & 2)

5.205 Having regard to the interventions described in Chapter 4, ComReg considers that the four regulatory options available to it are:

- **Option 1 –** No regulatory Intervention
  - This approach would maintain the status quo position with no intervention(s) proposed by ComReg.
- **Option 2 –** Ban Sender IDs
  - This approach would ban the use of SMS IDs and businesses/organisations would be unable the send SMS using a Sender ID.
- **Option 3** – Full Sender ID registry
  - This would require senders and aggregators to follow a set of rules or a code of practice which requires that they register their Sender ID thereby authenticating the source of such messages. This approach would implement a Full Sender ID registry as stated in the technical specification.
- **Option 4** – Partial Sender ID registry
  - This would be a hybrid of Option 2 and Option 3 whereby some Sender IDs are permitted, but all others are blocked. Sender ID Registration would be available for businesses/organisations that plan to send more than a certain volume of SMS per month (e.g., Banks, delivery companies), all other SMS using Sender ID would be blocked.

5.5.3 Impact on industry stakeholders, competition and consumers (Steps 3 & 4)

I. Impact on consumers

5.206 This section provides information on the impacts on consumers arising from the regulatory options outlined above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the direct benefits to consumers arising from the regulatory option is assessed (i.e., the reduction in monies lost to scam texts); and

II. Second, other relevant impacts (e.g., impact on trust) arising from the implementation of the regulatory options are assessed (i.e., other impacts).

Option 1: No regulatory intervention

I. Direct impacts

5.207 Under Option 1, the prevalence and harm (detailed in Chapter 3) from scam texts would likely remain high. There are numerous factors that could cause this harm to escalate (such as fraudsters increasing the rate of scam attempts) or moderate (consumers adapting their behaviour). However, absent any intervention, there is a notable risk that scams which impersonate organisations using Sender IDs would increase. Text scams are dynamic in nature and fraudsters adapt and evolve tactics to target consumers and so new forms of scams emerge over time. The harm is also likely to increase as the fraudsters become more ingenious even where consumers adapt to older scams

5.208 As outlined in Chapter 3[278], Europe Economics estimates that the current annual level of harm to Irish consumers and businesses from scam texts is approximately €115 million per annum[279]. For the purpose of the analysis in this draft RIA, it is sufficient to note that the harm to society under Option 1 is likely to remain substantial with the potential to increase even further.

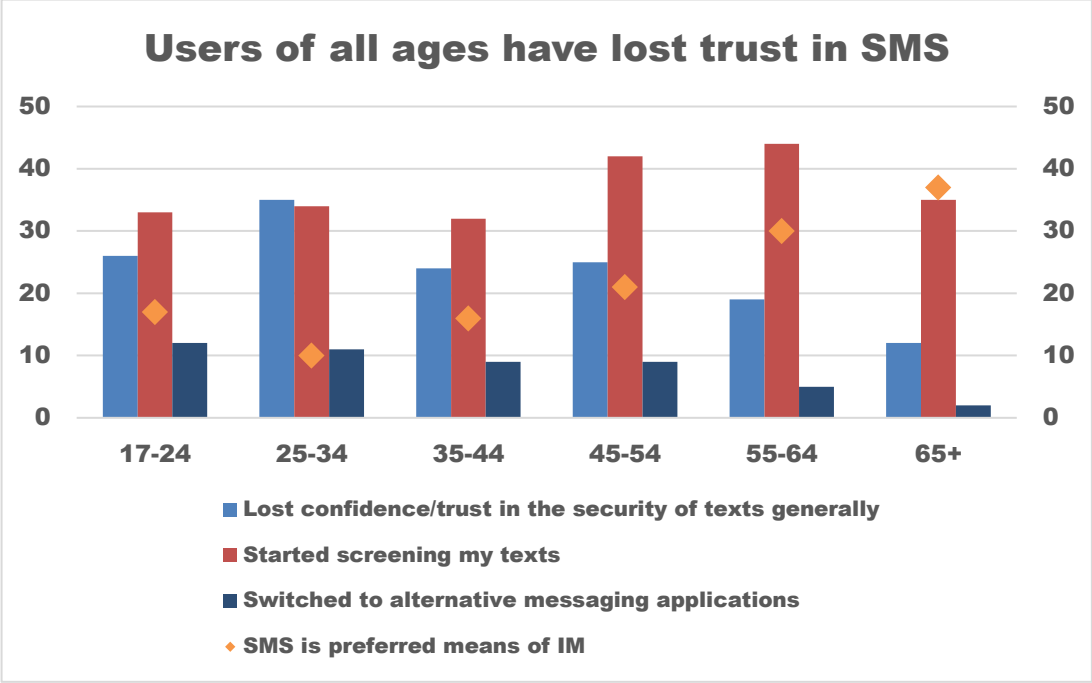
II. Other Impacts

Trust in SMS

5.209 Scam SMS reduce consumer trust with many consumers now screening or ignoring SMS altogether. Unsurprisingly, nearly 1 in 4 consumers have lost trust in SMS, with lost trust highest among younger consumers (see Figure 34below).

[278] See also Chapter 4 of the Europe Economics Report.
[279] Europe Economics Report page 63.

Figure 34: Loss of trust in texts as a result of scams[280]



Source: ComReg analysis of B&A Consumer survey data

5.210 Scam calls and text create a number of distinct effects that reduce trust and threaten the efficient and effective functioning of the numbering platform. Below we assess each of these effects (i.e., contagion, call reduction, feedback, and social effects) in relation to SMS.

Contagion

5.211 Contagion refers the uncertainty caused by the prevalence of scam SMS and/or a previous scam SMS experience which may infect a consumers' beliefs across all SMS regardless of who the sender is. Under Option 1, it is likely that contagion would multiply as consumers become increasingly suspicious about the SMS medium. As identified in Chapter 3, there are already a number of clear examples of contagion across the numbering platform. For example:

- Nearly 70% of consumers are concerned or very concerned about scam SMS. Those who have experienced a financial loss have a heighted level of being 'very concerned'[281].
- Over 59% of businesses are concerned or very concerned about scam SMS. Those using mobile numbers to communicate also show higher levels of concern[282].

[280] Q.38 In relation to your awareness of scam calls and texts, has any of the following happened? Q.5 Main way of sending and receiving instant messages?
[281] B&A Consumer Survey, slide 13.
[282] B&A Business Survey, slide 11

5.212 ComReg is of the preliminary view that SMS provided over the numbering platform even now suffers from contagion and this would likely intensify under Option 1.

SMS reduction

5.213 SMS reduction refers to reductions in the utility of SMS due to contagion. Contagion is causing consumers to read fewer SMS than they would otherwise, due to fear of being scammed. Consumers are now not reading SMS even from people they may know or from businesses providing services that consumers would ordinarily be interested in (e.g., deliveries, hospital appointments etc). ComReg's Consumer Survey results show that fraudsters impersonate organisations that a consumer would potentially be open to receiving information from. This reduces the volume of SMS received over the numbering platform as consumers decide to read less and less SMS. For example:

- 43% of consumers have stopped reading SMS that may be from businesses or government agencies[283] due to the prevalence of scam texts.
- 23% of consumers have lost confidence/trust in the security of SMS generally.

5.214 While only 8% of respondents have switched to OTT providers to date due to scams[284], this can be expected to grow as the harms further manifest. Absent intervention, it appears that this level of switching could increase, and amount to a serious threat to the use of SMS for P2P and B2C in the future. This risk is heightened as younger consumers, who are less likely to prefer SMS for messaging to begin with and consumers that lost money to a scam call or text (which grows cumulatively year on year) are more likely to move to alternatives. These groups represent an important and growing share of the market, and such consumers may not transition back to SMS as they gradually adopt other OTT services (e.g., instant messaging combined with voice & video).

5.215 As we have noted, this can occur not because consumers necessarily prefer alternative applications or because they view these alternatives as being essentially equivalent to one another. Rather, such migration usually occurs because the consumer decides that the harms and nuisance associated with using calls and/or SMS are so high that they try to avoid using SMS altogether. It stands to reason that if SMS messaging operated more effectively then consumers (or at least some consumers) would have less need to migrate to alternative means that they may not prefer or are uncomfortable using.

[283] B&A Consumer Survey, slide 31.
[284] B&A Consumer Survey, slide 31.

5.216 ComReg is of the preliminary view that the evidence it has gathered demonstrates that nuisance communications are supressing the volume of SMS to the detriment of consumers and businesses.

Feedback effect

5.217 The feedback effect refers to the reduced incentives for people and organisations to use SMS because of the reduction in people reading SMS. Businesses may decide not to send SMS because of the low answer rate (i.e., the SMS reduction creates a feedback effect). In such circumstances, businesses are likely to switch to alternative means of contacting consumers even though their preference may be to contact consumers using SMS on public networks. For example, 39% of businesses have made changes to how they communicate with consumers, with 23% relying more on alternative means of communications (e.g., email, secure messages, online portal, WhatsApp etc.).[285] Nevertheless, many businesses continue to make use of SMS for B2C. While some businesses report reducing their reliance on mobile networks (10%) or SMS aggregators (7%) to contact consumers[286], these remain in the minority. Therefore, SMS has not yet been abandoned and its further decline may be avoided if actions are swiftly taken.

5.218 ComReg is of the preliminary view that there is clear evidence of feedback effect under Option 1 with organisations particularly affected as they move to alternative ways of contacting consumers.

Social effect

5.219 The social effect arises where some services that would normally be provided through SMS moves to alternative platforms not readily available to some social groups. People's reluctance to engage with SMS due to fear of being scammed could have a particularly negative impact on vulnerable consumers for whom SMS provides an important social outlet or access to essential services (e.g., healthcare, social security). The social effects of reduced SMS volumes resulting from avoidance can therefore be particularly detrimental for those who may be dependent on one or more social services and such persons can often be the most vulnerable members of our society.

5.220 For example, older people are more likely to be affected by people and organisations (in particular) switching to alternative messaging services because older people are more reliant on SMS for instant messaging. The use by over 65s of alternative instant messaging platforms (e.g., WhatsApp, video calls, social media) is only a third of average users, and up to 5 times less when

[285] B&A Business Survey, slide 23.
[286] B&A Business Survey, slide 23.

compared to younger groups[287]. Notably, fewer older users report switching to alternative messaging applications due to the prevalence of nuisance communications.

5.221 Older people are also more likely to be concerned or very concerned about scam SMS (83%)[288]. The most commonly impersonated organisations are those which older people are likely to require (e.g., banks, HSE and other public bodies such as An Post). For example, the HSE has outlined to ComReg the potentially serious repercussions of this lack of trust in SMS in particular for its elderly patients, given its impact on missed appointments. It is for such reasons that the possible impacts of reduced trust on more vulnerable consumers must be carefully considered.

5.222 ComReg is of the preliminary view that there is clear evidence that scam SMS are having social effects under Option 1.

Option 2: Ban Sender IDs

I. Direct impacts

5.223 Under Option 2, a Sender ID ban would reduce the harm from scam SMS by preventing the use of Sender IDs entirely, including from businesses and government agencies. This would reduce the volume and effectiveness of scam SMS impersonating businesses/organisations because it prevents scam SMS using Sender ID spoofing. It would also reduce the susceptibility of consumers to fall for scams by reducing the ability of fraudsters to accurately impersonate businesses and organisations. Because many scam SMS arise from the impersonation of businesses/organisations using scam Sender IDs, there would be a reduction of around half of the current €166m in harms. However, this reduction in harm is likely to be only temporary as fraudsters inevitably divert all SMS scams to messages without Sender ID.

5.224 However, while effective at cutting scams using Sender ID any reductions in harm (even in the short run), would come at the cost of preventing businesses and organisations from using Sender ID to communicate with consumers. This option would unavoidably reduce the utility of SMS for B2C communications given that Sender ID, even in its current polluted form, is valued by businesses/organisations in communicating with consumers. Indeed, consumers would likely value Sender ID if they were assured that such communications were valid and originating from the intending organisation/business.

5.225 The overall impact on consumers is therefore likely to be mixed and would

[287] Mobile Consumer Experience Survey, slide 37. Link
[288] B&A Consumer Survey, responses to Q.5a "*How concerned are you about … Scam texts*"

depend on the consumer demographic and on how businesses/organisations agencies react to a ban on Sender IDs. Businesses/organisations may use SMS without Sender ID where SMS communications would display an originating number rather than a Sender ID. Ostensibly, consumers seem unlikely to prefer this because this simply moves the scam SMS using Sender ID to SMS more generally.

5.226 Alternative technologies (e.g., OTT) for B2C may be effective, particularly for younger demographics that are familiar with these technologies. In that regard, some consumers are likely to be indifferent about this option particularly for those who may already be wary of scam texts using Sender IDs. Indeed, some consumers may prefer all Sender ID's to be banned because it removes a potential avenue for fraudsters particularly for scams that appear within a genuine "thread" of text messages, and which is particularly egregious. For example, of consumers who did not respond to texts, 58% chose not to because they would prefer to communicate with the organisation in other ways[289].

5.227 However, these could be an inferior service to SMS because the use of alternatives may make it more difficult for organisations/businesses to communicate with older demographics who are less likely to engage with such forms of communications. This would result in lower effectiveness or efficiency of B2C and therefore higher cost to businesses. Conversely, SMS is universally used by all demographics which explains why businesses/organisations use it so widely but also why it is a target for fraudsters. Overall, the impact on consumers is likely to be mixed and consumers are likely to become more open to this Option in the event that scam SMS increase further.

I. Other Impacts

Trust in SMS

5.228 Under Option 1, there would be no trust issues in relation to SMS using a Sender ID since all such communications would be blocked. However, Option 1 would be unlikely to significantly improve trust in SMS generally. Fraudsters would still send scam SMS regardless of whether Sender IDs were blocked or not. Contagion and related effects would still occur as fraudsters would also continue to impersonate businesses through copying text their language format using normal or spoofed numbers. There is no reason to think that consumers would trust SMS communications more because a subset of those communications (i.e., Sender ID) are blocked.

Option 3: Full Sender ID registry

[289] B&A Consumer Survey, slide 38.

I. Direct impacts

5.229 Under Option 3, a full Sender ID registry would reduce the harm from scams by preventing fraudsters using Sender ID spoofing. Only businesses with Sender IDs that are registered would be permitted to send SMS to consumers using a Sender ID – all other Sender IDs would be blocked. This would be available for all businesses and organisations that are registered and would not be limited to the larger users of Sender IDs. Consumers could be confident that any SMS that they receive with a Sender ID is from a reputable organisation.

5.230 Europe Economics estimate that Option 3 would reduce the value of the present harm to consumers and businesses by €372 million over a seven-year period, or roughly €53 million annually[290]. However, similar to Option 2, this reduction in harm could be temporary as fraudsters divert any remaining SMS scams to messages without Sender ID.

II. Other impacts

Trust in SMS

5.231 Option 3 would restore and protect trust in SMS that use a Sender ID because consumers would have a high level of assurance that such SMS are valid and sourced from genuine businesses and organisations. This would prevent contagion from occurring at the outset and consumers would be significantly more likely to engage with such SMS thereby lowering the 'SMS reduction effect' and promoting the efficient use of the underlying number used to deliver such SMS. Higher rates of SMS engagement increase the effectiveness and efficiency of SMS as a means of communication, thereby increasing the utility and use of SMS by senders.

5.232 Most importantly, Option 3 preserves the benefit of Sender IDs to SMS as a means of B2C communications, as noted by Twillio: "*Benefits of messaging with Alphanumeric Sender ID….Higher message deliverability…Improved brand recognition…Increased open rates…Alternative to 10DLC A2P messaging"*[291]. The effectiveness of SMS for B2C would recover as Sender ID spoofing is prevented and consumers become more likely to trust, open and read SMS that use IDs. This is turn would lower the feedback effect by encouraging organisations and businesses to use SMS as a means to communicate with their consumers. Finally, such organisations that deliver important public and social services would be able to register their Sender ID allowing vulnerable groups to receive services without the worry of knowing whether such SMS are genuine or from fraudsters. For most businesses the

[290] See Table 9.10 and Table 9.11 the Europe Economics Report.
[291] Twilio Website "Alphanumeric-Sender-ID-for-Twilio-Programmable-SMS" Link

cost of registration would be likely to be of little consequence[292].

Option 4: Partial Sender ID registry

I. Direct impacts

5.233 Under Option 4, businesses and/or organisations which issue a large amount of SMS using Sender IDs (e.g., banks, delivery companies etc) would be required to register their Sender IDs and all other Sender IDs would be blocked. The purpose of this approach would be to ensure that only those businesses/organisations that are currently being impersonated or have a specific requirement for Sender IDs would be permitted to use them. This would reduce the range of Sender IDs that consumers receive, reducing confusion and potentially increasing engagement with businesses/organisations that have a strong requirement for using Sender IDs (i.e., banks and important public services).

5.234 The reduction in scams (and associated harm) would be substantial, noting that the majority of the Sender ID spoofing relates to a small number of businesses. Under Option 4, scam SMS using Sender ID spoofing would be significantly reduced because all the main Sender ID users (e.g., banks, postal delivery, etc.) would be included in the SMS Registry. This should reduce the effectiveness of scam SMS more broadly by removing key Sender IDs which can be used by fraudsters to impersonate businesses. Option 4 would be an enhancement compared to Option 1 and Option 2 because the largest users of Sender ID could continue using this method of communications and consumers would have a higher level of confidence that messages received with such Sender IDs would be valid. This would reduce the harm to consumers because a main avenue for impersonation would be closed off. Europe Economics estimate that Option 2 could reduce the present harm by as much as €317 million over a 7-year period[293].

5.235 However, Option 4 would restrict the business/organisations that would be able to use the registry. Some businesses/organisations that would prefer to be included in the registry would need to use alternative methods of communications which could be inferior to the current arrangements. The extent of this approach would depend on where the threshold for inclusion was drawn (not an insignificant task that could lead to other economic effects[294]) but ultimately some businesses/organisations would not be permitted to use Sender

[292] ComReg has not determined what fee, if any, would apply to Sender ID registration. By design, any such fee should be so low as to not prevent use, even to small companies that could realistically wish to make use of Sender IDs. This would be a matter for future consideration once ComReg has more information regarding the cost of a Sender ID registry and the demand for Sender IDs.
[293] See Table 9.9 of the Europe Economics Report.
[294] For example, ComReg's threshold could create unintended consequences of allowing some business in the registry but excluding competing businesses simply because the volume of texts used is smaller.

IDs.

5.236 Such businesses/organisations would likely include social clubs, local delivery services etc. While these businesses/organisations are not widely impersonated at the moment they may have a use for Sender IDs. Furthermore, placing a restriction on those businesses/organisations who currently use Sender IDs to only display their originating number instead would likely create some consumer confusion for those who are used to receiving SMS with Sender ID. Indeed, consumers may inadvertently become suspicious of genuine SMS received from those businesses/organisations that previously used Sender ID.

II. Other impacts

Trust in SMS

5.237 Option 4 would restore and protect trust in SMS in a similar way as described in Option 3 because consumers would have a higher level of confidence that such SMS are valid and sourced from genuine businesses and/or organisations. However, as previously noted some consumers may subsequently distrust valid SMS from smaller businesses/organisations who previously used Sender ID but would not be permitted to do so under this option.

Conclusion on impact on consumers

5.238 Based on the assessment above, ComReg is of the preliminary view that Option 3 (Full Registry) is likely to be preferred by consumers and businesses as it balances the benefits of preventing Sender ID spoofing with safeguarding the trust in and use of SMS, Sender ID and Irish MNs more generally. In particular, this option provides consumers a high degree of confidence that any SMS with Sender IDs are valid and that these Sender IDs are available to all businesses/organisations.

Figure 35: Reduction in harms under Option 1-4, relative to status quo

Option	Benefits to Irish society
Option 1 (No regulatory measures)	-
Option 2 (Sender ID Ban)	No precise figure – Reduction in harm from scam SMS offset by loss of Sender IDs
Option 3 (Full Sender ID Registry)	Over 7 year – €327 Million Annually - €53 Million
Option 4 (Partial Sender ID Registry)	Over 7 year – €317 Million

II. Impact on industry stakeholders

5.239 The relevant industry stakeholders among those outlined in Section 5.2.4, are the following:

1. Networks that terminate SMS traffic;
2. SMS aggregators; and
3. Other operators (resellers, including MVNOs).

5.240 ComReg does not gather information on SMS aggregators sending SMS traffic into Ireland, which likely includes firms with no presence in Ireland[295]. Based on discussions with different MNOs and businesses, ComReg estimates that there are approximately 30 such SMS aggregators.

5.241 This section provides information on the impacts on industry stakeholders (as outlined above) arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., Implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

5.242 For the purpose of this assessment, ComReg assumes that no costs have been incurred to date[296]. This approach appears most reasonable, as it considers the maximal impact of each option, as it presupposes all costs lie ahead of the operators. In this way, the assessment examines the impact of the Options on the "least prepared" or "greenfield" operator and is therefore conservative assuming no progress to date. MNOs have made some progress in implementing Sender ID filtering, and many of the relevant financial costs have already been incurred.

Option 1: Do Nothing

I. Direct impacts

5.243 Under Option 1, no regulatory interventions to combat scam SMS would be mandated on operators. Therefore, this option would not impose any direct financial costs on those operators.

II. Other Impacts

[295] Therefore not subject to ERAU registration.
[296] Under the status quo, operators may choose not to incur costs by electing not to undertake any technical measures to combat scams. Indeed, certain operators have informed ComReg that they would await a regulatory requirement before undertaking further work on technical specifications in this RIA.

5.244 The present level of scam SMS is reducing trust in Sender IDs and SMS and ultimately reducing the use of SMS for B2C.Therefore, absent intervention, scam SMS could negatively impact the revenues generated by operators from providing SMS services, and operating networks over which SMS services are generated. Under this option, the harms to operators would continue to occur and the scope for operators to benefit commercially from being able to offer networks of trust would be reduced because the present level of scam SMS are reducing trust in SMS.

5.245 Operator reputations would also continue to be damaged as scam SMS proliferate across society negatively impacting the revenues generated by operators from providing such services. Further, as consumers and businesses move away from SMS communications there is less scope for operators and aggregators to generate commercial opportunities. For example, Europe Economics notes that the survey shows that consumers have been moving away from traditional telecommunication by reducing their reliance on public phone networks and SMS aggregators for contacting customers (i.e., the feedback effect referred to earlier), a fact which should be concerning for operators and SMS aggregators.[297]

5.246 Therefore, operators are likely to prefer measures that reduce the rate of scam SMS and are unlikely to prefer Option 1.

Option 2: Ban Sender IDs

I. Financial impacts

5.247 Under Option 2, the three Irish MNOs (Eir, Three and Vodafone) would block all SMS messages containing a Sender ID. ComReg understands that all MNOs have this capability to some extent and could implement this measure at a relatively low cost.

II. Other Impacts

5.248 Despite its low cost and effectiveness in reducing the harms in the short run ComReg expects that no MNO or aggregator would likely prefer this Option over any of the alternatives, given the unavoidable negative impact this option would likely have on the use of SMS for B2C and resulting revenues (i.e., operators would be unable to provide this service to businesses/organisations) This would also negatively impact the business of SMS aggregators which originate and transit SMS for B2C on behalf of businesses (often with Sender IDs).

Option 3: Full Sender ID registry

[297] Europe Economics, page 53

I. Direct impacts

5.249 Under Option 3, MNOs would block all SMS with a Sender ID except those registered and sent from the registered owner via the correct participating aggregator. Interested organisations could apply to register Sender IDs via an online portal, open to all businesses/organisations meeting certain eligibility criteria. A list of protected sender IDs would be maintained by ComReg and shared with MNOs.

5.250 The costs of operating the registry would fall on ComReg, however it also imposes certain costs on the Irish MNOs and aggregators.

- For MNOs, the blocking component would entail some costs (including those SMS scams that could spoof Irish mobile numbers) to operators to implement, such as internal project activities i.e., design, implementation, testing. However, as noted above these are expected to be relatively modest.
- Aggregators would incur costs of setting up new connections to local MNO(s), if not in place already. They would also incur business costs of onboarding and authenticating new SenderID owners and implementing and validating the required sender ID filtering.

5.251 To inform ComReg's assessment, Europe Economics have estimated both the one-off costs (e.g., the cost of software purchase and installation) and on-going cost (e.g., on-going cost of software) of a partial Sender ID register for MNOs and aggregators. Europe Economics estimates one off costs of approximately €150,000 for each MNO with annual on-going costs of approximately €20,000[298], and one-off costs of €123,000 for each aggregator[299].

5.252 Therefore, Option 3 would impose a greater cost on Three, Vodafone, Eir and participating aggregators[300], as shown in Table 15 below.

II. Other Impacts

5.253 SMS aggregators may incur greater costs under Option 3 because they will no longer use least cost services which are difficult to secure and will instead connect a greater number of Sender IDs and Sender ID owners. However, it should be noted that there are commercial opportunities for participating aggregators in providing trustworthy services to businesses/organisations. In particular, under this option, any business/organisation in the State could register their Sender ID increasing the number of participating businesses/organisations compared to Option 1 where all Sender IDs would be

[298] Europe Economics Report, Table 9.3.
[299] Europe Economics Report, Table 9.4
[300] Any operator willing to undertake the necessary actions could become a patriating aggregator.

banned or Option 4 where only businesses/organisations above certain thresholds would be included. A more secure Sender ID regime would provide even greater value to SMS for B2C for large businesses, potentially generating greater revenues for MNOs and participating aggregators (either through increased demand at existing prices or through higher prices.).

5.254 Furthermore, any increased costs may be offset by increased revenues under Option 4, as a result of greater demand for SMS for B2C, potentially generating greater revenues for operators (i.e., increased demand at existing prices or through higher prices). This should be expected given the greater number of potential organisations using Sender ID and generating SMS traffic and improved trust in Sender IDs more generally.

Option 4: Partial Sender ID registry

I. Direct impacts

5.255 The direct impacts under Option 4 are the same as under Option 3 because both involve the implementation of the registry, and the same costs of implementation would be incurred by MNOs. This would impose slightly lower one-off costs of approximately €107,000 per SMS aggregator.

II. Other Impacts

5.256 Option 4 would reduce the harms from Sender ID spoofing and restore and protect trust in Sender IDs. This should help protect the long-term commercial interests of MNOs and SMS aggregators. However, because Option 4 would exclude many businesses from using Sender IDs for B2C, operators and aggregators are unlikely to prefer this option. This could reduce the number of businesses using Sender IDs which would limit the demand for these services.

5.257 Non-participating aggregators could be negatively impacted by a partial SMS registry through a reduction in transiting of SMS with Sender IDs. This is an unavoidable consequence of a Sender ID registry, which rely upon the actions of known and compliant aggregators. However, an aggregator can easily address this by undertaking the necessary actions to become a compliant participating aggregator. ComReg expects that most, if not all, SMS aggregators that send significant volumes of SMS traffic to Ireland at present would participate.

Table 15: One-off costs per stakeholder for each Option, relative to status quo

Option	MNOs	SMS Aggregators

Option 1 (Do nothing)	-	-
Option 2 (Ban Sender IDs)	Some loss of revenue	Some loss of revenue
Option 3 (Full Sender ID Registry)	€150,000	€123,000
Option 4 (Partial Sender ID Registry)	€150,000	€107,000

Conclusion on impact on industry stakeholders

5.258 Based on the assessment above, ComReg is of the preliminary view that Option 3 is likely to be preferred by most stakeholders because it balances the benefits of preventing Sender ID spoofing with the costs of implementation. More generally, the wider business community would prefer Option 3 because any businesses/organisations could continue to use Sender IDs. Those Sender ID owners excluded under Option 4, would therefore likely prefer Option 3 because SMEs are less likely to feature on a partial registry.[301]

III. Impact on competition

5.259 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the statutory objectives outlined in 55.12.2.25.16, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on the efficient investment arising from the regulatory option is assessed.

Option 1: Do Nothing

Efficient use of numbers

5.260 Against the objective of ensuring the efficient and effective use of numbers for the benefit of consumers, it is evident that under Option 1 the numbering resource is not being used efficiently or effectively and this is resulting in observable, significant consumer harm (as described in Chapter 3). In

[301] The threshold for inclusion on any potential partial Sender ID registry is currently unknown at this time and therefore only a small number of companies could be sure to access a Sender ID registry under Option 3 (e.g., banks)

summary, a situation where 38 million nuisance SMS and 14 million distressing SMS are made to consumers every year, with approximately 500 consumers a day being defrauded by scam SMS, is clearly not consistent with the efficient and effective use of the numbering platform and constitutes a serious misuse of numbers.

5.261 As noted above, numerous scam SMS exploit the lack of protection afforded to Sender IDs at present, with fraudsters using Sender ID spoofing to spoof businesses/organisations, including important public services. In this way, Sender IDs are being used to perpetuate fraud and undermine ECS networks more generally. Option 1 is therefore not consistent with the efficient use of Sender IDs (a form of numbers), and this constitutes misuse of an important national resource. As outlined above, should scam SMS using Sender ID continue, consumers may adapt by not reading SMS messages potentially undermining the legitimate use of Irish numbers.

5.262 Finally, given that such misuse has been allowed to proliferate over the last number of years, it is clear that operators do not have processes in place to reduce access to valid numbers by those who intend to misuse them. The misuse of the numbering resource is likely to continue and multiply under Option 1 as fraudsters become more sophisticated. Operators do not have processes in place to reduce access to numbers by those who intend to misuse them. In particular, the lack of any assignment processes used by operators has led to bad actors getting access to numbers that are ultimately used to perpetrate fraud. See Chapter 6 for more information on ‘Know Your Customer’ initiatives that operators could be enforcing in order to reduce the misuse of numbers.

Promoting competition

5.263 Competition has not delivered a satisfactory level of scam text protection to date. ComReg considers that there are a number of reasons for this which are similar to those previously set out in respect of voice services. These are outlined in paragraphs 5.123-5.126 above but in summary are as follows.

- The incentives to provide SMS protections are not sufficiently high because the majority of the harms due to scam SMS are not borne by operators themselves and are instead being borne by consumers and businesses that they serve. Absent this competitive pressure operators face little incentive to invest in scam protection in the short run.
- Operators are likely concerned that such investments even if they were made would prove inefficient if other operators did not replicate similar interventions. For example, operators may rationally underinvest in interventions whose effectiveness relies upon the coordinated implementation by many other parties. As outlined in Chapter 4, this is true

of a number of the interventions being considered in the Consultation, including the Sender ID registry – which relies upon implementation and coordination between operators and a large number of SMS aggregators.

- There is little evidence of key businesses attempting to procure better protected SMS services for B2C. This view is corroborated by the lack of action, and in certain cases the apparent disinterest, of key businesses in attempting to procure better protected services (e.g., ComReg is unaware of any business or bank switching SMS messaging provider to improve the protection to date[302]).
- Operators may be unconvinced that competing for customers on the basis of protection against nuisance communications would cause sufficient switching to justify relevant investments. This creates a feedback effect where consumers who may be willing to switch due to impact of scam SMS cannot do so because protected services are not being provided.

