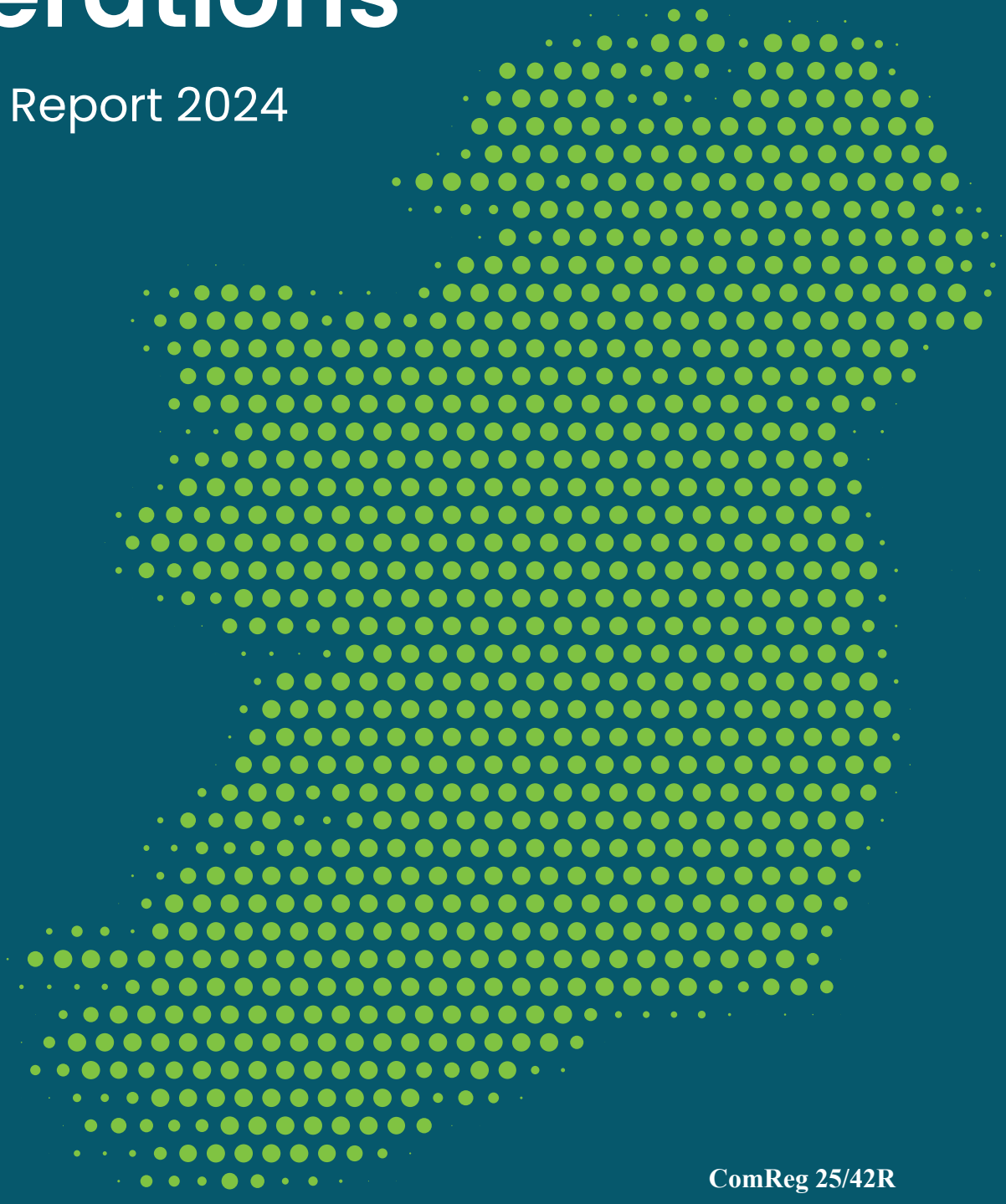
An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Operations

Annual Report 2024

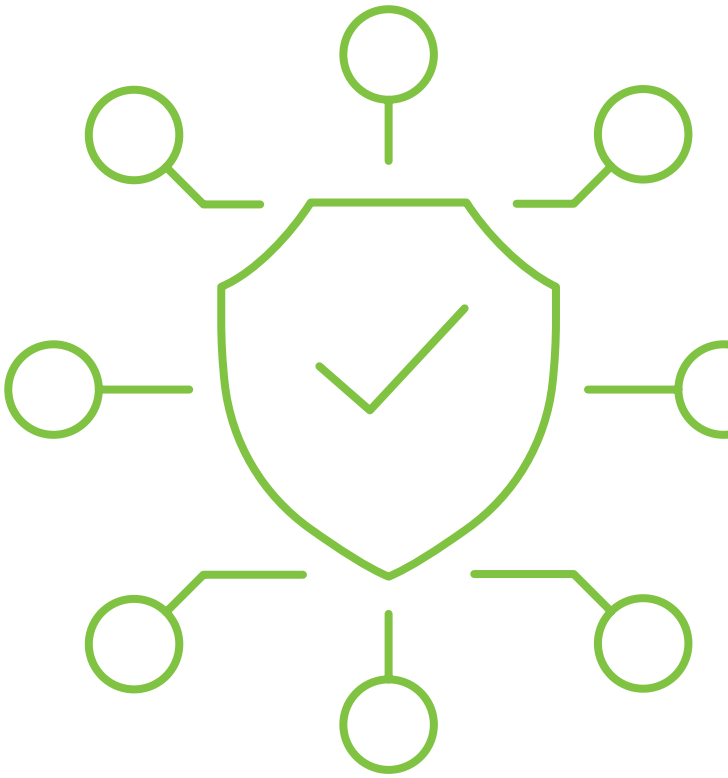


ComReg 25/42R
01/07/2025

ComReg.ie

Contents

1



Executive Summary

ComReg's Network Operations Unit ("NOU") is a specialised unit which, among other things, is focused on the resilience of Electronic Communications Networks ("ECN") and Electronic Communication Services ("ECS") and the analysis of the root causes of significant security incidents in respect of same.

The statutory obligations on providers and ComReg's associated powers are outlined in Part 2 ("Security of Networks and Services") of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, (the "Act of 2023"). The Act of 2023 brings more electronic communications services within scope, and the terms "Security"[1] and "Security Incidents"[2] are now explicitly defined. Part 2 of the Act of 2023 addresses both providers of: ECN and ECS and Number Independent Interpersonal Communication Service ("NI-ICS")[3]. Section 13 of the Act of 2023 provides that ComReg shall take reasonable steps to ensure that providers comply with the obligations placed on them.

An analysis of the causes of significant security incidents in Ireland during the period in question is provided. It should be noted that the European Union Agency for Cybersecurity ("ENISA"[4]) considers that faulty hardware (whether misconfigured or otherwise), faulty software and software bugs comprise system failures.

The main causes of the significant security incidents experienced during 2024 were storms and system failures; be it faulty hardware or software issues, including defective upgrades and bugs. Section 2 of this report explores these matters in more detail.

Significant security incidents such as storms could be better mitigated against by:
- Improved resilience of mains power supplies; and
- Improved routine maintenance of physical Infrastructure ("PI")

Systems failures can be lessened by:
- Improving testing, industry-wide, by both vendors and providers, of software and hardware;
- The presence of appropriately experienced staff, during swap-outs or upgrades; and
- Clearer escalation and roll-back procedures.

ComReg will continue to monitor significant security incidents and their causes, in the year ahead. In accordance with section 6 of the Act of 2023, operators of ECN and ECS must take care, in managing the risks to their networks and services; by ensuring appropriate measures are put in place to mitigate the risks identified.

---

1 'security of networks and services' means '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 service', see Article 2(21) of the EECC, as transposed in section 5 of the Act of 2023

2 'security incident' means 'any action that compromises the availability, authenticity, integrity or confidentiality of 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', see section 5 of the Act of 2023

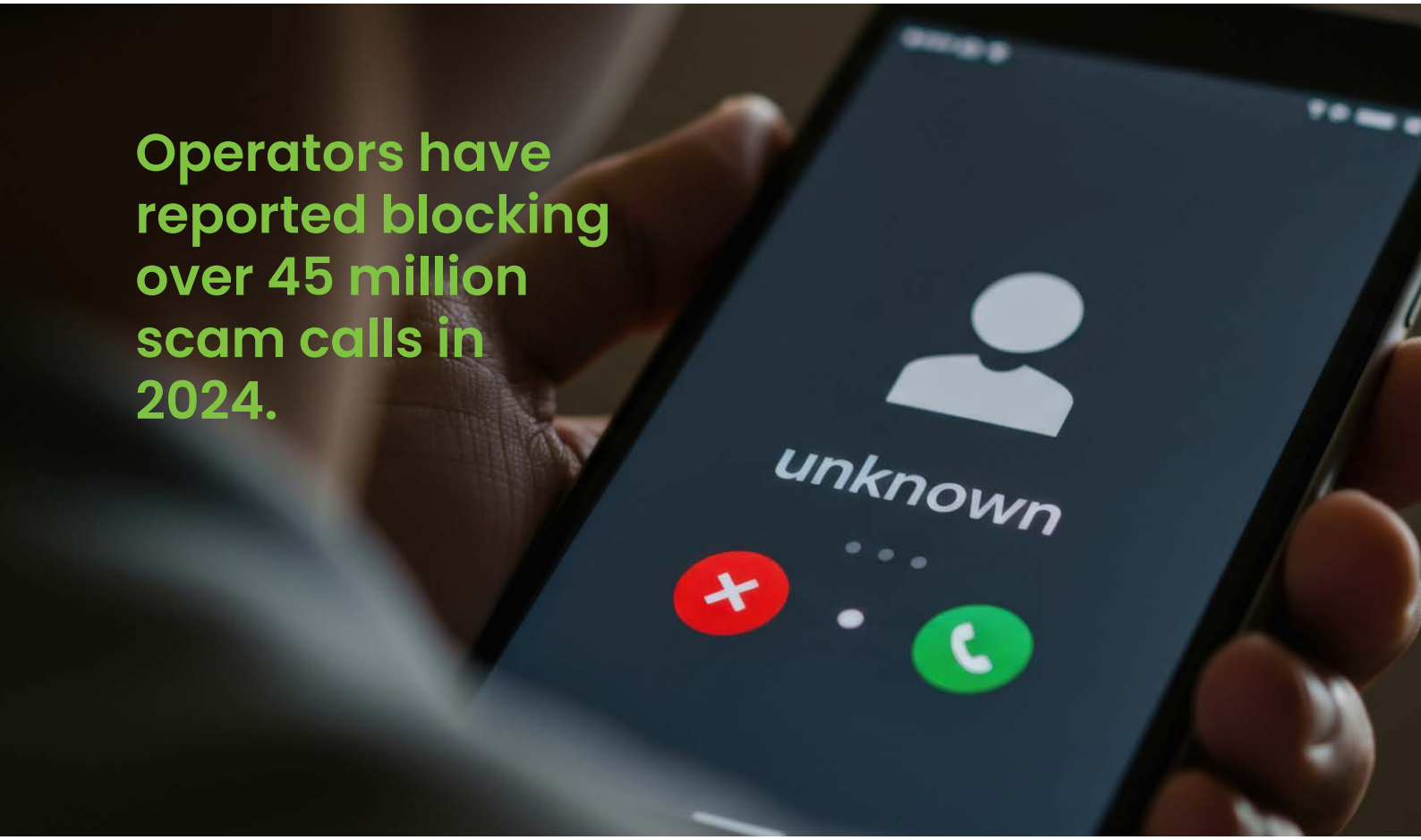
3 NI-ICS are as defined in Article 2(7) of the EECC and Regulation 2 of the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022"), and are now included in the revised definition of an ECS, as set out in Regulation 2 of the Regulations of 2022 and furthermore NI-ICS are now included in Article 2(4) of the EECC