5.264 Given the prevalence of scam SMS, it would appear that competition has not provided sufficient incentives to protect consumers, leading to a market failure and socially suboptimal levels of investment in measures to tackle scam SMS. If networks are not timely in offering sufficient protections, despite the significant harm caused by these communications, it would prima facie suggest a possible competitive failure. Clearly identifiable harms (as evidenced in Chapter 3) for important services (e.g., voice and SMS) should be addressed in a well-functioning competitive market over an appropriate period. However, that is clearly not the case with respect to scam SMS in Ireland. ComReg notes that industry-wide interventions may ultimately be required in order properly address nuisance communications.

5.265 Therefore, ComReg remains of the view there is a serious risk of continued under investment absent intervention. This is highly undesirable as, absent intervention, the present level of scam SMS and fraud may distort competition between providers of the following.

I. SMS services because declining use of SMS due to 'the SMS reduction effect' would lead to a reduced incentive to compete between providers of SMS services. It is unlikely that the current uncoordinated approach would lead to a similar level of protection across all operators and choice between operators could become distorted by perceived, and not actual level of protections afforded. The impact of any such distortions could be uneven as operators have different businesses, services and subscriber bases.

[302] ComReg has discussed this with key businesses and found little to no willingness or intention to switch SMS provider to reduce SMS scams and fraud.

II. SMS services and OTT/Instant Messaging platforms (e.g., WhatsApp) because consumers and businesses may no longer see SMS as a viable option which would reduce infrastructure-based competition. Consumers and businesses may move to alternative messaging platforms, despite preferring SMS at present[303] (e.g., OTT for P2P[304], or apps, email or push notification for B2C[305]). Such transitions to alternative messaging platforms may become permanent if consumers lose trust in SMS entirely as would likely be the case absent interventions. Finally, the declining use of SMS may lead to reduced investment and further reduce competition between providers of providing SMS services and alternative instant messaging platforms[306].

Efficient Investment

5.266 Under Option 1 there is a risk that the investments already made voluntarily by some operators would become inefficient. For example, investments by some operators who have already implemented or begun implementing Sender ID filters (or would do so in the future under this Option) could become inefficient if other operators do not make concurrent investments. As previously noted, any uncovered operator potentially undermines an operator's investment as fraudsters would likely exploit that 'gap' to reach all consumers including those that made an investment.

5.267 Further, under Option 1, operators would face lower incentives to invest in networks that provide voice communications to either improve or maintain the level of services. Investments made by operators prior to the mass onset of nuisance communications (i.e., 2018/2019) may now become inefficient because such investments were made on the basis of an effectively functioning numbering platform. This may also reduce the incentive for future investments if operators are of the view that such investments would be compromised by the actions of bad actors such as fraudsters.

Option 2: Ban Sender IDs

[303] Inferior in the sense that at present consumers and businesses choose SMS for certain services, revealing a current preference for SMS as a means of communications for those services.
[304] Which is potentially subject to more QoS issues due to latency and potentially less trusted due to a lack of numbers.
[305] Which are reliant on a consumer either downloading their app or checking their emails. Neither channel has the benefit of a Irish number, noting again that 59% of Irish consumers indicate that they would answer calls from unrecognised numbers if using a Irish GN.
[306] For example, there would be reduced incentives for operators to compete in providing numbering services to businesses (e.g., provision of freephone NGNs) if those businesses have a reduced need for services provided over the numbering platform.

Efficient use of numbers

5.268 Option 2 would prevent Sender ID spoofing, leading to reduced misuse of Sender IDs (which as previously discussed is a form of number). This would also reduce the misuse of mobile numbers by reducing the volume and effectiveness of scam SMS impersonating businesses/organisations because it would prevent scam SMS using Sender ID spoofing (which are popular with fraudsters at present). However, it is likely that fraudsters will continue to use scam SMS without Sender ID Spoofing. Indeed, it is likely that scam SMS that do not use Sender ID (because it would now be unavailable) are likely to increase in order to replace those scam SMS that previously would have been made using a Sender ID. Fraudsters would continue to impersonate businesses through copying text their language format (as done at present). Therefore, while there would be some short-term efficiency benefits to Option 2, they are likely to reduce over time.

5.269 Further, while fraudsters use Sender ID to impersonate businesses, the vast majority of text messages using Sender ID are valid and represent an efficient use of the numbering platform[307]. Option 2 would block the use of all these numbers in the same breath as blocking those which may be used for scam SMS. In effect, this option could result in a large number of what would have been efficiently made SMS being restricted in order to combat a comparatively smaller number of scam SMS. The extent to which this would impact the current efficient use of numbers would depend on how businesses/organisations react to potential implementation of Option 2. It could be the case that what previously constituted an efficient use of numbers would move to an alternative (and potentially inferior) platform because of the imposition of this Option. This would be particularly likely to occur absent any measures to protect other SMS communications (i.e., those that don't use a Sender ID).

5.270 Therefore, while this Option would clearly reduce the misuse of numbers compared to Option 1 the overall impacts on the efficient use of numbers are unclear and would depend on how businesses/organisations react to the blocking of Sender IDs.

Promoting competition

5.271 Currently, despite the prevalence of scam SMS, providers of SMS services compete to provide B2C services to businesses/organisations. Even if this competition is currently limited due to scam SMS (reducing the utility and use of SMS) there is at least some competition for these services. By contrast:

[307] Sender ID Ban would reduce the legitimate use of Sender IDs to contact Irish consumers. As noted in Sections 3.1-3.2, this is valued as an efficient and effective way businesses/organisations (including public services) to communication with citizens.

I. Under Option 2, competition between providers of SMS services would likely be distorted further because Sender IDs which are required by businesses/organisations, could not be offered because of the restriction created by Option 2. Further, it is not clear whether businesses/organisations would use SMS (without Sender ID) for B2C communications under Option 2 because consumers would face even greater difficulty in identifying legitimate SMS from businesses without a Sender ID.

II. Under Option 2 competition between SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would also be distorted because Option 2 removes a key product characteristic of SMS (i.e., the ability to use Sender IDs) and businesses/organisations may be forced to use alternative channels to reach consumers due to the reduced utility of SMS for B2C communications.

5.272 Therefore, competition would likely be reduced under Option 2.

Efficient Investment

5.273 As noted previously, Option 2 would likely reduce the utility of SMS services to businesses/organisations. Accordingly, service providers and businesses /organisations may need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient because it would be by driven by being unable to use Sender ID rather than the underlying effectiveness of Sender ID as a method to communicate with consumers. Investment in alternative platforms would entail an unnecessary and avoidable duplication of investment particularly for those businesses/organisations that are already using Sender ID, having invested in the provision of same.

5.274 Therefore, Option 2 is likely to lead to inefficient investment by service providers and businesses/organisations.

Option 3: Full Sender ID registry

Efficient use of numbers

5.275 As noted in Chapter 4, international experience indicates that full Sender ID registries are highly effective at reducing scam SMS that use Sender ID, and the evidence in Ireland indicates that many of the most common and effective scams utilise Sender ID spoofing. Under Option 3, scam SMS using Sender ID spoofing (and the underlying numbers) would be significantly reduced. In this way any of the SMS with Sender IDs that are used through the registry would be genuine and would constitute an efficient use of numbers because those SMS do not have the intention to commit fraud and may be of interest to receiving customers. This reduces the potential for numbers to be misused in a

way that harms consumers, increasing the overall efficiency of the numbering platform. Furthermore, by reducing the current prevalence of Sender ID Spoofing, Option 3 should enable even greater use of Sender IDs (compared to all other options) because consumers are more likely to trust, open and read SMS containing Sender IDs. This increases the overall utility of the numbering platform as businesses/organisations become satisfied that consumers are engaging more with the communications that they make via SMS.

5.276 Under Option 3, the reduction in misuse should be large because the majority of the scams and fraud appear to relate to a small number of Sender IDs (i.e., those Sender IDs that would be included in the Sender ID Registry). Therefore, Option 3 would likely be effective at preventing the misuse of Sender IDs, particularly in the short term prior to fraudsters adapting to the implementation of the registry. Importantly, and unlike Option 2, it would allow businesses/organisations (above certain volume thresholds) and who are currently using numbers efficiently to register their Sender ID and continue communicate with their customers using this preferred approach. This would allow these numbers to continue to be used efficiently. Further, by reducing the current prevalence of Sender ID spoofing, businesses/organisations should have increased confidence in using Sender ID to communicate with customers enabling even greater use of Sender IDs than at present further increasing the efficient use of the underlying numbers.

5.277 Therefore, Option 3 would likely result in the more efficient use of numbers.

Promoting competition

5.278 Option 3 represents a reduction in the competitive distortions resulting from scam SMS and Sender ID spoofing5.271, as a result of its greater impact on scam SMS, Sender ID spoofing and trust in and use of Irish numbers relative to Option 1 or Option 2. Therefore, Option 3 represents a reduction of competitive distortions in in general sense. In that respect, Option 3 would better incentivise the competition between aggregators and providers of ECS.

5.279 There are a number of reasons why competition has not delivered a satisfactory level of scam text protection to date, these are summarised in under Option 1 above. With that in mind, Option 3 would assist in resolving the coordination problem that operators face in ensuring that only SMS with valid Sender ID are received by consumers. Currently operators have no way of discerning which messages bearing Sender IDs are valid and which are genuine, and this information asymmetry provides opportunities for fraudsters to commit fraud. The Sender ID Registry allows businesses/organisations to select which Sender IDs are valid and this information is provided to operators who block Sender ID’s not on the registry. Therefore, Option 3 provides all operators with important information about which Sender IDs are genuine. This would not be possible

absent a registry because operators currently only have a limited insight into which Sender IDs are genuine (i.e. based on the services it already provides to businesses/organisations). Furthermore, under Option 3:

I. between providers of SMS services would likely increase because Sender IDs which are required by businesses/organisations would continue to be provided to those that require them. Further, providers would be able to offer SMS with Sender ID services that provide significant protection against Sender ID spoofing. Businesses/organisations should therefore have increased confidence in using Sender ID to communicate with customers enabling even greater use of Sender IDs – This is likely to attract new businesses/organisations which providers would compete for.

II. between SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would also be increased because Option 3 provides protection against spoofed Sender ID meaning the choice made by businesses/organisations would be based on the underlying effectiveness of the SMS platform rather than because of scam SMS. Option 3 preserves competition between providers of SMS services and other alternative messaging services, through protecting the use of SMS more generally.

5.280 Therefore, Option 3 would better promote competition compared to Option 1 and Option 2.

Efficient Investment

5.281 Option 3 would accord with and further the regulatory principle of promoting efficient investment and innovation in new and enhanced infrastructure by allowing operators to avoid what would otherwise be inefficient infrastructure investment. In particular, by preserving the use of and demand for SMS communication, Option 3 benefits operators that may otherwise need to invest in alternative communications channels in order to contact consumers. Such investment would be inefficient being driven not by unmet need but by a degradation of existing SMS network's ability to continue to meet the existing need for such services. Furthermore, SMS aggregators' investments in their business model may be unnecessarily supplanted by third parties offering B2C communications via OTT or via App.

Option 4: Partial Sender ID registry

Efficient use of numbers

5.282 Option 4 is similar to Option 3 in that it would block all spoofed Sender IDs. However, not all businesses/organisations would be able to benefit from the

protection provided by the registry. In particular, small businesses/organisations would need to use alternative platforms in order to communicate with consumers. This would lead to the same inefficiencies as identified under Option 2 save that it would apply to smaller number of potential users. The extent of these inefficiencies would depend on the criteria for inclusion in the registry, but it would, by definition include only a subset of businesses/organisations. This reduces the efficiency of the numbering platform because the volume of SMS used by those businesses/organisations would be reduced arising from a restriction on legitimate use of Sender IDs. Further, Option 3 would potentially restrict the use of what would have been genuine communications (and their underlying numbers) for the sake of a potentially smaller amount of scam SMS.

5.283 Therefore, while Option 4 would prevent the misuse of number in the same way as Option 2, it would not lead to the more efficient use of numbers compared to Option 3 because the numbers used by certain businesses/organisations would be restricted from using the Sender ID Registry.

Promoting competition

5.284 Similar to Option 3, Option 4 would also assist in resolving the coordination problem that operators face in ensuring that only SMS with valid Sender ID are received by consumers. This Option allows businesses/organisations to select which Sender IDs are valid and this information is provided to operators who block Sender ID's not on the registry. Importantly, however, Option 4 restricts the protection offered by the registry to certain businesses/organisations. These businesses/organisations would be even less likely to use SMS services for B2C because the restriction would prevent operators from competing to provide Sender ID services to businesses/organisations who would normally avail of such services. Furthermore, businesses/organisations that are currently availing of Sender ID services may be below any threshold for inclusion noting that Sender ID services are currently being availed of by businesses/organisations with relatively low SMS volumes (e.g., GAA clubs and local businesses). Operators that are currently providing these services may be unable to facilitate such businesses/organisations in the future and there would be no alternative providers that could provide SMS using Sender ID.

5.285 Further under Option 4, competition between:

I. providers of SMS services would likely remain relatively static. While Sender IDs which are required by the largest businesses/organisations would continue to be provided to those that require them, there would be restrictions because only a subset of businesses/organisations would be eligible for inclusion in the registry. In particular, the scope for competition would be limited by the extent of the restriction on the

registry.

II. SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would be limited by the extent of the restriction on the registry. Option 3 provides protection against spoofed Sender ID for larger businesses/organisations thereby increasing competition between providers of SMS services and other alternative messaging services. However, the restriction would mean that some businesses/organisations would use alternative platforms not because SMS is ineffective but because SMS using Sender ID would be unavailable.

5.286 Therefore, while Option 4 is better for competition than Option 1 or Option 2, it is less likely to promote competition compared to Option 3.

Efficient Investment

5.287 Under Option 4, operators would be required to implement each of the processes and associated costs required for the implementation of Sender ID Registry. However, because of the restriction imposed by this option it would be unable to reap the full benefit of those costs and would therefore be an inefficient investment.

Conclusion on impact on competition

5.288 Based on the assessment above, ComReg is of the preliminary view that Option 3 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

5.289 The above assessment and the Europe Economics Report demonstrate that there is currently a significant consumer and societal harm present due to scam SMS and much of this harm arises from spoofed Sender ID. Blocking all SMS that use Sender ID under Option 2 would clearly stop fraudsters spoofing and remove the harm created by spoofed Sender IDs. However, this would prevent genuine use of Sender ID and reduce the viability of the SMS platform, reducing competition between providers and across platforms. A partial registry under Option 4 would provide protection to those businesses/organisations that are most impersonated by fraudsters. However, its restriction to a subset of businesses/organisations means that the benefits of a viable SMS platform would be denied to those that require it, again reducing competition and creating inefficient investments. Option 3 however extends the benefit to all businesses/organisations who wish to use Sender IDs and because of this the protection it would provide would encourage other businesses/organisations that may have concerns to engage with the SMS platform. This would promote

greater competition between providers and across platforms. Therefore, ComReg is of the preliminary view that, on balance, Option 2 and is the preferred option in terms of its impact on stakeholders, competition and consumers.

5.290 ComReg notes that this draft RIA relates to scam SMS using Sender ID only, and other Scam SMS (e.g., those that do not use Sender ID) are discussed separately in the draft RIA that follows.

5.6 Draft SMS Scam Filter RIA

5.6.1 Policy Issues

5.291 In Section 5.2.1, ComReg noted that the two overarching policy issues relevant to all draft RIAs are

i. being to reduce the harm to consumers and businesses from scam calls; and

ii. to protect and renew trust in ECS Networks and Services.

5.292 ComReg is mindful of these policy issues in determining its preferred option. The remainder of this subsection further defines these main policy issues in order to appropriately assess the available regulatory options. With that in mind, ComReg notes that this draft RIA builds on the previous draft Sender ID RIA where the main policy issue was to reduce harm by identifying and blocking SMS making illegitimate use of Sender IDs. While the preferred option appropriately addresses that policy issue, it does not address all scam SMS and it may become less effective over time depending on how fraudsters react to its implementation.

5.293 In that regard, there are three areas that are not addressed by the preferred option in the draft Sender ID RIA.

- **First**, fraudsters often do not use Sender ID spoofing and may impersonate a business within the body of text or impersonate an ordinary person. The latter scenario has become increasingly common in recent months, with an increasing number of scams targeting family members. Such scams travel intermingled with potentially legitimate traffic, that cannot simply be blocked on the basis of the Sender ID route alone. Blocking such traffic requires an assessment of characteristics of the traffic itself, and not merely whether the route matches the messages' originating address. Fraudsters both at home and overseas may perpetuate such scams, with foreign fraudsters using Irish SIMs taken aboard or sending such messages via A2P 'grey routes'.
- **Second**, future scams may become more sophisticated as the Sender ID blocking takes effect. Any SMS a consumer might receive from whatever location could potentially be a scam and emerging evidence indicates that fraudsters abroad are using advanced artificial intelligence (AI) based software to create more realistic and believable text and instant messaging of people or even family

members in distress[308]. AI based scams could combine the relative strengths of human and automated scams; being able to both generate convincing text in real time and perpetuate such scam SMS at a massive scale[309].

5.294 Such scam SMS could be harmful where combined with Sender ID Spoofing or in the absence of spoofing (e.g., impersonating a family member in distress). A large share of Irish consumers could be targets for malware or impersonation by text-scripting software, given the ubiquity of information publicly available on social media (e.g., photos, names, names of friends, location, occupation) or from leaks (e.g., matching mobile phones numbers to names and social media accounts). Next-generation AI based scam SMS should be expected to reach Ireland and increase with time as the underlying technology becomes more widely available (e.g., software like ChatGPT for text[310]).

5.295 With that in mind, the main policy issue associated with this draft SMS Scam Filter RIA is to reduce the harm from scam SMS on consumers and increase trust in ECN by identifying and/or blocking as many scam SMS as possible, however and wherever they originate.

5.6.2 Regulatory Options (Steps 1 & 2)

5.296 As outlined in Section 5.2.2, the available interventions for the purpose of this draft RIA are:

- **Option 1 –** No SMS Scam Filter
  - No additional interventions to the Preferred Option outlined in 'Sender ID RIA", which is to implement the full Sender ID Registry with a phase-in as stated in the technical specification.
- **Option 2 –** Implement a SMS Scam Filter (in addition to the preferred option from the 'Sender ID RIA')
  - This approach would implement the SMS Scam Filter as well as the Sender ID registry, as stated in the technical specifications.

5.297 At the outset, ComReg notes that Option 2 introduces potential legal issues on the protections of end user rights in relation to interception and data protection as provided in the ePrivacy directive and the GDPR. It is ComReg's understanding that a change to current legislation to allow for such scanning is

[308] See for example The Strait Times online 12th March 2023 "*Broken English no longer a sign of scams as crooks tap AI bots like ChatGPT: Experts*" and 14th March 2023 ABC7 news online "*Thieves can use ChatGPT to write convincing scam messages with human-like language, experts warn*".
[309] For example, automated texts can reach many consumers but rely on pre-written messages, whereas scam texters are more convincing but can only hold a small number of conversations at once.
[310] https://openai.com/blog/chatgpt

necessary. ComReg has been in constructive and detailed meetings with the Department of the Environment, Climate and Communications in relation to these issues and the matter is currently under consideration.

5.298 With that in mind, this draft RIA has been written on the basis that such legislation would provide for the implementation of Option 2 where it is consistent with ComReg's statutory remit. To the extent that such legislation is not forthcoming, ComReg notes that other alternatives might be available for assessment at that time, including the implementation of the SMS Scam Filter on an 'Opt-in' basis[311].

5.299 The draft 'Scam Filter' RIA has been written on the basis that all consumers that use SMS would benefit from the SMS Scam Filter (i.e., All In). However, the form and manner of any forthcoming legislation may provide for "Opt-Out" or other related measures which could potentially reduce the numbers of consumers benefiting from the protection provided by the SMS Scam Filter. ComReg proposes to implement the SMS Scam Filter in line any forthcoming legislation and will consider any such measures in any subsequent RIAs it may provide.

5.300 Regardless of its exact form and manner, such legislation would likely enable the SMS Scam Filter to be significantly more effective at reducing scams compared to Option 1 (because most consumers would likely choose to be protected) and therefore may still be proportionate and appropriate to implement given the harms experienced by these consumers. Even, if legislation is not forthcoming, a SMS Scam Filter could be introduced as an "Opt-in" process, although such an approach would likely be sub-optimal, it may still represent an improvement on the current situation. ComReg will consider an Opt-in option further and relative to Option 1 should the need arise noting that even if such an option was proportionate and objectively justified in terms of its ability to reduce scam SMS, they would clearly be less effective (from a scam protection point of view) relative to a full SMS Scam Filter which is the subject of this draft RIA.

5.6.3 Impact on industry stakeholders, competition and consumers (Steps 3 & 4)

I. Impact on consumers

5.301 This section provides information on the impacts on consumers (as outlined above) arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

[311] An 'Opt-in' basis would involve consumers permitting operators to filter their text messages for scam texts.

I. First, the direct benefits to consumers arising from the regulatory option is assessed (i.e., reduction in time lost to scam calls and monies to fraud); and

II. Second, other relevant impacts arising from the implementation of the regulatory is assessed (i.e., trust in numbers, use of Voice calls).

Option 1 V Option 2

I. Direct impacts

Option 1: Preferred option from the 'Sender ID RIA'

5.302 As noted in the draft 'Sender ID' RIA implementing a Sender ID registry would significantly reduce the number of scam SMS and fraud because fraudsters frequently use spoofed Sender ID to impersonate businesses/organisations. Europe Economics estimate that the Sender ID Registry could reduce the harm to consumers and businesses by €53 million a year over a seven-year period, resulting in combined consumer benefits of €372 million over that same period[312.]

5.303 However, this intervention would not prevent all scam SMS, in particular those scam SMS that are not using Sender ID spoofing, including scams which impersonate Irish businesses or government agencies. As noted by Europe Economics "*scammers may be able to evade an intervention preventing scams at the aggregator node (e.g., sender ID screening) by sending SMS directly to a short message service centre (SMSC) and then onto operators, thus bypassing the aggregators. In this instance, operators would not be able to block these messages and thus an advanced SMS Scam Filter would be needed to reduce the scam risk*"[313] Under Option 1, fraudsters would likely continue using scam SMS without spoofing Sender ID.

5.304 Operators have reported to ComReg that national and international fraudsters have already begun attempting to secure Irish SIMs abroad to conduct scam calls or SMS in the State. An Garda Siochana have also reported intercepting a number of scam text operations based in the State, not all of which appeared to use Sender ID spoofing. Further An Garda Siochana have advised that the majority of scam SMS no longer involve Sender ID spoofing which is indicative of how fraudsters rarely concentrate on one type of scam at a time.

5.305 ComReg is aware of several existing types of scam SMS already present in Ireland that would bypass the SMS ID Registry. For example, a variety of scam SMS that have been conducted without Sender IDs such as SMS scams:

[312] See Table 9.9 and Table 9.11 of the Europe Economics Report.
[313] Europe Economics Report, page 77.

- impersonating business or government agencies (e.g., HSE/ An Post etc[314]);
- opportunistically impersonating new organisations or extending scams successfully used in other countries (e.g., eFlow[315]);
- targeting users of OTT platforms (e.g., Revolut[316], WhatsApp) with scam SMS that appears to be from the payments app.

5.306 Importantly, each of these scam text campaigns were used with and without spoofed Sender ID (e.g., some of the eFlow scam SMS show 'eFlow' as the sender ID while others displayed a mobile number). This highlights why a Sender ID registry on its own is insufficient to deal with scam SMS. Under Option 1, the spoofed Sender IDs would have been blocked (where eFlow registered their Sender ID) but the other eFlow scam SMS using mobile numbers would continue to occur. There would be little difficulty for fraudsters to transition all scams without Sender ID on a widespread basis.

5.307 Therefore, a significant amount of scam SMS and associated harm is likely to remain following the implementation of the static interventions (i.e., SMS ID Registry). However, the present volume and prevalence of such scam SMS is likely to increase in the future as domestic and international fraudsters adapt their operations to circumvent the interventions applied as part of the draft Sender ID RIA. ComReg expects the incidence of these and similar scams to increase following the implementation of any Sender ID registry as fraudster seek to contact and con Irish consumers. Therefore, while effective and beneficial, the impact of the Sender ID Registry should be expected to degrade over time.

5.308 In relation to more sophisticated scams in the future, ComReg notes that drafting text for phishing SMS can be difficult for fraudsters that are based abroad and whose first language is not English because they typically have a poor grasp of written English. Indeed, one of the main red flags that consumers have been advised to watch out for is poor grammar and spelling. Machine Learning algorithms such as ChatGPT can make life significantly easier for potential fraudsters by drafting messages in good conversational or business English (depending on the target). Fraudsters are improving the quality of their messages with AI, which rarely makes editorial mistakes. ChatGPT also understands tone commands, so phishers can up the urgency of their

[314] Scam text messages impersonating the HSE advising of a close contact and/or vaccine appointments also used both spoofed Sender ID with and without Sender ID.
[315] The scam SMS which appear as being sent from eFlow, ask customers to pay outstanding charges for a toll or to update their account details. However, the links sent in the messages are not legitimate and are an attempt to get the personal card and online banking details of the person.
[316] The SMS asks customers to verify their details with the threat of having their accounts frozen. The SMS contains a link that brings users to what appears to be a legitimate Revolut page. The fraudster then uses this as a way to trick customers into putting in their Revolut PIN.

messages that demand immediate payment or responses with passwords or PII.

5.309 For example, Europol has recently observed[317] that the ability of ChatGPT to draft highly realistic text makes it a useful tool for phishing purposes. This capability can be abused at scale to mislead potential victims into placing their trust in the hands of criminal actors. ChatGPT currently excels at producing authentic sounding text at speed and scale. This makes the model ideal for propaganda and disinformation purposes, as it allows users to generate and spread messages reflecting a specific narrative with relatively little effort.

5.310 Therefore, notwithstanding the current harm to consumers as identified above, these harms are likely to increase as the impact of having a Sender ID registry wears off and scam SMS without Sender IDs become significantly more sophisticated.

5.311 Given the above, consumers are highly unlikely to prefer Option 1.

Option 2: SMS Scam Filter in addition to the Preferred option from the 'Sender ID RIA'

5.312 The static interventions only target scam calls arriving from a specific route (i.e., the SMS ID Registry prevents a consumer from receiving SMS with a Sender ID that is not on the registry). However, the SMS Scam Filter is a dynamic intervention that is designed to intercept scam SMS regardless of whether they have Sender ID or not. It achieves this in two main ways.

5.313 **First**, a SMS Scam Filter applies to all originating or terminating traffic and Option 2 can therefore combat certain scam SMS that are not addressed under Option 1. This includes scam SMS that:

- originate via legitimate traffic using legitimate Irish numbers, in Ireland or abroad (e.g., using Irish MNs or SIM cards);
- exploit new vulnerabilities in network or consumer behaviour (e.g., spoofing numbers trusted by Irish consumers (+44 for the U.K)); and
- other, as of yet unknown or unidentified vulnerabilities in network that fraudsters find.

5.314 Although a SMS Scam Filter does not stop all scam SMS it has fewer obvious and avoidable gaps that fraudsters can target. In this way a SMS Scam Filter acts as a last line of defence against scam message delivery, being able to intercept scam calls that other interventions miss.

[317] The criminal use of ChatGPT – a cautionary tale about large language models | Europol (europa.eu)

5.315 **Second**, a SMS Scam Filter is dynamic and can be updated in real time to target new suspicious predictors of emerging scams, meaning that SMS Scam Filters can be updated to account for fraudsters' ever adapting strategies to avoid detection (e.g., adapting calling data and metadata to appear less suspicious). Following implementation of the Sender ID Registry, fraudsters can be expected to evolve their techniques in reaching and gaining the trust of Irish telephone users. Therefore, Option 2 represents a more dynamic means of combatting scams and fraudsters. This is even more important given the evidence of emerging next-generation AI based scam SMS, which can enable more realistic automated instant messaging at scale.

5.316 Under Option 2, the combination of a SMS Scam Filter and the Sender ID Registry would provide the greatest protection to Irish consumers. A SMS Scam Filter is conceptually different to the aforementioned interventions, in that it assesses the traffic itself (its data and metadata) and not its pathway alone. A SMS Scam Filter assesses each text and blocks or provides a warning about those deemed suspicious. While a certain level of scam SMS would persist, a SMS Scam Filter should reduce the effectiveness and thereby profitability of scam SMS campaigns undertaken by the fraudsters (i.e., 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).

5.317 Under Option 2 the MNOs would block scam SMS making clearly illegitimate use of Sender IDs while also blocking suspicious SMS originating in potentially legitimate traffic, using the Scam filtering. There would be some overlap between the scam SMS caught by a Sender ID registry and a SMS Scam Filter, however each also clearly addresses several distinct harms. In particular, the SMS Scam Filter would proactively identify and detect scam and malware campaigns as they occur increasing its effectiveness and providing real time protection to consumers (rather than a response being delayed over a period of days or weeks).

5.318 As noted by Europe Economics "*The SMS Scam Filter would be a dynamic solution and could quickly react to new scams based on analysis of all messages being sent as well as evolve to identify new and emerging SMS scam message types. This would be particularly valuable if scammers find ways of working around the sender ID registry intervention*." [318] As previously identified under Option 1, scam SMS that do not have Sender ID would continue to arrive on end user devices. Indeed, the implementation of a Sender ID Registry in isolation would encourage the fraudsters to simply send all scam SMS without a Sender ID.

[318] Europe Economics Report, p80.

5.319 Europe Economics notes that there is strong evidence demonstrating the effectiveness of the SMS Scam Filter from international case studies. A SMS Scam Filter can therefore be expected to reduce the number of scam calls reaching Irish consumers and resulting fraud and harm relative to the status quo. Based on its evidence, Europe Economics estimate that Option 2 could reduce the annual value of harm to consumers by €82 million, which could result in consumer benefits of €564 million over a seven-year period[319]. Therefore, Option 2 represents a greater reduction in harm from scam calls than Option 1 as shown by Table 16 below.

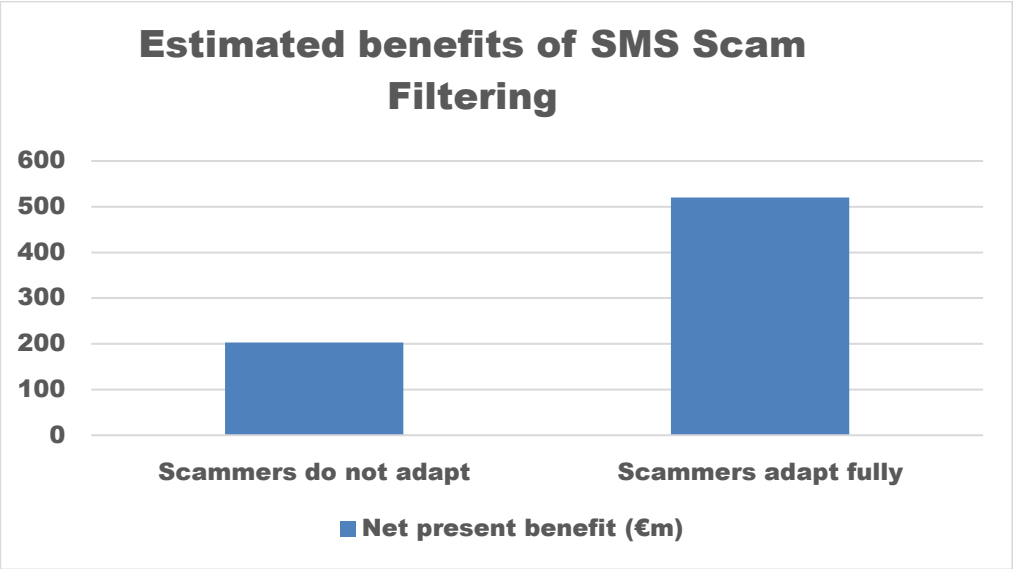
Table 16: Reduction in harms under Option 1 and Option 2

Option	Benefits to Irish society
Option 1 **(Sender ID Registry only)**	Over 7 year – €372 Million Annually - €53 Million
Option 2 **(Sender ID Registry & SMS Scam Filter)**	Over 7 year – €520 Million Annually - €82 Million

5.320 ComReg also notes that Option 2 represents a more "future-proofed" intervention. Indeed, the importance of the SMS Scam Filtering grows as fraudsters adapt to the Sender ID registry by either sidestepping (e.g., scam calls without Sender ID spoofing, impersonating P2P communications) or overcoming them (e.g., combinations of scam calls and SMS to convince the consumer of the authenticity of the sender). Europe Economics estimate that were fraudsters to perfectly adapt to the static interventions, the benefit of the SMS Firewall could be as much as 5 times greater at c. €520 Million euros over 7 years. The exact benefits of the SMS Scam Filter depend on the reaction of fraudsters to the static interventions – however it is highly likely to be closer to €520 million given how sophisticated scam SMS are expected to become in the future.

[319] See Table 9.10 and Table 9.11 of the Europe Economics Report.

Figure 36: Impact of SMS Scam Filtering, for different levels of fraudster adaptation



Trust in SMS

Option 1 v Option 2

5.321 As discussed in the draft Sender ID RIA, the Sender ID registry would restore and protect trust in SMS that use a Sender ID because consumers would have a high level of assurance that such SMS are valid and sourced from genuine businesses and/or organisations. However, this trust would not extend to all SMS because scams without Sender ID would continue regardless of the Sender ID intervention. Indeed, there is every reason to think that scam SMS without Sender ID will increase as fraudsters respond to being unable to use spoofed Sender ID. Furthermore, there is no reason to think that consumers would trust SMS communications more because a subset of those communications (i.e., Sender ID) are blocked. This could still entail a large loss of consumer welfare given the unique benefits of SMS for these use cases, as outlined in Section 2.1. Therefore, each of the effects on trust (i.e., contagion, feedback etc) would continue, reducing trust in the numbering platform.

5.322 Alternatively, under Option 2, the combination of a Sender ID Registry and a SMS Scam Filter would provide significant protection to Irish consumers by both blocking scam SMS using Sender ID Spoofing and by blocking suspicious SMS traffic not making use of Sender ID Spoofing. The SMS Scam Filter complements the protections provided by the Sender ID registry such that consumers overall experience of scam SMS will be significantly reduced regardless of where or how the scam originates.

5.323 Absent the Sender ID registry, some of those scam SMS may end up being received by consumers because, while effective, the SMS Scam Filter cannot provide full protection all of the time due to the evolution of nuisance SMS over relatively short periods[320]. Consequently, Option 2 would result in the greatest reduction in scam SMS, while protecting the use of Sender IDs. Therefore, Option 2 is likely to most protect the trust placed by consumers in Sender ID, SMS and Irish MNs, ComReg considers it likely to best safeguard and promote the continued use of SMS by Irish consumers and businesses.

5.324 This option is likely to reduce each of the effects assessed under Option 1 (e.g., contagion, feedback social effect). In particular, this reduces the contagion effect because consumer experiences of scam become rarer and they become more likely to trust, open and read SMS. This is turn would reduce the feedback effect by encouraging organisations and businesses to use SMS as a means to communicate with their consumers because they know that consumers are more likely to engage with the communications provided over the SMS platform. Finally, organisations that deliver important public and social services would be able to use SMS generally, allowing vulnerable groups to receive services without the worry of knowing whether such SMS are genuine or from fraudsters.

Conclusion on impact on consumers

5.325 Based on the assessment above, ComReg is of the preliminary view that Option 2 is likely to be preferred by consumers and businesses because it produces the greatest reduction in the harm from scam calls and best safeguards the trust in and use of SMS, Sender ID and Irish MNs more generally.

II. Impact on industry stakeholders

5.326 The relevant industry stakeholder among those outlined in Section 5.2.4, are operators that:

1. Terminate SMS traffic;
2. SMS aggregators; and
3. Other operators (resellers, including MVNOs).

5.327 This section provides information on the impacts on industry stakeholders (as outlined above) arising from the regulatory options above. ComReg notes that there are two broad categories of impacts relevant in this section:

[320] Absent the Sender ID registry, fraudsters would likely continue to spoof such Sender IDs, given the importance of such organisations to Irish consumers. As a SMS Scam Filter assesses many millions of texts and even a with high degree of accuracy a number of scam SMS with Sender IDs would not be blocked and still reach consumers. Even if only a small share of attempted scam SMS using Sender ID spoofing reached consumers, this is still a large number of scam SMS impersonating key organisations. Therefore, absent the Sender IDs registry, a SMS Scam Filter on its own is unlikely to protect consumers and fraudsters would likely continue to spoof such Sender IDs.

I. First, the financial costs on stakeholders arising from the implementation of the regulatory option(s) are assessed (i.e., Implementation costs); and

II. Second, other relevant impacts arising from the implementation of the regulatory option(s) are assessed (i.e., other impacts).

Option 1: 'Sender ID RIA"– Preferred Option

I. Financial impacts

5.328 There are no additional financial costs associated with Option 1 other than those included in the implementation of the Sender ID Registry as discussed in the draft Sender ID RIA.

II. Other Impacts

5.329 Under this option, the harms to operators identified (e.g., commercial benefits from being able to offer networks of trust etc) would be reduced and would positively impact trust in SMS services, particularly in the short run. However, as fraudsters adapt and transfer resources into sending scam SMS without Sender ID, the impacts will likely increase and negatively impact trust and use of SMS. Operator reputations would also continue to be damaged as scams proliferate across society negatively impacting the revenues generated by operators from providing SMS services.

Option 2: SMS Scam Filter

I. Financial impacts

5.330 A SMS Scam Filter is applied on originating and terminating SMS traffic and therefore the cost of this intervention is borne by terminating MNOs. The SMS Scam Filter would apply to Eir, Three and Vodafone. To inform ComReg's assessment, Europe Economics have estimated both the one-off costs (e.g., the cost of software purchase and installation) and on-going cost (e.g., on-going cost of platform maintenance) of SMS Scam Filter per operator. Europe Economics has estimated a one-off cost per MNO of approximately €1 million with ongoing costs of approximately €100,000.

Table 17: One-off costs per stakeholder for each Option, relative to status quo

Option	MNOs	SMS Aggregators	Sender ID owners
Option 1 **(Full Sender ID Registry)**	€150,000	€123,000	-
Option 2	€1,246,000	€123,000	-

(Full Sender ID Registry & SMS Scam Filter)			

II. Other Impacts

5.331 Under this option, the harms to operators (e.g., commercial benefits from being able to offer networks of trust etc) would be substantially reduced due to the combined effects of the static and dynamic interventions. Scam Sender IDs (not on the registry) would be blocked by operators causing consumers to trust the text which use Sender IDs. This is complemented by the SMS Scam Filter which will significantly reduce the prevalence of scam SMS. Over time it is likely that consumers will increase trust in the networks that deliver SMS services and become aware of the measures implemented by operators. This would also increase consumer confidence that operators are willing to protect their customers from criminal interference.

Conclusion on impact on industry stakeholders

5.332 Some operators may be of the view that a SMS Scam Filter is unnecessary given the implementation of Sender ID Registry. However, it is clear that a combination of the Sender ID Registry and the SMS Scam Filter is required to fully combat scam text messages. Absent the SMS Scam Filter, scam SMS will persist and proliferate as fraudsters avoid sending scam SMS using Sender ID. (See also footnote 348). Therefore, the extent to which operators prefer Option 1 or Option 2 depends on how operators view the effectiveness of the SMS Scam Filter relative to the cost of implementing same. ComReg is of the preliminary view that Option 2 is likely to be preferred by most stakeholders as it balances the benefits of reducing the harm from scams with the costs of implementing same. While the costs of implementing the SMS Scam Filter are not insignificant, they are a tiny fraction of annual revenues earned by operators and as noted previously, the well-flagged price increases by operators were made on the need to invest in their networks and services.

III. Impact on competition

5.333 This section provides information on the impacts on competition (as outlined above) arising from the regulatory options above. Based on the statutory objectives outlined in 5.12-5.16, there are three broad categories of impacts relevant in this section:

I. First, the impact on the efficient use of numbers arising from the regulatory option is assessed (i.e., impact on use and misuse);

II. Second, the potential distortionary impact on competition arising from the regulatory option is assessed (e.g., the incentives to compete); and

III. Third, the impact on the efficient investment arising from the regulatory option is assessed.

Option 1 v Option 2

Efficient use of numbers

5.334 Against the objective of ensuring the efficient and effective use of numbers, it has already been established in the previous draft RIA that the SMS Registry would effectively eliminate scam SMS using Sender ID and this would lead to an increase in the efficient use of the numbering resource. However, scam SMS that do not use Sender ID would persist and over time proliferate as fraudsters adapt to the implementation of the SMS registry. These include scam messages to businesses/organisations (including public services) without Sender ID spoofing and P2P communications (i.e., SMS to friends and family). Therefore, in the long run, Option 1 (and the use of an SMS Registry only) would do little to reduce the inefficient use of numbers that that is currently resulting in an observable and significant consumer harm including 38 million nuisance SMS and 14 million distressing and approximately 500 consumers a day being defrauded by scam SMS.

5.335 Alternatively, under Option 2, the combination of a SMS Scam Filter and the Sender ID Registry would better promote the efficient use of numbers because all sources of current inefficient use (e.g., scams) would be significantly reduced. In particular, the use of the SMS Scam Filter addresses the misuse of numbers that are not addressed under Option 1. Furthermore, because Option 2 is future proofed, it provides ongoing protections against the inefficient use of numbers. More generally this suite of measures makes it less likely that fraudsters will target Ireland reducing the need for fraudsters to source and misuse Irish SIMs and the underlying numbering resource. This should safeguard and even promote the legitimate use of SMS and Irish numbers more generally.

5.336 Therefore, Option 2 clearly best promotes the efficient use of numbers by best minimising their misuse and promoting their legitimate use.

Promotion of competition

5.337 Option 1 would promote competition but only within the context of blocking scam SMS that use Sender IDs to impersonate businesses/organisations. Scams that impersonate businesses/organisations using spoofed Sender IDs are likely to be more effective for fraudsters and the removal of this approach by the Sender ID Registry will reduce the effectiveness of scam SMS.

5.338 Importantly, this intervention would be highly unlikely to promote competition in the long run because its effectiveness is likely to wear off in the future as scams

become more sophisticated and fraudsters inevitably divert all SMS scams to messages without Sender ID. Because fraudsters already use such scam messages in parallel with those that used spoofed sender IDs (e.g., the eFlow text scam are with and without spoofed Sender ID), fraudsters can be expected to adapt relatively quickly and competition between ECS operators will likely remain distorted.

5.339 Furthermore, scam SMS are becoming significantly more sophisticated with the advent of AI and ML. Therefore, over time, scam SMS without Sender ID are likely to become highly effective at impersonating businesses/organisations. Therefore, Option 1 would better promote competition but only in the short run.

5.340 Under Option 2, the combination of both the Sender ID Registry and the SMS Scam Filter would significantly reduce the prevalence of scam SMS that currently exists while also providing ongoing protection to consumers as scams evolve in the future. In this way, Option 2 would maximise benefits to consumers by appropriately and proportionately addressing significant consumer harms (as evidenced in Chapter 3) for clearly important services. Option 2 would reduce the rate of scam SMS and play an important role in reducing any competitive distortions by mandating measures that that one would expect to be provided in a well-functioning competitive market over an appropriate period.

5.341 Because the Sender ID Registry only reduces scams that spoof Sender IDs, the addition of the SMS Scam Filter would extend the consumer protection much wider to better cover the types of scams that are currently occurring. Further, as previously stated, the Sender ID Registry would not protect long run competition because it is highly likely that scams will evolve once the Sender ID is in place. Indeed, absent the implementation of the voice firewall it is highly likely that further regulatory interventions will be required in the short-term as more sophisticated scams come on stream. Furthermore under Option 2, competition between:

I. providers of SMS services would likely increase because providers would be able to offer SMS with Sender ID services that provide significant protection against all scam communications. Businesses/organisations should therefore have increased confidence in using SMS to communicate with customers enabling even greater use of SMS – This is likely to attract new businesses/organisations which providers would compete for.

II. SMS services and Instant Messaging platforms (e.g., infrastructure-based competition) would also be increased because Option 2 provides protection against all scam SMS meaning the choice made by businesses/organisations would be based on the underlying effectiveness of the SMS platform rather than because of the nuisance created by scam SMS.

5.342 Therefore, Option 2 clearly best promotes the efficient use of numbers by best minimising their misuse and promoting their legitimate use.

Efficient Investment

5.343 As long as competitive distortions persist investment in the SMS platform is likely to be hindered. This is particularly acute for B2C SMS services which has a more diverse and specialised ecosystem (e.g., the networks of large and international SMS aggregators serving Irish businesses). Indeed, as investment is forward looking, even the expectation that distortions to competition would or could emerge could negatively impact investment. This is of heightened risk as operators are likely to know that fraudsters would adapt to static measures to continue to perpetuate scam calls. A SMS Scam Filter would act as a strong complement to the static interventions in terms of promoting efficient investment, by reducing potential distortions to competition and the misuse of numbers.

5.344 Option 2 would encourage efficient investment and innovation in new and enhanced infrastructures by encouraging the rollout of SMS Scam Filters to protect consumers, promoting innovation and ensuring the efficient use and effective management of the national numbering resource. Such investments would be efficient because there is a clear requirement for such interventions given the harms outlined in Chapter 3 and it is highly likely that such technologies would be implemented at some point in the future. However, the implementation of this infrastructure now would prevent consistent and ongoing harm to both consumers and operators. Option 2 clearly best prevents inefficient investment by best protecting the current and future investment in SMS services and networks, and the use of Irish numbers.

Conclusion on impact on competition

5.345 Based on the assessment above, ComReg is of the preliminary view that Option 2 best promotes the efficient use of numbers, competition and efficient investment in ECS markets.

Assessment and the Preferred Option (Step 5)

5.346 The above assessment and the Europe Economics Report demonstrate that there is currently a significant consumer and societal harm present due to scam

SMS and this harm arises from scam SMS with or without Sender ID. The Sender ID Registry would be highly effective at reducing rates of scam SMS with Sender ID. However, this intervention has no impact on scam SMS without Sender ID which would likely proliferate as fraudsters react to the introduction of the Sender ID Registry. Furthermore, fraudsters are becoming ever more sophisticated with the advent of AI, and scam SMS without Sender ID will become increasingly effective at targeting vulnerable consumers.

5.347 Option 2 fills this gap by providing additional protections to consumers reducing the rate of scam through SMS (particularly those without Sender ID). Importantly, the SMS Scam Filter would be able to address scam SMS in real time through the use of advanced real time data analytics using Machine Learning and Artificial Intelligent techniques to detect and act upon unusual patterns of content or hyperlinks in SMS messages. Option 2 would also promote greater competition between providers and across platforms because the SMS platform would not be compromised by scam communications, reducing its effectiveness for end users. Therefore, ComReg is of the preliminary view that, on balance, Option 2 and is the preferred option in terms of its impact on stakeholders, competition and consumers.

5.348 In this Consultation, ComReg assesses the intervention but does not include a D.I as any D.I would be dependent on potential new legislation.

5.7 Assessment of the Overall Preferred Option (Step 5)

5.349 ComReg is of the preliminary view that the proposed package of interventions as discussed in each of the draft RIAs above are the best means of combating scam call and SMS in terms of its impact on consumers, industry stakeholders and competition and in line with its statutory objectives.

5.350 ComReg now examines the cumulative cost and benefit of all interventions on identified industry stakeholders given the interdependencies between interventions. This informs ComReg's assessment of the Overall Preferred Option.

5.351 The remainder of this section summarises the Overall Preferred Package in terms of its:

I. Impact on Irish consumers and businesses;

II. Impact on industry stakeholders; and

III. Against ComReg's statutory objectives (Step 5)

5.7.1 Impact on Irish consumers and businesses

5.352 ComReg considers that the Overall Preferred Option best reduces the current and future harm described in Chapter 3 and is also best placed to protect and restore trust in Irish numbers as described in each of the draft RIAs. EE estimate that all interventions have positive estimated net benefits[321]. However, the total benefit of the Overall Preferred Option depends on the reaction of the fraudsters to each of the individual interventions again noting that fraudsters have the capability to switch between technologies and scams in response to each of the interventions[322].

5.353 As noted by Europe Economics, the voice firewall and SMS Scam Filters are important and provide net benefits in the hundreds of millions even where fraudsters only minimally adapt to the static interventions, because they offer protection that cannot be provided by the static interventions (e.g., against scams originating in Ireland). However, they become increasingly more important the more fraudsters adapt to ComReg's static interventions, rising to €1.3 Billion collectively in a scenario where fraudsters fully adapt (i.e., where

[321] This is shown by examining the effectiveness of the firewalls as a standalone intervention, which leads to a far greater impact. This is the result of the firewalls, in this case, hoovering up the same share of the now greater remaining harm.
[322] Each of the draft RIAs above carefully considered the impact of other relevant interventions (e.g., the Voice Firewall RIA took into consideration that Mobile and Fixed CLI blocking would also be implemented.).

the benefits of the static interventions come to zero).

5.354 In reality, fraudsters will use a mix of methods, and while fraudsters are likely to adapt to ComReg's static interventions, this will require time and it cannot be ruled out that they may reinitiate old scams in the future. The reaction of fraudsters will fall somewhere between not reacting at all or fully adapting to the interventions. However, regardless of how fraudsters adapt, the benefits of the Overall Preferred Option will range between €1.4 and €1.6 billion over seven years[323]. This corresponds to a benefit of €50 for every €1 spent on the interventions.

5.355 However, it should be noted that any delay in implementing these interventions may lead to considerable harm. For example, Europe Economics have estimated that a 1-year delay in implementing the SMS Scam Filter would result in approximately €90 million of additional harm to Irish consumers and businesses.

Table 18: Europe Economics estimates of benefit of the interventions, dependent on level of adaptation by fraudsters

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers fully adapt to static interventions
Voice interventions			
Static Voice interventions	€8m	€896m	-8m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS Scam Filter	€6.2m	€197m	€514m
Combined			
Total	**€31m**	**€1.6bn**	**€1.4bn**

[323] ComReg takes the median of this range provided by these scenarios, €1.5 billion, as the expected net benefit of the proposed package of interventions, as scammers will undoubtedly adapt to some degree.

5.7.2 Impact on industry stakeholders

5.356 ComReg considers that the Overall Preferred Option best protects the business interests of affected operators in the long-term by protecting and promoting the trust in and use of Voice and SMS calls as described in each of the RIAs. However, ComReg is cognisant that it is primarily operators that bear the cost of implementing such interventions (with the exception of ComReg for Sender ID registry). ComReg has taken care to ensure that the proposed package of interventions is delivered in the least onerous form (see Section 5.2.2-5.2.4) and without imposing an excessive cost on any individual operator (see "Impact on Stakeholders" within each RIA).

5.357 Further, while the cost of individual interventions was assessed in each draft RIA, it is the total cost of all interventions that will be borne by operators. Therefore, ComReg assesses the burden of the interventions on identified industry stakeholders, by examining the cumulative one-off cost associated of the Overall Preferred Option.

5.358 For each of the MNOs, the cumulative upfront cost of all the interventions is approximately €3 million per operator or €9 million for mobile industry (i.e., the three mobile operators). This corresponds to one half of one per cent (0.005%) of total retail revenues earned in 2022. These revenues are all likely to increase in 2023 and beyond, in line with operators well flagged price increases. ComReg notes that some operators have defended their recently announced annual price increases (first increase commenced in April 2022) based on generating revenues to finance investment in the upgrade of networks and services. It is inconceivable that such upgrades would not include measures to protect their customers from criminals who are committing fraud using the very same services provided over their networks. The annual ongoing costs of these interventions to mobile operators is a modest cost of doing business (given the benefits it provides) and very minor relative to other annual operating costs (e.g., Three spends around €11 million annually on marketing)

5.359 Similarly, in relation to Virgin and BT the proposed interventions across both its fixed and mobile customers would amount to approximately €1 million or a fraction of a percent of eithers annual revenues. Similarly, the annual operating costs are approximately €100,000, a fraction of a per cent of its current annual cost of sales. Furthermore, the cost of implementation accounts for around [✂…✂] of total annual capital expenditure. Virgin Media has also announced significant price increases from April of this year to invest in technology and give a better experience to customers, among other things.

5.360 The one-off costs for remaining operators are all low and represent a small cost of doing business relative to the size and scale of those operations. For example, while there are potentially small voice originators that would be required to implement the DNO/PN List, the estimated one-off cost is approximately €30,000.

5.361 More generally, the one-off costs for all affected parties of implementing their respective interventions are dwarfed by their annual revenues, as shown in Table 19 below. Indeed, the entire NPV cost of the interventions (€31 million) to industry is equivalent to around 5% of mobile and fixed operators total capital expenditure for 2022 alone. Moreover, the annual ongoing costs of these interventions to operators is a modest cost of doing business (given the benefits it provides) and very minor relative to other annual operating costs (e.g., Three spends around €11 million annually on marketing). It therefore appears unlikely that the cumulative cost of the interventions is excessive on any of the firms that are required to implement the interventions.

5.362 Finally, while ComReg takes account of costs likely to arise from its proposed measures, it also recognises that any such impacts should be balanced against the benefits of achieving relevant statutory objectives, including promoting the interests of other users (i.e., consumers), protecting consumers more generally, promoting competition, and ensuring the efficient and effective use of numbers.

Table 19: Estimated one-off costs per stakeholder for all interventions

Operator Type	Interventions	Approximate cost	Annual ECS revenues in Ireland[324]
MNOs	All Voice and SMS	€3.3 million	**Three** - €578 million[325] **Vodafone** - €936 million[326] **Eir** - €1.8 billion[327]
Virgin	All Voice, lower cost for Mobile CLI	€1.2 million	€381 million[328]
Large IGO	All Voice excl. Firewall	€900,000	Over €300 million[329]
Other IGOs	DNO/PN, Mobile and Fixed CLI Call Blocking	€80,000	€10 million-€100 million[330]
SMS Aggregator	Sender ID registry	€130,000	€1 million -€10 million[331]
Voice originator	DNO/PN	€30,000	€1 million -€10 million [332]

[324] These represent the most recent data available to ComReg. Where data was unavailable ComReg has provided expected lower bounds. Revenues and expected revenues are presented to enable comparison between the implementation cost and operators' revenues, to highlight the difference in magnitude.
[325] Three Ireland (Hutchinson) Limited, "*Directors' Report and Financial Accounts for the year ended 31 December 2021*".
[326] Vodafone Ireland Limited, "*Annual Report and Financial Statements for the year ended 31 March 2022*".
[327] Eircom Limited, "*Directors' Report and Financial Statements for the year ended 31 December 2021*".
[328] Virgin Media Ireland Limited "*Directors' Report for the year ended 31 December 2021*".
[329] BT Communications Ireland Limited "*Directors' Report and Financial Statements for the year ended 31 March 2021*".
[330] This broad range is informed by CRO filings, noting that information was not available for all operators.
[331] This broad range is based on judgement, noting that SMS Aggregators are not necessarily based in Ireland and ComReg therefore has limited visibility of such operators' revenues.
[332]This estimated lower bound is informed by CRO filings, noting that information was not available for all operators.

5.7.3 Preferred Options across the RIAs – Mandate all measures (Step 5)

5.363 Considering the above, ComReg is of the preliminary view that the preferred option in terms of the impact on stakeholders, competition and consumers (the "Overall Preferred Option") is to require:

a) DNO/PN by all originators of Voice traffic capable of terminating on public networks;

b) Fixed and Mobile CLI Call Blocking by all IGOs carrying Voice traffic capable of terminating on public networks into the State;

c) A Voice Firewall by all MSPs with more than 330,000 subscribers or lines capable of terminating Voice calls;

d) A full Sender ID registry by all MSPs capable of terminating SMS with more than 270,000 subscribers capable of terminating SM; and

e) A SMS Scam Filter by all operators of public mobile networks in the State with more than 270,000 subscribers capable of originating or terminating SMS.

5.364 This assessment has considered the impact of the various options from the perspective of industry stakeholders, as well as the impact on competition and consumers, and should aid stakeholders' understanding of the relative merits of the different regulatory options.

5.365 The following section assesses the Overall Preferred Option against ComReg's other relevant functions, objectives and duties.

Assessment of the Overall Preferred Option against ComReg's other relevant statutory objectives

5.366 The preceding draft RIAs considered a number of interventions potentially available to ComReg within the context of the RIA analytical framework as set out in the ComReg's RIA Guidelines (i.e., impact on industry stakeholders, impact on competition and impact on consumers). It necessarily also involved a complex evaluative analysis of the extent to which various interventions would serve to facilitate ComReg in achieving certain statutory objectives in the exercise of its functions. In particular, it involved an analysis of the extent to which the proposed interventions would serve to promote competition and ensure that there would be no distortion or restriction of competition in the electronic communications sector, whilst at the same time promoting innovation and encouraging the efficient use and ensuring the effective management of

the national numbering resource This would in turn enable ComReg to ensure that users would derive maximum benefit in terms of choice and quality.

- The draft CLI Blocking RIA concluded that a combination of Option 2 and Option 3 and the implementation of the DNO/PN List and the Fixed and Mobile CLI Blocking (i.e., the static interventions) are, on balance, the Preferred Options in terms of its impact on stakeholders, competition

- The draft Voice Firewall RIA concluded that, on balance, Option 2 and the implementation of a Voice Firewall is the preferred option in terms of its impact on stakeholders, competition and consumers because it was needed to address scams not covered by the static interventions, including protection against future scams which are likely to become more sophisticated.

- The draft Sender ID RIA concluded that Option 3 and the implementation of a full Sender ID Registry is the preferred option in terms of its impact on stakeholders, competition and consumers.

- The draft SMS Scam Filter RIA concluded that Option 2 and the implementation of an SMS Scam Filter is, on balance, the Preferred Option in terms of its impact on stakeholders, competition because it was needed to address scams not covered by the Sender ID Registry including protection against scam SMS without Sender ID and future scams which are likely to become more sophisticated.

5.367 In this section, ComReg assesses the Preferred Option in the context of other statutory provisions relevant to management of Ireland's numbering resource (which are summarised in Annex 2 of this document). It is not proposed to exhaustively reproduce those statutory provisions here. However, set out below is a summary of all statutory provisions which ComReg considers to be particularly relevant to the management and use of numbering resource with an assessment (to the extent not already dealt with as part of the draft RIAs) of whether, and to what extent, the Preferred Option accords with those provisions. In carrying out this assessment, ComReg has highlighted below some of the relative merits / drawbacks which would arise if it was to select some of the alternative options assessed under the draft RIA above.

5.368 For the purposes of this section, the statutory provisions which ComReg considers to be particularly relevant to the management of the radio frequency spectrum in the State are grouped as follows:

- general provisions on competition;

- contributing to the development of the internal market;
- to promote the interest of users within the Community;
- efficient use and effective management of numbers;
- regulatory principles;
- relevant Policy Directions and Policy Statements; and
- general guiding principles:
    - Objective justification;
    - Transparency;
    - Non-discrimination; and
    - Proportionality.

General provisions on competition

5.369 There is a natural overlap between the aims of the draft RIAs and an assessment of ComReg's compliance with its statutory remit including, in particular, its core statutory objective under section 12(2)(a) of the 2002 Act to promote competition by, amongst other things:

- ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality;
- ensuring that there is no distortion or restriction of competition in the electronic communications sector; and
- encouraging efficient use and ensuring effective management of numbering resources.

5.370 In so far as the promotion of competition is concerned, Regulation 4(3)(b) of S.I. No. 444 of 222[333] further requires ComReg to promote competition in the provision of electronic communications networks and associated facilities, including efficient infrastructure-based competition, and in the provision of electronic communications services and associated services. A further relevant general objective is set out in Regulation 4(3)(d), namely, to promote the interests of the consumers and businesses in the State, by enabling maximum

[333] S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022.

benefits in terms of choice, price and quality on the basis of effective competition.

5.371 Certain other provisions also relate to ComReg promoting and protecting competition in the electronic communications sector including:

- Regulation 4(5)(d) of S.I. No. 444 of 2022 which requires ComReg inter alia to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles by promoting efficient investment and innovation in new and enhanced infrastructures;
- Regulation 4(5)(b) of S.I. No. 444 of 2022, which requires ComReg to ensure that, in similar circumstances, there is no discrimination in the treatment of providers of electronic communications networks and services; and
- General Policy Direction No. 1 on Competition (26 March 2004) which requires ComReg to focus on the promotion of competition as a key objective, including removing barriers to market entry and supporting new entry (both by new players and entry to new sectors by existing players).

5.372 Based on the assessment provided in the draft RIAs above, ComReg's view is that the Overall Preferred Option in the draft RIAs would best safeguard and promote competition to the benefit of consumers. In particular, ComReg refers to '*Impact on consumers' and 'Impact on competition'* within each Draft RIA.

Contributing to the development of the internal market

5.373 In achieving the objective of contributing to the development of the Internal Market, another of ComReg's statutory objectives under section 12 of the 2002 Act[334], ComReg considers that the following factors are of particular relevance in the context of combatting Nuisance Communications:

- the extent to which the Overall Preferred Option would encourage the establishment and development of trans-European networks and the interoperability of pan-European services, by facilitating, or not distorting or restricting, entry to the Irish market by electronic communication services providers based or operating in other Member States; and

[334] Section 12(1)(a)(ii) of the Communications Regulation Act 2002, as amended.

- to ensure the development of consistent regulatory practice and the consistent application of EU law, the extent to which ComReg has had due regard to the views of the European Commission, BEREC and other Member States in relevant matters, in selecting an option and considering any regulatory action required by ComReg in respect of such an option.

5.374 These are assessed in turn below.

I. Encouraging the establishment and development of trans-European networks and the interoperability of pan-European Services

5.375 ComReg notes the overlap between this objective and the objective of promoting competition in the provision of ECN/ECS. Encouraging the establishment and development of trans-European networks requires that operators from other Member States seeking to develop such networks are given a fair and reasonable opportunity to obtain numbers required for such networks. Accordingly, options which would restrict or distort competition or otherwise unfairly discriminate against potential entrants (such as through exposing entrants to greater security risk or lower QoS) would not, in ComReg's view, satisfy the requirements of this objective.