4 ENISA is the European Union Agency for Cybersecurity, see https://www.enisa.europa.eu/.

ComReg gathers information regarding reported security incidents, trends and their resolution. The evidence collected will assist ComReg in determining whether operators of ECN and ECS are managing their various risks appropriately and in accordance with their obligations.

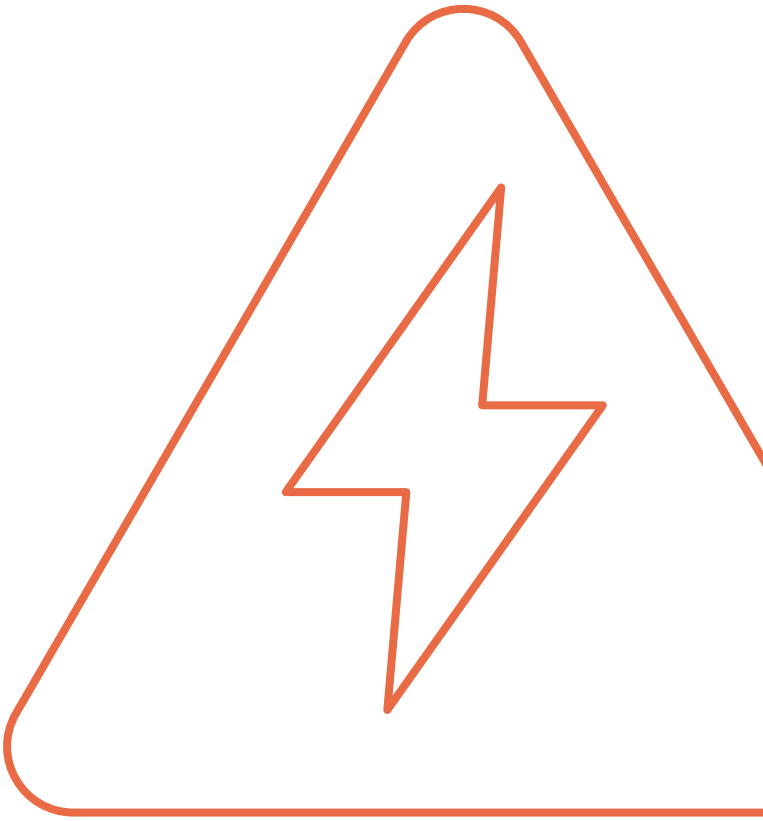
If operators are found wanting in their obligations, ComReg will consider using the powers available to it under Part 2 of the Act of 2023, to ensure that operators meet their obligations. Section 3 of this document provides detail on the Outdoor Mobile Coverage Map and it's integrity. ComReg's Outdoor Mobile Coverage Map shows ComReg's predicted mobile outdoor coverage across Ireland.

Finally, Section 4 outlines ComReg's newly established Network Trust function. Network Trust's primary aim is to work with operators to identify and deploy a series of network based counter measures to mitigate the frequency and volume of scam calls and texts. Operators began to deploy practical measures to combat voice scams in 2024. Operators have reported **blocking over 45 million scam calls in 2024**, showing the real-world effectiveness of these interventions. Additional counter measures aimed at further reducing scam calls and tackling scam texts are planned for deployment in 2025.



Operators have reported blocking over 45 million scam calls in 2024.