5.376 In this regard, ComReg refers to the draft RIAs and the preliminary finding that the Overall Preferred Option would likely be preferred by those stakeholders that wish to protect consumers and enhance their network security. This is because the Preferred Option would reduce the prevalence and harm from scam calls and reduce the potential distortions to competition. In particular, businesses/organisations from other Member States are currently impacted by scam calls in Ireland. For example, a consumer that purchases goods and services from abroad (e.g., online) may receive a call or SMS from a foreign businesses/organisation. However, research shows that consumers are less likely to engage in such communications due to fear of scams and because they are less likely to recognise an international number. Because the Overall Preferred Option reduces scam communications, consumers are more likely to engage with calls and SMS from abroad. Therefore, the Overall Preferred Option best promotes the establishment and development of trans-European networks and the interoperability of pan-European Services.

II. Promoting the development of consistent regulatory practice and the consistent application of EU law

5.377 In relation to contributing to the development of the internal market, ComReg

continues to cooperate with other National Regulatory Authorities ('NRAs')[335] which includes closely monitoring developments in other Member States to ensure the development of consistent regulatory practice and consistent implementation of the relevant EC harmonisation measures and relevant aspects of the European Electronic Communications Code as transposed. For example:

- ComReg has considered international trends in the regulation of CLI and Sender IDs, as well as use of Voice Firewall and SMS Scam Filters (see Chapter 4) and this has informed its consideration in developing its Overall Preferred Option.
- ComReg has held meetings with other NRAs to better understand their views on the regulation of CLI and Sender IDs, as well as Voice Firewall and SMS Scam Filters (see Section 2.7).
- ComReg issued a Request for Information and received 19 responses from members of the IRG provided a response to the IRG RFI which ComReg issues in order to gather, among other things, the most up to date information on actions being undertaken by other NRAs in relation to the regulation of CLI and Sender IDs, as well as Voice Firewall and SMS Scam Filtering to combat scam calls (see Section 2.7);
- Europe Economics has had clear regard to the effectiveness of DNO, PN, Mobile CLI Blocking and Fixed CLI Blocking, Voice Firewalls, Sender ID registries and SMS Scam Filtering used in other countries in forming its recommendations[336]; and
- ComReg has held meetings with members of the NCIT, and bilateral meetings with individual NCIT members to discuss, among other things, their views on the potential interventions that could be implemented in relation to the regulation of CLI and Sender IDs, as well as Voice Firewall and SMS Scam Filters (see Section 2.7).

5.378 Furthermore, ComReg met with and considered the detailed views of the European Union Agency for Law Enforcement and Cooperation (EuroPol) the law enforcement agency of the European Union. ComReg also considered the recent Europol in report titled "*ChatGPT: The impact of Large Language Models*

[335] In accordance with section 12(2)(b)(iv) of the Communications Regulation Act 2002 as amended, which provides that: "In relation to the objectives referred to in subsection (1)(a), the Commission shall take all reasonable measures which are aimed at achieving those objectives, including— in so far as contributing to the development of the internal market is concerned—co-operating with electronic communications national regulatory authorities in other Member States of the Community and with the Commission of the Community in a transparent manner to ensure the development of consistent regulatory practice and the consistent application of Community law in this field".

[336] See Europe Economics Report Appendix 1 and Appendix 2, in particular Table 9.8.

on Law Enforcement" published in in March 2023[337].

To promote the interest of users within the Community

5.379 The impact of the Overall Preferred Option and other options on users within the community and other stakeholders and in the context of ComReg's objective to promote competition has been considered in the context of the draft RIAs and it is not proposed to consider this matter further here. In particular, ComReg refers to '*Impact on stakeholders'* and *"Impact on Consumers"* within each draft RIA.

5.380 ComReg also observes that most measures set out in Section 12(2(c) (i) to (vii) of the 2002 Act, aimed at achieving this statutory objective, are more relevant to consumer protection, rather than to the management of numbers.

Efficient use and management of numbers

5.381 Under section 10(1)(b) of the 2002 Act, it is one of ComReg's functions to manage the national numbering resources in accordance with a Policy Direction under section 13 of the 2002 Act. Importantly, in pursuing its objective to promote competition under section 12(1)(a), ComReg must ensure the efficient use and management of numbers (section 12(2)(a)(iv)). Section 12(3) of the 2002 Act also requires that in carrying out its functions, ComReg shall seek to ensure that measures taken by it are proportionate having regard to the objectives set out in section 12.

5.382 ComReg is of the view that the Overall Preferred Option is one that would safeguard and promote those interests. In addition, the Overall Preferred Option best encourages the efficient use of numbers and reduces the misuse of numbers. ComReg refers to '*Efficient use of numbers'* within each draft RIA. In summary, the Overall Preferred Option would prevent or reduce the misuse of numbers, through reducing the ability of fraudsters to

- spoof the CLI of key Irish businesses and government agencies, as well as the ability of international fraudsters to spoof Irish Fixed and Mobile CLIs more generally; and

- spoof CLIs within the state, exploit any gaps or otherwise circumvent the Voice CLI interventions (e.g., taking an Irish Mobile SIM abroad to originate calls from abroad using an Irish mobile number, hacking an Irish company to originate calls with Irish CLI); and

[337] ChatGPT - the impact of Large Language Models on Law Enforcement | Europol (europa.eu)

- to spoof the Sender ID of key Irish businesses and government agencies initially, and any business and government agency once fully implemented; and

- send scam SMS to Irish mobile users, which may include spoofing the Sender ID of key Irish businesses and government agencies.

5.383 Furthermore, it would safeguard the legitimate use of numbers by reducing the harm from scam calls and SMS which could reduce the trust and use of Voice calls and SMS by Irish consumers and businesses (e.g., as consumers either switch to alternative channels or stop answering certain types of calls (e.g., answering calls from Irish numbers, or stop reading SMS messages, with or without Sender ID)).

Regulatory principles

5.384 Under Regulation 4(5) of S.I. No. 444 of 2022, ComReg must, in pursuit of its policy objectives under Regulation 4(3), apply impartial, objective, transparent, non-discriminatory, and proportionate regulatory principles by, amongst other things:

a) promoting regulatory predictability by ensuring a consistent regulatory approach over appropriate review periods; and

b) promoting efficient investment and innovation in new and enhanced infrastructures.

Regulatory Predictability

5.385 ComReg notes that it places importance generally on promoting regulatory predictability and as illustrated below, has complied with this principle in carrying out the current process.

5.386 In the present context, ComReg considers the following objectives to be of particular importance to achieving the aims of this regulatory principle:

- promoting regulatory predictability in relation to use of numbers by applying an open, transparent, and non-discriminatory approach to accessing and using numbers; and

- promoting regulatory predictability in relation to ensuring that the use of numbers is predictable and not subject to significant change such that it would compromise efficient investments.

5.387 In relation to the first objective, ComReg's Overall Preferred Option is consistent with its general treatment of a scarce national resource that is subject to misuse such that ComReg would stipulate rules on its use or make interventions that promote legitimate use and prevent misuse. Noting the significant harm from scam calls and SMS to Irish consumers and businesses, and the potential for its persistence to compromise the use of such services in the future, operators should expect that ComReg would seek to implement rules regarding the use of CLI and SMS and require technical interventions. Further, as noted in Section 2.6, ComReg has dealt with instances of Nuisance Communications in the past and made proportionate regulatory interventions to alleviate harm to consumers. Similarly, ComReg introduced measures to address the cost of using non-geographic numbers to tackle confusion among consumers about the differences between the numbers[338].

5.388 In relation to the second objective, ComReg refers to its assessment under '*Efficient Investment'* within the draft RIAs, and its preliminary view that the conditions for promoting efficient investment and innovation in new and enhanced infrastructures investment involves ComReg taking its regulatory functions in an appropriate and predictable fashion as provided under the Overall Preferred Option.

5.389 Considering the above, ComReg is of the view that the Overall Preferred Option complies with the regulatory principle of promoting regulatory predictability.

Relevant Policy Directions and Policy Statements

5.390 ComReg notes that the core policy objectives, principles and priorities set out therein are broadly in line with those set out in the 2002 Act and in the European Electronic Communications Code (which has repealed the Common Regulatory Framework), as transposed in S.I. 444 of 2022 (and the Act of 2023) and, in turn, with those followed by ComReg in identifying the Overall Preferred Option.

5.391 Section 12(4) of the 2002 Act requires ComReg, in carrying out its functions, to have regard to policy statements, published by or on behalf of the Government or a Minister of the Government and notified to it, in relation to the economic and social development of the State. Section 13 of the 2002 Act requires ComReg to comply with any policy direction given to ComReg by the Minister as he or she considers appropriate to be followed by ComReg in the exercise of its functions.

5.392 ComReg has taken due account of relevant Policy Directions contained in the February 2003 Ministerial Policy Direction, namely:

Policy Direction 5 – Regulation only where necessary;

[338] Non-Geographic Numbers | Commission for Communications Regulation (comreg.ie)

Policy Direction 6 – Policy Direction on Regulatory Impact Assessment; and

Policy Direction 7 – Policy Direction on consistency with other Member States.

5.393 In relation to I and II the four draft RIAs considered a variety of different options against each other, including the option of doing nothing. In all cases there was strong evidence in support of the Preferred Options and the Overall preferred Option. In relation to III, ComReg refers to the discussion within each RIA as to how ComReg has promoted the development of consistent regulatory practice and the consistent application of EU law.

General guiding principles (in terms of number management and conditions).

5.394 ComReg notes that it is required to comply with the guiding principles of objectivity, transparency, non-discrimination and proportionality in carrying out its functions under the 2002 Act and under the European Electronic Communications Code (which has repealed the Common Regulatory Framework), as transposed by S.I. 444 of 2022. In relation to the current process, ComReg considers that these principles are most relevant in terms of its functions concerning use and management of numbers and attaching conditions to rights of use.

5.395 In relation to number management and use, ComReg notes that:

a) ComReg's function under section 10(1)(b) of the 2002 Act is to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act are to ensure the efficient management and use of numbers from the national numbering scheme in the State;

b) Regulation 79 of SI 444 of 2022 provides that ComReg:

- shall grant rights of use for numbers for all national numbering resources for all publicly available ECS by application of procedures which are objective, transparent, non-discriminatory; and
- shall ensure that adequate numbering resources are provided for the provision of publicly available electronic communications services.

c) Regulation 79(4) of S.I 444 of 2022 provides that: "any *person who assigns to locations, terminals, other persons or functions on public*

communications networks numbers from the national numbering plan that the regulator has not specifically allocated to the person in connection with the provision of publicly available electronic communications services commits a hybrid offence".

5.396 ComReg notes that the above guiding principles are Irish and EU law principles that ComReg abides by in carrying out its day-to-day regulatory functions.

5.397 ComReg also notes a relevant power under Regulation 83(2) of SI 444, which provides that "*ComReg may require providers of public electronic communications networks or publicly available electronic communications services to block on a case by case basis, access to numbers or services where this is justified by reason of misuse or fraud and to require that in such cases those providers withhold relevant interconnection or other service revenues, where this is justified by reason of fraud or misuse and to require undertakings to withhold relevant interconnection or other service revenues*".

5.398 ComReg further notes a relevant power under Regulation 4(1) of SI 444 which provides: "*The Regulator and other competent authorities, in carrying out their regulatory tasks specified in these Regulations insofar as it gives effect to the Directive, shall take all reasonable measures which are necessary and proportionate for achieving the objectives set out in paragraph (3)*." Relevant general objectives listed in Regulation 4(3), which ComReg has to pursue in the context of its tasks, are the following: "*promote the interests of the consumers and businesses in the State, …, by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules …*"

5.399 ComReg notes that each of the draft RIAs and the supporting Chapters (i.e., Chapter 3 and Chapter 4) provide strong evidence of the misuse of numbers in relation to both voice and SMS which are used to perpetuate fraud. For example, Europe Economics estimate that 59 million scam calls were received by consumers which equates to approximately 161,000 scam calls being received each and every day and over 47 million scam messages a year were received which equates to an average of approximately 129,000 scam texts being received each and every day.

5.400 Overall, it is estimated that there were approximately 365,000 cases of fraudulent scams in Ireland over the last 12 months with losses ranging from €5 to €5,000, with scam calls accounting for a higher share of large scams (e.g., >€500). In effect, around 1,000 people are defrauded every single day over ECN.

5.401 A further relevant power is ComReg's power under Regulation 104 of SI 444, which gives ComReg the power to, for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the SI 444 Regulations, to issue directions to an operator or undertaking to do or refrain from doing anything which the Regulator specifies in the direction.

5.402 ComReg is of the preliminary view, having regard to the applicable legislation and legal principles, its draft RIAs and other analyses, its expert advice and reports, and the material to which it has had regard, that the Preferred Option is objectively justified, transparent, proportionate, and non-discriminatory. In particular, the Preferred Option:

a) is objectively justified given the detailed assessment provided in the draft RIAs, including that it would be unlikely to distort or restrict competition and it better encourages the efficient use of the numbers;

b) would not give rise to discrimination in the treatment of undertakings because:

- any difference in costs incurred as a result of the Overall Preferred Option arise because the situation of some operators is materially different from others.
- the cost of combating scam calls is not dependent on the stakeholder but rather on their traffic and how scams are originated.

c) is transparent because, among other things:

- ComReg provides an assessment of the potential impact of DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, a Sender ID Registry and SMS Scam Filter on affected stakeholder groups by types of traffic carried, including an estimated cost to affected operators, in the draft RIAs above; and
- Europe Economics and ComReg have published the estimates of the costs and benefits to society from a DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, a Sender ID Registry and SMS Scam Filter and the CBA based on same, with detailed explanation of the underlying methodology set out in Chapter 5 and the Europe Economics Report;
- Europe Economics has provided the necessary information for operators to understand its estimated cost of DNO, PN, Fixed and Mobile CLI Blocking, a Voice Firewall, a Sender ID Registry and SMS Scam Filter which may assist operators in understanding and seeking necessary internal approvals for

undertaking the actions and budget required for implementation.

d) is proportionate because, among other things:

- in relation to the Overall Preferred Option
  - it would accord with ComReg's statutory objectives and regulatory principles as described above;
  - there does not appear to be less onerous means by which these objectives and principles could be achieved, and wherever possible, ComReg has scoped the interventions to reduce their cost and complexity on industry and allow operators to implement the decision in a cost efficient way (e.g., allowing MNOs to implement Mobile CLI blocking on behalf of MVNOs or smaller IGOs, only applying a Voice Firewall to networks exceeding a subscriber-based threshold);
  - the majority of affected stakeholders are members of the NCIT and have previously agreed to implement some of these measures; and
  - these measures are in line with measures implemented by operators in several other EU member states to protect their consumers, in many cases without any regulatory requirement.
- in relation to costs specifically:
  - The social cost of these interventions are not excessive to its benefits. Europe Economics has found that the social benefit of preferred package vastly outweighs the social cost of the interventions. ComReg has already established that the social benefit of the preferred package far outweighs its social cost (see above). Indeed as noted in the Irish Governments Public Spending Code "*The difficulty for the public sector is that it must consider the wider implications for society – the social costs and benefits*."[339]; and
  - The cost of the preferred package to affected operators does not appear prohibitive, relative to the size of revenues generated and capital expenditures made by

[339] Department of Public Expenditure and Reform "*A Guide to Economic Appraisal: Carrying Out a Cost Benefit Analysis*"

those operators from providing ECS in the State, (see Table 19 above).

- In relation to timelines specifically:
  - the deadline for implementing each intervention takes into account the scale of the work and time necessary involve, as determined as reasonable (see Chapter 4);
  - in each case this timeline exceeds and extends the voluntary deadlines of the NCIT by a number of months; and
  - the majority of affected stakeholders are members of the NCIT and have previously agreed to implement these measures well in advance of these timelines.

Conclusion

5.403 In light of the above, ComReg is of the preliminary view that the Overall Preferred Option complies with those statutory functions, objectives and duties relevant to its management of the national numbering resource.

Chapter 6

6 Updating the Numbering Conditions

6.1 This Chapter proposes changes to ComReg's Numbering Conditions of Use and Application Process document ("the Numbering Conditions")[340] to ensure that the numbering conditions of use align with the proposed interventions. It also provides a guide to KYC processes which should be used in combatting nuisance communications.

6.2 ComReg aims to review and update the Numbering Conditions approximately every two years - the last review and update was in 2021[341]. The main purpose of such reviews is to address any issues that have arisen since the prior update, by proposing and introducing new or amended conditions of use where needed. Since the last Numbering Conditions update in 2021, the surge in nuisance communications that makes use of CLI or SMS Sender ID spoofing, now necessitates a review of that document, particularly in relation to the CLI conditions of use ("CLI conditions"). ComReg's updated draft Numbering Conditions, which is published with this consultation, includes all proposed new and amended conditions of use. In that regard, and unless otherwise stated, references to a particular section or appendix shall be taken to mean the section or appendix in the draft Numbering Conditions document.

6.3 The remainder of this Chapter is set out as follows

- Section 6.1 Updates in light of the Voice interventions
- Section 6.2 Updates in light of the SMS interventions
- Section 6.3 General updates to CLI Conditions
- Section 6.4 General updates to provide CLI Guidance
- Section 6.5 The evolution of KYC
- Section 6.6 Future Number management

6.1 Updates in light of Voice interventions

Background

6.4 Appendix 12 of the Numbering Conditions sets out the meaning of CLI as a service within telecommunications networks that provides users with

[340] ComReg 15/136R3
[341] ComReg 21/75 - Review of the Numbering Conditions and Application Process - Response to Consultation, Decision and Further Consultation

capabilities of sending, receiving, and displaying International ITU-T E.164[342] numbers. Appendix 12 also provides the meaning for the two types of CLI, namely the presentation CLI[343] and network CLI [344].The CLI service also incorporates end-user preferences such as the caller's preference to have their number displayed to the called party or not.

6.5 In this section of the consultation, ComReg assesses the CLI conditions that are needed to align with each of the four voice interventions described in this document, and as follows:

i. Do-Not-Originate List;

ii. Protected Numbers List;

iii. Fixed CLI Call Blocking; and

iv. Mobile CLI Call Blocking.

6.6 The DNO intervention requires operators to block calls that spoof Irish fixed phone numbers that are never used by organisations to make outgoing calls. A more detailed description of this intervention is provided in Section 4.2(1) of this consultation.

6.7 The Protected Numbers intervention requires operators to block calls that spoof certain Irish fixed and mobile telephone numbers that are not assigned. A more detailed description of this intervention is provided in Section 4.2(2) of this consultation.

6.8 To combat incoming fraudulent calls from abroad, the Fixed CLI Call Blocking intervention requires International Gateway Operators ("IGO") to block any calls from abroad that use an Irish fixed CLI. This intervention is in line with the intended use of Irish fixed CLIs which should only originate on the Irish PSTN.

6.9 The implementation of the Fixed CLI Call Blocking intervention means that any such use of Irish fixed number CLIs in the origination of calls from international PSTNs would be unsuccessful, as these call attempts would be blocked at all points of international interconnect to the Irish PSTN. A more detailed description of this intervention is provided in Section 4.2(3) of this consultation.

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

[343] The presentation CLI enables a called party to view the calling party's number before answer and, if needed, use that CLI information to make a call-back.

[344] While the presentation CLI and network CLI have equivalent SIP terms, the consultation will use the terms presentation and network CLI throughout.

6.10 In 2022, ComReg published Information Notice 22/114[345] which detailed the Fixed CLI Call Blocking intervention and the transition arrangements that organisations needed to carry out to cater for their customers. ComReg also wrote to NCIT and non-NCIT operators to communicate the same information. In addition, and as requested by operators, these letters provided a high-level summary of the current CLI conditions. This consultation will seek to support the transition arrangements by proposing amendments to the Numbering Conditions where necessary.

6.11 To further combat incoming fraudulent calls from abroad, the Mobile CLI Call Blocking intervention requires IGOs to block any inbound calls to the Irish PSTN that use an Irish mobile CLI. There are exceptions to this blocking, specifically calls into Ireland from outbound roamers and calls to inbound roaming users in Ireland. A more detailed description of this intervention is provided in Section 4.2(4) of this consultation.

CLI Conditions - Assigned Number

6.12 Section 3.1 (5) of the Numbering Conditions sets out the conditions associated with CLI use. The Numbering Conditions requires that the originator of a call must ensure that the CLI is the assigned number for the calling party. Furthermore, the CLI is restricted to certain classes of number as identified in the Numbering Conditions. However, clarity for operators on the use of CLI is critical to the successful implementation of the nuisance communications voice interventions. Therefore, ComReg proposes to rephrase the key CLI condition in the Numbering Conditions to highlight as a stand-alone condition the requirement that the CLI must be the assigned number for the calling party. To that end, ComReg proposes to add the following underlined text as a new paragraph “i” in Section 3.1 (5) (a) and delete the text as indicated;

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

Do Not Originate

[345] ComReg 22/114 - Nuisance Communications: Fixed CLI Blocking Intervention Arrangements for International Operations

6.13 By submitting its assigned numbers to the DNO list, an organisation confirms that it does not use those numbers as a CLI. Furthermore, ComReg notes that, if originating operators comply with Section 3.1 (5) (a)(i) of the Numbering Conditions by ensuring that only the assigned numbers for the calling party are used as CLI, then no numbers on the DNO list can legitimately appear as CLI on calls originating on the Irish PSTN.

6.14 To support the management of the DNO list, ComReg proposes to introduce the following text as part of new paragraph 4 of Section 1 "Introduction";

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

Protected Numbers

6.15 It is an offence under Regulation 79(4) of the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444/2022)[346] to use numbers that have not been assigned by ComReg. Therefore, the Protected Numbers blocking intervention is in accordance with Regulation 79(4). Furthermore, the condition which requires that the originator of the call ensures that the number used as CLI is the assigned number for the calling party, aligns with that intervention.

6.16 To support the management of the Protected Numbers list, ComReg proposes to introduce the following text as part of new paragraph 4 of Section 1 "Introduction";

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

Fixed CLI Call Blocking

Background and Scope

6.17 Chapter 4 of this consultation provides details of the CLI Call Blocking intervention. To align the Numbering Conditions with this intervention, ComReg proposes to carry out updates to the Numbering Conditions as follows:

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

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

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

ii. Furthermore, to provide for the intended use of long-lining as described in Section 4.2 of this consultation, ComReg proposes to add a new paragraph 9 in Section 3.2 of the Numbering Conditions as follows;

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

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

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

6.18 ComReg has introduced long-lining to address the business needs raised by operators who wish to provide a service to their business customers in Ireland with overseas branch offices or call centres. ComReg will monitor the implementation of long lining to ensure that it is being correctly applied by operators.

6.19 However, while long-lining enables certain calls from overseas to originate on the Irish PSTN, and so prevents the blocking of such calls by the Fixed CLI Call Blocking intervention, ComReg has concerns regarding the use of Irish geographic numbers as CLI on these calls. In its Response to Consultation[347] on a review of the Numbering Conditions, ComReg notes that its Consumer Survey[348] provides evidence that consumers have concerns regarding fraud if the link between area codes and geographic areas is removed. This issue is of particular concern with the upsurge in nuisance communications.

[347] [347] ComReg 21/75 - - Review of the Numbering Conditions of Use and Application Process Response to Consultation 21/28, Decision and Further Consultation - Section 4.1 paragraph 395
[348] ComReg 21/28b - Geographic Numbering Survey - Quantitative report

6.20 To address such concerns, ComReg will carry out a review within the next 2 years of the options that would balance the needs of business while maintaining consumer confidence in the use of numbers. For example, ComReg sees the use of NGNs by Irish overseas branch offices or call centres as a possible alternative that, while still requiring long-lining to prevent call blocking, might better meet consumer expectations concerning the origin of a call.

6.21 ComReg notes that, as part of the Fixed and Mobile CLI Call Blocking interventions, the blocking of calls from Irish fixed and mobile numbers to inbound roamers must be avoided. This issue will be addressed in the following section on the Mobile CLI Call Blocking intervention.

Mobile CLI Call Blocking

Background and Scope

6.22 As with Fixed Irish phone numbers, a common tactic used by criminals to defraud victims is to spoof Irish mobile phone numbers. These fraudsters, many based abroad, often spoof Irish mobile numbers as their CLI, knowing that recipients in Ireland are more likely to answer. To combat these fraudulent calls, the NCIT has agreed the Mobile CLI Call Blocking intervention.

6.23 The Mobile CLI Call Blocking intervention, as set out in Section 4.2 of this consultation, provides for the blocking by operators of all calls with Irish mobile CLIs that seek to ingress onto the Irish PSTN from non-Irish PSTNs. This intervention specifically applies to Irish operators (IGOs) who route calls from overseas PSTNs into the Irish PSTN.

6.24 As specified by 3GPP[349], international roaming is a service whereby a UE (i.e., mobile station) of a given Public Land Mobile Network ("PLMN") is able to obtain service from a PLMN of another country while visiting. Furthermore, the specification indicates that the availability of International Roaming is subject to inter-PLMN agreements.

[349] 3GPP TS 22.011 V11.3.0 (2013-03) – Technical Specification Group Services and System Aspects; Service accessibility - Section 2.2

6.25 The Mobile CLI Call Blocking intervention allows for both outbound and inbound roaming. The term "outbound roamer" means an Ireland based mobile user who is roaming on an international PSTN. Calls to Ireland from these roamers will present an Irish mobile CLI. "Inbound roamer" means an international based mobile user who is roaming in Ireland. Calls from fixed and mobile numbers in Ireland to an inbound roamer will be routed initially to the visitor's home operator and then back via an international operator to an Irish IGO where it will present the fixed or mobile Irish CLI for the caller. Such calls to inbound roamers will use a Mobile Station Roaming Number ("MSRN") as part of the calling process. The Mobile CLI Call Blocking specification sets out the method of preventing the inadvertent blocking of calls from outbound roamers or calls to inbound roamers by, respectively, enabling the IGO to establish that the CLI is from an outbound roamer or that the called mobile number is one from a designated MSRN range.

Numbering Conditions Update

6.26 To support the Mobile CLI Call Blocking intervention, ComReg proposes to manage the MSRN list. To that end, ComReg proposes the following text as part of a new paragraph 4 of Section 1 "Introduction";

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

CLI-Analysis

6.27 Originating operators must carry out CLI-Analysis to enable them to comply with the numbering condition that only the calling party's assigned number, from within a certain set of number classes, is permitted as CLI. Therefore, for the avoidance of doubt, ComReg proposes to insert the following clarification as a new paragraph "e" in Section 3.1 (5) in the Numbering Conditions:

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

6.2 Updates in light of the SMS interventions

Background

6.28 In addition to the four voice interventions, ComReg also proposes two interventions to address SMS Spoofing, a technique often used in Smishing. The specification for one of these interventions, entitled "Sender ID Registry", is provided in Section 4.3(9) of this consultation. This intervention involves the registration of permitted SMS Sender IDs, hereafter referred to as Sender IDs, and the concept of participating aggregators (PA) in the forwarding of SMSs to Irish mobile operators.

6.29 The term Sender ID, in the context of this consultation, refers to an alphanumeric originating address in the TP-OA[350] field of the SMS-TPDU[351] of an SMS message. This SMS Sender ID address has a maximum of 11 standard characters, each one of which is taken from a defined set of numbers, letters and symbols. A "number" is defined at Regulation 2(1) of S.I. No. 444 of 2022 as including "a character and a combination of numbers or characters or both". Therefore, a Sender ID meets the definition of a number.

6.30 In the context of Nuisance Communications, the maintenance of trust in numbers shall also apply to the Sender ID. To that end, ComReg proposes an Sender ID Registry (Registry) intervention.

6.31 Under the proposed process for the Registry, an organisation wishing to originate SMS using a Sender ID applies to ComReg to have its chosen Sender ID included in the Registry. Mobile Network Operators (MNO) would only accept SMSs with a registered Sender ID, delivered via one of a pre-determined set of 'participating aggregators'. This proposed requirement will prevent scam SMSs purporting in the Sender ID to originate from particular organisations. By maintaining a Sender ID registry, ComReg can effectively manage the Sender ID resource.

Numbering Conditions Update - Sender ID

Class of Number

6.32 ComReg proposes to include the Sender ID as a class of number in the Numbering Conditions by adding Table 5 to Appendix 10 "Classes of Numbers" as follows;

Code	*Designation*	*Notes*
Alpha-numeric	*Sender ID*	*Recognised Sender IDs are included in the SMS Sender ID Registry intervention. The Registry shall include information such as the Sender ID, Sender ID Owner (SIDO) and*

[350] Transfer Protocol Originator Address – See Section 9.2.3.7 of 3GPP TS 23.040
[351] Transfer Protocol Data Units - See Section 9.2.3 of 3GPP TS 23.040

		Participating Aggregator (PA).

Management of the Registry

6.33 To support the management of the Sender ID Registry, ComReg proposes to introduce the following text as part of new paragraph 4 of Section 1 "Introduction" ;

> *(4) As set out in its Response to Consultation XX and Decision XX on Nuisance Communications, ComReg supports industry by managing the following:*
>
> *(iv) SMS Sender ID Registry*

6.34 ComReg notes that this consultation provides details of a manual process in the application and assignment of Sender IDs. However, to increase efficiency in the management of Sender IDs, ComReg will in due course investigate the options for increased automation of the process.

Timeline for Activation

6.35 To ensure that SIDOs use their registered Sender IDs in a timely manner, ComReg proposes to add the following underlined text to Section 3.2 paragraph 1 of the Numbering Conditions:

> *Unless ComReg otherwise consents, a number shall be activated by its holder (a) within 12 months of the date on which the right of use for the number was first granted to the holder; or (b) within 3 months of the date on which the right of use for the number was transferred, as applicable. In the case of 1800 Freephone and 0818 Standard Rate Numbers, applications shall be submitted on the Fixed Number Portability (FNP)[352] system which shall support the activation of these numbers on networks. In the case of Sender ID, and unless ComReg otherwise consents, a Sender ID shall be activated by its holder (a) within 3 months of the date on which the right of use for the Sender ID was first granted to the holder; or (b) within one month of the date on which the right of use for the Sender ID was transferred, as applicable.*

Switching PA

[352] This is the industry FNP system provided by PortingXS

6.36 To promote competition, a SIDO shall be able to switch their serving PA and to have that switch completed within a reasonable timeframe. To that end, ComReg proposes to insert the following underlined text as new paragraph 8 in Section 3.1 "General Authorisation conditions" of the Numbering Conditions;

> *(8) SMS SenderID Portability – In support of the objectives of ComReg to promote competition (Part 2 Article 3b of SI 444), undertakings shall ensure that SIDOs can, upon request, retain their SMS SenderIDs independently of the undertaking providing the service.*
>
> In the event of a SIDO switching between PAs:
>
> i. the recipient PA must notify ComReg in advance and perform the switch within 2 working days of the scheduled date
>
> ii. the donor PA must facilitate the switch and remove any configuration which is no longer required no more than 5 days after the switch has completed

Rights of Use Conditions

6.37 ComReg proposes to insert Sender ID Rights of Use Conditions as a new Section 6 paragraph 1 in the Numbering Conditions as follows:

> *(a) SMS Sender IDs are encoded according to the GSM 7-bit default alphabet[353] and as such a Sender ID can have a maximum length of 11 characters*
>
> *(b) The following are the valid characters which are permitted:*
>
> ***a-z 0-9 @ ! # % & ( ) * + , - . / : ; < = > ? [Space]***
>
> *(c) Any character not on the above list is not permitted354.*
>
> *(d) Sender ID registration and filtering is case insensitive. A given Sender ID is assigned to a SIDO to use in whatever choice of case they prefer, however the messages should be treated identically irrespective of the case used.*

General Application Criteria

[353] ETSI TS 123 038 Section 6.2.1

[354] For example: Not permitted are all characters with accents (E.g. è Ç), Greek letters (E.g. Ω Ψ) and the following: £ $ " ' ¡ €. Given the limited number of available characters in the GSM 7-bit default alphabet, the Irish language fada is not supported

6.38 Sender IDs will be assigned on a “first come, first served” basis. To that end, ComReg proposes to add the following underlined text in Section 7.1(1) “General Application Criteria” of the Numbering Conditions”;

> (1) ComReg will grant rights of use for numbers to authorised undertakings in an open, objective, transparent, non-discriminatory and proportionate manner and generally on a “first come, first served” basis though ComReg may hold open competitions before granting rights of use for newly-opened number ranges. *For the avoidance of doubt, Sender IDs will also be assigned on a “first come, first served” basis.*

6.39 A PA may apply for a Sender ID by submitting an application that includes the completed application form in Appendix 1 of the Numbering Conditions and an order from the customer for that Sender ID. To that end ComReg proposes to amend the Numbering Conditions as follows:

i. Adding the following underlined text to Section 7.1 paragraph 15(b)

> (b) Applications for numbers other than 1800 and 0818 *and for Sender IDs* must comply with the following:

ii. Adding the following underlined text to Section 7.1 paragraph 15(b)i

> (i)Applicants must complete and sign a copy of the application form in Appendix 1, attaching a completed copy of any relevant form from Appendix 2 – 7 8 for the class of number being requested. For applications for Geographic or Mobile Numbers, the form in Appendix 4 or Appendix 5 must be completed with respect to Geographic or Mobile Numbers already granted to the applicant. *For applications for Sender ID, the Customer Order form in Appendix 9 must be completed.*

iii. Inserting the underlined text and deleting the indicated text in the Appendix 1 application form as follows;

Number, ~~or~~ code or Sender ID requested, if not included in a separate Appendix:

iv. Inserting the template Sender ID customer order form as new Appendix 9 as follows;

An organisation that wishes to apply to have a Sender ID included in the Sender ID registry shall complete the following customer order form and submit to their Participating Aggregator (PA). The PA shall

apply to ComReg for the requested Sender ID by completing and signing a copy of the application form in Appendix 1 and attaching the completed customer order form.

Sender ID Requirement	***Please complete this column***
Participating Aggregator ***(To confirm authorisation of the PA please refer to ComReg's Service Register at https://serviceregister.comreg.ie/)***	
Sender ID Requested ***(The Sender ID must comply with the format set out in the Numbering Conditions – Section X "RoU")***	

Organisation Details	***Please complete this column***
Organisation Name	
Organisation Address	
Responsible person	
Name	
Job title	
Email address	
Telephone number	
Secondary contact person	
Name	
Job title	
Email address	
Telephone number	

Declaration

I have followed the necessary approvals in my organisation prior to submitting the Sender ID customer order form.

I am fully authorised to submit the Sender ID customer order form on behalf of:

(Organisation Name)

Signature:

Name in Block Letters:

Organisation Name:

Date of Submission:

Eligibility Criteria

6.40 ComReg proposes to include eligibility criteria for Sender IDs by adding a new paragraph 8 in Section 7.2 of the Numbering Conditions as follows;

(a) The SIDO must have a connection with Ireland. The connection with Ireland shall be demonstrated by the SIDO submitting the following information;

(i) A company's Irish CRO number, Revenue VAT number or registered business number.
(ii) A sole trader/partnership's Irish VAT number in their own name(s), or proof of their business or Irish income tax registration.
(iii) For a trademark holder that holds a trademark that is enforceable in Ireland, the trademark number or a digital copy of the trademark certificate.

(b). ComReg reserves the right to refuse applications where the proposed name is likely, in ComReg's view, to lead to confusion; to facilitate fraud or misuse; to incorrectly suggest state sponsorship; or cause offence.(XX)

Q.1 Do you agree with ComReg's proposal to amend the text in the Numbering Conditions as set out above? Please explain the basis for your response in full and provide supporting information.

6.3 General updates to CLI Conditions

Geographic Numbers

6.41 With the increase in nuisance communications and the need to maintain consumer trust in numbers, ComReg considers it worthwhile highlighting its 2021 consultation[355] on the Numbering Conditions. In that consultation, ComReg requested submissions on the retention of Section 4.1 (2) of the Numbering Conditions which sets out a CLI condition for Geographic numbers as follows:

> *"A Geographic Number shall only be assigned to an end-user whose residential/business premises is physically located within the designated minimum numbering area (MNA)[356] for that Geographic Number".*

6.42 For the purposes of this consultation, this will be known as the "*physical location"* condition.

6.43 As previously noted in this Consultation, ComReg's Consumer Survey[357] provides evidence for, among other things, consumer concerns regarding fraud calls if the link between Area Codes and geographic areas is removed. Therefore, given the increase in scam calls using CLI spoofing, the physical location condition remains an essential tool in combatting nuisance communications and is retained.

6.44 However, an end-user may be assigned geographic numbers in more than one MNA. Therefore, to provide further clarity on the use of Geographic numbers as CLI and to maintain trust in numbers, ComReg proposes the following underlined amendment to Section 3.1(5)(a) of the Numbering Conditions;

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

Non-Geographic Numbers ("NGN")

[355] ComReg 21/28 - Review of the Numbering Conditions of Use and Application Process - Consultation

[356] Appendix 9 contains a list of the Area Codes and Minimum Numbering Areas (MNAs).

[357] ComReg 21/28b - Geographic Numbering Survey - Quantitative report

6.45 While the Fixed CLI Call Blocking intervention will permit IGOs to block calls with Irish fixed numbers as CLI that ingress onto the Irish PSTN, ComReg also considers it timely to review the assignment of NGNs to end-users, particularly with the current surge in nuisance communications.

6.46 ComReg notes that NGNs are intended mainly for use by business end-users. It is not envisaged that individual end-users will seek these numbers. At present the Numbering Conditions do not explicitly require an end-user to be based in or have an association with Ireland to be assigned an Irish NGN. ComReg considers that a requirement for an end-user to, for example, demonstrate that it is carrying out business in Ireland, would reduce the risk of the misuse of NGNs.

6.47 In the case of NGNs, ComReg worked in collaboration with industry to develop the assignment system for individual 1800 and 0818 numbers. This system is known as the Individual Number Assignment (INA) system and operators use it to automatically obtain 1800 and 0818 numbers. In agreement with industry, the design of the INA Solution leverages the existing industry Fixed Number Portability (FNP) System provided by PortingXS[358].

6.48 As NGNs are part of the national numbering resource they should, in ComReg's view, be reserved for use by those carrying out business in Ireland. Sections 4.3 and 4.4 of the Numbering Conditions set out that an authorised undertaking shall only be granted the Rights of Use of (1800 Freephone or 0818 Standard Rate) Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for, together with the end-user's unique identifier. To ensure that businesses seeking NGNs are carrying out business in Ireland, ComReg proposes to amend Sections 4.3 and 4.4 Rights of Use conditions as follows:

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

[358] PortingXS website

And add the following underlined text to proposed paragraph 2 of Section 4.4;

Furthermore, as 0818 Standard Rate numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 0818 Standard Rate number, a business end-user shall be required to provide the following:

i. A company's Irish CRO number, Revenue VAT or business number, [and/or]

ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration.

6.49 With regard to the retrospective application of this proposed condition, ComReg notes that there are approximately 66,000 (1800 Freephone) and 55,000 (0818 Standard Rate) numbers assigned to operators. It is ComReg's view that, given the relatively large number of NGNs already in use, requiring operators to apply this proposal to existing NGN customers is not proportionate. Therefore ComReg proposes that the condition be implemented by operators for new applications only.

1800 Freephone

6.50 In response to requests from some operators for clarity on the use of 1800 as CLI, ComReg notes the following:

i. Section A.8.1 of the revised Annex A of ITU Recommendation E.164[359] states that "*Any number within the responsibility of an Administration, which does not conform to the structure, length and uniqueness as defined in the main body of this Recommendation, is not an international E.164-number, and is termed a National-Only Number*". Thus 1800 Freephone is a national-only number as it is dialable on Irish networks but not generally dialable from abroad.

ii. Section 4.3 of the Numbering Conditions sets out the conditions of use that attach to 1800 Freephone numbers.

6.51 As previously noted, Section 3.1 paragraph (5)(a)(i) of the Numbering Conditions provides for the use of 1800 Freephone as presentation CLI as follows;

"that the presentation CLI for the call shall be the assigned Customer

[359] **ITU Rec E.164** Revised Annex A: Clarification and explanation of the structure and function of international ITU-T E.164-numbers

Support Short Code (for on-network calls), ***a Freephone Number****, a Geographic Number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number for the calling party"*

6.52 Section 3.1 paragraph (5)(a)(ii) of the Numbering Conditions sets out the permitted numbers for use as network CLI as follows;"

"that the network CLI for the call shall be the assigned Geographic Number, 076 Standard Rate Number[360], Mobile Number or M2M number for the calling party"

6.53 Therefore, in relation to the use of 1800 Freephone as CLI, ComReg notes the following:

a. 1800 Freephone numbers may be used as presentation CLI.

b. 1800 Freephone numbers may not be used as network CLI.

c. The Fixed CLI Call Blocking intervention provides for the blocking of international calls using Irish fixed numbers. Fixed numbers include 1800 Freephone so that any incoming international call using this number as presentation CLI will be blocked.

6.54 In conclusion, and for the avoidance of doubt, an end-user may use its assigned 1800 Freephone number as a presentation CLI, and this is provided for in Section 3.1 paragraph (5)(a)(i) of the Numbering Conditions. ComReg does not propose to amend this provision.

Emergency Numbers

6.55 ComReg received a request from the Emergency Call Answering Services (ECAS)[361] to permit ECAS to originate calls with 112 and 999 as presentation CLI.

6.56 The 112 number is the single European emergency number. The national emergency number 999 is a national-only number. Dialling 112 or 999 will contact ECAS when dialled on the Irish network. The 112 and 999 numbers will be collectively known as the "emergency numbers".

[360] Please note that, as 076 NGNs have now been withdrawn from service, an administrative update to the Numbering Conditions will delete references to 076 where appropriate.
[361] ECAS website

6.57 The use-case is that, where an emergency call to ECAS breaks down, ECAS may make a call-back to the emergency caller using one of the emergency numbers as CLI. This may encourage the emergency caller to answer the call-back.

6.58 ComReg considers that using the emergency number as CLI on a call-back would indeed encourage answer by the emergency caller. Therefore, ComReg proposes to permit the use of emergency numbers as presentation CLI. To that end, ComReg proposes to add the following underlined text to Section 3.1 paragraph (5)(a)(ii) of the numbering Conditions:

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

6.59 Notwithstanding its proposal to permit emergency numbers to be used as presentation CLI, ComReg recommends that this use case is considered further by ECAS and industry to ensure there are no unintended consequences in using 112/999 as presentation CLI. For example, the impact of call blocking mechanisms both here and abroad and communication among PSAPs throughout the EU should be considered further.

Q. 2 Do you agree with ComReg's general updates to the CLI Conditions as set out above? Please explain the basis for your response in full and provide supporting information.

6.4 General updates to provide CLI Guidance

6.60 In this Section, ComReg proposes a number of principles that aim to guide operators on the general use of CLI and improving the quality of CLI data. These principles include the need for authentication of the CLI on nationally originated calls and also the need for the presentation CLI to be dialable. International originated calls are also addressed. ComReg additionally explores the application of these principles in two CLI use cases that have been raised by operators, namely the use of private networks and nomadic services.

General

6.61 Regulation 97 of SI No. 444 of 2022 provides for specification of additional facilities, including CLI.[362] [363] As previously noted, the current CLI conditions are set out in Section 3.1 (5) of ComReg's Numbering Conditions[364] document. In Section 6.2 of this consultation, ComReg highlighted the suite of nuisance communications voice interventions that were agreed at the NCIT and, where necessary, proposes new or amended CLI conditions to align with these interventions.

6.62 With the increasing variety of telecoms services, including Cloud Services, that are available to end-users, operators have asked for guidance on the implementation of CLI to ensure compliance with the CLI conditions. To that end, ComReg proposes a number of principles on which these conditions are based. Furthermore, ComReg applies these CLI principles to certain use cases that have been raised by some operators.

CLI Conditions

CLI Definitions

6.63 A CLI condition is a numbering condition that is attached to the General Authorisation (a "GA Condition"). Section 2 of the Numbering Conditions provides for the following;

> *" "GA Conditions" are attached to the General Authorisation, pursuant to Regulation 8 and Part A of the Schedule to the Authorisation Regulations. GA Conditions apply equally to all authorised undertakings (or to such categories or groups of authorised undertaking as may be specified). Any authorised undertaking which uses a number must comply with the GA conditions which apply to use of that number."*

[362] S.I. No. 444 of 2022 - EUROPEAN UNION (ELECTRONIC COMMUNICATIONS CODE) REGULATIONS 2022 – Provision of additional facilities - Schedule 5 part B

[363] For the purposes of this consultation, and as previously noted, a CLI service is one that enables a called party to view the calling party's number before answer and, if needed, use that CLI information to make a call-back. The service also incorporates end-user preferences.

[364] ComReg 15/136R3 - ComReg's Numbering Conditions of Use and Application Process (Numbering Conditions) – Section3.1(5)

6.64 The presentation and network CLI types are defined in Appendix 12 of the Numbering Conditions as follows:

> *(i)* ***"presentation CLI"*** *means a number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI.*
>
> ***(ii)*** ***"network CLI"*** *means a line identity that comprises a unique E.164 number (or from which that number may be reconstructed) that unambiguously identifies:*
>
> > *(i) the Network Termination Point (NTP); or*
> >
> > *(ii) the line identity that has been provided to an individual end-user or terminal/telephone with non-fixed access to the public telephone network.*

6.65 ComReg notes that the current definitions of presentation and network CLI in the Numbering Conditions are technology neutral. Nevertheless. some operators in the NCIT have maintained that, while the implementation details for presentation and network CLI are well understood for traditional networks, the equivalent details for CLI use in IP technology are less so. ComReg's preliminary view, however, is that the current definitions in the Numbering Conditions are sufficiently clear for operators to ensure their compliance irrespective of the technologies used and that implementation details should be left for industry to discuss and agree.

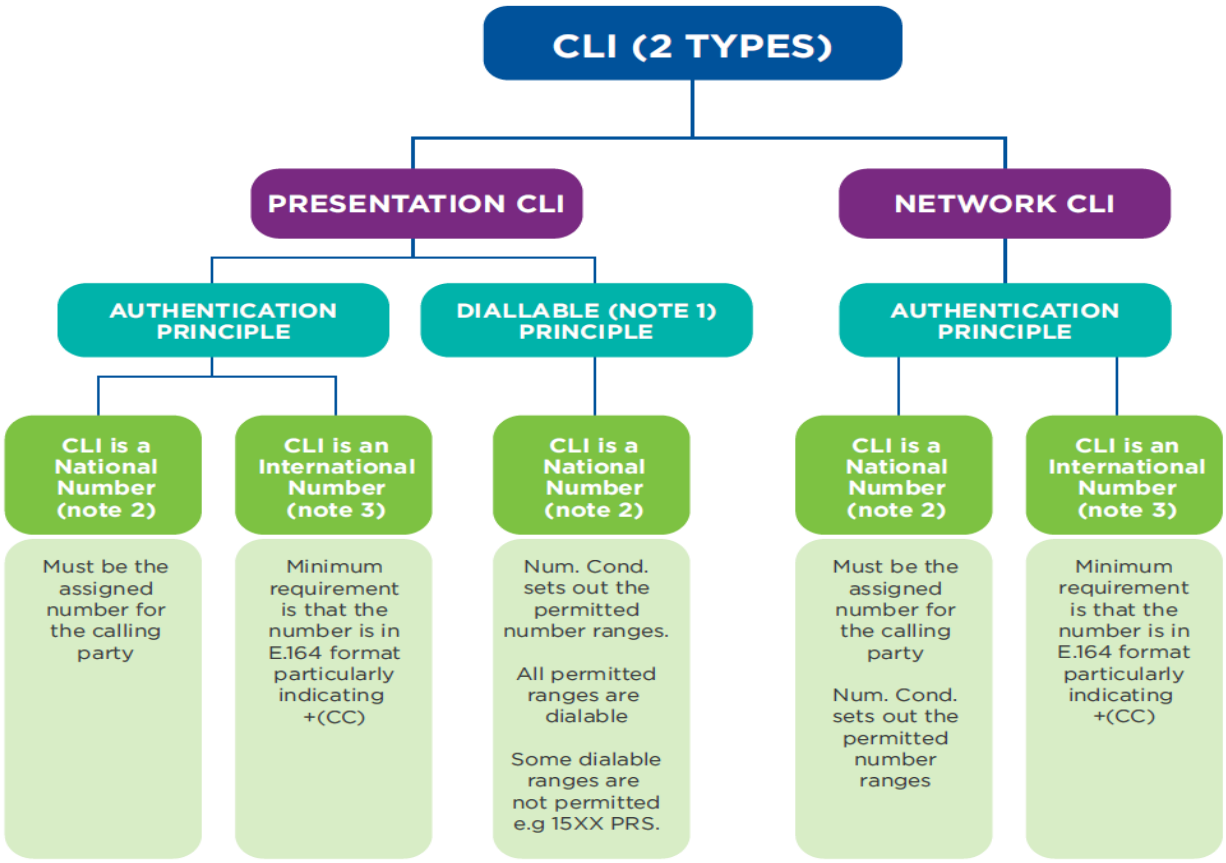
Metrics

6.66 The metrics arising from the implementation of nuisance communications interventions, such as call blocking data, are required to ensure adequate monitoring of the effectiveness of those interventions. Metrics are included in the draft technical and/or functional specifications for the interventions and no new or amended conditions of use are required to address this topic.

CLI Principles

6.67 This section addresses the CLI conditions in terms of ComReg's proposed high-level principles of CLI use. As previously noted, the presentation CLI enables a called party to view the calling party's number before answer and, if needed, use that CLI information to make a call-back. Therefore, the presentation CLI needs to be a dialable number. Another key principle is that the presentation and network CLI authenticates the calling party. The latter principle is particularly important given the recent surge in nuisance communications; an overview of these principles is provided in Figure 37Figure 37 below.

Figure 37: Overview of the CLI Principles



Note 1: International numbers may not easily be assessed as dialable
Note 2: Calls originate on the Irish PSTN only
Note 3: Calls transit onto the Irish PSTN via an IGO

6.68 This consultation seeks to clarify the use of CLI in terms of its impact on end-users. Given the upsurge in nuisance communications, any CLI service should seek to protect the calling and called parties by including the following features:

i. The presentation and network CLI must be authenticated. Authentication would enable the called party to be confident that the presentation CLI correctly identifies the caller including their location,

and they can make an informed decision on whether to answer the call or not. In the case of the network CLI, it will, in summary, uniquely identify the Network Termination Point (NTP) or line identity for the end-user; and

ii. The presentation CLI must enable a call back by the called party if they wish. This requires the presentation CLI to be dialable. All the Irish Fixed phone numbers permitted for use as presentation CLI in Ireland are valid, meaning that they are E.164 numbers, and that they are dialable.

6.69 ComReg notes that operators must support End-User (Calling and Called parties) preferences, such as Calling Line Identification Present (CLIP)[365] and Calling Line Identification Restriction (CLIR)[366]. The CLIP supplementary service provides the Called Party with the possibility of receiving identification of the calling party. The CLIR supplementary service enables the calling party to prevent presentation of their number to the called party.

6.70 As discussed in Section 4.2 of this consultation, Long-lining is a means for operators to serve their Irish customers that have international branches or call-centres that wish to use their Irish number as presentation CLI. Long-lining maintains the principle that the presentation CLI is dialable. Furthermore, the call originates on the Irish PSTN and the customer's Irish serving operator, as the originating operator, must ensure that only the customer's assigned phone number is used as presentation CLI. However Long-lining does not meet the principle of CLI authentication in terms of the location of the caller. Notwithstanding, in view of the business usage case, ComReg considers long-lining as a suitable mechanism to meet certain Irish business requirements.

Calls Originating on National Networks

6.71 With regard to CLI authentication, ComReg notes the following:

1. The originator of the call must ensure that the CLI is the calling party's assigned number;

2. An end-user cannot transfer the right to use their number as CLI to another end-user;

3. The condition that the calling party's assigned number must be used as presentation CLI allows certain flexibility for the caller. For example, a Call Centre may wish to present a particular assigned number as presentation CLI to encourage customers to

[365] ETS 300 089 – ISDN Calling Line Identification Presentation (CLIP) supplementary service; Service description
[366] ETSI 300 090 – ISDN Calling Line Identification Restriction (CLIR) supplementary service; Service description

call-back on that number. This Call Centre might also, for redundancy purposes, have several outgoing call routes, possibly across several operators at the same location. While maintaining the CLI conditions associated with for example Geographic numbers, the use of the Call Centre's assigned number as presentation CLI on calls outgoing on these routes is permitted by the CLI conditions;

4. The CLI is dialable, as each of the classes of number that are permitted as CLI are dialable. ComReg notes that some of the permitted numbers, namely the Geographic, Mobile and 0818 Standard Rate Numbers, are all internationally dialable while the remaining numbers, namely the 1800 Freephone Number and Harmonised Code of Social Value are national only dialable numbers.

Calls that Ingress onto the Irish PSTN from International PSTNs

6.72 The aim of ITU Recommendation E.157[367] ("E.157"), as set out in Section 1 of that document, is to provide *" guidance for the delivery of calling party numbers across different countries to improve their security (i.e., integrity) and minimize possible misuse, and risk of fraud and technical harm as called for by Article 42[368] of the Constitution".*

6.73 Section 3.2 of E.157 defines the Calling Party Number ("CPN") as "*the ITU-T E.164 number of the originator of the call or a special allocated number*". Section 6 of E.157 sets out that *the CPN shall be provided by the originating operator, transmitted transparently by the transit operators and received by the terminating operator. Presentation of the calling party number may be restricted by the calling party (the originator of the call) based on applicable national laws and regulations, however, the provisions of this Recommendation shall apply*". Thus E.157 requires the integrity of the call to be maintained on cross-border calls. Nevertheless, where nuisance calls are concerned, operators may take certain actions, as set out in Regulation 83(2) of SI 444[369], to tackle such calls.

6.74 Due to the current upsurge in nuisance communications, particularly from international sources, ComReg wishes to review the conditions of use associated with international CLI. To that end, ComReg notes the following:

[367] ITU Rec E.157 - **SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS International operation – Operation of international telephone services**
[368] ITU Constitution - **Constitution of the International Telecommunication Union**
[369] S.I. No. 444 of 2022 - Part 10 - Access to numbers and services

i. Section 3.1(5)(d) of the Numbering Conditions allows an operator the option of modifying an international CLI as follows;

> "*for international calls originating from outside the State, the CLI may be modified with appropriate prefixes including "00", "+" and the relevant country code*"

ii. However this option is intended to facilitate an operator who has received a trusted international call, but the CLI is not provided. There is no condition at present that requires, for example, that the CLI is in E.164 format. Such a requirement would provide a minimum, although insufficient, indication that the CLI is dialable. Therefore ComReg considers is timely to consider if mandatory conditions should be in place for international CLI.

iii. Regarding the validity of CLI on calls, Section 3.1 (5)(e) of the Numbering Conditions provides for the following:

> *" a presentation CLI may shall be marked as "Caller ID unknown" or equivalent if an operator cannot ensure that the presentation CLI information is valid"*

iv. ComReg notes that this condition implicitly applies only to international calls. This is because, as ComReg has previously highlighted in this consultation, originating operators on the Irish PSTN must ensure that the CLI is the assigned number for the calling party so that the CLI must always be valid.

v. Given the above analysis, ComReg proposes that the current Section 3.1(5)(d) and Section 3.1(5)(e) be replaced with a new Section 3.1 (5)(d) as follows;

> *"That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code". If the international call is untrusted and the CLI not in E164 format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".*

vi. Furthermore, ComReg recommends that operators enter into an understanding with their international operator partners that all reasonable efforts are made by that partner to ensure that only calls that are authenticated and dialable are transmitted.

CLI Usage Cases - Examples

i) Private Networks

6.75 According to ETSI[370] , a Private Integrated Services Network (PISN) is "*A network serving a pre-determined set of users (different from a public network which provides services to the general public). The attribute "private" does not indicate any aspects of ownership."* For the purposes of this consultation, the term fixed private network ("private network") means the provision by an operator of fixed telephony services to an organisation with a pre-determined set of end-users across various locations. Among other things, end-users of the private network are typically provided with reduced or free call costs and feature rich telephony services when communicating with each other. In other instances, the organisation may use its private network to realise call-cost savings when calling subscribers on the PSTN.

6.76 For example, the organisation's end-users could call PSTN subscribers at remote locations by "breaking-out" their call at those remote locations. Further call-cost benefits might be realised by allowing certain public network subscribers to "break-in" to the private network at one location and then break-out at another remote location, a scenario called break-in/break-out. This section of the consultation addresses the CLI used in such scenarios with reference to the principles of authentication and the presentation CLI being dialable.

ii) National Private Network

6.77 For the purposes of this consultation, a national private network is one where all the private network locations are in Ireland. In considering the previously described break-out and break-in/break-out scenarios, ComReg notes the following:

i. In the break-out scenario, a private network end-user, for example in the Cork (021) area code, may wish to call a public network subscriber at a remote location, for example in the Dublin (01) area code, by breaking out of the private network at the remote location. In this scenario, if the caller wishes to use a Geographic number as CLI then it must be their assigned geographic number for the relevant MNA[371] within the Cork (021) area code. They may also use their assigned NGN.

ii. In the break-in/break-out scenario, a public network subscriber located for example in the Cork (021) area code, may have permission to dial into a

[370] ETS 300 415 Private Integrated Services Network (PISN) – Terms and definitions-Section 4.3
[371] Minimum Numbering Area (MNA) - means one of the 106 geographic areas associated with Geographic Numbers, as defined in the "the National Numbering Plan";

local private network and break-out of that network at a remote location in, for example, the Dublin (01) area code. In this scenario, if the caller wishes to use a Geographic number as CLI then it must be their assigned geographic number for the relevant MNA[372] within the Cork (021) area code. They may also use their assigned NGN.

iii) International Private Network

6.78 For the purposes of this consultation, an international private network is one where the private network locations are in more than one country. In considering the previously described break-out and break-in/break-out scenarios, ComReg notes the following:

i. In the break-out scenario, a private network end-user, for example in the U.K., may wish to call a public network subscriber in, for example Dublin, by breaking-out from the private network in Dublin. This usage case is similar to the long-lining of an organisation's international location, such as a call centre. Therefore, on the ingress to the Irish Public network, the CLI for the caller may be their international number or an Irish number that meets the CLI conditions.

ii. In the break-in/break-out scenario, the U.K. caller's international number must be used as CLI.

Q. 3 Do you agree with ComReg's general updates to provide CLI Guidance as set out above? Please explain the basis for your response in full and provide supporting information.

i) Nomadic Services

6.79 For the purposes of this consultation, a nomadic service is one provided by an operator to an individual customer whereby that individual may use the SIP capabilities of their communications equipment (device) to make and receive calls on that device using their assigned Irish fixed phone number while travelling. For the purposes of this consultation, this individual is referred to as a nomadic user.

6.80 With regard to outgoing calls made by a nomadic user from their device, ComReg notes the following:

i. The nomadic user may use their assigned Irish number as CLI regardless of their location or where they are dialling; and

ii. In the case of the Fixed CLI Call Blocking intervention, operators must provide

[372] Minimum Numbering Area (MNA) - means one of the 106 geographic areas associated with Geographic Numbers, as defined in the "the National Numbering Plan".

a service solution for their nomadic customers that are travelling abroad and wish to use their assigned Irish number as CLI for outgoing calls to Ireland. Operators must ensure that calls from these customers only originate on the Irish PSTN. Otherwise, these calls will be blocked by IGOs under the intervention.

6.81 ComReg's preliminary view is that no amendment to the Numbering Conditions is required in respect of the use of CLI on outgoing calls from devices using nomadic services.

6.82 With regard to incoming calls to a nomadic user's Irish phone number, Section 4.1(4) of the Numbering Conditions provides for the termination of a Voice over Internet Protocol (VoIP) call outside the designated MNA for that number, thereby facilitating calls to a nomadic user's Irish numbers, irrespective of where the nomadic user is located internationally.

6.83 Therefore, in view of the sufficient support for nomadic services in the existing Numbering Conditions, ComReg does not propose to make any amendments to these conditions.

6.5 Know Your Customer

6.84 Finally, a key factor in preventing phone scams is ensuring that numbers are only assigned to customers who plan to use them lawfully. Operators providing numbers should therefore know their customers, taking into account the customer and the nature of their relationship and have processes in place to report on and deal with any issues arising with the use of those numbers. To that end, ComReg provides a guide to KYC processes which may be used in combatting nuisance communications. Although these guidelines are not mandatory, operators are encouraged to implement the suggested processes to reduce the risk of bad actors being provided with numbers. For reference, ComReg proposes to publish the KYC guidelines as a stand-alone document.

Background

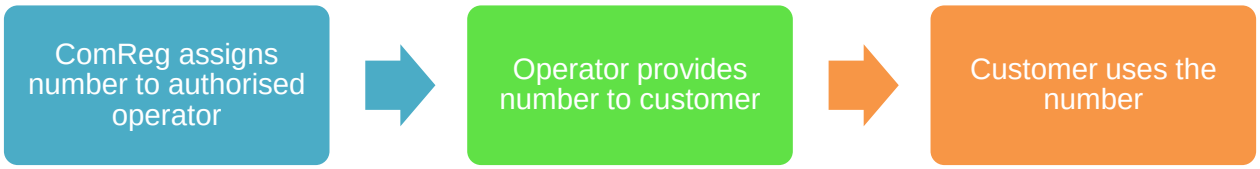
6.85 Numbers are a national resource - they must be protected and used correctly. The rules in place for the use of numbers in Ireland are set out in ComReg's Numbering Conditions. ComReg manages the national numbering resource and assigns phone numbers to authorised operators.[373] Operators in turn provide numbers to their customers (individuals and organisations) as requested.