2



Resilience, Security Incidents and Reporting, Decision Instrument D08/24

2.1 Resilience of Networks and Services

Resilience as the term relates to ECN or ECS (including NI-ICS), describes the ability of a provider's network or service, to return to its normal state following a disruptive security incident. Security incidents are defined in section 5 of the Act of 2023 as

> *"any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services".*

In order to ensure that providers' ECN or ECS are appropriately resilient, section 6 of the Act of 2023 obliges providers to appropriately manage the risks to their ECN and ECS. When a significant security incident occurs, providers must report such incidents to ComReg. Following such incidents, providers through their root cause analyses – including user hours lost as an indication of scale, and with a view to the obligations under section 6 above in respect of ECS and ECN resilience, should consider learnings from these experiences and take appropriate measures to mitigate future security incidents – particularly to minimise user hours lost.

The resilience of an ECN or ECS includes its core[5], distribution, or access networks. Each of these can adversely affect the provider, its customers, or other providers of ECN or ECS who might rely on wholesale access or interconnection to the impacted network or service. Furthermore, a large security incident that affects a provider's network resilience, at the core or distribution level, can have effects that spread beyond Ireland, such as those affecting international switching or routing or a damaged international fibre network.

In April 2023, ComReg published its Decision Instrument D08/24, together with its Response to Consultation 24/23[6] in respect of Network Incident Reporting Thresholds. This revised and replaced ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards) ("Consultation").

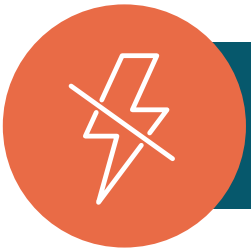
5 The core includes all relevant Operational and Business Support Software (OSS and BSS) necessary to manage the network
6 Network Incident Reporting Thresholds: Response to Consultation | Commission for Communications Regulation

2.2 Security Incidents

Security Incidents are defined in section 5 of the Act of 2023 as "any action that compromises the availability, authenticity, integrity or confidentiality of 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". Typically, causes of security incidents can include:

Weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms

Third party damage including: vehicular impact, cable theft; fibre cuts, deep diving submarines, remotely operated vehicles ("ROV"), anchor, cable plough or trawler related, cable damage



Power outages due to weather, including: prolonged power outages over a number of days, insufficient protection (for example surge protection) of mains supply, insufficient or no back-up power and poor maintenance of back-up power

System failures including but not limited to hardware and software failure; insufficient redundancy; poor procedures, particularly 'roll-back' procedures[7]; poor supervision of both own and outsourced staff

Malicious acts: theft, Telephony Denial of Service ("TDoS") incidents, Distributed Denial of Service ("DDoS") incidents, cyberattacks, vandalism, espionage, and sabotage

7 This is where a software or hardware change is restored to its original state prior to the implementation of the change

2.3 Reporting of Security Incidents and Thresholds and Obligations on providers.

ComReg's approach to the management of reported security incidents and the coordination of its response to these incidents, is set out in its its Decision Instrument D08/24 (see Network Incident Reporting Thresholds: Response to Consultation, ComReg Document 24/23 ("Document 24/23")).

At sections, 11, 13, 14,15 and 16 of the Act of 2023. ComReg notes that the security incident reporting obligation applies to all "providers" of ECN and ECS, the term 'provider' having been defined in section 5 of the Act of 2023. Further, it should be noted that failure to comply with section 11 (subsections, 1, 3 and 6) of the Act of 2023 is an[8] offence .

Document 24/23 sets out the updated thresholds for reporting Security Incidents to ComReg. See figure below:

	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1%-2%					
2%-5%					
5%-10%					
10%-15%					
>15%					

Table 1: Thresholds, as a Percentage of National User Base and Incident Duration[9]

Providers must also report any security incident affecting availability, greater than or equal to one million (1,000,000) User Hours and any security incident impacting 1% or more of the National User Base and which affects the confidentiality, integrity or authenticity of that service.

All significant security incidents **must** be reported to ComReg using the prescribed incident reporting portal.

Once ComReg has been notified by a provider of a security incident that has had a significant impact on the operation of ECN or ECS; ComReg must in turn inform the Minister for Culture, Communications and Sport (the "Minister")[10] who then may rely on this information when apprising Government and Dáil Éireann.

Following the agreement of the Minister and if other Member States ("MS") are affected then, if necessary, ComReg must also notify the respective NRAs or Competent Authorities ("CA") in other MS and ENISA[11].