[373] ComReg's number management function, and its objectives, duties and powers in relation to that function, are set out in the Communications Regulation Act 2002 to 2023; and the European Union

6.86 Figure 38Figure 38 sets out the typical number provision scenario. In this scenario:

- ComReg assigns phone number to an authorised operator
- Operator provides customer with number
- Customer (individual or organisation) uses the number.

Figure 38: Typical Number Provision Scenario in Ireland



6.87 Currently, if an issue arises with an assigned phone number, ComReg will contact the operator to whom the number was assigned (the "number holder"). As set out in Section 2.4 of the Numbering Conditions "*undertakings which use numbers, or which have been granted rights of use for numbers are expected to adhere to applicable international standards and established best practices in relation to numbers and number usage*." So, when numbers are assigned to operators, they are expected to ensure that those numbers are used effectively and efficiently.

6.88 Operators are therefore expected to carry out appropriate checks and safeguards before providing numbers to customers. There are very important reasons for customer checks, including the possibility for fraudsters to spoof CLIs of unassigned numbers or numbers used by well-known services such as banks. The NCIT has introduced call blocking interventions, such as the recent DNO List initiative[374], to deal with scam calls. However, fraudsters may also seek to be assigned phone numbers (i.e., those not yet in use) to facilitate their activities. From discussions at the NCIT and operator bilateral meetings, ComReg is aware of problems due to fraudsters obtaining new phone numbers. This suggests that some operators are not carrying out proper and stringent checks before providing numbers to their customers.

KYC and SIM cards

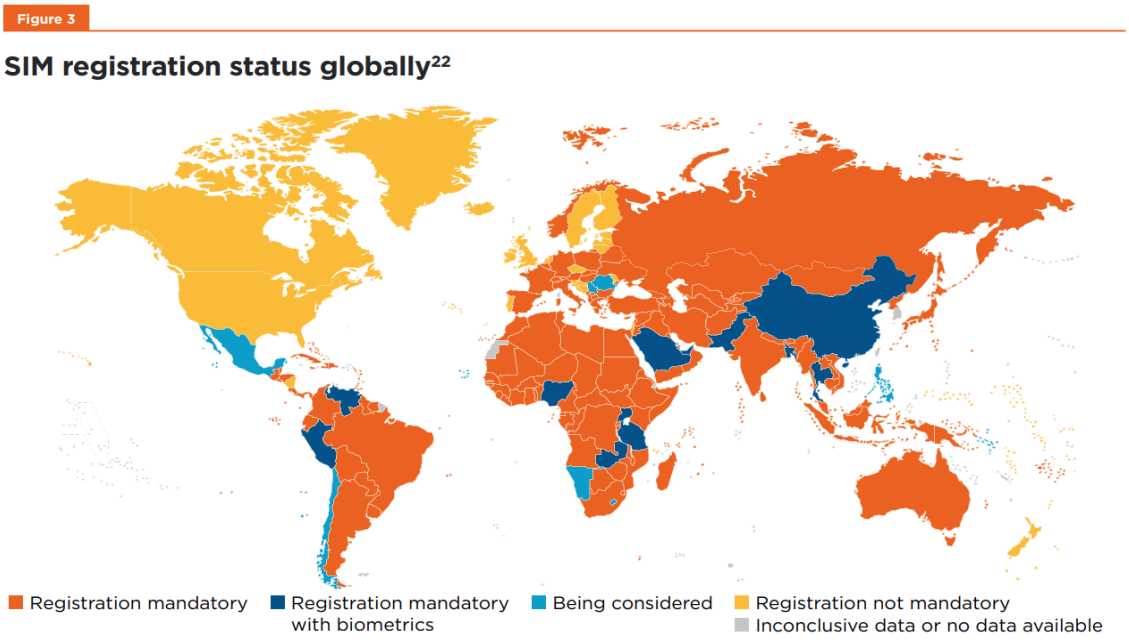
(Electronic Communications Code) Regulations 2022, which transpose the European Electronic Communications Code (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018).

[374] See https://www.comreg.ie/industry/licensing/numbering/do-not-originate-list/

6.89 Operators are expected to mitigate the risk of fraudsters accessing new phone numbers by carrying out KYC checks before providing numbers to customers. Operators are expected to establish the legitimacy of customers so that they may be identified and contacted if there are any problems. Operators therefore need to record and retain basic information on their customers[375], to protect consumers from fraud, to safeguard the operator's reputation, and to ensure that swift action may be taken in the event of any problems.

6.90 Ireland is now one of only a few countries without mandatory SIM registration (for prepaid mobiles). Mandatory SIM registration is a policy that requires MNOs to collect and/or verify their customers' identification credentials and other personal information (such as name, ID number and address) in order to register or activate a prepaid mobile SIM card in their name. As of early 2021, 157 countries require mandatory prepaid SIM registration, with 10 more countries currently considering its introduction.[376] In the majority (80%) of these countries, operators are required to collect and store this information, and only in a few countries are operators required to share and/or validate this information with the government.

Figure 39: SIM registration around the world



Source: GSMA as of 2021. Note that Sweden and Denmark now have mandatory registration (and therefore should be orange).

[375] In the case of mobile customers, it is bill pay customers that are referred to
[376] GSMA "*Access to Mobile Services and Proof of Identity 2021 Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19 April 2021"*

6.91 A number of European countries have introduced prepaid SIM registration in recent years (Austria in 2019, Denmark and Sweden in 2022) to combat scams using prepaid SIM cards. Requiring registration of newly issued SIMs is straightforward but existing SIMs pose a challenge. Any introduction of mandatory registration could be undermined by the existence of millions of prepaid SIM cards that can still be acquired and used by fraudsters to make scam calls and send scam SMS messages.

6.92 In recent years a number of National Regulatory Authorities (NRAs) have required the registration of all existing SIM cards, with unregistered SIMs being deactivated after a particular deadline. Registering existing prepaid SIM cards, either digitally (as in the Philippines)[377] or by in-person registration (as in Ghana)[378] where mobile users' queue to verify their SIMs at designated centres, is arduous. Notwithstanding, there is some early evidence of SIM registration having an impact on the prevalence of scam SMS, with the Philippine NRA reporting that complaints regarding scam SMS have fallen by as much as 90% as a result of SIM registration[379].

6.93 At present, ComReg is not minded to require the registration of existing and new prepaid SIMs, given the potential for the future use of voice and SMS firewalls and Scam filters to combat scam communications. However, should such firewalls be absent, ComReg may well need to revisit this issue.[380]

6.94 Notably, eSIM represents a fresh start of sorts for mobile user registration, as operators have few if any existing eSIM subscriptions. Operators can implement eKYC policies to ensure all 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. This would achieve many of the benefits of mandatory registration, without the administrative effort and potential confusion arising from ex-post registration. Therefore, operators should view eSIM as an opportunity to implement better KYC policies via eKYC. ComReg has discussed this matter with all MNOs and will engage further with MNOs and MVNOs on this matter.

Cloud Services

377 https://www.cnnphilippines.com/news/2022/10/10/Marcos-signs-SIM-Card-Registration-Act.html
378 'This could be done in a much better way' - Subscribers complain as long queues characterise SIM card re-registration - MyJoyOnline.com
379 For example, the National Telecommunications Commission (NTC) said the number of reports about text scams, which plagued Filipino mobile users in 2022, has plunged by over 90% after the implementation of SIM registration. Link
380 Note mandatory SIM registration is no replacement for voice or SMS firewalls, given its inability to assess legitimate traffic or act as a last line of defence. However, in the absence of such firewalls, ComReg would need to consider all potentially applicable measures.

6.95 Cloud communications services provide global delivery of voice calls, using infrastructure that can potentially be located anywhere in the world. A Cloud platform may be used to route voice calls which originate nationally or internationally to ingress the Irish PSTN via an international gateway. For example, as part of its ongoing work with the NCIT, ComReg has been made aware that approximately 200,000 voice calls per week, using Irish Geographic CLIs, are being delivered to one major Irish operator via Cloud platforms located outside Ireland.

6.96 ComReg understands that some of this traffic that ingresses the Irish PSTN may be nationally originated or may be international traffic originating from branches of Irish businesses based abroad. However, it likely also includes some scam traffic. This is because fraudsters, 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.

6.97 The NCIT has agreed to the introduction of a Fixed CLI Call Blocking intervention to address calls with spoofed fixed Irish CLIs that ingress the Irish PSTN. However, based on discussions with NCIT members at bilateral meetings, ComReg is also aware of scam calls originating from genuine numbers. These are numbers that may have been unwittingly assigned by an operator to fraudsters . One major Irish operator reported several instances where Irish Geographic numbers, which had been provided to a Cloud platform provider, had subsequently been used to commit fraud.

6.98 In response to these reports, ComReg notes the following;

- Operators, including cloud service providers, must ensure compliance with the Numbering Conditions Section 4.1(2), which 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 and cloud providers shall establish the location of their customers before providing Geographic numbers. ComReg also notes that compliance with this condition is part of the wider objective of ensuring trust in numbers.

- ComReg expects that all operators, including cloud service providers, adopt a KYC process, as set out in this section of the consultation, without delay.

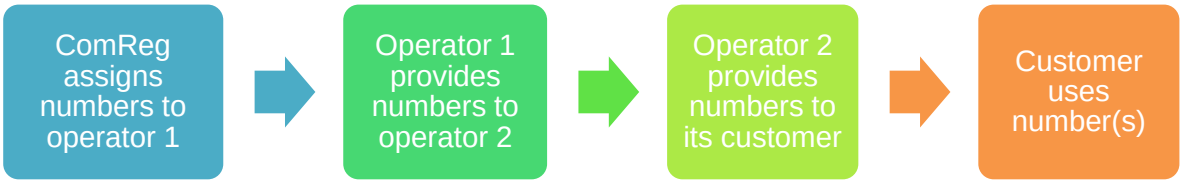
Clarification on certain number arrangements

6.99 Before setting out the KYC checks that ComReg expects operators to carry out, it is important to clarify the types of number arrangements that are permitted in Ireland and those that are not (see Figure 40). Furthermore, given the recent rapid increase in nuisance communications, ComReg proposes to amend the permitted types of number arrangement to enable more visibility and therefore better management of number use.

Figure 40: Status of certain number arrangements in Ireland

6.100 In a typical scenario for number provision, ComReg assigns a block of numbers to an operator who in turn uses these numbers in the provision of number-based services to its customers. However, ComReg is aware of an irregular delivery scenario as follows;

Figure 41: Irregular Number Provision scenario



6.101 In this scenario, Operator 1 is assigned numbers by ComReg and is therefore the number holder. Operator 1 then provides numbers to Operator 2. However, in Section 3.12 of Consultation 15/60[381], ComReg states that the terms and concepts "sub-allocation" or "secondary allocation" are not supported by legislation and are no longer used. For clarity, according to ECC report 311[382], sub-assignment is the assignment of numbering resources by an assignee to another entity that is not an end user. Therefore, number sub-assignment/sub-allocation is not permitted in Ireland. Thus, while Operator 1 remains the number holder and is therefore responsible for the conditions of use attached to those numbers, it is Operator 2 that is using those numbers. In ComReg's view this scenario is inappropriate as it creates unnecessary complexity for the number holder in ensuring compliance with the Numbering Conditions.

6.102 To simplify the management of the use of numbers, ComReg proposes that the operator serving the customer, i.e., Operator 2 in the irregular scenario above, must apply to ComReg for the necessary numbers. This would enable the number holder to have the greatest visibility of the use of phone numbers as it would have a direct relationship with the customer.

6.103 In response to questions raised by operators concerning the use of the number transfer process, ComReg notes Section 8 paragraph 1 of the Numbering Conditions in this regard. This outlines that ComReg may grant a right of use for any class or description of number to any undertaking, as ComReg considers appropriate, and that ComReg shall specify whether such a right may be transferred by the holder and under what conditions.[383] Thus, number transfers are permitted in Ireland.

[381] ComReg 15/60 "Numbering Conditions of Use and Application Process". Consultation document - Section 3.12 "Transfer of numbers between operators".
[382] ECC Report 311 - Sub-assignment and number hosting - Implementation models, rights of use and obligations for E.164 numbers across the electronic communications supply chain
[383] Formerly Regulation 13(1) and 13(6) of the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2011 (S.I. 335/2011), now Regulation 10(1) of, and Part E of Schedule 1 to, the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022).

6.104 Furthermore, in relation to number transfers, Section 8 paragraph 3 of the Numbering Conditions sets out that a transfer occurs when two undertakings agree that one will transfer rights of use of its numbers to the other and such transfers usually occur in bulk i.e., several hundred or several thousand numbers are transferred at the same time. The envisaged use cases for number transfer are, for example, to enable the transfer of rights of use of large blocks of mainly unused numbers between operators or where the number holder had no need for the assigned numbers, for example due to cessation of trading or market exit. In the case of individual 1800/0818 NGNs, unused numbers should be terminated and made free for assignment to another authorised operator on the PortingXS system. As indicated in Section 8 paragraph 4 of the Numbering Conditions, number transfers do not replace or change the typical number assignment or number porting processes. Furthermore, for the avoidance of doubt, the transfer process is not intended as a substitute for sub-assignment.

6.105 In view of the arguments set out above that the operator serving a customer should apply to ComReg for its own numbers rather than receive those numbers from another operator, ComReg proposes the following amendment to Section 7.1 of the Numbering Conditions;

(2) Undertakings are obliged to only use their assigned numbers for their own end-users. Sub-assignment to other undertakings is not permitted.

6.106 With regard to the retrospective application of this proposed condition, ComReg notes that it does not currently have sufficient data on the extent of such number use by operators to determine the proportionality of retrospective action at this time. Therefore ComReg proposes that the condition shall apply from the date set out in the D.I. for the Numbering Conditions update but may return to this issue.

Know Your Customer – Guidance Document

6.107 ComReg proposes a draft KYC Guidance document that sets out the minimum KYC checks that ComReg expects operators to carry out when providing numbers to customers. This Guidance will also set out the steps operators are expected to take to monitor number use and to report potential number misuse.

6.108 The proposed Guidance will include the following Sections:

- Know Your Customer checks before number provision
- Monitoring compliance and assessing number misuse risk
- Responding to misuse incidents ComReg considers that the proposed

KYC checks do not place additional burdens on operators beyond those set out in the Numbering Conditions and which operators should already be meeting.

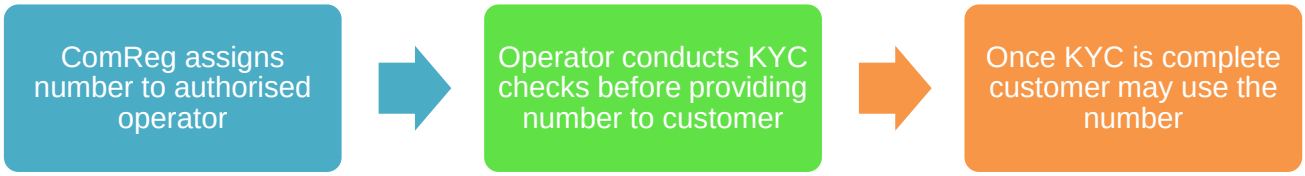
6.109 The proposed KYC Guidance is intended for use by all authorised operators (fixed and mobile) who provide Irish phone numbers[384] to customers. For the avoidance of doubt, authorised operators includes cloud service providers that are an Electronic Communications Service/Electronic Communications Network and provide phone numbers as part of their service.

6.110 The proposed KYC Guidance document is as follows:

KYC – Guidance Document

6.111 Operators are expected to conduct KYC checks before providing phone numbers[385] to customers. They must establish the bone fides of customers and be able to identify and contact those customers, and to ensure that regulatory obligations are met (see Figure 42).

Figure 42: Know Your Customer checks before number provision



6.112 Some customers may need more stringent KYC checks than others e.g., an organisation requesting a batch of numbers will need more rigorous checks than an individual customer requiring a single phone number.

6.113 Operators are expected to carry out the following minimum KYC checks before providing Irish phone numbers to customers (See below):

Figure 43: Minimum Know Your Customer checks before number provision

KYC checks for Individual Customers	KYC checks for Organisation/Business Customers
• Customer name • Customer address (including Eircode) * • Contact email • Contact phone number	• Contact name • Organisation/business name (registered name and trading name) • Registered office address (including Eircode) * • Business address (if different from registered office address)

[384] Geographic, Non-Geographic and mobile numbers (bill-pay).
[385] Geographic, Non-Geographic and mobile numbers (bill-pay).

	• Nature of business • Existing phone numbers and business websites • Contact details of senior manager with responsibility for numbering e.g., email address and direct phone number • Information about the business customer's network and services provided • Volume of number requests versus intended use of numbers • Confirm business information - Companies Registration Office number, Revenue VAT or business number and/or a partnership/sole trader's VAT number.
* Geographic Numbers may only be provided to customers whose residence/business premises is located within the relevant Minimum Numbering Area.	

6.114 Regarding specific types of numbers, as set out in the Numbering Conditions Section 4.1(2), **"*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 and cloud providers shall establish the location of their customers before providing Geographic numbers.

6.115 In the case of Non-Geographic Numbers (1800 Freephone and 0818 Standard Rate), Section 4.3(2), of the Numbering Conditions sets out that "*An authorised undertaking shall only be granted the Rights of Use of 1800 Freephone Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for together with the end-user's unique identifier*". Section 4.4(2) of the Numbering Conditions sets out a similar condition in respect of 0818 phone numbers. In addition, the order shall include certain customer business information as also set out in sections 4.3 and 4.4 of the Numbering Conditions. This order shall form the basis of the KYC check before providing NGNs to customers.

6.116 Operators are also expected to check how business customers plan to use the numbers provided to them. If additional numbers are requested, further checks should be conducted. The level of checks will depend on the scale of the additional number request.

6.117 Operators should ensure that they are not providing numbers to high-risk customers. Indicators include:

- Incorrect, incomplete, inaccurate information about the intended use of numbers or contact details
- Volume of the request for numbers does not match the intended use of numbers (e.g., volume of numbers requested is not consistent with the intended use)
- Previous complaints about numbers provided to the business customer
- Unusual activity on existing customer numbers e.g., high volume of calls/SMS, especially where the calls are short or often dropped.

6.118 Operators are expected to make their KYC check processes clear to their customers and document the checks they carry out before providing numbers to customers. A senior manager should oversee that numbers are only provided in accordance with the operator's KYC process. If a potential risk is identified, the senior manager should decide if numbers are to be provided and document the reasons for same.

Monitoring compliance and assessing number misuse risk

6.119 Operators are expected to have a process in place to monitor the risk of number misuse and to deal with non-compliant behaviour. Contracts with customers should set out that numbers must be used in compliance with the Numbering Conditions.

6.120 Operators are also expected to review the level of risk posed by their customers and monitor for potential misuse of numbers. Reviews should be tailored to the customer (e.g., customer using many numbers will need more checks than a customer using only a small volume of numbers) and any risks that have been identified.

6.121 As set out in Section 3.1 (5) of the Numbering Conditions, operators shall carry out CLI-Analysis on all originated calls to authenticate the calling party. Operators should check the volume and duration of outbound calls generated by their customers and routed through the operator's network. Testing frequency should be based on the level of risk associated with each customer, e.g., a business customer with no history of number misuse will likely need less frequent monitoring than one for whom number misuse may have arisen.

6.122 Risk assessments should be reviewed by operators on an ongoing basis, and if there are any significant changes[386], they should be updated.

6.123 Operators are also expected to have robust procedures to address non-compliant customer behaviour. If there is a report of number misuse, the operator should first engage with the customer to understand the nature of the problem and consider how to resolve it. This may require increased monitoring and supervision of that customer's number use or, if appropriate, the suspension or withdrawal of numbers from the customer.

Responding to Number Misuse Incidents

6.124 Operators are expected to deal with number misuse incidents quickly and proactively, to reduce the potential for consumer harm. Operators should have a process for handling complaints of potential and actual misuse of numbers, and to record investigations, actions, and outcomes.

6.125 Consumers and organisations should be able to notify operators quickly and easily of suspected number misuse incidents. Complainants should also be made aware of the outcome of any misuse incident as soon as possible.

6.126 Operators are expected to review and examine any evidence received about potential misuse before taking action. They should consider the severity and impact of the incident, and work with other organisations, e.g., law enforcement, as appropriate. If an operator has been informed of or identified a potential concern, it should take action to prevent number misuse. This may include temporarily blocking numbers or customer accounts, suspending services, or withdrawing numbers. Action should always be proportionate to the evidence the operator has received and the potential risk.

[386] E.g., if the operator receives complaints about the business customer's use of numbers, if the business customer refuses to engage with the operator or is reluctant to provide information, or if there are any major changes to the business customer's company structure e.g., buying or merging with another company.

6.127 Operators are expected to put in place contractual controls to prevent numbers being misused. They should also provide support and information to any affected customers, cooperate with ComReg, other regulators, law enforcement and other relevant organisations.

6.128 If an operator becomes aware of an incident of number misuse, they are expected to report it to ComReg for potential enforcement action. Such incidents include

- Incidents where there was significant consumer harm
- Repeat incidents with a particular customer
- Misuse incidents that were not investigated in a timely or appropriate manner.

6.129 Operators should routinely review their number provision processes to ensure they are robust and up to date. This should include updating processes to incorporate lessons learned from previous misuse incidents.

6.130 As part of any investigation into number misuse, ComReg may contact operators and request information on or audit operators' KYC processes.

Q. 4 Do you agree with ComReg's views on KYC and the proposed draft Know Your Customer Guidance document ? Please explain the basis for your response in full and provide supporting information.

6.6 Future Number Management – Needs and Developments

Background

6.131 ComReg's overarching function is to manage the national numbering resource by, among other things, encouraging efficient and effective use of these resources. Nuisance communications is an ongoing problem for the Irish consumer and ComReg needs to address the misuse of phone numbers as part of its management function. Currently, fraudsters, often from abroad but not exclusively so, can place thousands of calls or SMS to consumers at low cost, often without reprimand.

6.132 ComReg must help restore trust in Ireland's telecommunications services by taking an active and enduring role in preventing nuisance communications. Therefore options for developing national numbering management should be based on increasing effectiveness and efficiency and must also address the evolving nature of nuisance communications.

Number Assignment Process

6.133 ComReg currently assigns geographic numbers in blocks of 1000 and 100 numbers, and mobile numbers in blocks of 100,000 numbers. Number applications are submitted by PDF/paper to ComReg and, if the application is successful, ComReg issues assignment schedules by email to the applicant. This is a manual process which would benefit from automation particularly if it helped industry to combat nuisance communications.

6.134 In 2019, an Individual Number Assignment (INA) system was introduced to initially facilitate the migration of many thousands of subscribers on legacy 1850, 1890 and 076 NGNs to new 1800 and 0818 numbers. A key benefit of the INA is the replacement of the manual assignment process for NGNs with an automatic system. There is no requirement for manual intervention by ComReg as the INA provides an automatic and controlled process for operators to self-help in the assignment of individual 1800 and 0818 NGNs. Another benefit is the rapid opening up of assigned NGNs on telecoms networks. This system rapidly reduced the time between an NGN application being made and an assigned NGN being made live on networks, thereby allowing the operator to quickly provide services to its customers.

6.135 Furthermore, to manage the efficient use of numbers, applicants may only apply for an NGN on the basis of a customer order. The importance of this requirement has been highlighted by the increase in nuisance communications and the need to prevent bad actors being assigned numbers. The benefit of KYC in this regard is explored in the previous Section in this consultation.

6.136 ComReg will continue to seek to improve the systems and processes for managing the national numbering resource. The benefits realised by the INA system for NGNs i.e., automated number assignment while maintaining the efficient use of numbers through the use of mandatory customer orders, needs to be explored further in respect of other classes of number.

Nuisance Communications

6.137 In considering the current approach to nuisance communications, the NCIT[387] recognises that the current voice interventions are static and only address specific current tactics being deployed by fraudsters. For example, the DNO, Protected Number and Fixed/Mobile CLI Call Blocking interventions all deal with some calls from overseas that are 'spoofing' Caller IDs to look like Irish telephone numbers. But this is only one tactic being deployed by fraudsters, and these interventions will likely be overcome.

6.138 Therefore, the need to combat nuisance communications will be a key priority for ComReg in considering improvements to its number management systems and processes. The introduction of the Protected Numbers intervention, which block calls from unassigned numbers, has resulted in the blocking by operators of large numbers of scam calls on their networks. Nevertheless, this intervention relies on the current block assignment process which does not allow visibility of the status of individual numbers. If a more granular view was available, then a greater quantity of unassigned numbers would be viable for blocking by industry.

6.139 The challenge for ComReg and industry is to agree on suitable systems and processes to automate the number assignment process as much as possible while including requirements to combat nuisance communications. For example, a network might only permit the routing of calls from authenticated individual numbers. It would also incorporate more dynamic interventions that would address for example scam calls from numbers that had been inadvertently assigned to "bad actors".

Stir/Shaken

6.140 Spoofing caller IDs continues to be a major problem and a source of significant harm to Irish consumers. As part of its work on nuisance communications, ComReg will review and assess the potential impact of technology solutions which may help to reduce caller ID spoofing. Some of the solutions addressed in this consultation include emerging technologies such as voice policy engines and voice firewalls.

[387] ref

6.141 In Section 4.2 of this consultation ComReg assessed STIR/SHAKEN as a potential voice intervention. STIR/SHAKEN is a technology framework designed to help reduce CLI spoofing through implementation of CLI authentication. It takes a standards-based approach, comprising a suite of protocols and procedures. The purpose of CLI authentication is to provide a mechanism by which the terminating network can be assured that the CLI data received, along with call, has been input by a known party and has not been tampered with during transmission to the called party.

6.142 Following its assessment, ComReg considered STIR/SHAKEN as a potential long-term global solution for CLI validation. However, ComReg also set out its preliminary view that STIR/SHAKEN is not a valid regulatory option for the purpose of this consultation, and consequently is not considered further at this time. Nevertheless, ComReg considers that the introduction of STIR/SHAKEN in Ireland may have some merit, as a potential solution to reduce consumer harm from spoofed CLIs. ComReg therefore intends to monitor developments of this technology, as well as international deployments of STIR/SHAKEN, in order to better inform its views.

Summary

6.143 In summary, Ireland needs a Call Authentication Framework, which incorporates dynamic and evolving interventions to deal with the ever-evolving threat of nuisance communications.

6.144 As an example of future interventions and measures, the NCIT should progress from static interventions to outsourcing the role of blocking scam calls and SMS to specialist firewall providers who have the expertise to keep up with fraudsters. These firewalls might, for example, use Artificial Intelligence (AI) and machine-learning to detect patterns of calling and scrutinise multiple parameters before deciding to block a call or text. Some of this blocking intelligence might also automatically be crowd-sourced from consumers, who install an app on their mobile phone, in return for availing of call/text blocking services. Number authentication frameworks such as STIR/SHAKEN will also be evaluated.

6.145 Advancing to modern numbering systems and processes, as well as implementing number authentication governance frameworks and technologies are integral to the fight against nuisance communications and crime in general.

Q. 5 Do you have any views on ComReg's assessment of future number management as described? Please explain the basis for your response in full and provide supporting information.

Chapter 7

7 Draft Decision Instruments

7.1 This chapter sets out ComReg's draft Decision Instruments, together with Intervention Annexes, based on the views expressed by ComReg in the preceding chapters and their supporting Annexes.

7.2 As most provisions of the Communications Regulation and Digital Hub Agency (Amendment) Act 2023, and S.I. No. 444 of 222, the European Union (Electronic Communications Code) Regulations 2022, namely the legislation transposing the European Electronic Communications Code in the State have now been commenced by the Minister for Communications, as at the time of publication of this consultation, so therefore, the Decision Instruments below refer to the Code legislation as appropriate, as opposed to the 2011 set of Regulations.

7.1 Draft Decision Instrument for Do Not Originate (DNO)

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Block" means to prevent a call from terminating, with a tone;

"Commission" or "ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"DNO list" means a list of numbers maintained by ComReg of telephone number assigned to organisations which are never to be used for outgoing calls

"DNO number" means a number on the DNO List

"E.164 number" means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"Originating Voice Operator” or “OVO” means an Irish Undertaking originating calls on the Irish PSTN capable of terminating on public networks;

“Presentation CLI” means a number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Public Switched Telephone Network” or “PSTN” is the collection of global telephone networks which provide services available to the public for originating and receiving national and international calls and access to emergency services using E.164 telephone numbers.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter];

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely those undertakings that are:

- either OVOs or IGOs; and

- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all calls that use a number on the DNO List as a Presentation CLI;

b. update their blocking systems with the DNO numbers which are to be blocked no later than two working days after receipt from ComReg of updates to the DNO List;

c. record the daily number of:

i. calls blocked under (1) a; and

ii. all calls completed by the undertaking; and

d. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked under (1) a; and

ii. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply as from the date of the making of this Decision Instrument and shall be implemented no later than six months after the date of making of this Decision Instrument

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.2 Draft Decision Instrument for Protected Numbers

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"Originating Voice Operator” or “OVO” means an Irish Undertaking originating calls on the Irish PSTN capable of terminating on public networks;

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Protected Numbers” means telephone numbers which have not been assigned by ComReg;

“Protected Numbers List” means a list of Protected Numbers, managed by ComReg;

“Public Switched Telephone Network” or “PSTN” is the collection of global telephone networks which provide services available to the public for originating and receiving national and international calls and access to emergency services using E164 telephone numbers;

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- either Originating Voice Operators or IGOs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all calls that use a number on the Protected Numbers List as a Presentation CLI;

b. update their blocking systems with the Protected Numbers which are to be blocked no later than two working days after receipt from ComReg of updates to the Protected Numbers List;

c. record the daily number of:

iii. all calls blocked under (1) a; and

iv. all calls completed by the undertaking; and

d. provide to ComReg, on a monthly basis no later than 10 working days from the final day of the calendar month, the daily number of:

v. all calls blocked under (1) a; and

vi. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply as from the date of the making of this Decision Instrument and shall be implemented no later than six months of the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.3 Draft Decision Instrument for Fixed CLI Call Blocking

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“E.164 number” means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"Fixed Numbers” means Irish numbers which are Geographic Numbers (numbers linked to a particular geographic region that is identifiable from the area code) or Non-Geographic Numbers;

“Geographic Numbers” means a telephone number that are linked to a particular geographic region that is identifiable from the area code;

“International Gateway Operator” or “IGO” means an Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

“M2M” means Machine to Machine;

“Mobile Service Provider” or “MSP” means an Irish Undertaking providing End Users with land based/terrestrial publicly available mobile telephony services using a mobile network;

‘MSRN’ means Mobile Station Roaming Number;

“Non-Geographic Numbers” means a telephone number that is not linked to a particular geographic location identifiable from the number;

“PSTN” or “Public Switched Telephone Network” means any network providing transmission and switching functions as well as features which are available to the general public, not restricted to a specific user group. The PSTN provides access points to other networks or terminals only within a specific geographical area;

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- IGOs; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all inbound international calls where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 fixed number except where:

i. the called party number for the call is an Irish E.164 number assigned for use for MSRN.

ii. the Presentation CLI for the call is an Irish E.164 number from the 088 range assigned for M2M applications;

b. record the daily number of:

i. calls blocked as a result of the Fixed CLI Call Blocking; and

ii. all calls completed by the undertaking; and

c. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked as a result of the Fixed CLI Call Blocking; and

ii. all calls completed by the undertaking.

(2) Relevant undertakings that are Mobile Service Providers shall inform ComReg three months in advance of any changes to their Irish MSRN number ranges.

PART V– EFFECTIVE DATE

Decision (1) to (2) above (applicable as described to Relevant undertakings) shall apply as from the date of the making of this Decision Instrument and shall be implemented by no later than six months from the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.4 Draft Decision Instrument for Mobile CLI Call Blocking

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Block" means to prevent a call from terminating, with a tone;

"Commission" or "ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"E.164 number" means a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"E.146 Mobile Number" means a mobile number that has a string of decimal digits that satisfies the three characteristics of structure, number length and uniqueness specified in Annex A of ITU-T Recommendation E.164. The number contains the information necessary to route the call to a specific termination point associated with this number;

"International Gateway Operator" or "IGO" means an Irish Undertaking providing the conveyancing of call traffic from international PSTNs to the Irish PSTN;

"IP" means Internet Protocol;

M2M means "Machine to Machine";

"MAP Protocol" means a Signalling System No. 7 ('SS7') Mobile Application Part protocol;

"Mobile Number" means a number assigned to the use of Mobile telephony services, primarily for P2P communications (e.g., 083, 085, 086, 087 and 089);

"Mobile Service Provider" means an Irish Undertaking providing End Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network;

MSRN means "Mobile Station Roaming Number";

“Presentation CLI” means number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI;

“Public Switched Telephone Network” or “PSTN” means any network providing transmission and switching functions as well as features which are available to the general public, not restricted to a specific user group. The PSTN provides access points to other networks or terminals only within a specific geographical area;

“Roamer check” means the facility provided by MSPs to IGOs, through the use of network signalling protocols and for the purposes of verifying whether the Presentation CLI of an international call is from an Irish mobile user who is roaming internationally;

“Roaming Proxy Server” means an interworking facility operated by MSPs with the purpose of handling Roamer check queries without requiring IGO direct access to individual MSP networks;

“VoLTE” means Voice over Long Term Evolution, that is, a managed voice service that benefits from prioritisation over other traffic.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is hereby made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- IGOs and MSPs; and

- deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. block all inbound international calls where the Presentation CLI for the call is a validly formatted or malformed Irish E.164 mobile number, except where the:

i. the user of the mobile number has been determined, by the IGO or another undertaking on its behalf, to be roaming internationally, by verifying against the Roamer Check facility of the user's MSP.

ii. the called party number for the call is an Irish E.164 number assigned for use as a MSRN.

iii. the Presentation CLI for the call is an Irish E.164 number from the 088 range assigned for M2M applications.

b. record the daily number of:

i. calls blocked under (1) a; and

ii. all voice calls completed by the undertaking.

c. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of:

i. calls blocked under (1) a; and

ii. all voice calls completed by the undertaking.

(2) Relevant undertakings that are MSPs shall:

a. provide a Roamer Check facility based on use of MAP protocol to all requesting IGOs; and

b. ensure that ComReg is informed three months in advance of any changes to their Irish MSRN number ranges.

(3) Relevant undertakings that are MSPs shall implement:

a. the Roaming Proxy Server; and

b. upgrade the Roamer Check to include VoLTE check capability.

PART V– EFFECTIVE DATE

Undertakings that are IGOs shall implement Mobile CLI blocking, that is Decisions (1) and (2) above, no later than six months of date of the making of this Decision Instrument.

Undertakings that are MSPs will implement Decision (3) no later than two years of the date of the making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.5 Draft Decision Instrument for Voice Firewall Specification

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

“2002 Act” means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

“2022 Regulations” means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

“2023 Act” means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

“Block” means to prevent a call from terminating, with a tone;

“Classification” means assigning each terminating call into one of multiple categories of probability that such a call is a Scam call;

“Commission” or “ComReg” means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

“Fixed Service Provider” or “FSP” means an Undertaking providing End-Users with publicly available voice telephony services using a Fixed Number at a fixed location, irrespective of the underlying technology over which such services are delivered;

“M2M” means “Machine to Machine”;

“MBB” means a wireless broadband connection delivered via a mobile network;

“Mobile Service Provider” or “MSP” means an Undertaking providing End-Users with land based/terrestrial publicly available mobile voice telephony services using a mobile network;

“Modify” or “Modified” means to allow the call, set the presentation CLI indicator to restricted and where technically feasible send the caller display name as “Likely Scam”;

“Network FSP” means an FSP that operates a network for the purposes of providing End-Users with publicly available voice telephony services using Fixed Numbers at a fixed location, irrespective of the underlying technology over which such services are delivered;

“Network MSP” means a MSP that operates a 2nd, 3rd, 4th, or 5th Generation digital wireless network, or any intermediate evolution of those, using Mobile Numbers, in which seamless handover and roaming features are provided;

“Scam Calls” mean voice calls aimed at defrauding end users by deceiving them into revealing personal or financial details, taking actions that would cause them to be defrauded and/or into making a payment;

“Voice Capable Subscriber” means a subscriber to Voice Capable Subscription;

“Voice Capable Subscription” means any mobile subscription or fixed line that is capable of originating and terminating a voice call on a public network;

“Voice Firewall” means a network platform that monitors in real-time each terminating call and provides a Classification for these calls using a process incorporating the use of data including signalling information for the call, patterns of traffic volumes and call durations, and phone number data.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. having had regard to its powers, functions, objectives and duties, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to its statutory objective under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to its statutory objective under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to its general objective under regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard to its duty under regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached.

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely undertakings that are:

- MSPs or FSPs with over 330,000 Voice Capable Subscribers (except those MSPs or FSPs whose requirements below are satisfied by a Network MSP and/or Network FSP); and

- deemed to be authorised under Regulation 6 of the 2022 Regulations.

Relevant Undertakings who are also a Network MSP and/or Network FSP shall satisfy the requirements below for other Undertakings who are MSPs and/or FSPs and for whom they provide a voice call origination and termination service, where technically feasible.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) Relevant undertakings shall:

a. use a Voice Firewall:

i. to identify any terminating voice calls that have a Classification with the highest probability of being a Scam Call; and

ii. to identify any terminating voice calls that have a Classification with a high probability of being a Scam Call other than the highest probability of being a scam call.

b. block all terminating voice calls that have a Classification with the highest probability of being a Scam Call;

c. Modify all terminating voice calls that have a Classification with a high probability of being a Scam Call that is other than the highest probability of being a scam call

d. record the daily number of

i. all calls blocked under 1 (b) and modified under 1 (c); and

ii. all calls completed by the undertaking.

e. provide to ComReg, on a monthly basis no later than ten working days from the final day of the calendar month, the daily number of

i. all calls blocked under 1 (b) and modified under 1 (c); and

ii. all calls completed by the undertaking.

PART V– EFFECTIVE DATE

The Decisions above (applicable to Relevant undertakings as described) shall apply as from the date of the making of this Decision Instrument and shall be implemented no later than 18 months of the date of making of this Decision Instrument.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.6 Draft Decision Instrument for Sender ID Registry

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"Block" means to prevent a SMS from originating or terminating or being transited or forwarded;

"ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"ComReg Quarterly Key Data Report" means the statistical data collected by ComReg from authorised undertakings on a quarterly basis, and published on ComReg's website on a quarterly basis;

"Directly Connected" means that the computer system which originates SMS within the SIDO or its third-party technical contractor, uses and maintains a connection at the application protocol level, directly with the systems which accept SMS within the PA;

"MBB" a wireless broadband connection delivered via a mobile network;

"Mobile Service Provider" or "MSP" means an undertaking providing End-Users with land based/terrestrial publicly available mobile telephony services using a mobile network;

"Modify" means that the Sender ID is replaced with "LikelyScam";

"Network MSP" means a MSP that operates a 2nd, 3rd, 4th, or 5th Generation digital wireless network, or any intermediate evolution of those, using Mobile Numbers, in which seamless handover and roaming features are provided;

"Non-Participating MSP" means an MSP which has not deployed the necessary technical filtering function and business processes to enable it to accept A2P messages bearing a Sender ID from one or more PAs;

"Participating Aggregator" or "PA" means a SMS Aggregator that is permitted to transit or forward a SMS carrying a Registered Sender ID from the SIDO to one or more MSPs within Ireland;

"Participating MSP" means an MSP in the state which has deployed the necessary technical filtering functions and business processes to enable it to accept A2P messages bearing a Sender ID from one or more PAs;

“Registered Entities” means the SIDO, Registered PA and Registered MSP for a given Registered SMS Sender ID;

“Registered MSP” means a MSP that is permitted to transit or terminate a SMS carrying a Registered Sender ID;

“Registered PA” means the Participating Aggregator that is permitted to transit a SMS carrying a particular Registered Sender ID;

“Registered Sender ID” means a Sender ID which is registered with ComReg for use in terminating SMS;

“Securely Authenticated” means the process of verifying the identity of the sender using technical means such as a secure username/password combination or other cryptographic means;

“Sender ID” means an alphanumeric originating address sent in SMS messages.;

“Sender ID owner” or “SIDO” means the entity to which a Sender ID is assigned by ComReg for use with transiting or terminating SMS. A SIDO could contract a third party to send their messages via an PA rather than send them directly;

“Sender ID Registry” means the register managed by ComReg of all Registered Sender IDs, SIDOs and the Registered Entities which may transmit or terminate specific Registered SMS Sender IDs;

“SMS Aggregator” means a service provider that acts as an intermediary between businesses or individuals (SIDOs) that wish to send A2P (Application to Person) SMS messages, and an SMSC function within mobile telecommunication networks;

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. Having had regard to the powers, functions, objectives and duties of ComReg, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of 2022 Regulations, for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to ComReg's statutory duty under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to ComReg's statutory duty under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to ComReg's general objective under Regulation 4(3) of the 2022 Regulations of promoting the interests of consumers and businesses in the State by maintaining the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services) and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. having regard, inter alia, to ComReg's duty under Regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

j. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

k. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Regulation only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

l. having considered all relevant evidence before it, including from Voluntary Information Requests;

m. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

n. having regard to the consultants' reports commissioned in relation to this matter;

o. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to relevant undertakings, namely those undertakings that are:

- MSPs with over 270,000,000 Mobile Subscribers, excluding M2M and MBB, and Participating Aggregators; and
- deemed to be authorised under Regulation 6 of the 2022 Regulations.

Relevant Undertakings who are also a Network MSP shall satisfy the requirements below for other Undertakings who are MSPs and for whom they terminate SMS, where technically feasible.

PART IV - THE DECISIONS

ComReg hereby makes the following decisions:

(1) When delivering an SMS with a Sender ID, relevant undertakings that are Participating MSPs shall Modify the Sender ID where that Sender ID:

a. is not registered; or

b. is registered, but sent by a source other than the Registered PA or a participating MSP.

(2) When delivering an SMS with a Sender ID, relevant undertakings that are Participating MSPs shall block the Sender ID where that Sender ID:

a. is not registered; or

b. is registered, but sent by a source other than the Registered PA or a participating MSP.

(3) Relevant Undertakings that are Participating MSPs shall apply the same treatment as in (1) and (2) to all SMS except for SMS sent to:

a. visitors within the State who are roaming; and

b. their own end users roaming in another country, where not technically feasible.

(4) Following any updates to the SMS Sender ID Registry, and within five working days, update all information related to the Registered Entities used by the undertaking to achieve (1) and (2).

(5) Relevant Undertakings that are PAs shall:

a. Implement direct connections to SMS infrastructure of one or more Participating MSPs.

b. Block any SMS destined for an Irish number with a Sender ID which is not registered to the associated directly connected SIDO which has been Securely Authenticated.

c. Forward any SMS destined for an Irish number with a Sender ID which is registered to the associated directly connected SIDO which has been Securely Authenticated, to a Participating MSP via the direct connection(s) referred to in (a) above.

(6) All undertakings shall:

a. Record the daily number of SMS with a sender ID destined for Irish numbers:

i. which have been blocked or modified for each Sender ID; and

ii. which were not blocked or modified for each Sender ID;

b. provide to ComReg, on a monthly basis no later than 10 working days from the final day of the calendar month, the daily number of SMS with a sender ID destined for Irish numbers:

i. which have been blocked or modified for each Sender ID; and

ii. which were not blocked or modified for each Sender ID;

(7) Undertakings that are MSPs must block any SMS bearing an originating number in the Irish number range, fixed, mobile or a short code, when presented for delivery from an SMSC which is not operated by an Irish MSP.

PART V– EFFECTIVE DATE

Decision (1) (3) and (4) above shall apply 12 months after the date of the making of this Decision Instrument, for a period of 6 months.

Decision (2) above shall apply 18 months after the date of the making of this Decision Instrument.

Decisions (5) (6) and (7) above shall apply on the date of 12 months after the date of the making of this Decision Instrument.

All other Decisions in this Decision Instrument shall be construed in accordance with these dates.

PART VI – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VII - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

7.7 Draft Decision Instrument for Numbering Conditions of Use and Application Process

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022)

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023;

"ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and this Decision Instrument.

PART II – LEGAL BASIS

This Decision Instrument is made by ComReg:

a. Having had regard to the powers, functions, objectives and duties of ComReg, including, without limitation, those specifically listed below;

b. pursuant to its power under Regulation 83(2) of the 2022 Regulations to require providers of public electronic communications networks or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reason of fraud or misuse;

c. pursuant to its power under Regulation 104 of the 2022 Regulations to issue directions for the purpose of further specifying requirements to be complied with relating to an obligation imposed by or under the 2022 Regulations;

d. pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

e. pursuant to the Commission's statutory duty under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in section 12(1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

f. pursuant to the Commission's statutory duty under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, associated facilities, and numbering;

g. pursuant to the Commission's general objective under Regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

h. pursuant to its function under section 10(1)(b) of the 2002 Act to manage the national numbering resource and its objectives in the exercise of that function as set out in section 12 of the 2002 Act;

i. pursuant to ComReg's power to specify conditions to be attached to a right of use for numbering resources under Regulation 10(1) of the 2022 Regulations;

j. pursuant to ComReg's power under Regulation 14(1) of the 2022 Regulations to amend the rights of use for numbering resources;

k. having regard, inter alia, to its duty under Regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent, non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

l. having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services (which definition as per section 5 of the 2023 Act includes the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the authenticity of those networks and services);

m. having, pursuant to section 13 of the 2002 Act, complied with the following Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

n. having considered all relevant evidence before it, including from Voluntary Information Requests;

o. having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument;

p. having regard to the consultants' reports commissioned in relation to this matter;

q. for the reasons set out in its written response to Commission Document [-] to which this Decision is attached;

PART III – SCOPE AND APPLICATION

The requirements below shall apply to undertakings that:

- have been assigned or use numbers from the national numbering resource; and
- are deemed to be authorised under Regulation 6 of the 2022 Regulations.

PART III – THE DECISIONS

Thereby makes the following decisions:

(1) The Numbering Conditions of Use and Application Process (currently Commission Document 15/136R3, version four) shall be amended as and from [-] as follows (and shall be titled 15/136R4, with consequential numbering and pagination updates):

(A) Insert the following text as a new paragraph 4 in Section 1 “Introduction”, as follows:

(4) As set out in its Response to Consultation XX and Decision XX on Nuisance Communications, ComReg supports industry by managing the following:

i. Do Not Originate (“DNO”) List;

ii. Protected (“PN”) List;

iii. Mobile Station Roaming Number (“MSRN”) List; and

iv. SenderID Registry.

(B) Add the following underlined text in Section 3.1 (5)(a) :

(a) “the undertaking which originates a call *on the Irish PSTN* shall ensure:”

and add the following underlined text as a new paragraph “i”, with consequential numbering updates:

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

and delete the indicated text and add the underlined text in proposed paragraph “ii” as follows:

(ii) that the presentation CLI for the call shall be ~~the assigned~~ a Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number appropriate to the designated MNA for that number, a Harmonised Code of Social Value, a Mobile Number, or a Standard Rate Number, the single European emergency number 112 or the national emergency number 999 ~~for the calling party~~ .

(C) that the current Section 3.1(5)(d) and Section 3.1(5)(e) be deleted as indicated and replaced with the text of a new Section 3.1 (5)(d) as follows:

~~(d) for international calls originating from outside the State, the CLI may be modified with appropriate prefixes including "00", "+" and the relevant country code; and~~

~~(e) a presentation CLI may be marked as "Caller ID unknown" or equivalent if an operator cannot ensure that the presentation CLI information is valid~~.

(d) That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code". If the international call is untrusted and the CLI not in E164 format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".

(D) insert the following text as a new paragraph "e" in Section 3.1 (5) in the Numbering Conditions:

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

(E) insert the following text as a new paragraph 8 in Section 3.1 "General Authorisation conditions" of the Numbering Conditions, with subsequent numbering changes:

(8) SMS SenderID Portability – In support of the objectives of ComReg to promote competition (Part 2 Article 3b of SI 444), undertakings shall ensure that SIDOs can, upon request, retain their SMS SenderIDs independently of the undertaking providing the service.

In the event of a SIDO switching between PAs:

i. the recipient PA must notify ComReg in advance and perform the switch within 2 working days of the scheduled date

ii. the donor PA must facilitate the switch and remove any configuration which is no longer required no more than 5 days after the switch has completed

(F) Add the following underlined text to paragraph 1 of Section 3.2 "Rights of Use Conditions" as follows:

Unless ComReg otherwise consents, a number shall be activated by its holder (a) within 12 months of the date on which the right of use for the number was first granted to the holder; or (b) within 3 months of the date on which the right of use for the number was transferred, as applicable. "In the case of 1800 Freephone and 0818 Standard Rate Numbers, applications shall be submitted on the Fixed Number Portability (FNP) system which shall support the activation of these numbers on networks. *In the case of SMS SenderID, and unless ComReg otherwise consents, a SMS SenderID shall be activated by its holder (a) within 3 months of the date on which the right of use for the SMS SenderID was first granted to the holder; or (b) within one month of the date on which the right of use for the SenderID was transferred, as applicable"*

(G) insert the following text as a new paragraph 9 in Section 3.2 as follows:

(9) Long-lining – Undertakings shall only implement long-lining for their own end-users

(H) Add the following underlined text to paragraph 2 of Section 4.3 in the case of 1800 Freephone and proposed paragraph 2 of Section 4.4 in the case of 0818 Standard rate:

(2) An authorised undertaking shall only be granted the Rights of Use of 1800 Freephone Numbers if it is in receipt of a written order from an end-user for the number(s) being applied for together with the end-user's unique identifier. This identifier shall be the end-user's name, or suitable alternative such as account number or order number which enables ComReg to validate the authenticity of the assignment order. Furthermore, as 1800 Freephone/0818 Standard Rate numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 1800 Freephone/0818 Standard Rate number, a business end-user shall be required to provide the following:

i. A company's Irish CRO number, Revenue VAT or business number; or

ii. A partnership/sole trader's Irish VAT number in their name(s) or proof of their business or Irish income tax registration

This condition shall apply to new 1800/0818 applications only, from the date of commencement of this Decision Instrument.

(I) insert SMS SenderID Rights of Use Conditions as a new Section 6 RoU Conditions entitled "SMS Sender ID Rights of Use" in the Numbering Conditions as follows, with subsequent numbering changes:

(1) SMS SenderIDs are encoded according to the GSM 7-bit default alphabet (section 6.2.1 of [2]) and as such a SMS SenderID can have a maximum length of 11 characters

(2) The following are the valid characters which are permitted:

*a-z 0-9 @ ! # % & ( ) * + , - . / : ; < = > ? [Space]*

Any character not on the above list is not permitted .

(3) SMS SenderID registration and filtering is case insensitive. A given SMS SenderID is assigned to a SIDO to use in whatever choice of case they prefer, however the messages should be treated identically irrespective of the case used.

(J) insert the following underlined text in paragraph 1 of proposed Section 7.1 "General Application Criteria" of the Numbering Conditions";

(1)ComReg will grant rights of use for numbers to authorised undertakings in an open, objective, transparent, non-discriminatory and proportionate manner and generally on a "first come, first served" basis though ComReg may hold open competitions before granting rights of use for newly-opened number ranges. For the avoidance of doubt, SMS SenderIDs will also be assigned on a "first come, first served" basis.

(K) Insert the following text as new paragraph 2 of proposed Section 7.1 "General Application Criteria" of the Numbering Conditions;

(2) Undertakings are obliged to only use their assigned numbers for their own end-users. Sub-assignment to other undertakings is not permitted.

This condition that Undertakings only use their assigned numbers for their own end-users shall apply to new applications only, from the date of commencement of this Decision Instrument.

(L) Add the following underlined text to proposed Section 7.1 paragraph 15(b)as follows:

--

(15b)Applications for numbers other than 1800 and 0818, and for SMS SenderIDs, must comply with the following:

(M) Adding the following underlined text to proposed Section 7.1 paragraph 15(b)(i);

(i)Applicants must complete and sign a copy of the application form in Appendix 1, attaching a completed copy of any relevant form from Appendix 2 – 7 8 for the class of number being requested. For applications for Geographic or Mobile Numbers, the form in Appendix 4 or Appendix 5 must be completed with respect to Geographic or Mobile Numbers already granted to the applicant. For SMS Sender ID, the customer order form in Appendix 9 must be completed.

(N) Insert the following as new paragraph 8 of proposed Section 7.2 "Eligibility Criteria" which identifies the information to be supplied with the customer order:

(8)Rights of use for SenderID may only be granted once the following criteria are met

(a) The SIDO must have a connection with Ireland. The connection with Ireland shall be demonstrated by the SIDO submitting the following information:

i. A company's Irish CRO number, Revenue VAT number or registered business number.

ii. A sole trader/partnership's Irish VAT number in their own name(s), or proof of their business or Irish income tax registration.

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

(b). ComReg reserves the right to refuse applications where the proposed name is likely, in ComReg's view, to lead to confusion; to facilitate fraud or misuse; to incorrectly suggest state sponsorship; or cause offence.(XX)

(O) Deleting the indicated text and inserting the underlined text in the Appendix 1 application form as follows;

Number, ~~or~~ code or *SMS SenderID* requested, if not included in a separate Appendix*:*

(P) Inserting the template SMS SenderID customer order form as new Appendix 9 as follows;

Appendix: 9 SenderID Customer Order Form

An organisation that wishes to apply to have a SenderID included in the SenderID registry shall complete the following customer order form and submit to their Participating Aggregator (PA). The PA shall apply to ComReg for the requested SenderID by completing and signing a copy of the application form in Appendix 1 and attaching the completed customer order form.

SenderID Requirement	***Please complete this column***
Participating Aggregator ***(To confirm authorisation of the PA please refer to ComReg's Service Register at https://serviceregister.comreg.ie/)***	
SenderID Requested ***(The SenderID must comply with the format set out in the Numbering Conditions – Section X "RoU")***	

Organisation Details	***Please complete this column***
Organisation Name	
Organisation Address	

Responsible person	
Name	
Job title	
Email address	
Telephone number	
Secondary contact person	
Name	
Job title	
Email address	
Telephone number	

Declaration

I have followed the necessary approvals in my organisation prior to submitting the SenderID customer order form.

I am fully authorised to submit the SenderID customer order form on behalf of:

Organisation Name _____

Signature: _____

Name in Block Letters: _____

Organisation Name: _____

Date of Submission: _____

(Q) insert SMS SenderID as a class of number in the Numbering Conditions by adding Table 5 to proposed Appendix 10 “Classes of Numbers” as follows:

Code	***Designation***	***Notes***

Alpha-numeric	*SenderID*	*Recognised SenderIDs are included in the SMS SenderID Registry intervention. The Registry shall include information such as the SenderID, SenderID Owner (SIDO) and Participating Aggregator (PA).*

(R) insert the following text as a definition for long-lining in proposed Appendix 12 "Definitions" as follows:

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

(S) Delete the indicated text and to insert the underlined text in proposed Appendix 12 "Definitions" of the Numbering Conditions as follows;

> - In the definition of "Network CLI" add the following text *"In SIP based networks, the Network Number is carried in a "P-Asserted-Id" header field, as defined in RFC 3325[388] as amended"*
>
> - In the definition of "*Presentation CLI"* add the following text *" In SIP based networks, the Presentation Number is carried in the "From" header field, as defined in RFC 3261[389] as amended"*;
>
> *"Sender ID Registry" means the register managed by ComReg of all Registered Sender IDs, SIDOs and the Registered Entities which may transmit or terminate specific Registered SMS Sender IDs;*
>
> *"Sender ID owner" or "SIDO" means the entity to which a Sender ID is assigned by ComReg for use with transiting or terminating SMS. A SIDO could contract a third party to send their messages via an PA rather than send them directly;*
>
> *"Registered Entities" means the SIDO, Registered PA and Registered MSP for a given Registered SMS Sender ID;*
>
> *"Mobile Service Provider" or "MSP" means an undertaking providing End-Users with land based/terrestrial publicly available mobile telephony services using a mobile network;*

[388] RFC 3325 Private Extensions to the Session Initiation Protocol for Asserted Identity within Trusted Networks. Available here: RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (rfc-editor.org)
[389] RFC 3261 SIP: Session Initiation Protocol. Available here: RFC 3261: SIP: Session Initiation Protocol (rfc-editor.org)

Part IV– EFFECTIVE DATE

A revised version of the Numbering Conditions of Use and Application Process (currently Commission Document 15/136R3, version four), which shall be titled Numbering Conditions of Use and Application Process, ComReg 15/136R4, reflecting the decisions above, shall come into effect on the date of the making of this Decision Instrument..

The fourth version of the "Numbering Conditions of Use and Application Process" (Commission Document No. 15/136R3) shall stand revoked from [-] (save that this document shall remain in full effect insofar as it may apply to any relevant matters as may occur prior to its revocation).

PART V – STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation

Chapter 8

8 Making a submission and the next steps

8.1 Submitting Comments

8.1 All input and comments are welcome. Please set out your reasoning and all supporting information for any views expressed. It would make the tasks analysing responses easier if comments were referenced to the relevant section/paragraph number in each chapter and annex in this document.

8.2 The consultation period will run until 17:00 on Friday 28 July 2023 during which time ComReg welcomes written comments on any issues raised in this paper.

8.3 Responses must be submitted in written form (email) to the following recipient, clearly marked – Submissions to ComReg 23/52:

Mr. Donnacha Hennessy

Commission for Communications Regulation

Email: marketframeworkconsult@comreg.ie

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

8.5 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).

8.6 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:

- 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

- 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.

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

- Confidential information contained within a paragraph must be highlighted with a chosen particular colour,
- Square brackets must be included around the confidential text (one at the start and one at the end of the relevant highlighted confidential information),
- A Scissors symbol (Symbol code: Wingdings 2:38) must be included after the first square bracket.

8.8 For example, "*Redtelecom has a market share of [✂<25%].*"

8.2 Next Steps

8.9 When it has concluded its review of all submissions received and other relevant material, ComReg's intention would be to publish a Response to Consultation, and Final Decision(s).

Annex: 1 Econometric analysis of victims of fraud

A 1.1 This Annex contains information on ComReg's econometric analysis of the survey data of B&A on scam victimhood and monies lost as a result of scams.

A 1.2 As outlined in Chapter 5, ComReg's work will reduce the prevalence of scams, and thereby restore consumer trust in networks in the long term. This work may be complemented by consumer awareness efforts, which could potentially further reduce the effectiveness of scams[390].

A 1.3 While many organisations have made information available on scams, ComReg is not aware of any organisation that have engaged in proactive targeted awareness campaigns. The purpose of the research is to aid organisations in conducting their own scam awareness campaigns, by enabling them to target information at the most at-risk consumers. By targeting those most at-risk of scams, organisations can use finite budgets to combat scams most effectively

A 1.4 .This research overcomes certain identified information deficits that would otherwise impede such targeted campaigns. ComReg considers that a number of organisations may wish to raise consumer awareness of scams, including:

- Impersonated businesses (e.g., Irish retail banks)
- Impersonated Government agencies
- Enforcement agencies

Targeted campaigns can reach the most at-risk users

[390] It is the responsibility of organisations to raise their consumers awareness and immunity to scams.

A 1.5 For readability, the key takeaways are presented first, followed by the econometric analysis which is unavoidably technical. Accordingly, this Annex is laid out as follows:

I. How targeted awareness campaigns can combat scams
   a. The benefit of targeted awareness campaigns
   b. How a lack of information on scam victims impedes targeted campaigns
   c. Key findings for organisation undertaking such campaigns

II. ComReg's econometric analysis of the consumer survey data

I. How targeted awareness campaigns can help combat scams

a. The benefit of targeted awareness campaigns

A 1.6 Many impersonated organisations engage in passive consumer awareness, by making information available via online press releases or dedicated webpages. This approach relies upon the consumer using key search terms to find the information. In either case, consumers are likely to encounter such information upon searching for it.

A 1.7 Active awareness campaigns are likely to be most important in further raising consumer awareness for a number of reasons, which includes:

- First, consumers that view passive ads are less likely to be susceptible to scams. After all, passive ads are seen by consumers that likely already are suspicious, having searched for this information (e.g., having searched for "scam text an post?").
- Second, as many consumers do not engage with or permit direct communications, a large share of unsuspecting consumers can be reached by indirect communications like advertising.
- Third, as passive campaigns are widespread, they are likely having most if not all of their effect already - further raising scam awareness depends upon further action.

A 1.8 Certain organisations have also raised awareness of scams actively, through attempting to put that information in front of consumers that are not searching for it (e.g., publishing it in a newspaper)[391]. Active campaigns work best where they involve targeting specific groups.

[391] Companies can reach consumers in a number of ways, including via direct communications (e.g., emails, in-app messages) or indirect communications such as via advertising on print, broadcast, online and social media.

A 1.9 Traditionally, proactive campaigns target consumers by choice of media channel[392] However with digital advertising, organisations can choose the audience directly, based on an individual's demographic characteristics, such as their age, gender, income, education, and location); or their online behaviour (e.g., websites they visit, search terms they use, or products they purchase).

A 1.10 In Ireland, online media platforms allow organisations to place information in front of specific user groups, by selecting the demographic profile of the audience[393]. This can greatly enhance the effectiveness of a campaign where certain users are most relevant or at risk. However, to engage in proactive advertising campaign, organisations must know which consumer groups to target.

b. How a lack of information on scam victims impedes targeted campaigns

A 1.11 At present, any organisation planning a proactive awareness campaign to combat scams is impeded by a lack of accurate information on what consumers are likely to be scammed.

A 1.12 ComReg is not aware of the existence of any representative data on scam victimhood in Ireland. Organisations can only be aware of consumers that report having been scammed. ComReg's survey analysis indicates the majority of scams are not reported. Moreover, individual organisations could only be aware of scams reported to them, which represents a small share of the fraction of scam victims that report a scam. Furthermore, organisations may wish to target different outcomes, either scam prevalence or reducing to reduce the total value of monies stolen (i.e., targeting high value fraud more)[394].

A 1.13 This lack of information lowers the effectiveness and return on active awareness campaigns. Unlike passive advertising, proactive advertising necessarily incurs a cost, and organisations have a finite budget for such campaigns. An inability to target most at-risk consumers lowers the return-on-investment to proactive awareness campaigns and thereby inhibit their use.

c. Key findings

[392] For example, advertising in the Irish Farmers Journal to sell to farmers.
[393] See for example, the policies of Google and Meta.
[394] The latter may be an objective for organisations with a greater incidence of high-value frauds, noting that amounts scammed can vary between €5 and €5,000.

A 1.14 Based on the analysis below, ComReg recommends that an organisation attempting to reduce the incidence of fraud target people under 25 years of age.

A 1.15 This is the most statistically and economically significant predictor of an individual's risk of being scammed, with those under 25 years of age being 14 times more likely to report having lost money to a scam, controlling for other variables.

A 1.16 Given the age cohort most at-risk from current scam SMS and calls in the past 12 months, awareness campaigns conducted in schools or universities may also be effective.

II. ComReg's econometric analysis of the consumer survey data

A 1.17 ComReg analysed data on scam victimhood, payments and demographic information gathered as part of the B&A Consumer Survey. ComReg examined the following question: Are certain groups of consumers more likely to become scam victims or lose greater amounts when defrauded.

A 1.18 To ComReg's knowledge, this analysis is unique not only in Ireland, but internationally.

A 1.19 The analysis is divided into the following sections:

a) Literature review;
b) Methodology;
c) Data;
d) Results; and
e) Assessment of the results.

a) Literature review

I. Determinants of scam victimhood

A 1.20 Most research on scam victimhood appears to have focused on the psychological and not demographic determinants of scam victimhood. While interesting, this is of little use to organisations combatting scams, as these traits are not readily observable and targetable characteristics[395]. Research on scam victimhood is complicated by the lack of reliable data on actual rates of victimhood. Much of the literature is based on reported scams, which likely comprise only a fraction of actual scams given the low levels of reporting.

[395] https://onlinelibrary.wiley.com/doi/abs/10.1111/jasp.12158, https://link.springer.com/article/10.1007/s10610-020-09458-z https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2448130

A 1.21 The key findings of ComReg's literature review are summarised below. The literature is inconclusive on whether any specific demographic group is most susceptible to scams overall. Indeed, different demographics appear most susceptible to differ scams, consistent with fraudsters using a variety of scams to target many groups. Indeed, research has found that different groups (male vs. female, young vs. old) are more likely respond to a scam solicitation depends on the type of scams (Button et al. 2009).

A 1.22 By far the most studied characteristic is age. An interesting finding in the literature is that in spite of a widespread belief that older people are most susceptible there is evidence that scam victimhood is spread across age cohorts with different cohorts appearing most susceptible to different scams (Hanoch & Wood, 2021). The scant research on the demographic determinants of SMS and Voice to date, typically carried out by banks such as Barclays and PTSB, indicates that younger consumers are more susceptible to scams.[396] In the Irish context the evidence is mixed regarding what consumers are most at-risk. While research by Amárach on behalf of AIB indicates that consumers "*aged over 55 were more likely to be targeted by fraudsters*", while research conducted by BehaviorWise on behalf of Permanent PTSB[397] found that consumers "*under 45 (are) more likely than older people to fall victim to financial fraud*".

Table 20: Key findings of demographic determinants of scam victimhood

Characteristics	Effect
Age	***Over 65s: Inconclusive – higher for some scams*** While a number of studies have found that that older adults (65 years old and over) are more likely to be targeted by fraudsters (Burnes et al., 2017; Lichtenberg et al., 2016) and more likely to become victims (James et al., 2014), a number of studies have found that older adults face a reduced risk of becoming a victim compared with middle-aged adults (Anderson, 2019; Office for National Statistics, 2016; Titus et al., 1995).
	Middle age - Inconclusive – appears higher for some scams Some research indicates that middle-aged adults are the age group with the highest rate of victimization (Office for National Statistics, 2016). Focusing on scams related to COVID-19, a report by the Federal Trade Commission (2021) found that adults between the ages of 30 and 39 reported the highest number of COVID-19 fraud complaints, a finding that roughly matches Anderson's (2019) report that individuals ages 35 through 44 were most likely to report falling victim to mass-marketing solicitations
	Younger adults – appears higher for SMS and Voice scams In relation to recent scams • In the UK, younger people were significantly more likely to be victims of fraud with those aged 20 to 39 accounting for 39% of all reports to Action Fraud. • Recent research by Barclays band found that 21–30-year-olds being fifteen times more likely to be a victim compared with those aged over 70 . • Recent Research by Permanent TSB found that victims are more likely to be young (under 45, particularly Millennials) living in Dublin or urban areas.
Sex	A survey on scams in 30 European countries (European Commission, 2020) found that males are more likely than females to report being victimized.

[396] Other NRAs, such as Ofcom, that have studied scams have focused more on scam prevalence and not published any information on the demographic profile of victims.
[397] Reflecting Ireland consumer research, published on 23 November 2022. Link

	The ACMA has found that men and women report a falling victim to a similar number of scams, however men typically lose money.[398]
Economic Status	The Office for National Statistics (2016) in the United Kingdom, for example, has reported that individuals with higher incomes report higher rates of victimhood. A survey on scams in 30 European countries (European Commission, 2020) has provided similar insights, finding that more educated individuals and individuals with higher incomes are more likely to report being a victim of fraud, and also that males are more likely than females to report being victimized. DeLiema and colleagues (2020) and Whitty (2019a, 2019b) also reported that being better educated was associated with higher rates of reporting being defrauded in investment-type scams. In contrast, studies by Wood et al. (2018) and Mueller et al. (2020) suggest that higher education is associated with a lower intention to respond to mass-marketing solicitations.
Nationality	Anderson (2019), who reported that Hispanic Americans and Black Americans are more likely than White Americans to report falling victim to fraud

II. Appropriate empirical approach

A 1.23 The econometric analysis of scam victimhood and losses is made complex as a result of the "zero-inflated problem", which arises as few consumers have been scammed. Zero-inflated problem in econometrics is a phenomenon in which an excessive number of zero values are observed in a dependent variable, leading to skewed and biased estimates of the statistical model. A variety of approaches have been used in the literature given the zero problem. In line with Eisenberg et. Al (2015)[399] ComReg has applied both a two-stage hurdle model and separate models for the process of scam victimhood and amounts paid, given that there is no censoring of data or latent structure.

A 1.24 In this instance, as the results of the two-stage model supported the results of the separate models, with the same variables achieving the same level of statistical significance. ComReg considers that it has little additional useful information to offer an organisation designing awareness campaigns. Therefore, to aid readability ComReg only reports the results of the separate models here[400].

b) Methodology

[398] ACMA "*Targeting scams report 2021*" available here
[399] Eisenberg, Theodore and Eisenberg, Thomas and Wells, Martin T. and Zhang, Min, "Addressing the Zeros Problem: Regression
Models for Outcomes with a Large Proportion of Zeros, with an Application to Trial Outcomes," 12 Journal of Empirical Legal Studies
161-186 (2015)
[400] Moreover, a hurdle model is typically used where the observed party commits two consecutive decisions, whereas in this instance, the consumers make choices that enable the scam, but does not choose the amount being stolen (e.g., the payment is set by the fraudster, or the fraudster empties the bank account).

A 1.25 Using logistic regression, ComReg has examined whether certain groups of consumers more likely to become scam victims. A logistic regression, is used to model the relationship between a binary dependent variable (e.g., scammed or not scammed) and one or more independent variables[401]. In this instance, the OLS regression can be used to establish whether a statistically significant relationship exists between a consumer's demographic characteristics and the likelihood of them being scammed. The coefficients in the output of the logistic regression are given in units of log odds. Therefore, the coefficients indicate the amount of change expected in the log odds when there is a one unit change in the predictor variable with all of the other variables in the model held constant. Odds ratios that are greater than 1 indicate that the event is more likely to occur as the predictor increases.

A 1.26 The logit regression can be shown as follows:

$$logit(Y) = log\left(\frac{p(Scammed_i)}{1 - p(Scammed_i)}\right) = \beta_0 + \beta_1 Charateristics_i + \varepsilon_i$$

A 1.27 Using ordinary least squares ("OLS") regression, ComReg has examined whether certain groups of consumers lose more money if scammed. An OLS regression is a statistical technique used to model the linear relationship between a dependent variable (also known as the response or outcome variable) and one or more independent variables (also known as predictor or explanatory variables) [402]. In this instance, the OLS regression can be used to establish whether a statistically significant relationship exists between a scam victims demographic characteristics and the amount lost to the scam.[403]

A 1.28 The OLS regression can be shown as follows:

$$AmountScammed_i = \beta_0 + \beta_1 Charateristics_i + \varepsilon_i$$

c) Data

[401] The goal of logistic regression is to estimate the coefficients of the independent variables that best predict the binary outcome, and to estimate the probability of the binary outcome given the values of the independent variables. Logistic regression assumes that the probability of the binary outcome follows a logistic function, which is an S-shaped curve that ranges from 0 to 1. The logistic function maps a linear combination of the independent variables and their coefficients to the probability of the binary outcome.

[402] The goal of OLS regression is to estimate the parameters of a linear equation that best fits the observed data. In an OLS regression, the line of best fit is determined by minimizing the sum of the squared differences between the observed values of the dependent variable and the predicted values based on the independent variables. This is known as the least squares criterion.

[403] In line with Eisenberg (2015), ComReg also examined this effect using a two-stage regression, specifically a hurdle model. ComReg considered this appropriate given that 0 values were observed (i.e., not being scammed). However, in this instance, as the results supported the results of the OLS, with the same variables achieving the same level of statistical significance, ComReg considers that it has little additional useful information to offer organisation designing awareness campaigns. Therefore, to aid readability ComReg only reports the results of the OLS here. Moreover, a hurdle model is typically used where the observed party commits two consecutive decisions, whereas in this instance, the consumers make choices that enable the scam, but does not choose the amount being stolen (e.g., the payment is set by the fraudster, or the fraudster empties the bank account).

A 1.29 This dataset records the experiences of scam calls and SMS for a representative sample of 1,219 consumers above the age of 16. This sample was constructed in terms of the age, gender, socio-economic class and region of respondents to reflect the profile of the adult population of the Republic of Ireland. As part of this survey respondents were asked to report whether they had lost money as a result of a scam call or text, and if so, how much money was lost. The demographic information gathered includes the age, gender, socio-economic class, region of participants.

Table 21: Descriptive statistics for possible predictors of victimhood

Variables	Victims		Non-Victims		Whole sample	
	Mean	SD	Mean	SD	Mean	SD
Male	.55	.50	.50	.50	.50	.50
Age	34.24	13.97	47.33	15.74	46.57	15.94
High SES	.45	.50	.53	.50	.52	.50
Urban	.25	.44	.35	.48	.34	.48
National	.82	.39	.82	.39	.82	.39
Kids	.62	.49	.63	.48	.63	.48
N	71		1,148		1,219	

d) Regression results

A 1.30 Table 22 below presents the results ComReg's regression analysis.

Table 22: Regression coefficients and their statistical significance

Variables	Victimhood			Amount lost (€)
	Calls	SMS	Any	Calls or SMS
	Logit	*Logit*	*Logit*	*OLS*
Male	1.90** (.62)	1.50 (.48)	1.59* (.44)	-861.76*** (284.39)
High SES	1.05 (.33)	1.00 (.31)	0.95 (.26)	-567.96** (277.51)
GenZ	18.49*** (8.8)	21.56*** (10.87)	14.78*** (6.07)	
Millennials	3.12*** (1.32)	4.59*** (2.02)	2.96*** (1.00)	
Over65s	0.47 (.37)	0.61 (.5)	0.46 (.29)	
Age	-	-	-	-11.76 (10.19)
Kids	2.73** (.98)	2.24** (.77)	2.69*** (.84)	
Non-national	1.26 (.51)	1.20 (.49)	1.03 (.34)	
UrbanRural	0.84 (.31)	0.56 (.21)	0.76 (.29)	
Region 2	1.17 (.47)	1.42 (.56)	1.46 (.5)	
Region 3	0.63 (.29)	0.93 (.4)	0.73 (.28)	

Region 4	0.60 (.30)	0.72 (.35)	0.62 (.27)	
_cons	0.01*** (.01)	0.01*** (.1)	0.02*** (.01)	1554.184 (432.5603)
R^2	0.1355	0.1421	0.1257	0.1586
Observations	1,219	1,219	1,219	68

Standard errors in parentheses, *<p<0.1, ** p<0.05, *** p<0.01

e) Assessment of the results.

Victimhood

Age

A 1.31 The coefficient for the dummy variables *GenZ* and *Millennial* are statistically significant at the 1% level in both OLS regressions for scam calls and SMS[404]. The size of the effect is large, with GenZ and Millennials roughly 14 and 3 times more likely to report having been scammed by call or text in the prior 12 months respectively, compared to older age cohorts.

Sex

A 1.32 The coefficient for the dummy variable male is statistically significant at the 5% level for scam calls or at all, but not for SMS specifically[405]. The size of the effect is moderate, with men roughly twice as likely to report having been scammed in the prior 12 months respectively, compared to women.

Other variables

A 1.33 The coefficient for the dummy variable *Kids* is statistically significant at the 1% level in both OLS regressions. The meaning of *kids* is ambiguous, as this merely records whether children under the age of 18 are in the respondents' households. These may be children or siblings, with the latter more likely in the case of respondents under 25. Nevertheless, this may support parents being more susceptible to scams, noting the evidence of scams targeting parents specifically[406].

A 1.34 None of the other demographic factors demonstrate a statistically significant relationship with victimhood.

Money lost

Sex

[404] As the sign of the coefficient is negative, this means we can reject with 99% confidence that GenZ and Millennials are not more susceptible to scam calls or texts.
[405] As the sign of the coefficient is negative, this means we can reject with 95% confidence that men are not more susceptible to scam calls.
[406] For example, "Hi Mum" scams.

A 1.35 The coefficient for the dummy variable male is negative and statistically significant at the 1% level[407]. The size of the effect is large, with scammed women losing approximately 800 euro more on average than men, controlling for age and socio-economic status. This is consistent with the distributions of men and women among payees: while more men report having lost money to scams, women were overrepresented among those who paid more than €100, and in particular above €1,000[408].

Socio-Economic status

A 1.36 The coefficient for the dummy variable *SES* is statistically significant at the 5% for the OLS regressions for the value of amounts reported as being lost to scam calls.[409] This is consistent with the distributions of high and low SES among victims: low SES were overrepresented among those who paid more[410].

Conclusions

Age

A 1.37 The analysis indicates that younger users are far more likely to report having been scammed. Age is clearly the key predictor of scam victimhood.

Sex

A 1.38 The analysis indicates that men are more likely to fall victim to scams; but women typically lose more money when scammed. ComReg places less weight on this finding in constructing its advice to given the:

- mixed effects of gender on scam victimhood and monies lost; and
- unavoidably small sample for the impact on monies lost.

Other factors

A 1.39 ComReg places less weight on the remaining factors given the difficulty in this into reliable, advice given uncertainty in regarding sample size or the effect.

[407] As the sign of the coefficient is negative, this means we can reject with 99% confidence that women do not pay more than men when scammed by call or texts.
[408] The significance values for these findings were corroborated by the 2SLS hurdle model.
[409] As the sign of the coefficient is negative, this means we can reject with 90% confidence that high SES do not pay more than low SES when scammed by call.
[410] The significance values for these findings were corroborated by the 2SLS hurdle model.

Annex: 2 Summary of statutory objectives and legal framework relevant to interventions relating to nuisance communications

A 2.1 The Communications Regulation Acts 2002 as amended[411] (the "2002 Act"), the Communications Regulation and Digital Hub Development Agency Act 2023, and S.I. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022, set out, amongst other things, powers, functions, duties and objectives of ComReg that are relevant to interventions relating to nuisance communications. For the purposes of this Annex, "nuisance communications" means unwanted, unsolicited communications generally directed at large groups of the population. Nuisance communications often have the intent to mislead the receiver, so that they unknowingly provide sensitive personal information.

A 2.2 This Annex seeks to set out the primary legal powers currently available to ComReg in relation to dealing with nuisance communications[412].

A 2.3 ComReg recognises that the previous European Common Regulatory Framework for ECN and ECS has been superseded by the European Electronic Communications Code[413] ("EECC"). On 20 December 2018, the EECC entered into force.

A 2.4 With some limited exceptions (see Article 124 of the EECC), Member States had until 21 December 2020 to transpose the EECC into national law[1].

A 2.5 Most of the EECC (including numbering provisions) is being transposed into Irish law by secondary legislation, namely S.I. No. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022[414]. The other relevant transposing legislation is the Communications Regulation and Digital Hub Development Agency Act 2023.

---

411 The Communications Regulation Act 2002 (as amended), the Communications Regulation (Amendment) Act 2007, the Communications Regulation (Premium Rate Services and Electronic Communications Infrastructure) Act 2010 and the Communications Regulation (Postal Services) Act 2011.

412 For completeness, relevant criminal law relating to fraud, although enforced by An Garda Siochana rather than ComReg, is also noted below.

413 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11th December 2018 establishing the European Electronic Communications Code.

[1] With the exception of Articles 53(2), (3) and (4), and Article 54 (See Article 124).

414 pdf (irishstatutebook.ie)

A 2.6 For the avoidance of doubt, ComReg is satisfied that, to the best of its knowledge, use of the legal powers discussed in this Annex as interventions to deal with nuisance communications would not conflict with the objectives of the EECC or the obligations likely to be imposed on ComReg under national legislation implementing same.

A 2.7 This Annex is intended as a general guide as to ComReg's role in this area, and not as a definitive or exhaustive legal exposition of that role. Further, this annex restricts itself to consideration of those powers, functions, duties and objectives of ComReg that appear most relevant to the matters at hand and generally excludes those not considered relevant (for example, in relation to postal services, premium rate services or market analysis). For the avoidance of doubt, however, the inclusion of particular material in this Annex does not necessarily mean that ComReg considers same to be of specific relevance to the matters at hand.

A 2.8 All references in this annex to enactments are to the enactment as amended at the date hereof unless the context otherwise requires.

Primary Objectives and Regulatory Principles under the 2002 Act

Relevant statutory functions and objectives

A 2.9 The ComReg statutory functions contained in section 10 of the Communications Regulation Act 2002, as amended, that are particularly relevant to this project are the following:

- Section 10(a): "to ensure compliance by undertakings with obligations in relation to the supply and access to electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such facilities";
- Section 10(b): "to manage … the national numbering resource, in accordance with a direction under section 13"; and
- Section 10(d): "to carry out investigations into matters relating to- (a) the supply of, and access to, electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such networks…".

A 2.10 The ComReg statutory objectives contained in section 12 of the Communications Regulation Act 2002, as amended, that are particularly relevant to this project include the following:

- Section 12(1)(a): “the objective of the Commission in exercising its function in relation to the provision of electronic communications networks, electronic communications services and associated facilities shall be as follows: (i) to promote competition; (ii) to contribute to the development of the internal market, and (iii) to promote the interests of users within the Community”;
- Section 12(1)(b): “to ensure the efficient management and use of … numbers from the national numbering scheme in the State in accordance with a direction under section 13”.

A 2.11 Further to section 12(2), in relation to the objectives referred to in section 12(1)(a), ComReg shall take all reasonable measures which are aimed at achieving those objectives, including:

(as set out in section 12(2)(a)), in so far as the promotion of competition is concerned-

(i) ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality;

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

(iv) encouraging efficient use and ensuring the effective management of radio frequencies and numbering resources,

as set out in section 12(2)(c)) in so far as promotion of the interests of users within the Community is concerned-

- (ii) ensuring a high level of protection for consumers in their dealings with suppliers…;
- (iii)contributing to a high level of protection of personal data and privacy;
- (iv)promoting the provision of clear information…”
- (vii) ensuring that the integrity and security of public communications networks are maintained”.

A 2.12 Section 12(3) of the 2002 Act provides that in carrying out its functions, ComReg shall seek to ensure that measures taken by it are proportionate having regard to the objectives set out in section 12.

A 2.13 Section 12(5) of the 2002 Act provides that in carrying out its functions, ComReg shall have regard to international developments with regard to electronic communications networks and electronic communications services, associated facilities… and numbering.

A 2.14 To note that section 10(3) of the 2002 Act provides that ComReg shall have all such powers as are necessary for or incidental to the performance of its functions under the 2002 Act or any other Act.

Powers relating to Numbering

A 2.15 ComReg's powers in relation to the rights of use for numbers are further detailed in the S.I. 444 of 2022, the European Union (Electronic Communications Code) Regulations 2022.

A 2.16 Relevant general objectives listed in Regulation 4(3), which ComReg has to pursue in the context of its tasks, are the following: "promote the interests of the consumers and businesses in the State, by ensuring connectivity and the widespread availability and take-up of very-high-capacity networks, including fixed, mobile and wireless networks, and of electronic communications services, by enabling maximum benefits in terms of choice, price and quality on the basis of effective competition, by maintaining the security of networks and services, by ensuring a high and common level of protection for end-users through the necessary sector-specific rules and by addressing the needs, such as affordable prices, of specific social groups, in particular end-users with disabilities, elderly end-users and end-users with special social needs, and choice and equivalent access for end-users with disabilities".

A 2.17

Under Regulation 79(1) of S.I. 444, the granting by ComReg of rights of use for all national numbering resources for all publicly available electronic communications services is subject to ensuring the proper management of the national numbering plan in accordance with ComReg's objectives under section 12 of the 2002 Act, and Regulation 4 of S.I. 444.

1. Regulation 78(7) of SI 444 provides: "the Regulator may, without prejudice to the generality of Regulation 10, attach conditions to rights of use for numbering resources (a) to ensure the efficient and effective management of all numbering resources, and (b) to ensure that person granted numbering resources does not discriminate against a provider of publicly available electronic communications services".

2. Pursuant to Regulation 10(1) of SI 444, the Regulator shall specify conditions to be attached to a right of use for numbering resources, only as are listed in Part E of Schedule 1 to the Regulations. The key word to be aware of here is "only". There is a relatively narrow list of conditions that that can be attached to a numbering right of use set out in Part E of Schedule 1 – a criminal penalty applies if these conditions

are breached (Regulation 10(5) and (6)). Regulation 10(1) transposes Article 13 of the EECC.

3. Relevant conditions which may be attached to rights of use for numbering resources under Part E of the Schedule to SI 444 are: (2) Effective and efficient use of numbering resources in accordance with these Regulations.

Relevant provisions of the EECC, and transposition legislation, relating to numbering

A 2.18 Note: The numbering function under section 10 of the 2002 Act and the numbering objective under section 12 of the 2002 Act are not affected by the EECC, or by transposition legislation.

A 2.19 Article 93 of the EECC sets out provisions relating to numbering resources, and Article 94 sets out the procedure for granting of rights of use for numbering resources.

A 2.20 Part 10 of S.I. 444 of 2020 deals with access to numbers and services, and related provisions, and transposes Articles 93 and 94 of the EECC.

Current provisions relating to CLIs

A 2.21 General Authorisation Condition 3.1(5) of the Numbering Conditions of Use[415] (which Condition applies to all authorised undertakings) sets out, amongst other things, that:

(a) The undertaking which originates a call shall ensure:

(i) that the presentation CLI[416] for the call shall be the assigned Customer Support Short Code (for on-network calls), a Freephone Number, a Geographic Number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number for the calling party;

(ii) that the network CLI for the call shall be the assigned Geographic Number, 076 Standard Rate Number, Mobile Number or M2M number for the calling party; and

(iii) that a Mobile Number is not used as the presentation or network CLI for any call that originates from a fixed terminal.

[415] Numbering Conditions of Use and Application Process, ComReg-15136R3.pdf
[416] "presentation CLI" is defined for the purposes of the Numbering Conditions of Use (in Annex 11) as meaning a number that can identify a caller or be used to make a return call. The presentation CLI must be a number assigned to the caller and is supported by an underlying network CLI.

Power relating to misuse of numbers

Under Regulation 83(2) of SI 444, the Regulator may require providers of public electronic communications networks or publicly available electronic communications services to block on a case by case basis, access to numbers or services where this is justified by reason of misuse and to require that in such cases those provides withhold relevant interconnection or other service revenues. See further discussion on this below.

Powers relating to security

A 2.22 Obligations on operators regarding security and integrity are set out in Part 2 of the Communications Regulation and Digital Hub Development Agency Act 2023.

A 2.23 Further to section 6(1): “Providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services.” It should be noted that further to section 6(2): “Measures taken in accordance with subsection (1) shall ensure a level of security appropriate to the risk presented having regard to the state of the art. It should also be noted that further to section 6(3): “In particular, measures, including the use of encryption where appropriate, shall be taken by providers to prevent security incidents and minimise the impact of any security incident on users and on other networks and services.”

A 2.24 It is important to note that the definition of “security of networks and services” means as per section 5 of the Act of 2023: “the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services”.

A 2.25 There is a statutory duty on ComReg under section 13 of the Act of 2023 to seek to ensure compliance by providers with Part 2: “The Commission shall take reasonable steps to ensure that providers comply with the obligations placed on them by or under this Part.”

Relevant provisions of the EECC, and transposition legislation, relating to security

A 2.26 Article 40 of the EECC sets out provisions relating to security of networks and services. Article 40(1) provides as follows: “Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.” Article 40(1) is transposed in section 6 of the 2023 Act.

A 2.27 Article 2(21) of the EECC defines “security of networks and service” as meaning 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. This definition is transposed in section 5 of the 2023 Act.

A 2.28 Article 41 of the EECC relates to implementation and enforcement. Article 41 is transposed in sections 14 to 16 of the Communications Regulation Bill.

E-Privacy issues

A 2.29 Regulation 5(1) of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011), provides that: “Without prejudice to section 98 of the Act of 1983[417] and section 2 of the Act of 1993[418] and except where legally authorised under a provision adopted in accordance with Article 15(1) of the Directive on privacy and electronic communications, the listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is prohibited.”

A 2.30 It should be noted that if operators obtain the consent of users of their services to the interception of communications in order to prevent nuisance communications from reaching those users, then it would appear that the prohibition in Regulation 5(1) is not breached.

Interception - The 1983 Act

[417] Postal and Telecommunications Services Act 1983.
[418] Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

A 2.31 Section 98(1) of the Postal and Telecommunications Services Act 1983 provides that: “A person who- (a) intercepts or attempts to intercept, or (b) authorises, suffers or permits another person to intercept, or (c) does anything that would enable him or another person to intercept, telecommunications messages being transmitted by the company or who discloses the existence, substance or purport of any such message which has been intercepted or uses for any purpose any information obtained from any such message shall be guilty of an offence.”

A 2.32 Exceptions to section 98(1) are set out in section 98(2), which provides as follows:

“Subsection (1) shall not apply to any person who is acting—

(a) (i) for the purpose of an investigation by a member of the Garda Síochána of a suspected offence under section 13 of the Post Office (Amendment) Act, 1951 (which refers to telecommunications messages of an obscene, menacing or similar character) on the complaint of a person claiming to have received such a message, or

(ii) in pursuance of a direction issued by the Minister under section 110 , or

(iii) under other lawful authority, or

(b) in the course of and to the extent required by his operating duties or duties for or in connection with the installation or maintenance of a line, apparatus or equipment for the transmission of telecommunications messages by the company.

3) (*a*) The company may, with the consent of the Minister, make regulations to carry out the intentions of this section in so far as concerns members of its staff.

(*b*) The Minister, after consultation with the company, may direct the company to make regulations under *paragraph (a)* or to amend or revoke regulations made under that paragraph and the company shall comply with that direction.

(*c*) A person who contravenes any regulation under this subsection shall be guilty of an offence.

(4) (*a*) The Minister may make regulations prohibiting the provision or operation of overhearing facilities in relation to any apparatus (including private branch telephone exchanges) connected to the network of the company otherwise than in accordance with such conditions as he considers to be reasonable and prescribes in the regulations.

(*b*) A person who contravenes any regulation under this subsection shall be guilty of an offence.

A 2.33 It should be noted that for the purposes of section 98, “interception” means: “listening to, or recording by any means, or acquiring the substance or purport of, any telecommunications message without the agreement of the person on whose behalf that message is transmitted by the company and of the person intended by him to receive that message” (section 98(5)).

Interception - The 1993 Act

A 2.34 Section 2 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 is entitled “Authorisation of interceptions”. Section 2(1) provides as follows: “The Minister may give an authorisation, but only for the purpose of criminal investigation or in the interests of the security of the State”.

A 2.35 Further to section 2(3) of the 1993 Act, the Minister shall not give an authorisation unless he considers that the conditions specified in section 4 or 5 of the Act, as may be appropriate, stand fulfilled, and that there has not been a contravention of section 6 of the Act, in relation to the proposed interception.

Power relating to unsolicited communications

A 2.36 Further to Regulation 13 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011), a person shall not use or cause to be used any publicly available electronic communications service to send to a subscriber or user who is a natural person an unsolicited communication for the purpose of direct marketing by means of- (a) an automated calling machine, (b) a facsimile machine, or (c) electronic mail, unless the person has been notified by that subscriber or user that he or she consents to the receipt of such a communication.

A 2.37 Further to Regulation 13(15), a person who commits an offence under Regulation 13 is liable- (a) on summary conviction, to a class A fine, or (b) on conviction on indictment- (i) in the case of a body corporate, to a fine not exceeding €250,000, or

A 2.38 (ii) in the case of a natural person, to a fine not exceeding €50,000.

A 2.39 Regulation 30(1) which is entitled “Enforcement of Regulations by the Regulator” provides that subject to the performance by the Data Protection Commissioner of the functions under Regulation 17, it shall be a function of the Regulator (i.e. ComReg) to monitor compliance with Regulation 7, 8, 9, 10, 11, 12, 13, 14 or 15 and to issue such directions as may be necessary, from time to time, for their effective implementation. The Regulator, in consultation with the Commissioner, may also specify the form and any other requirements regarding the obtaining, recording and rescinding of consent of subscribers for the purpose of these Regulations.

A 2.40 Pursuant to Regulation 30(3), the Regulator may give directions to an undertaking to which Regulation 7, 8, 9, 10, 11, 12, 13, 14 or 15 applies requiring the undertaking to take specified measures or to refrain from taking specified measures for the purpose of complying with the provision.

A 2.41

Criminal law relating to fraud

A 2.42 For completeness, although not enforceable by ComReg, the following specific criminal offences under the Criminal Justice (Theft and Fraud Offences) Act 2011 could be relevant to nuisance communications, depending on the circumstances:

A 2.43 Section 6 – Making gain or loss by deception - 6.—(1) A person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception induces another to do or refrain from doing an act is guilty of an offence. (2) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 5 years or both.

A 2.44 Section 7 – Obtaining services by deception - 7.—(1) A person who dishonestly, with the intention of making a gain for himself or herself or another, or of causing loss to another, by any deception obtains services from another is guilty of an offence.(4) A person guilty of an offence under this section is liable on conviction on indictment to a fine or imprisonment for a term not exceeding 5 years or both.

A 2.45 To note that fraud cases are investigated by the Gardaí, with the Garda Bureau of Fraud Investigation (GBFI) investigating serious and complex cases of commercial fraud.