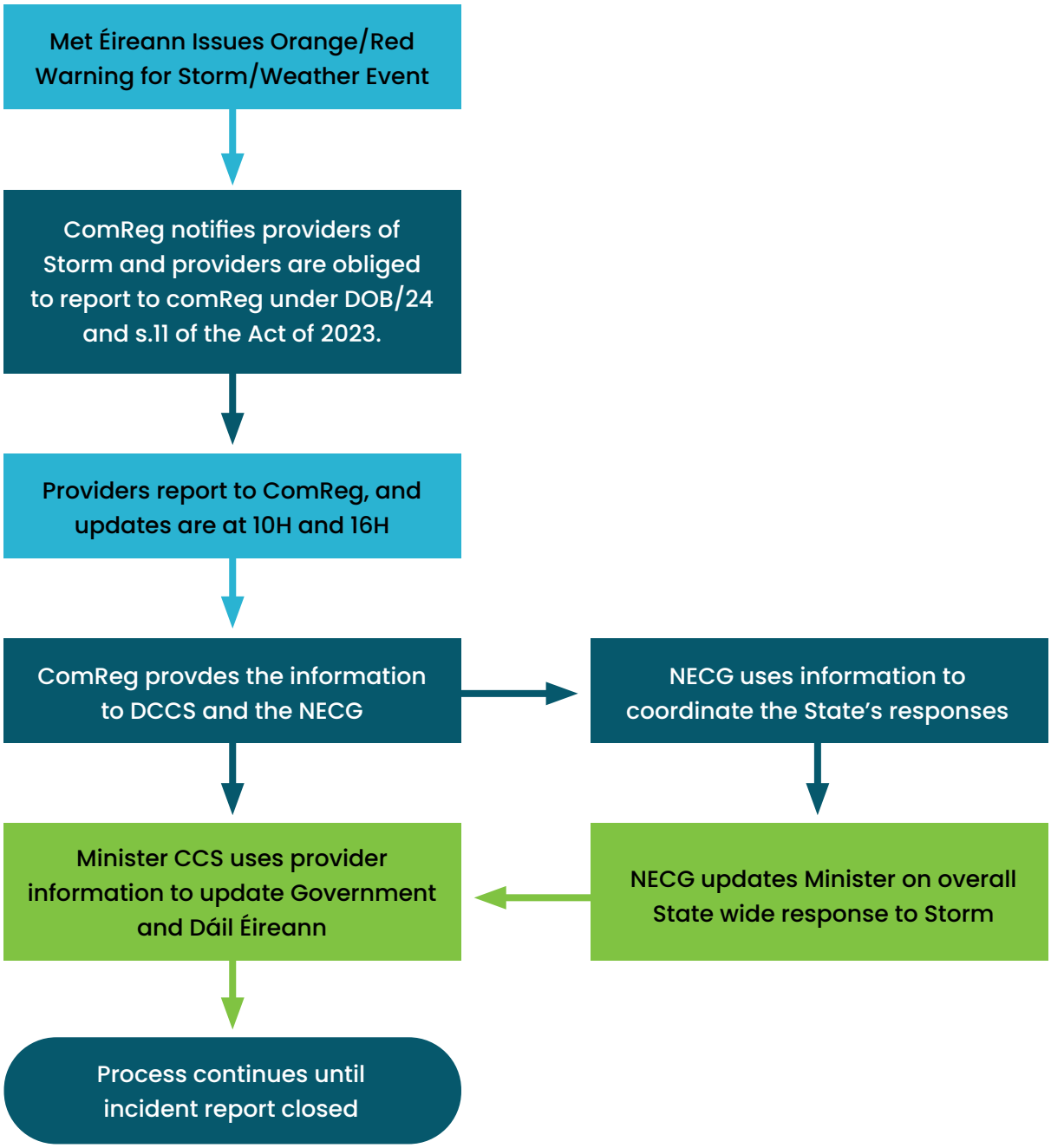
8 Under section 11(8)a and b of the 2023 Act: Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, Section 11

9 The red area denotes that a significant security incident has occurred and that the threshold has been reached or exceeded.

10 Minister for the Environment, Climate and Communications as of 2024

11 ENISA is the European Union Agency for Cybersecurity, see https://www.enisa.europa.eu/

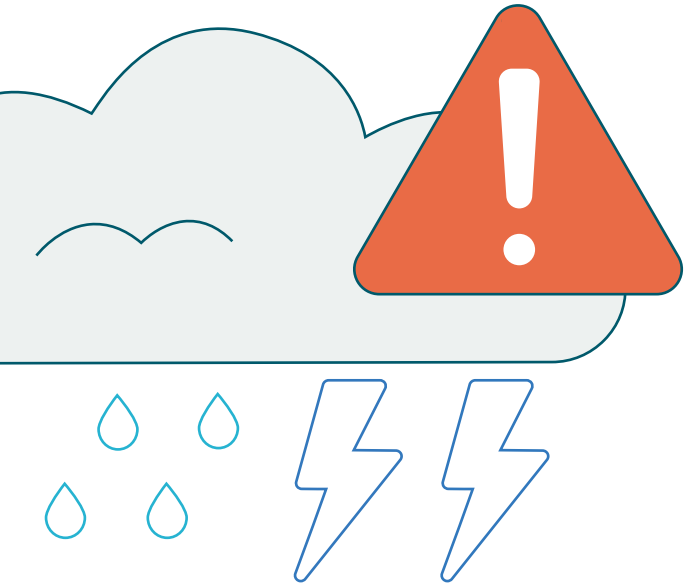
Incident Reporting and Information Flow



ComReg must also submit a summary report annually to the Minister, the European Commission and ENISA regarding the security incidents notified to it. The report for 2024 was lodged with ENISA in February 2025.

2.4 Storms and their Effect on Resilience

During 2024, ComReg monitored both weather and Space Weather[12] events that could affect the provision of ECN and ECS in Ireland.



Storm reporting involves monitoring Met Éireann[13] warnings. If an orange-level warning or named storm is announced by Met Éireann, ComReg monitors it as it develops and, where necessary, communicates with providers of national networks, seeking twice daily reports at 10H00 and 16H00, as required by its Decision D08/24. This information is then passed on to the National Emergency Coordination Group ("NECG") via the Department of the Environment, Climate and Communications ("DECC") (now the Department of Culture, Communications and Sport or "DCCS") and Minister, as appropriate.

Requests for assistance from providers are passed via the NECG to appropriate State agencies, to assist where possible in a quicker resolution of any outage, than the operator might achieve of itself.

2.5 Overview of incidents reported to ENISA in 2024

The main highlights of the 2024 Annual Summary Report to ENISA are as follows:

15
Incidents reported to ComReg in 2024
(Compared to 16 in 2023)

32,574,831
Total user hours lost in 2024
(Compared to 22,818,885 in 2023)

Figure 2 provides the count of security incidents reported in 2024 and figure 1 provides the comparison of security incidents in 2023 and 2024.

12 In relation to Space Weather ComReg uses the tools offered by the NOAA and a useful information on Space Weather and its possible effects is here: https://www.swpc.noaa.gov/news/space-weather- educational-video

13 using tools which rely upon data from the European Centre for Medium-Range Weather Forecasts ("ECMWF") model and from the US National Oceanic and Atmospheric Administration ("NOAA"). The latter can give advance warning of Atlantic storms that originate as Atlantic Hurricanes and also gives warning of Space Weather Events. There were two major G5 Geomagnetic space weather events in May and October 2024, neither of which had any reported effects on ECN and ECS in Ireland.

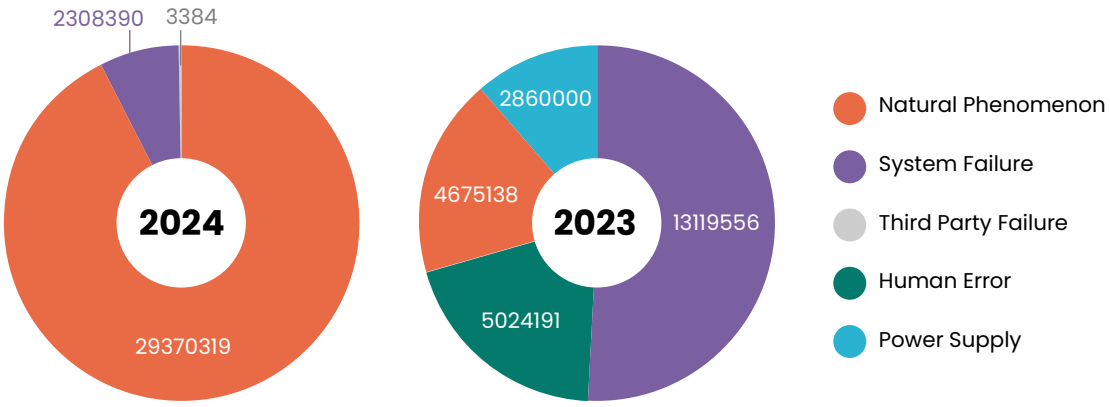


Figure 1: Comparison of security Incidents in 2023 and 2024

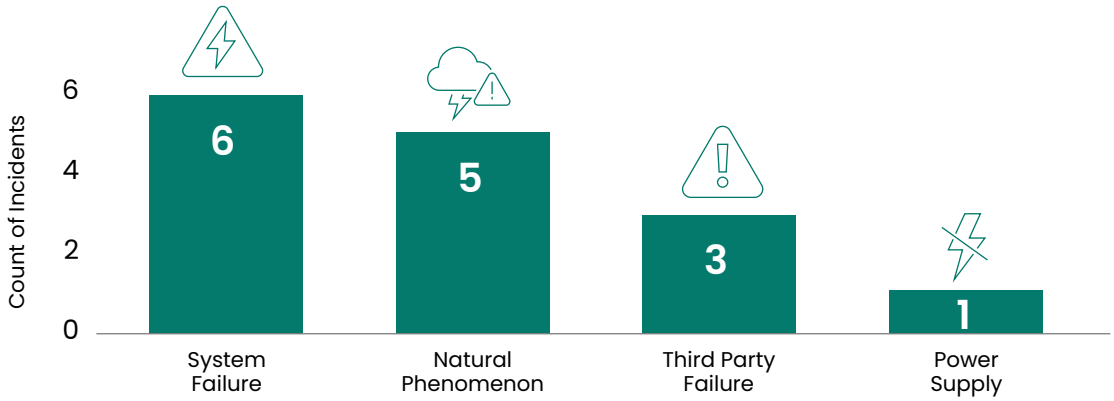


Figure 2: Count of security Incidents in 2024

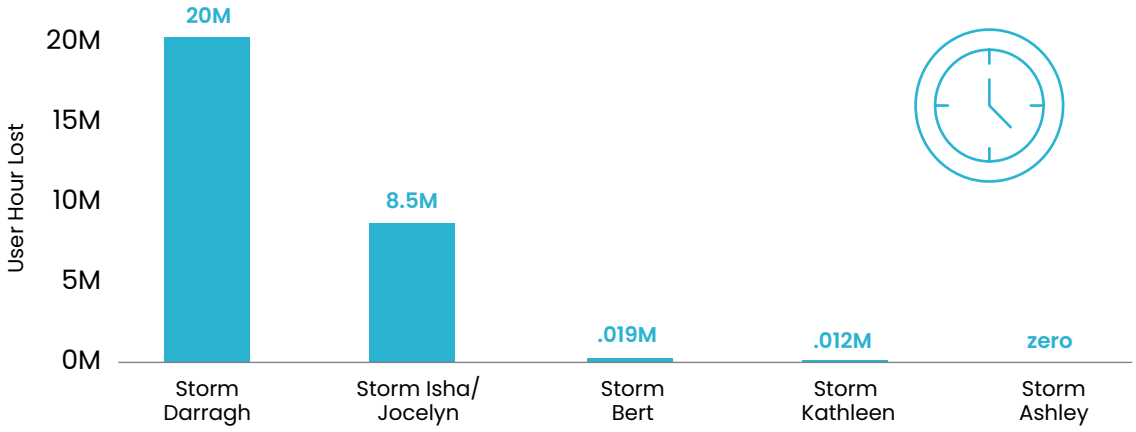


Figure 3: User hours lost due to storms in 2024.

3

Outdoor Mobile Coverage Map

The outdoor mobile coverage map is regularly updated with three revisions taking place during 2024.

ComReg's outdoor mobile coverage map allows consumers to gauge the level of mobile coverage they might reasonably expect to experience in their own localities. Amongst other things, this information helps consumers to make an informed choice regarding their mobile service provider. The outdoor mobile coverage map is regularly updated with three revisions taking place during 2024. The revisions take account of new sites and incorporate changes to the technology used which not only positively impacts coverage but can also lead to an improvement in services.

To ensure the integrity of ComReg's Outdoor Mobile Coverage Map, ComReg conducts numerous drive tests, via its contractor, in specific locations nationwide and collects network measurements from each of the mobile operators networks.

Through its contractor, ComReg deploys network measuring equipment in up to 30 vehicles that drive multiple routes, numerous times in specific locations, for a specific period, collecting network measurements from the mobile operators networks. These network measurements are then used to contrast real user experience with the Outdoor Mobile Coverage Map. This allows ComReg to identify aspects of the Outdoor Mobile Coverage Map that might require model retuning to better replicate real user experience.

4

Nuisance Communications

4.1 Background

Ireland is heavily reliant on telecommunications which are deeply embedded in our every-day lives. The emergence of scam calls and texts and their unrelenting frequency, means that many Irish consumers have lost trust, when their phone rings or the Sender ID appears on a text message. The Behaviour & Attitudes ("B&A") Survey, commissioned by ComReg in 2023, revealed a frightening picture and highlighted the sheer scale of this scourge:

50%
of consumers now require some confirmation of the legitimacy from the caller or sender of a text, before they will even answer a call or reply to a text.

40%
of consumers that use SMS services have lost trust in this form of communication and increasingly pay less attention to it.

90%
of adults in Ireland have received a scam call, while 84% have received some form of scam text.

1 in 4
consumers pay no attention at all whatsoever to SMS messages they receive.

€300m+
Scams are costing Irish society in excess of €300m each year.

Given the complexity and interrelation of the actions required to combat this epidemic, ComReg continues to work with communications operators and other stakeholders to identify and deploy implement a series of network-based counter measures and interventions.

Five anti-scam measures are being deployed to reduce the prevalence of scam calls and these are described in more detail below. Further, an as an initial measure to help address scam messages, ComReg is deploying an SMS Sender ID Registry which it is planned will go live in July 2025.

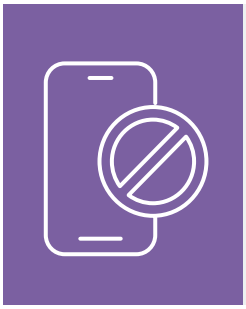
ComReg is pleased to note that these interventions are already having a significant effect and is grateful to the communications industry for its unceasing commitment to combatting scams.

Protected Numbers ("PN")

The PN list contains number ranges, sub-ranges or individual numbers that have not been allocated by ComReg to any operator. Spoofed calls that attempt to use a Protected Number as a Calling Line Identification ("CLI") are illegitimate and are now being blocked.

Do-not-originate list ("DNO")

Many organisations have telephone numbers that are never used for making outgoing calls. These are usually phone numbers that consumers call for service information, such as reporting a lost credit card. Using CLI spoofing, fraudsters can make calls appear to originate from these "inbound-only" numbers to trick consumers into answering their bogus calls. A list of such "inbound-only" numbers is called a Do Not Originate list. All operators now block calls from these numbers to prevent fraudsters impersonating legitimate organisations.

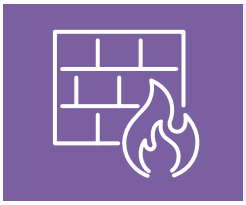


Fixed CLI call blocking

Using CLI spoofing to disguise their identity and exploit the trust consumers place in Irish numbers, fraudsters based overseas can make calls appear to originate from an Irish landline. The Fixed CLI call blocking intervention identifies and blocks scam calls originating from outside the country presenting with spoofed Irish landline numbers.

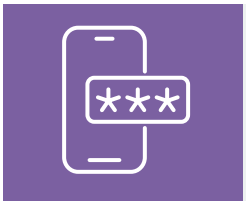
Mobile CLI call blocking

This intervention helps protect against spoofed Irish mobile calls originating from abroad. Operators now identify and block most internationally originated scam calls presenting Irish mobile numbers, preventing fraudsters impersonating legitimate Irish organisations.



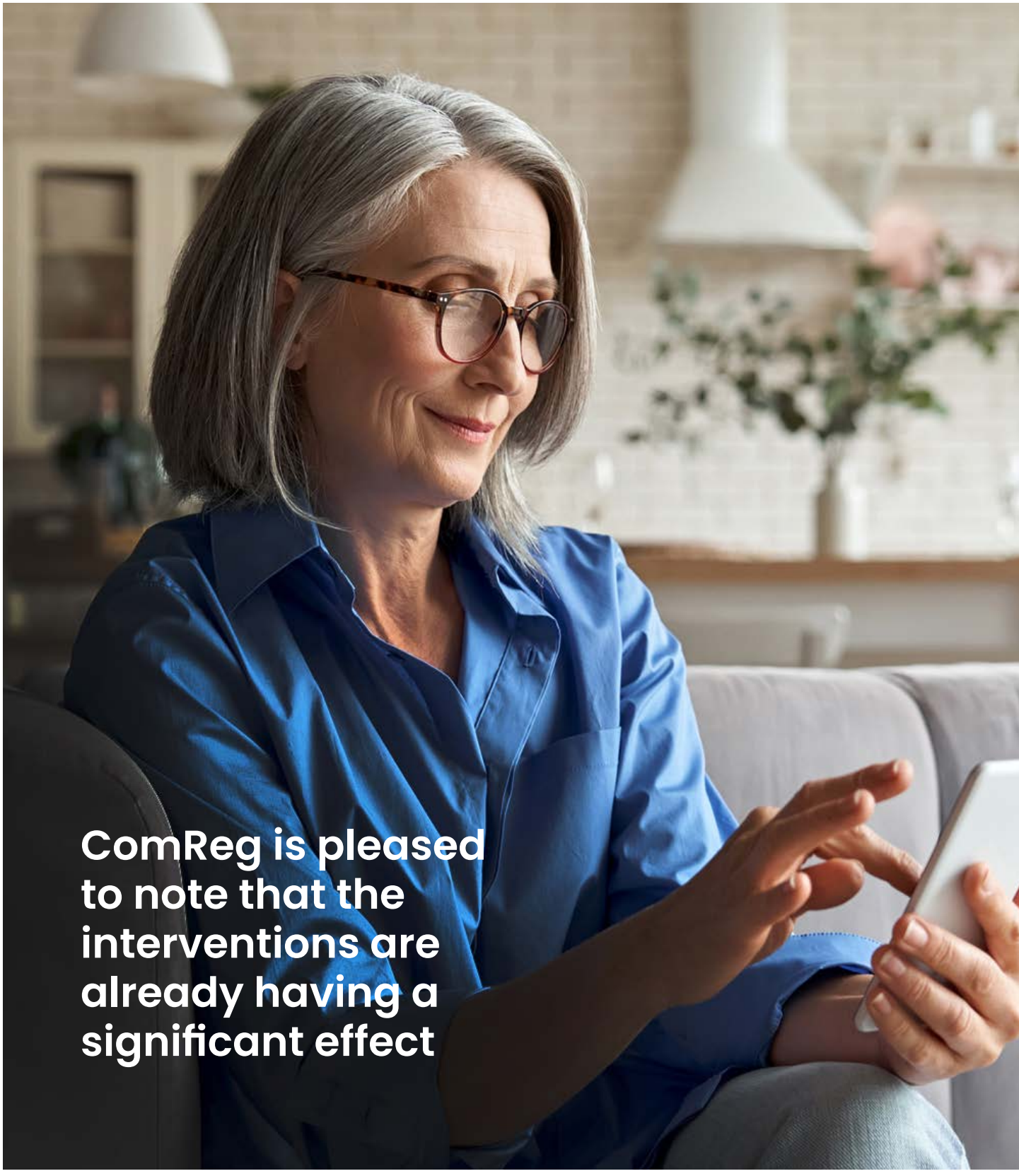
Voice Firewall

This dynamic intervention will utilise machine learning to block spam calls when they arise in Ireland or abroad and will help to protect against current and future sophisticated scams.



SMS Sender ID registry

This intervention will allow businesses to register their SMS Sender ID. Operators will then block any message bearing a sender ID from any source other than the registry.



Note that both the Voice Firewall and the SMS Sender ID Registry listed above, as mandated in Doc 24/24 will both become active in the second half of 2025.

An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation