



An Coimisiún um  
**Rialáil Cumarsáide**  
Commission for  
**Communications Regulation**

# Combating scam calls and texts

Non-confidential submissions to Consultation  
23/52

**Submissions to Consultation**

**Reference:** ComReg 24/24s

**Date:** 03/04/2024

## Submissions Received from Respondents

Document No:	24/24s
Date:	03/04/2024

Consultation:	23/52
Response to Consultation:	24/24

# Content

<b>Section</b>	<b>Page</b>
1 ALTO.....	5
2 Bandwidth (t/a Voxbone).....	6
3 Bank of Ireland.....	7
4 Banking & Payments Federation Ireland .....	8
5 BT Ireland.....	9
6 Cellusys.....	10
7 Eir.....	11
8 Ericsson .....	12
9 Hiya .....	13
10 i3forum .....	14
11 IBEC - Telecommunications Industry Ireland.....	15
12 Imagine .....	16
13 Joe Sheerin .....	17
14 Johnny Bugler .....	18
15 Magrathea.....	19
16 Mobile Ecosystem Forum (MEF) .....	20
17 Microsoft.....	21
18 Netnumber .....	22
19 Openmind.....	23
20 Risk & Assurance Group (RAG) .....	24
21 Revolut.....	25
22 Sky .....	26
23 Tanla .....	27
24 Tesco Mobile.....	28
25 Three.....	29
26 Twilio .....	30
27 Verizon .....	31

28	Viatel .....	32
29	Virgin Media .....	33
30	Vodafone .....	34
31	XConnect .....	35

# 1 ALTO

# alto

alternative operators in the communications market

**Consultation: (“Combating scam calls and texts”) on network based interventions to reduce the harm from Nuisance Communications - Ref: 23/52**

**Submission By ALTO**

**Date: August 31<sup>st</sup> 2023**

ALTO is pleased to respond to the Consultation: (“Combatting scam calls and texts”) on network-based interventions to reduce the harm from Nuisance Communications – Ref: 23/52.

ALTO welcomes this opportunity to comment on this important consultation. ALTO also expressly acknowledges three items:

1. ComReg’s publication of the Draft Technical and Functional specifications for each intervention proposed;
2. ComReg’s willingness to engage with some 23 clarification questions arising from industry and the transparency obvious from that approach, as set out in ComReg document Reference: 23/75 (while ALTO had not submitted its own clarification questions it was aware of and supported the approach taken by IBEC TII and supported that approach);
3. ComReg’s willingness to extend the time for Consultation from 28 July 2023 until 31 August 2023, as is also set out in ComReg document Reference: 23/75.

### **Preliminary Remarks**

The backdrop to this Consultation arises from a political commitment by ComReg to endeavour to combat scam calls and texts. This is clearly an area of concern across society and one in which the telecommunications industry has a role to play. That said, combatting mercurial and often criminal or fraudulent conduct is complex and not without cost and very significant challenges – to some extent it is appropriate to comment that fixing the issue of scam calls and texts entirely may be impossible.

As can be seen from the market leading Verizon Data Breach Incident Report (“DBIR”) of 2023,<sup>1</sup> many of the scam calls and texts arise in order to scam individual users and citizens in some way or another. Incidences of fraud remain extremely high and in 50% of scenarios pretexting over telecommunications networks, whether by cold calling, SMS, or spam messaging appears to catch users out. The DBIR calls out that users are, in the main – and up to the 80<sup>th</sup> percentile, responsible for fraud, and being accountable for data or cyber security breaches.

In ALTO’s submission, there is no substitute for ComReg engaging in information campaigns concerning messaging frauds and user education, as it should do as the regulatory agency with responsibility for numbering and communications in Ireland.

ALTO is aware of the various workstreams that operate and have operated under the Nuisance Calls Intervention Taskforce (“NCIT”) over the past 18 months and also some of the solutions that have been addressed in the various NCIT working groups.

ALTO is also aware of the wishes of ComReg to implement a Nuisance Calls Firewall solution on the market. While we support the ultimate aims of this initiative, it cannot be an effective solution if certain operators either fail to invest, or neglect regulations. The issue being that a firewall is useless in scenarios where it is not ubiquitous. Scam calls will simply re-route within moments, to achieve the intended purpose of their initiation on telecommunications networks and to defraud users. ComReg must carefully assess the proportionality of intervening in a manner that may be costly and ultimately useless.

ALTO observes that the time has come for ComReg to consider re-establishing the Numbering Allocation Panel (“NAP”) or a form of new NAP to consider and properly debate issues surrounding number allocation; number sub-allocation; number hosting; and the entire area of innovative Interpersonal Communications Services (“IPS”) which arise variously in Directive (EU) 2018/1972 of the European Parliament

---

<sup>1</sup> <https://www.verizon.com/business/resources/reports/dbir/>



and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“EECC”). We note in particular Articles 2, 12, 61, and 93 of the EECC in that regard.

ALTO observes that sub-allocation of numbering has been a feature of the Irish market for many years at this stage, and the fact of the matter is that some operators are present on the market, perhaps as facilitators of or are Over The Top (“OTT”) providers, that may be using sub-allocated numbering to facilitate communications services. This is no criticism of ComReg or indeed Ireland’s pro-competitive stances when handling numbering and innovation historically, however, ComReg appears to have either deleted or removed sub-allocation from the National Numbering Conventions in or around 2015, despite what the industry might have understood the regulatory position to have been. ALTO submits that ComReg should take a liberal approach to pre-existing operations and operators that might rely on either sub-allocation or hosting solutions, rather than taking a guillotine approach to regulation in this particular space.

There are various forms of operators on the market that should be fully considered by ComReg prior to the making of a formal decision in relation to how numbering should operate. Examples: White-Label Network Operators; and Switchless Resellers; Virtual Access Operators (FVNO and MVNO). ALTO favours an approach to numbering that is both regulated and sub-allocation permissive with certain criteria, an example of this is available for ComReg to review on the Polish market, where one level of sub-allocation is permitted with strict reporting criteria as against the operator engaged in the sub-allocation. Where pre-existing sub-allocation is extant on the market here, we submit that ComReg should continue to permit the practice but only so as not to force expensive migrations away from existing solutions. Examples of a more flexible approach can be found on at least two European markets.

## **Network Based interventions**

Reporting: Some operators on the market are unable to provide relevant information due to the legacy systems they used and it would be disproportionate to require them to invest in a new system for the sole purpose of reporting. ALTO suggests that ComReg changes the reporting requirement into a voluntary arrangement, following a similar approach as in the UK market, that in our submission is in order.

International Mobile CLI blocking: Both interventions identified by ComReg at phase 1 and 2 are very costly and burdensome. ALTO believes it is disproportionate to require the industry to make an important investment twice, first for the design and implementation of a MAP protocol-based roamer check solution and then for the design and implementation of a IP based solution.

Furthermore, there is a very limited pool of fixed Communications Providers who have developed a mobile call query functionality on their switches. We are also unaware of which operators intend to offer a wholesale service to smaller providers. In any case, it is essential that the tariff of such a wholesale solution is defined in a clear and transparent way in order to maintain the competitiveness of smaller players.

## **Know Your Customer – KYC**

KYC is fundamental to ensure Communications Providers are confident of how their customers use valid numbers. Using a third-party risk management vendor could also ensure a high level of consistency in the approach taken by providers while removing the burden from them – ALTO encourages ComReg to consider this further, in line with our comments above.

ALTO believes the ComReg guide includes some helpful suggestions for those Communications Providers who have yet to fully implement processes to ensure

they know their business customers. Communications Providers who have already implemented robust and efficient processes should not be required to implement new processes. Amongst other things the risk profile of business customers should be considered. For example, it is not proportionate to require Communications Providers to implement new and highly prescriptive processes for corporate and enterprise customers. These types of customers will have low risk profiles with regard to number misuse.

By definition, the measures mentioned in the ComReg guide are only suggestions and ComReg should avoid being prescriptive on measures Communications Providers are expected to implement to ensure their compliance with their regulatory obligations. Rather, ComReg should focus its guidance on encouraging Communications Providers to support the principle of assigning numbers to low risk and/or reputable customers, while allowing them flexibility to define the relevant measures for their customer base and service offerings.

### **Prohibition on sub-allocation of numbers**

ALTO submits that sub-allocation of numbers is essential for the continuity of pre-existing wholesale offerings on the market and we consider (as we state above) that a more flexible approach such as the one taken by Ofcom should also produce positive results (ensuring that wholesale customers also have KYC process in place). We note that Ireland's historically pro-competitive approach to numbering and innovation should not stall as a result of a fear of fraudulent behaviours. Regrettably, and as is clear, a one-size-fits-all model will not work on the market and very careful consideration of number dependent OTT or IPS providers and other forms of provider will need to be undertaken – perhaps under the auspices of a newly formed NAP.

## **Response to Consultation Questions**

**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.**

A. 1 ALTO generally supports ComReg's proposals concerning DNO; Protected Numbering; Fixed CLI blocking; and Mobile CLI blocking. ALTO welcomes appropriate regulation to enable these innovations to occur on a proportionate level.

ALTO submits that ComReg must avoid a situation where regulation deployed does not fit the technological deployments active on the market, e.g., obviously, the future will likely involve SIP rather than POTS voice technology and signalling.

**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.**

A. 2 ALTO supports ComReg's proposals concerning:

- the deletion of the 076 range, given the position that now engages on the market. the new clause 1.4 of the Draft Numbering Conditions, noting that fixed numbers appear to be omitted (unless this was an intentional omission);
- the introduction of long lining text as set out; and
- better identification parameters for 1800 and 0818 ranges and proposals concerning pre-existing ranges as allocated and operating.

**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.**

A. 3 ALTO broadly agrees with and supports ComReg’s general updates to provide CLI guidance.

ALTO limits its remarks to remind ComReg that there are already Communications Providers active on the market in various guises who will be impacted, and in some instances, at high cost and expense to them by the proposals in the ComReg CLI Guidance. This is a strategic matter that must be properly considered by ComReg.

ALTO notes the position on CLIP and CLIR and would call on ComReg to issue a bulletin style standalone Guide on this at a later time and once its deliberations result in a decision on the issues arising on the topic of CLI Guidance more broadly.

**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**

A. 4 ALTO reminds ComReg that it recognises resellers on the Irish market and has done so for many years. While the KYC proposals are broadly agreeable to ALTO, there is a requirement to contemplate how to facilitate existing business. We have made comments above concerning the Polish model and indeed we know that the regulators in the UK and French markets have grappled with similar issues. ComReg should consider those markets and consulting their colleagues widely perhaps through BEREC on the issues arising with KYC. That suggestion is made is in order to find a flexible solution to facilitate pre-existing Service Providers active on the market and other forms of potentially innovative business models that may not have been fully considered.

**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**

A. 5 ALTO repeats that there is now a requirement to “*dust down*” the NAP, or perhaps to reinvent it with an ongoing eye to the issues handled in the NCIT working groups.

The ComReg political commitment to combat scam calls and texts is intrinsically linked to the management and operation of the national numbering resources with an eye on technological developments and avoiding disproportionate cost versus effort initiatives. As previously mentioned, scams are mercurial and usually linked to overarching fraudulent and or criminal enterprise. As soon as a mechanism to block calls arises, another way to route or defraud is usually found to confront the unsuspecting consumer and market with further ways to fall victim via technology.

ComReg should avoid measures that appear to impact any particular form of call flow or attempt to implement measures that could impact the wider EU market, whether inadvertently or not. ALTO has always represented the interests of some of the world’s largest communications carriers and it is obvious that those carriers are now carefully considering ComReg’s proposals with a view to whether or not international traffic and calling is being disproportionately treated.

ALTO reminds ComReg of the International Destination and Dialler Scam Blocking incident in 2004 concerning ComReg’s directions to block certain destinations from accessing and originating calls from the Irish market.<sup>2</sup> Those directions were ultimately reversed very soon after ComReg directed implementation owing to international pressure.<sup>3</sup> ALTO had met with the Ambassador to the Solomon Islands

---

<sup>2</sup> ComReg Decision Notice, D13/04

<sup>3</sup> Page 38 of 313 of the Consultation paper references the Decision, but not the fact that the planned network interventions were effectively disallowed. Link: <https://www.siliconrepublic.com/enterprise/regulator-rolls-back-modem-hijacking-prevention-steps>

and with other embassy staff and representatives of blocked destinations at the time. It was not a workable solution unfortunately.

As mentioned above, an appropriate forum should be introduced or reintroduced to deal with all issues arising, concerning numbering, nuisance calls, CLIP/R, and text scams even if those with a historical institutional knowledge of the NAP within ComReg might demur from such a suggestion.

**ALTO**

**31<sup>st</sup> August 2023**

## 2 Bandwidth (t/a Voxbone)



## Combatting scam calls and texts

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

Bandwidth Inc., and its wholly-owned operating carrier in Ireland, Voxbone S.A, (“Bandwidth”) welcomes the opportunity to comment on Comreg’s public consultation regarding network based interventions to reduce the harm from nuisance communications (hereinafter referred to as “the Consultation”). Bandwidth has been an active leader in the industry’s efforts to protect consumers from fraud and abuse in the form of illegal robocalling for a number of years. Bandwidth looks forward to supporting Comreg’s efforts to stem the proliferation of illegal activity in the global communications marketplace while simultaneously continuing to advance policies that support valuable consumer-driven innovative cloud communications in Ireland as well. Bandwidth commends Comreg for undertaking a thorough and comprehensive analysis of a very complex set of issues and objectives in this Consultation and appreciates the opportunity to share its perspectives and experiences as the consultation proceeds.

#### **A Do Not Originate (“DNO”) list and Protected Numbers (“PN”)**

Among the proposed tools that are aimed at preventing robocalling fraud and abuse are the adoption of methods to utilize DNO and PN lists. Bandwidth welcomes the introduction of a DNO list in Ireland. Implementation of a DNO list is a relatively low cost measure which has shown significant effectiveness in other jurisdictions, as evident from the experience in Australia, Belgium, the UK and the US.

Equally, we consider the blocking of unallocated numbering ranges as a sensible and effective measure. The process by way of monthly confirmation from Comreg of protected numbers along with the DNO list is a practical way for providers to be kept up to date on which numbers to block. We would like to emphasize the need for providers to be given sufficient time to update their systems before any numbering ranges are removed from the protected numbers list and made available for allocation. We believe 6 months is a reasonable timeline for providers to implement both the DNO and PN list.

#### **STIR/SHAKEN**

In the Consultation Comreg considers the technical feasibility, viability and effectiveness of implementation of STIR/SHAKEN in Ireland. Bandwidth appreciates Comreg’s position in the Consultation that given the continued proliferation of traditional non-IP networks in Ireland, it does not believe that STIR/SHAKEN is a viable option at this point.<sup>1</sup> While it is a fair and accurate reflection of the

---

<sup>1</sup> See: The Consultation at Sec. 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.”



current marketplace dynamics in Ireland, and in many other markets globally, Bandwidth firmly believes that consumers will benefit to the greatest degree from continued adoption of Internet Protocol-based (“IP”) networks and services, which include the benefits of STIR/SHAKEN helping to restore trust in global voice calling while also continuing to advance robust consumer-driven feature functionality as well.

#### Voluntary implementation among IP operators

Bandwidth has been a leader in VoIP services in the United States and at the forefront of advancing STIR/SHAKEN as a competitively and technologically neutral way to reinstall trust into the voice calling ecosystem. To that end Bandwidth, has also made the commitment to support efforts to implement STIR/SHAKEN as broadly as possible through a newly formed commercially operated STIR/SHAKEN framework that is designed to support trusted cross-border IP traffic exchange globally, including in Ireland (“Cross Border Framework”). Proactively embracing near term options such as this can significantly help to advance the objectives that are set forth in the Consultation with an eye toward the IP future ahead.

Together with other founding members Microsoft, Google and RingCentral, Bandwidth is advancing a non-jurisdictional governance authority that includes critical expert support of the telecoms standards body ATIS as well as the established policy administrator (“PA”) in the United States, iconnectiv. The Cross Border Framework that is being developed is aimed to operate across international borders to support IP-based services that are fundamentally global in nature in the future. Because the Cross Border Framework will operated according to the STIR/SHAKEN global technology standards, it is not tied to a particular country and can be available to voice service providers in countries where token-based CLI authentication has not been implemented on a national basis as well as interoperating in a trusted and transparent manner with those jurisdictions that have established their own STIR/SHAKEN frameworks as well. Ultimately it is intended to allow trusted voice service providers that have IP networks and services to interoperate and exchange authenticated traffic with each other ubiquitously according to the technologically and competitively neutral standards of STIR/SHAKEN.

For providers transitioning to IP networks, the use of STIR/SHAKEN on a voluntary basis can provide standardized technical tools to support call-handling solutions to better protect their respective subscribers from threat of illegal spoofed calls. By leveraging call attestation information providers can enhance the overall trust of their services. Furthermore, originating providers also acknowledge the value of STIR/SHAKEN in mitigating the increasing risk of their customers’ calls being improperly blocked by terminating providers. By voluntarily implementing STIR/SHAKEN authentication among a group of providers with IP networks, participating providers can ensure the seamless delivery of legitimate calls to both national and international destinations.

#### Recognizing the need for cross-border attestation:

Comreg notes that the effectiveness of STIR/SHAKEN as a tool in combatting fraud and abuse in the form of robocalling would depend on widespread adoption of IP networks and services across operators in Ireland and on at least a quasi-global scale. As noted above, Bandwidth recognizes Comreg’s assessment of current marketplace conditions but believes the public interest demands that Comreg continue to work to advance the adoption of innovative IP-based networks and services. Rather than relying on outdated network technologies and implementing heavy handed regulatory restrictions that will balkanize voice communications in Ireland and elsewhere, advancing well-established standards in a



reasonable manner will enhance consumer choice and marketplace benefits. A Cross Border Framework can address this gap.

The Cross Border Framework is establishing processes to ensure that voice service providers meet strict requirements for participation. Having selected iconectiv as its PA, the Cross Border Framework will have processes for vetting and approving service providers and certification authorities, issuing tokens, verifying originating providers for terminating and gateway providers, and enforcing Cross Border Framework policies.

Each service provider must provide the policy administrator with information necessary to authenticate the provider and determine they are legitimate and trustworthy. This includes evidence of legal status, contact details, authorization to provide communications services, and other information concerning their compliance and service history. Service providers are required to have processes to identify problem users and support traceback requests. The policy administrator will also evaluate whether the service provider is technically capable of deploying SHAKEN. Once accepted, registered as a qualified member, an originating service provider can obtain a token for signing calls from a certification authority approved by the PA. Other established framework policies such as “token revocation” will support monitoring for abuses of the system and mitigate against such abuses with tools such as the suspension or removal of participants if they violate “right to use” policies or engage in other activities inconsistent with the Cross Border Framework.

#### Implementation plans and Conclusion

Founding member voice service providers are actively working to initiate a commercial Cross Border Framework now. Soon we expect to be able to provide attestations when sending traffic to each other in countries without a SHAKEN framework already established. Considerable progress has been made and initial interest has been positive among other industry voice service providers who are hoped to become members in the coming months ahead to expand the universe of participants and advance IP-communications more broadly in Ireland and globally.

Bandwidth appreciates the opportunity to submit these comments in this Consultation and looks forward to continued engagement with Comreg to achieve more progress toward an increasingly trusted and effective voice communications ecosystem.

## **3 Bank of Ireland**



# Bank of Ireland Submission to ComReg 23/52

31 August 2023

## INTRODUCTION & BACKGROUND

Bank of Ireland welcomes the opportunity to provide its views to the Commission for Communications Regulation on its consultation ref. 23/52 on network based interventions to reduce the harm from nuisance communications. Bank of Ireland welcomes the work to date by ComReg to combat nuisance communications and the range of potential interventions now being considered by ComReg to further protect consumers and businesses.

Scam calls and texts are a significant enabler of serious criminal activity with negative impacts on consumers, businesses, banks, and the wider economy. Bank of Ireland take a wide range of steps to protect our customers and the Bank from this criminal activity, including:

- Resourcing a dedicated fraud team which works 24/7 to catch fraud attempts and alert and protect customers, and to attempt to retrieve customers' money when a fraud attempt is successful;
- Investing in a range of fraud services, tech systems, and upgrades to enhance consumer and business protection from fraud;
- Running ongoing fraud-awareness campaigns directed at customers and the wider public, and supporting the sector in similar activity through our membership of the Banking and Payments Federation of Ireland (BPF);
- Maintaining very active working relationships with national and international police forces and inter-governmental agencies to track emerging threats and help trace criminals;
- Collaborating with a range of stakeholders including telecommunications operators in Ireland and in other jurisdictions to share intelligence on new and emerging fraud trends; and,
- Assessing where national policy initiatives may be brought forward to further bolster Ireland's resilience against fraud, for example the development of a National Financial Crime Strategy and a Shared Fraud Database.

Combined, Bank of Ireland's fraud prevention systems and personnel have prevented c.70% of all attempted fraud by criminals against our customers this year. In the remaining cases, where a fraud was successful, all efforts were made by our teams to recover funds for customers.

The Bank also engages in proactive targeted awareness campaigns to customers through TV and radio advertising, social media activity, email alerts, media interviews, and messaging through its digital banking channels. These targeted awareness campaigns are facilitated by ongoing customer research and analysis of fraud patterns and data. We will continue to invest in these campaigns through 2023 and into 2024.



However, it is also our view that more action is required to protect consumers. Defeating fraudsters and combating criminal activity is a collective effort. Collaboration between telecom providers, social media companies, financial institutions, law enforcement agencies and State organisations is essential to better protect consumers from fraud attempts manifesting on social media or via text messages or phone calls.

## **CURRENT COLLABORATION WITH THE TELECOMMUNICATIONS SECTOR**

Bank of Ireland has collaborated with the telecommunications sector in Ireland and in other jurisdictions over recent years to prevent criminal activity. This has included constructive direct relationships with the fraud and security teams in the telecoms operators and wider engagement through cross-sectoral working groups.

Examples of this positive interaction have included:

- Sharing intelligence on current and emerging text and voice fraud trends;
- Identification and shutdown of phone numbers confirmed as being used for fraudulent purposes;
- Identification and blocking of sender ID's being used to distribute fraudulent SMS content; and
- Collaboration on a number of law enforcement investigations.

Bank of Ireland are also members of the Mobile Ecosystem Forum's (MEF) Sender ID Registries in Ireland and in the UK. While MEF's initiative has offered some protection against fraudulent text messages using Bank of Ireland's genuine sender ID's and against text messages impersonating Bank of Ireland by using fraudulent sender ID's, we recognise its limitations and welcome ComReg's proposal for a more comprehensive intervention in this area.

As noted above, combating criminal activity is a collective effort, so we look forward to building on the positive collaboration to date between Bank of Ireland and the telecommunications sector.

## **THE CURRENT FRAUD LANDSCAPE**

Scam calls and texts are highly prevalent and Bank of Ireland's research findings on the percentage of consumers who have received a scam call or text in recent months is broadly in line with the results of ComReg's B&A surveys.

However it is important to note that in a constantly evolving fraud landscape, the brands now being impersonated in scam calls and texts have changed since ComReg's B&A surveys were completed in 2022.

Our latest research (Red C, June 2023) and observation of current fraud patterns has highlighted that scam phone calls are now most commonly impersonating a streaming service, a parcel delivery



company, or a Government agency. Scam text messages are now most commonly impersonating a parcel delivery company, a road toll provider, or a bank.

It is also important to note that Bank of Ireland have taken a number of actions that have led to a significant reduction in the volumes of scam text messages impersonating Bank of Ireland. These scam text messages typically ask customers to click on a link to a fake website – while we can't definitively say how many scam text messages are sent, we do know the numbers of these associated fake websites. This number peaked in H2 2021 and has been steadily reducing since then.

The average monthly number of fake Bank of Ireland websites for the most recent 6 months to August 2023 is down by 91% on the 2022 monthly average and down by 98% on the H2 2021 peak.

It should be further noted that, within this reducing volume of scam texts impersonating Bank of Ireland, the percentage sent from an imposter Bank of Ireland sender ID has also fallen significantly. In the most recent 6 months to August 2023, over 70% of scam texts impersonating Bank of Ireland were sent from mobile numbers and not from sender ID's.

This move away from scam texts being sent from sender ID's, to scam texts being sent from mobile numbers, has been seen across all brands, including the most common current scam texts impersonating parcel delivery companies, road toll providers, or family members.

The vast majority of scam texts impacting Bank of Ireland's customers are now being sent from mobile numbers. In this context, while we welcome ComReg's proposed intervention on Sender ID, we agree with ComReg's view that an SMS Scam Filter would offer far more comprehensive and future-proofed protection for consumers and businesses and believe that such an SMS Scam Filter is vital to ensure that consumers and businesses are protected.

## **POTENTIAL TECHNICAL INTERVENTIONS TO COMBAT NUISANCE COMMUNICATIONS**

While we note that ComReg's proposed interventions will mainly fall to telecommunications providers to implement, we note the following on ComReg's proposals.

### **POTENTIAL VOICE INTERVENTIONS**

**Do Not Originate (DNO):** Bank of Ireland welcomed the trial of this intervention from September 2022. Our experience of the similar intervention operated by Ofcom in the UK market has been good and we believe that DNO is a positive development for consumers and businesses. Bank of Ireland have submitted a list of relevant phone numbers to ComReg and will continue to support this intervention.

**Protected Numbers list / Mobile CLI blocking / Fixed CLI blocking:** As with DNO, these are positive interventions and Bank of Ireland fully support their implementation as soon as possible.



**Voice Firewall:** We believe that this proposed intervention will be key to protecting consumers and businesses into the future. We look forward to working with ComReg and operators to support its rollout.

## **POTENTIAL SMS INTERVENTIONS**

**Sender ID Registry:** Bank of Ireland welcome this proposed intervention but note as above that it will only have an impact on a (reducing) percentage of scam texts, i.e. those that are sent from a sender ID.

Bank of Ireland uses a number of communications providers to carry text messages but does not deal directly with the entities like SMS aggregators that comprise the rest of the SMS delivery chain. We understand that communications providers can use multiple aggregators as part of their normal processes and that messages can be routed through different aggregators or redirected from one aggregator to another. However, Bank of Ireland use only a small number of Sender ID's and are happy to register these in any new Sender ID Registry in line with the rules or code of practice to be outlined by ComReg.

**SMS Scam Filter:** This would give the most comprehensive and future-proofed protection to consumers and businesses so we strongly welcome the proposed intervention. As ComReg have noted, a Scam Filter would be dynamic and able to evolve to meet new threats – given the constantly evolving nature of scam texts, this is a key consideration.

We acknowledge, as ComReg have outlined, that content scanning would be necessary for effective implementation. We note also that SMS Scam Filters operate very successfully in other jurisdictions to protect consumers and businesses and to prevent fraud.

## **CONCLUSION**

Bank of Ireland welcomes the work to date by ComReg and by telecommunications providers to combat nuisance communications and the range of potential interventions now being considered to further protect consumers and businesses.

Bank of Ireland supports the proposed interventions and will continue to work with the telecommunications sector to support their implementation.

We will also continue to invest in fraud prevention technologies and in fraud awareness programmes to protect our customers.



# 4 Banking & Payments Federation Ireland

## **Banking and Payments Federation Ireland Response to Consultation on Combatting Nuisance Communications**

### **Introduction**

The Banking & Payments Federation Ireland welcomes ComReg's consultation on measures to combat nuisance communications via calls and texts. In recent years, the fraud landscape in Ireland has evolved significantly. Fraud previously consisted of criminals hacking into bank systems, online scams and even some in-person attempts. Nowadays fraudsters have found that it is easier to manipulate the customer directly into handing over personal and financial information. The most prevalent channels being text and online.

The other change that we have noted is the modus operandi of fraudsters, when BPFi first set up our fraud awareness programme in 2017 (FraudSMART), the most common scam no matter the channel was bank impersonation scams. Due to prevention measures and extensive education and awareness through FraudSMART, we now see ourselves in a very different environment. Given that so many businesses and sectors use text messages to communicate and for payment, fraudsters now impersonate delivery companies, government departments and as we have seen the most prevalent text scam this year being eflow. In fact, our members estimate that currently up to 85% of text scams are non-bank impersonation scams and when it comes to phone scams circa 95% of these are purporting to be a utility company or an online provider such as Amazon or Microsoft.<sup>i</sup>

Financial institutions have a clear role to play in preventing fraud, a commitment which the industry takes very seriously through a range of measures both at industry level and within each individual financial institution. However, it is important to note that generally the first sight a financial provider will have of any fraud is when a payment is made i.e. transaction is made. Engagement between the consumer and the fraudster has already taken place, whether that be a text, phone call or an online engagement therefore we know that financial institutions cannot combat fraud alone. We echo ComReg's call out that a National Strategy to combat all types of fraud is required.

We agree with the consultation that to effectively combat fraud, Ireland needs a centrally led, 'whole of system' response where social media companies, telecoms, financial services, the State, and An Garda Síochána can collaborate to devise appropriate strategies to better share intelligence, implement protections for consumers, and develop barriers to criminals.

This sentiment was also echoed in the Hamilton Report published by the Department of Justice in December 2020 which encourages greater inter-agency co-ordination, collaboration, and information sharing, and also recommends a clear cross-government financial crime strategy.

*"Ireland has at present, no national strategy for combating economic crime and corruption. Given the range of agencies involved, the Review Group recommends the development of a multi-annual strategy to combat economic crime and corruption and an accompanying action plan. This will facilitate a joined-up and cohesive approach to combating economic crime and corruption in this jurisdiction and provide a basis for measuring progress."*

Prevention measures are an important building block of the future of a national economic crime strategy in Ireland. The initiatives outlined in the proposal will further protect consumers and provide innovative solutions to nuisance calls and texts. This is why BPFi and our members support *all the initiatives* called out in the consultation. With text messages being the most common type of fraud that consumers fall victim to, we have outlined some feedback on the solutions, detailed below. We are particularly keen to develop any cross-sector initiatives and collaborate further on education and awareness through FraudSMART. We would welcome ComReg as partner in an annual campaign on nuisance communications.

In addition, we have attached our most recent FraudSMART monitor. This shows industry fraud levels across all types of fraud for 2022 had gross losses of €88m. Further break down by payment type can be found in the report and we are happy to provide additional information where needed.

### **Education & Awareness (Consultation Reference 1.3, 1.4, 1.11, 1.17, 1.18)**

As per the consultation we are strong believers in education and awareness. In 2017, BPFi launched our FraudSMART programme which was developed in conjunction with our members and aims to arm consumers and businesses with the information needed to stop themselves falling victim to fraud.

- FraudSMART raises awareness about all types of scams with a particular focus on text and calls. We target three key demographics – youth, older persons and businesses. The programme provides information on the tactics fraudsters use, key warning signs and red flags to help consumers and individuals become more vigilant and protect themselves from fraud.
- Empowering consumers and businesses through education helps to close the gap that fraudsters exploit when manipulating customers.
- Year to date we have had monthly awareness campaigns, events, and email alerts to keep consumers and businesses abreast of current trends. Most recent areas covered eflow text message scams, parcel delivery, mum and dad WhatsApp scams and investment scams. We use social media, general media, radio and in person events to deliver messages. We have had 6 in person events so far this year with Age Friendly Ireland with 3 more planned along with our business events - one with SFA and another with AIB Merchant Services and National Retail Excellence Ireland.
- FraudSMART has also included resources from ComReg to maintain a cross sector approach. The “Do Not Originate” initiative is included in the FraudSMART Business Brochure and we encourage all businesses to use the solution.

### **Proposed Voice Interventions (Consultation References 1.22-1.24, 4.9, 4.38)**

BPFI is supportive of all five interventions – Do Not Originate, Protected Numbers, Mobile CLI blocking, Fixed CLI blocking, Voice Firewall.

- Do Not Originate – Members have been supporting this project since its initiation in September 2022 with lists of numbers entered on the register. All businesses could use this service, we highlighted this at the National Retail Excellence Conference and our collaboration with Small Firms Association.
- Voice Firewall – we believe this would require most effort from the operator’s perspective but due its substantial positive impact, we strongly endorse its implementation.

BPFI supports all of the above interventions, we believe they will further protect consumers and while we note that our members won’t be directly impacted by these changes, except for the “Do Not Originate” we ask that our members technical teams to be able to assess the initiatives in their implementation stage which would allow for an understanding of the current routing of members calls on the phone networks and identifying any necessary adjustments. We do believe it is unlikely that there would be any significant issues.

### **Proposed SMS Interventions (Reference 1.25-1.28, 4.3, 4.57 - 4.65, 4.69, 4.86, 5.289, 5.223)**

BPFI fully support both initiatives – Sender ID and SMS Scam Filter. The SMS Scam Filter would result in not requiring the Sender ID initiative as it would cover texts with and without Sender IDs however we are aware of the need of legislative changes required for this option so in the intervening period the Sender ID would assist in the prevention of text scams sent with Sender ID.

#### Sender ID Registry:

- This is a positive development however it will only impact scam SMS’s that are sent from / impersonating a genuine Sender ID, e.g. ‘Bank Brand A’. An increasing majority of scam SMS are sent from mobile numbers and a Sender ID Registry would have no impact on these. It will close off this avenue to fraudsters and decrease decreases the sophisticated look of the scam which convinces consumers that it is a real text. It will likely this will further push fraudsters to attempt fraudulent texts from sent from mobile numbers. This diversion to SMS scams without Sender ID’s (i.e. from mobile numbers) has already happened and the majority of scam SMS are now sent from mobile numbers rather than sender ID’s. The potential benefit may not be as expected but still very worthwhile.
- Members have commercial relationships with a range of communications providers but do not deal directly don’t deal directly with or influence entities such as the SMS aggregators that comprise the rest of the SMS delivery chain.

#### SMS Scam Filter:

Noting such an intervention requires legislative changes making it a more complex intervention (both legislatively and technically) but is the one that would have by far the bigger positive impact. SMS Scam Filters are already in place in other jurisdictions, and we have seen the effectiveness on comparable spam filters on email inboxes. BPFI would support legislative changes and offer assistance if required.

**Summary:**

Overall, we are very supportive of all of the initiatives in the consultation and would like to continue and increase our cross-sector collaboration on any initiatives. Members have many prevention measures of their own in place and constantly looking at other solutions, new and emerging, that will tackle the issues consumers face. These initiatives will happily share details of in our ongoing engagement with the sector. Our FraudSMART education and awareness campaigns continue, and we welcome cross sector engagement to further boost the message.

---

<sup>i</sup> *These figures vary per each member. Fraud figures can vary between typologies year to year depending on campaigns by criminals.*

## 5 BT Ireland

# **BT Response to the ComReg Consultation**

## **Combatting scam calls and texts**

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

Issue 1 – 31<sup>st</sup> August 2023

#### **1.0 Introduction**

##### **1.1 Nuisance Calls Firewall**

We welcome this consultation which as ComReg indicated is to address a problem that is harming society in Ireland. We fully support ComReg’s initiative to fully regulate the voluntary nuisance call firewalls as such creates a national firewall to stop nuisance traffic. We are concerned the alternative scenario would have seen substantial investments made by some totally wasted if the nuisance callers simply route via other operators that have not invested. We can demonstrate to ComReg that nuisance calls auto re-route within seconds to bi-pass a part firewall – we observed this when we implemented the Do Not Originate and Protected Number Blocks. We also know in today’s world of the internet and cheap connections through clouds etc. that operator size is largely irrelevant to carrying volumes of nuisance calls and in our view, there should not be a market subscriptions threshold for voluntary implementation. Essentially, it’s pointless having a firewall with gaps in it and ComReg will be doing the Irish society an injustice should it allow anything but fully regulated and complete firewall.

We acknowledge the work undertaken by ComReg to analyse the nuisance call issues in this consultation and separately we acknowledge the detailed work that ComReg has undertaken over the past year to drive progress. This has ensured the industry has already implemented several solutions described within the consultation, with others at an advanced stage of development. We would also acknowledge this is a subject that will be with us for many years and largely welcome ComReg’s statements on Future Number Management – Needs and development for what will be a second-generation approach.

##### **1.2 ComReg - Clarification of the Existing Sub-Allocation Rules and possible consequences**

Whilst we are generally supportive of the solutions proposed to address the nuisance calls firewall, we are concerned that the clarification of the existing numbering rules may act to create a distraction as it now appears to undermine a key segment of the Electronic Communications Provider market and a significant area of competition, in particularly from international competition into Ireland.

##### **1.3 Responses to the specific ComReg Questions.**

We address the detailed ComReg questions in our response at section 3.0 but before we address these, we would like to address our thoughts to the Sub-Allocation issue as this has potentially serious operational and competition impacts to the market. Also as addressed in the ComReg clarification response of the 10<sup>th</sup> of August we look at hosting in the Irish market.

##### **1.4 EECC issue.**

With the EECC legislation coming into operation we would ask ComReg look to review the regulation of number dependent vs number independent services to avoid potential confusion going forward in what seems likely to be a growing area.

## 2.0 Sub-Allocation Clarification

To try to explain our concerns we have provided Table 1 below followed by a methodical look at how the clarification appears to address both traditional, modern, and potentially future solutions to meet the needs of end customers, operators and ComReg.

Table 1 - Clarification of certain numbering rules

	Network Operator	Virtual Network Operator (Mobile or Fixed)	Switchless Reseller (Mobile or Fixed)
Service requirements	Routing code, CLI Management Porting, Hosting of VNOs KYC	Number Allocations Porting KYC	KYC
Example	Eir, Vodafone	Virgin Media, Amazon	Pure, 48

As per table 1 above the management of numbers is different depending on what aspect of the market a party is trading.

### 2.1 Network Operators

Network operators are regulated and provide the various network facilities for managing numbers such as assigning numbers to their end-users, routing calls, supporting number porting, Data Retention and Legal Interception etc. Since the early 2000s White Label products have largely been provided by Network Operators to Switchless Resellers through products such as Regulated Wholesale Line Rental WLR and more recently through VoIP Voice products over Broadband Next Generation Access (NGA) and Fibre Broadband Access. Switchless Resellers are akin to the retail operation of an incumbent and generally do not own or control a network whether physical or virtual.

WLR has existed since circa 2004 with the full involvement of ComReg who over the years has issued Decisions supporting and evolving the regulation around this white label approach to providing services.

In this case the network operator is allocated the numbers and provides a white label service to the retailer who manages providing the numbers to its end-users. This model has existed for approximately two decades in Ireland and hundreds of thousands of customers are supported through this product type.

We would propose ComReg leave this solution in place as it's the outcome of regulatory remedies and to unwind it would be very disruptive to the market.



## 2.2 Switchless Resellers

As discussed above Switchless reselling in the Irish market has been established for considerable years, supporting genuine providers long before the more recent scam call issues, and is largely considered to have facilitated the growth of competition in the Irish market and others across Europe including the UK.

We are genuinely finding the ComReg clarification of the sub-allocation regulation confusing with respect to Switchless resellers as this currently supports considerable competition in Ireland and indeed Single Billing<sup>1</sup>, the public name of WLR was promoted by ComReg in 2004. Also referenced in the footnote is one of the many ComReg regulatory documents bringing forward Single Billing/WLR<sup>2</sup>

We are assuming the ComReg clarification (we have provided the Switchless approach in Figure 1 below) does not have the intention of closing this mature and successful market and is an oversight. We would consider the Know Your Customer (KYC) proposal would look to be sufficient to meet ComReg's objective of knowing the end customers in this case.

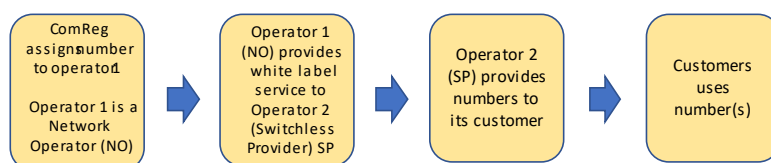


Figure 1 - Current Irish Switchless Provider Model using WLR and VoIP

## 2.3 Virtual Network Operators VNO's

Given the maturity of the Internet (secure tunnels) and IP cloud connectivity a new generation of Operator is emerging which supports connectivity to a group of paying customers but requires a full network operator to provide connectivity to the PSTN for routing and to support facilities such as legal interception, data retention and other facilities that a full network operator would support.

This scenario could be characterised by the term Virtual Network Operator who would purchase a number hosting facility from a network operator rather than establish itself as an interconnecting network operator. Unlike the Switchless Operator these providers have an access network and have a

<sup>1</sup> [Microsoft Word - PR291004.doc \(comreg.ie\)](#)

<sup>2</sup> [Implementation of CPS Single Billing Products: Wholesale Line Rental \(SB-WLR\), Agency Rebilling \(SB-AR\), Wholesale Ancillary Services \(WAS\): Decision Notice D2/03 | Commission for Communications Regulation \(comreg.ie\)](#)

level of access control over the end-customers network solutions, but don't support interconnection or the facilities of a Network Operator.

Numbering and (VNO's) – the argument to support Fixed Virtual Network Operators FVNO's in Ireland.

Given the ComReg clarifications (Reference ComReg doc. 23/52) the VNO's would have numbers directly assigned by ComReg. However, for this to work in practice, particularly for the delivery of inbound calls, other operators would have to be informed as to which Network Operator is hosting the VNO.

## 2.4 Private Network Solutions

We found it unusual for ComReg to describe private network solutions within the consultation as this brings us back to the 1980s and 1990s where a company would self-build its own private networks using leased lines to avoid the high long-distance call costs of that time and the absence of the internet as we know it today.

Like self-build computer networks, we see very low incidence of truly private networks due to wide availability of more advanced and efficient cloud-based solutions with integrated security.

Where corporate extension-to-extension telephony requirements are supplied by cloud-based "OTT" service providers, they are effectively providing "number-independent based interpersonal communications services". However, when making or receiving calls to or from the PSTN, the call must break out to the PSTN in the country of origin.

We would be concerned if a private network were being proposed to convey public electronic communications services whether voice, data in a novel commercial OTT solution across borders as this is merely the provision of publicly available electronic communications services in a repackaged form. In our view such a service provider should be authorised as a network operator, and this would be in line with EECC view of using Number based Interpersonal Communications Services. Otherwise, it subverts the integrity of the IGO firewall.

## 2.5 Conditions of Use

We understand clause 7.2 of the proposed draft concerning eligibility criteria proposes to retain the allocation of mobile numbers to "OTTs", This language predates the EECC which clearly delineates number-independent based interpersonal communications services from number-dependent based interpersonal communications services. We suggest that section 7.2 of the Conditions of Use needs to be clarified, and entitlements be set out on an equivalent and transparent basis for fixed and mobile network operators and virtual network operators.

2.7 Potential Consequences of ComReg's clarification of Sub-Allocation – i.e. No sub-allocation in Ireland.

We would like to address the ComReg clarification of regulation concerning Sub-Allocation of the 10<sup>th</sup> of August where ComReg ask for thoughts on hosting. Below is a practical first look at what might need to happen to fully establish hosting in Ireland. Even this first high-level look raises several practical issues that would need to be addressed. We acknowledge that it's quite possible hosting already exists or has existed in Ireland but is not publicised.

**2.7.1 History of Sub-Allocation** - The Irish industry has grown up on sub-allocation over the past decades and the market appears to have a dependency on this facility for ComReg to codify the removal of Sub-Allocation (Draft Number Conditions 7.1.2). Industry would need a substantial sunset period to manage such a change.

**2.7.2 Competition** – it's often claimed Ireland is an open market and the competition provided by international players is important. If this market is to be migrated away from sub-allocation care is needed to ensure the transfer can be managed with minimal impact on end customers which are most likely business customers. Like the Nongeographic number migration which completed early 2022 a substantial sunset period for operators is required for them to update their arrangements both contractual and technical and to migrate their customers with minimal disruption. Whilst some could become network operators' others may prefer to use hosting solutions.

**2.7.3 Know your Customer and Audits** – In the absence of switchless resellers every number would become a direct retail number and would need to be registered / re-registered with ComReg. Any refresh of end user information will be the same for Network Operators, Virtual Network Operators and switchless resellers with a period required to review end user data.

**2.7.4 Finding a Host** – Virtual Operators dependent on Sub-Allocation today would need to be directly allocated their numbers and would be required to contract with a network operator providing hosting services. I.e., the hosting network operator would provide at least the actual routing of calls to and from the virtual operator. The inbound operation is shown in Figure 2, but the virtual operator would be wholly responsible for the numbers allocated to it. It would be expected all re-sellers (now providers) would require authorisation in Ireland. Ancillary services to support legislation such as Data Retention, Legal Interception and ECAS location information would also need to be addressed to support the hosting solution.

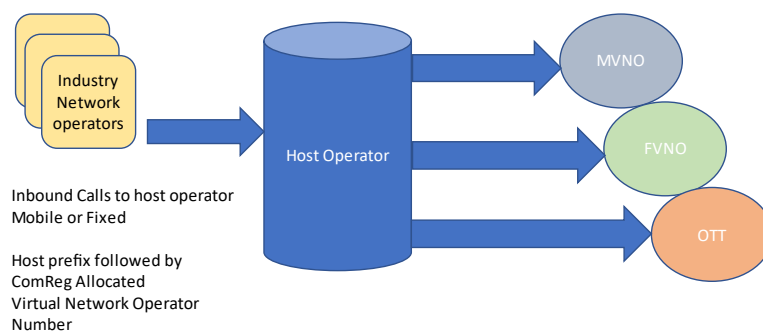


Figure 2 – Network Hosting Solution For Inbound

**2.7.5 Routing Prefix** – Virtual Operators (new providers) will not need their own routing prefix because (by definition) they are not an interconnecting network.

**2.7.6 Updating PXS** – Significant modification of the industry porting database back in 2018 means the industry largely depends on the PortingXS porting database for fixed routing, and we would expect there would be a need to update the current prefixes as sub-allocated operators’ re-contract with host providers. We have looked at the list of operators on PXS and updating re-sellers to host prefixes would appear to be a manageable task as the list is small. A key obligation for a virtual operator (new provider) is they would have to contract with PXS to use its system and the new provider would need to support the associated porting processes. We assume similar will be required for the mobile porting system.

**2.7.7 Going Forward** - BT Ireland has worked on industry projects in Ireland involving change and evolution, and indeed we are currently working on Internet Access Switching. A common learning is changes as far-reaching as these can’t responsibly be delivered overnight.

**2.7.8 Inclusion of Hosting in the Draft Numbering Conditions** – BT requests that ComReg provide for Number hosting within the Conditions of Use and Application Process.

### **3.0 Response to the detailed Questions**

**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.**

BT Response 1

We fully agree ComReg’s proposals concerning DNO, Protected Numbers, Fixed CLI call blocking and Mobile CLI call blocking and welcome that ComReg is bringing forward regulation to ensure these happen. In our view all operators should be required to provide the appropriate firewalls and that any voluntary regime, even thresholds based won’t work. We are not commenting to the proposal for SMS regulation as we do not provide this service and don’t have the local expertise to provide informed comment in this matter.

Long-lining - We support and welcome the proposal to support Long-lining for own end-users, though we suggest this should be restricted to non-geographic CLI and distinguished from occasional nomadic use outside Ireland. We would note that the most likely technology used will be SIP rather than Ethernet or legacy TDM.

**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.**

We generally agree with the proposals and would like to provide the following comments.

1. We agree with the new clause 1.4 of the 'Draft Numbering Conditions' document and wonder whether it's an editorial error that Fixed Numbers are not included. If not, an error we propose to add it to this text.
2. We support the introduction of the long lining text; we suggest it be restricted to 0818 or 1800 CLI.
3. We agree with the proposal for better identification of customers using 1800 and 0818 number and consider the proposal to effectively grandfather numbers already supplied as pragmatic, and we support this approach.
4. We agree with the deletion of 076 given this range has been withdrawn but we observe a small trickle of these calls are still entering national Irish interconnects.

**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.**

We would like to offer the following comments:

1. Technology issues with CLI. We generally agree with ComReg that the CLI aspects between SIP and TDM are largely aligned be it with different terminology. One aspect that was an issue at the international boundary was earlier enterprise versions of SIP had problems managing the international prefix and the leading '1' used for 1800 services, causing the number to be presented as 018XX instead of 18XX. Carrier versions of SIP did not have this issue.
2. Metrics – we agree with ComReg that metrics are required to help in the battle with nuisance calls as such highlighting changes and trends to inform ComReg and hopefully industry what is working well, what is not, and also what is changing. Whilst we are not seeking commercial information from this data, it would be helpful for ComReg to keep the industry informed of what is happening as operators may be able to tune their solutions as appropriate.
3. Authentication of Numbers. We note ComReg's later discussion for assigning numbers to providers whether operators or not which should provide a static list of ownership. The current NCIT solutions are largely barriers based on simple general rules and we would refer ComReg to our answers to question five concerning the future approach.
4. We agree with ComReg's comments on CLIP and CLIR.
5. We fully support and welcome ComReg's pragmatic approach to longlining as such increase's wider competition of services (not just telecoms) in the Irish market. Indeed, some call centres are located in Ireland handling calls to other countries. We suggest restricting longline solutions to non-geographic CLI.
6. Doctor's Surgery Example - As a separate issue one of the standard reasons for allowing presentation numbers to be different to the network CLI (Paid field) was the doctors surgery example. I.e., whilst the doctor was on his rounds the aim was to present the surgery number rather than the doctor's private handset CLI. The surgery and the doctor are clearly related hence the doctor has a right to both assigned numbers, so we assume this fundamental example is valid, though the non-geographic condition should apply.
7. International Calling – we fully agree with the correct use of CLI according to E164 and welcome the solution in 6.74iii where the call can be marked as "Caller ID unknown" or equivalent if an operator cannot ensure that the presentation CLI is valid. We would add that a common equivalent is to strip out the presentation number and present with nothing. We would add that as an international gateway operator we are working with other country

partners to try and do this, however it worth noting that most calls come from large international hubs and we usually do not have a direct relationship with the originating carrier.

8. Private Networks Retail Customers – We welcome the national and international described scenarios and would agree with the analysis and that such solutions are long established certainly from the 1990's and earlier work well. Truly private implementations are rare. Modern virtualised customer infrastructure blurs the lines between private switches and the PSTN. We would therefore not agree with ComReg's suggestion that virtual private networking should be exempted from the obligations of an international gateway operator.

**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.**

**BT Response**

We would like to offer the following comments:

Please see Section 2.0 and the two items here for our response to this question.

**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.**

**BT Response**

BT welcomes ComReg's discussion assessing solutions for future number management and there is much in this section we agree. We would like to offer the following, and hopefully, constructive comments.

1. Automated Number Assignment

We would support automated number assignment for efficiency purposes and note the ComReg individual Number Assignment (INA) process has worked well for non-Geographic numbers. As a supplier of business services assignment in blocks is important for our customers and for us to manage the end-user allocation.

2. Nuisance Call solutions

We agree that the current set of solutions have static elements, and we believe this leads to at least the following issues:

- We are concerned with ComReg setting further regulation for two years' time for something that is yet unknown, with no specification, cost etc. This is not good regulation and undermines the industry ability to comply with fiduciary legislation to ensure the management of share owners. We cannot simply agree direct regulatory obligations for the unknown and with no view of the level of investment required. We would challenge whether this is compliant with good regulatory practice, and such may need to be challenged at the European notification level.

- Today a sizable number of operators are developing solutions, so the industry cost is the number of operators multiplied by their individual development cost which could be considerable. This suggests research is needed into more effective and efficient 'common' solutions. We would agree with ComReg's approach to date as an initial response but consider such unsustainable in the medium to longer term and not in line with what some other nations are doing.
- As regards Stir/Shaken we would say the Jury is still out as we assess the US solution, and it will be interesting to see how the French Stir shaken performs once launched. We note the US and French solutions have key differences, but the key element of asserted numbers and secure networks is common and ComReg should be investing in looking at common non-proprietary solutions, so an endless industry disparate approach is avoided. A key advantage of a common approach is an upgrade of the common aspects would benefit all and should significantly reduce further investment costs. Money is tight and we are all required to be efficient.

### 3. Need to re-establish the Number Advisory Policy Working Group.

Internationally BT is finding numbering a constant source of operational problems often due to regulatory changes to limit fraudulent calls. Whilst its laudable to curtail fraudulent activity it's also important to recognise the fraudsters are largely copying the international Call centre model (and we believe they are likely using their own call centres). The constant changing of numbering rules across Europe is inadvertently damaging an important and genuine international market sector. We acknowledge and thank ComReg for listening and adopting the long lining approach, but the disparity of European solutions is hindering the ability for genuine trading and is potentially holding back more innovative and competitive developments. There needs to be a change of culture that rightly addresses stopping nuisance calls but also addresses how to protect/facilitate genuine calls. This latter part appears to be missing in the current approach and not just in Ireland.

As with the forming of Irish competitive numbering market in the late 1990's and the early 2000's industry is again changing rapidly, and we believe there is a need for an improved frequency of discussion (say every six months) between the regulator and the industry through a policy forum. The NCIT is more focused on the delivery of specific targets, and we would suggest an alternative policy forum is re-established rather than such distracting the implementation work of the NCIT.

**End**

## 6 Cellusys



# Submission from Cellusys Limited to the Commission for Communications Regulation in response to Consultation 23/52 on the subject of combatting scam calls and texts

---

## Executive Summary

Cellusys has long championed better security in telecommunications. We welcome the Commission's (ComReg's) publication 23/52 (the Consultation) and the prospect that ComReg contemplates mandating some relatively simple and not exorbitantly expensive measures to address the acknowledged problem of nuisance communications.

Ireland has an even longer history of bringing forth companies with expertise in analysing and controlling signalling in telecommunications networks—the means to address the problem in hand. Many of the industry's leading lights are Irish or have significant Irish heritage. It is therefore disappointing that, collectively, we have failed yet to convince operators of local telecommunications networks of the benefits of protecting their customers from nuisance communications over allowing such threats to proliferate.

The substantive issue is real. The approach adopted by ComReg is practical, consistent with activities undertaken and being undertaken by telecommunications regulatory authorities (TRAs) worldwide to protect consumers, and it will work. Providers of relevant technology, companies like Cellusys and its competitors, are ready to deliver working solutions "off-the-shelf".

The Consultation provides a comprehensive treatment of the problem, its context and effects, and the regulatory measures being contemplated. As a specialist provider of technology (specifically software) that can be used to mitigate the problem, Cellusys frames its submission response to the Consultation in terms of Section 4, "The potential technical interventions to combat Nuisance Communications". In doing so we refer to the regulatory instruments discussed in Sections 5.3 to 5.6, and have regard for giving effect to Section 6, "Updating the Numbering Conditions".

Our contribution suggests a single approach that can, as required, be used to enforce any or all the contemplated regulatory instruments, delivering in what is defined nationally on a more global scale, using technology immediately and competitively available, including locally, at costs significantly lower (in aggregate) than those suggested by the Consultation.

## Background

### Voice Firewall and SMS Scam Filter: An Overview

The fundamental architecture of any system designed to provide what are separately termed “voice firewall” and “SMS scam filter” is a single technical element. Apart from the ability to examine the contents of an SMS or MMS<sup>1</sup> message, specific to the respective SMS or MMS firewall, it is generally known as a signalling firewall.

Signalling is the portion of the overall telecommunication traffic that is used to control the network from within and to keep track of the services being used by subscribers to the network. Signalling is not transmitted in the voice communications channel, but separately from it. When we pick up a fixed line phone or dial a number on a mobile, signalling messages are sent from our device to the network that advise the network we wish to make a call. Dial tone is a signal that the fixed network is ready to receive dialled digits. Ring tone is a signal from the network that our call is connected to the device of the person we’re calling. Our phone ringing, similarly, is a signal someone is calling us.

Note that the SMS service was initially designed to be carried in the signalling channel.

### Signalling in a Nutshell

The oldest signalling currently in widespread use is Signalling System Number 7<sup>2</sup>. This protocol was developed in the 1970s and 80s and defined by the International Telecommunications Union Standardisation Sector (ITU-T)<sup>3</sup> for a world where the providers of telecommunication services worldwide were principally governments, through what were known as PTTs<sup>4</sup>. Given the trusted community of worldwide networks at the time—neither national competition nor mobility was yet a fact—security was not even remotely a consideration.

As we evolved to a highly competitive and mobile world, signalling protocols needed also to evolve. As they did, they evolved to interwork with the extensive installed base of SS7 networks—and security vulnerabilities were handed down to successive signalling protocols, as if genetically.

Historically, SS7 was reasonably difficult to hack and hackers needed to be relatively sophisticated and to have sometimes expensive equipment, but with democratisation through widespread adoption and of the text-based SIP protocol in fixed and mobile networks, hacking is easier now than it has ever previously been—evidenced, one might suggest, by the burgeoning prevalence of nuisance communications—and requires no sophistication whatsoever: a laptop, internet connection and a minimal degree of skill.

### Securing Signalling Networks—The Signalling Firewall

Given signalling’s role in controlling networks and the increasing ease of hacking it, applying security to signalling would appear to be important, even imperative. Perhaps if the intended victim could control the signalling, or those controlling the signalling were the target, it would have been addressed.

A signalling firewall ingests and processes network signalling according to specific rules, as a baseline in compliance with recommendations principally of the GSM Association (GSMA)<sup>5</sup>. These documents

---

<sup>1</sup> The multimedia message service (MMS, <https://www.openmobilealliance.org/release/MMS>), an evolution of SMS, is outside the scope of the Consultation, but can be considered in some ways similar to SMS in the sense of firewalling it.

<sup>2</sup> [https://en.wikipedia.org/wiki/Signalling\\_System\\_No.\\_7](https://en.wikipedia.org/wiki/Signalling_System_No._7)

<sup>3</sup> <https://www.itu.int/en/ITU-T>

<sup>4</sup> [https://en.wikipedia.org/wiki/Postal,\\_telegraph\\_and\\_telephone\\_service](https://en.wikipedia.org/wiki/Postal,_telegraph_and_telephone_service)

<sup>5</sup> [www.gsma.com](http://www.gsma.com)

define recommended actions, by protocol and service, to secure signalling networks and those most referred to are summarised in Table 1.

Table 1—A selection of relevant GSMA signalling security recommendations<sup>6</sup>

Protocol or Service Referred to	Recommendation
Signalling System No.7 (SS7)	FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines
	IR.82 SS7 Security Network Implementation Guidelines
Diameter Signalling System	FS.19 Diameter Interconnect Security
General Packet Radio System (GPRS) Tunnelling Protocol (GTP)	FS.20 GPRS Tunnelling Protocol (GTP) Security
Session Initiation Protocol (SIP)	FS.38 SIP Network Security
SS7 Short Message Service (SMS)	FS.12 A2P SMS Bypass and Fraud—Methods, Detection and Mitigation
	IR.70 SMS SS7 Fraud
	IR.71 SMS SS7 Fraud Prevention

Not to concern ourselves with the technicalities of the signalling itself, or of the recommendations, other than to note many have existed for a long time, it is worth pointing out that, for signalling security purposes, signalling is placed into categories, which are of importance when considering the interventions contemplated by the Consultation. These categories, upon which certain filtering rules are based, are generalised and greatly simplified in Table 2.

Table 2—General categorisation of signalling messages within and between networks  
 (after GSMA recommendations)

Category	Description
Category-1	CAT.1 signalling messages are on-net or intra-network messages. If a CAT.1 message arrives at, or is being sent out of, a network it can be blocked—it is supposed to exist and be used only within a network.
Category-2	CAT.2 signalling messages are those that should be received by a mobile network only in respect of a visitor, an inbound roamer. If a CAT.2 message in respect of an inbound roamer is received, and if the message is checked against the rules and e.g., found not to be from the roamer's home network, the message can be blocked.
Category-3	CAT.3 signalling messages are supposed to be received only from an overseas network where a traveller, an outbound roamer, is attached. If a CAT.3 message in respect of a subscriber arrives at the home network, and if the subscriber is found not to be roaming, the message should be blocked.

Because without signalling there can be neither a voice call nor an SMS, and because each service has specific associated structures in signalling, the voice firewall and the SMS firewall (or SMS scam filter) are each just applications of a signalling firewall: a common and affordable security device, routinely deployed by networks worldwide.

In respect of firewalling SMS, filtering of the Short Message Peer-to-Peer (SMPP) protocol is necessary, as well as an additional application, not itself directly relevant to the signalling, but

<sup>6</sup> The recommendations themselves are confidential to the GSMA, its members (typically mobile network operators), rapporteurs and associate members (of which Cellusys is one).

generally integrated into the signalling firewall platform, that can be used to identify nuisance, malicious and fraudulent SMS and MMS messages based, for example, on patterns within the content of the messages.

## Regulatory Interventions Under Consideration by ComReg

Table 3—Regulatory interventions considered feasible, with comments<sup>7</sup>

Ref	Suitable Intervention	Implementing the Intervention
1.	Do Not Originate (DNO)	Numbering conditions: Signalling firewall
2.	Protected Numbers (PN)	Numbering conditions: Signalling firewall
3.	Fixed CLI Call Blocking	Malicious signalling: Voice or signalling firewall
4.	Mobile CLI Call Blocking	Malicious signalling: Voice or signalling firewall
5.	Sender ID Blocking	Numbering conditions: Signalling firewall
6.	SMS Registry	Industry regulation
7.	SMS Scam Filter	Malicious or fraudulent Messaging: SMS firewall (also MMS firewall)

## Potential Technical Interventions to Combat Nuisance Communications

In the foregoing section, we sought to place the operation of a signalling firewall and its ability to function as both a voice firewall and SMS scam filter in context, as separately described at a high level in ComReg’s documents “*Voice Firewall Functional Requirements Specification*” and “*SMS Scam Filter Functional Requirements*”<sup>8</sup>, each dated 26 June 2023 and provided in association with the Consultation.

### Desirable Characteristics of a Signalling Firewall

A signalling firewall, generically a well understood term, may frequently incorporate features that amount to an SMS or voice firewall—neither of which terms, as the list of features expands, is as unambiguous as signalling firewall. The best systems provide for comprehensive and flexible implementation of highly customisable rules and employ smart technology and access to external resources to maintain accurate blocking capability.

- Multi-protocol capable (SS7 (including MAP, ISUP, INAP and CAP<sup>9</sup>), Diameter, SIP most relevant for voice and SMS) with cross-protocol checking capability<sup>10</sup>
- Flexible in respect of ability to create and maintain rules and rulesets or policies—enabling speedy response to emerging threats
- Easy to use, and including comprehensive reporting on threats and firewall actions (which are not limited to allow/block)

<sup>7</sup> This table expands on Table 7 from the Consultation (page 95).

<sup>8</sup> Previously “*Anti-malware content scanning, url detection and classification*”.

<sup>9</sup> Protocols in the SS7 “family” of protocols often used in delivery of voice services: MAP: Mobile User Part; ISUP: ISDN User Part; INAP: Intelligent Network Application Protocol and CAP: CAMEL Application Part (CAMEL is: Customised Applications for Mobile networks Enhanced Logic)

<sup>10</sup> Some malicious actors use multiple protocols in a single attack to avoid detection by less sophisticated firewalls.

- Capable of being readily integrated with third party systems, e.g., fraud management systems, network management systems, numbering and url databases, CRM, etc.

The implementation of a fully functional signalling firewall provides a single, accessible point for a network operator to implement all signalling security policies. A typical firewall has significant capacity for maintaining lists of numbers for various filtering purposes, including blacklists and whitelists, to be considered in respect of numbering conditions interventions.

Such systems should also be capable of readily integrating with native or third-party applications that provide the extra functionality required for effective and dynamic voice and SMS firewalling.

### Basic Signalling Firewall Function

The fundamental task of a signalling firewall in a mobile network is to categorise signalling traffic according to the GSMA's applicable recommendations and ultimately block unauthorised traffic where identified. In performing this task, it will inevitably reduce the volume of malicious or fraudulent traffic entering (or leaving) networks. Analogous processes can be applied to voice signalling for fixed line networks.

### Application in Respect of Do-Not-Originate and Protected Number Interventions

The Consultation speaks<sup>11</sup> to the implementation, initially on a trial basis of do-not-originate (DNO) and protected number (PN) lists, by some operators prior to its full launch in September 2022.

A fully featured voice firewall may include lists of numbers from DNO/PP lists, not only from Ireland, but from a wealth of worldwide sources, greatly increasing the protections offered. These lists can in some cases be refreshed in real time via API through subscription to a suitable numbering database service.

### Application in Respect of Fixed and Mobile Call Blocking

Universally, the ITU-T, in its recommendation E.164, "*The international public telecommunication numbering plan*", mentioned frequently in the Consultation<sup>12</sup>, publishes and maintains a list of worldwide numbering plans. Similarly, in recommendation E.212<sup>13</sup> "*The international identification plan for public networks and subscriptions*" it collates valid mobile country codes (MCC) and mobile network codes (MNC), designators widely used in signalling and together comprising the International Mobile Subscriber Identity, or IMSI. These resources are openly available and providers of numbering database services incorporate them, along with a wealth of other public domain numbering information, into their offerings.

As a basic feature upon delivery, any firewall will be populated with a database of valid number ranges, in the case of a mobile operator, having regard for its roaming agreements. In mobile, this is referred to as the IR.21<sup>14</sup>, "*GSM Association Roaming Database, Structure and Updating Procedures*", being the GSMA permanent reference document (PRD) that so defines.

### Application in Respect of SenderID Blocking

In signalling firewall terms, SenderID blocking is a simple case of another blacklist to be consulted by a firewall—and blocked or otherwise dealt with.

---

<sup>11</sup> Paragraphs 2.4 (page 22) and 4.9 ff (page 69).

<sup>12</sup> Initial mention in paragraph 6.4 on page 212, see <https://www.itu.int/rec/T-REC-E.164/en>

<sup>13</sup> <https://www.itu.int/rec/T-REC-E.212/en>

<sup>14</sup> This is a document confidential to GSMA members, rapporteurs and associate members.

## Application in Respect of SMS Registry

Again, for purposes of signalling firewalling, SMS registry could readily be presented as a whitelist.

## Application in Respect of SMS Scam Filter

Apart from nuisance communications that affect end-users/consumers of telecommunication services, there is a more widespread problem with fraud across the SMS sector, especially in application to person (A2P) messaging. Twilio mentions this problem in a submission to ComReg<sup>15</sup>. While it is generating a frenzy of activity in the segment, much of it unhealthy, it is also outside the scope of the Consultation.

After the mitigations that can be achieved through use of a signalling firewall as already described, an approach to further combatting nuisance SMS traffic to consumers—SMS spam and SMS phishing (or Smishing)—is for the system to examine the content of SMS messages.

This approach is typically adopted by mobile network operators seeking to assure the integrity of A2P messaging revenue streams, which can be significant. In this use case, the SMS firewall is populated with certain patterns of characters that indicate, e.g., transmission of an OTP or 2FA key, and, where such a message is arriving on an unexpected link, known as a grey route, e.g., from a roaming partner, or from a SIM on the home network<sup>16</sup>, blocking it.

In respect of Smishing, transmitting fraudulent urls to consumers in SMS messages, it is again possible to connect the firewall to a database of web addresses-white- or blacklists, or to subscribe to a url reputation database that provides real-time information on the known status of a particular web address. These systems can also unroll shortened urls, e.g., goo.gl, bit.ly, tinyurl.com, etc.

## Beyond the Scope of the Consultation

### Verified Roaming

An approach adopted in some countries where Cellusys has worked with TRAs and MNOs is cross-network verified roaming. This fundamentally is an extension of what we've described as CAT.3 filtering in Table 2, above, but applied nationally.

In this use case, signalling from a customer of one Irish network (the home network) arrives at another Irish network (the handling network) from an overseas network<sup>17</sup>. and the handling network queries the home network about the roaming status of the subscriber. The home network provides a binary response (or otherwise if required) to the handling network. If the subscriber is not roaming (which would include an instance where the number is not in service) the message is fraudulent and can be blocked.

## Implementing a Solution

While an effective solution is almost required to be what would be described as "on-premises", in the sense that it must analyse on-net or intra-network signalling, a range of possibilities still exists for implementing a signalling firewall.

Each facilities-based operator could individually implement a solution. Tenant operators, e.g., MVNOs in the case of MNOs, can, if they have their own core network, implement independently, or as a

---

<sup>15</sup> Paragraph 4.67 (page 85).

<sup>16</sup> When arriving on a home network service, this may indicate presence of SIM box fraud, also capable of being identified and mitigated by a signalling firewall.

<sup>17</sup> Consider an eir customer on holiday in Spain, calling a 3 customer back home. The principle can also be applied to fixed line networks.

tenant of the host network. Thin MVNOs (those simply reselling the host's service) might be covered by the sponsor network—or could be set up as a tenant.

Where a smaller fixed network exclusively uses the services of a single international signalling provider, a cloud-based solution, hosted by the signalling provider could be adopted—but on-net signalling would need to be sent to the platform in the cloud for processing.

Cellusys has implemented signalling firewalls on several very small mobile networks (<100,000 subscribers) and is currently delivering a voice firewall on a start-up fixed network, as mandated by the local TRA.

Deployment, once the specification and mode of deployment are agreed, is a cooperative effort between the operator and provider and it while can be as short as one month more typically takes in the range of two to three months to complete.

It may also be worth considering the possibility of a 'national' subscription to suitable number database and/or url reputation database, whereby discrete firewalls in several networks would make a call to the respective database transparently using a centrally managed account, managed, e.g., by ComReg, by one network on behalf of all, or by some third-party honest broker. This would be an economical approach as database subscriptions are typically volume based and the unit price of a call decreases with the number of calls made—and they represent an ongoing cost.

## Financial Considerations

The Consultation provides some estimated costs of implementing the various interventions contemplated<sup>18</sup>.

It is Cellusys' view—bearing in mind that the requirements are not in any sense well defined—that the costs for the larger operators are overstated by a small multiple.

We reserve this comment from MNOs, down the table to large IGOs. The same cannot be said to applying to other IGOs, SMS aggregators or voice originators.

## Conclusion

Nuisance communications, much of it attempts to defraud people or networks, is a hugely profitable and dynamic field. To be successful, the work of combatting it needs to be equally dynamic. It is a game of cat-and-mouse. The GSMA collectively, and providers of signalling security solutions independently, endeavour to tip the scales in our favour with a range of 'Threat Intelligence Services'. These are often bundled with firewall offerings.

The consultation is welcome, as is the approach contemplated. Technical solutions across the board are readily available, relatively straightforward and economical. More importantly, they are adaptable, not static. To date, however, there has been little impetus to adopt them.

Cellusys, a local company with a wealth of global experience, places itself at the Commission's disposal, we would be pleased to share with ComReg and/or the NCIT or individual operators our experience of signalling control deployments across the world, serving more than 1 billion subscribers. We would also be willing to workshop some approaches and address and specific use cases of concern to operators. Our interest in this regard, in the context of the Consultation, is to educate.

---

<sup>18</sup> Table 19 (page 196).

## 7 Eir



**eir**

**Response to ComReg Consultation:**

**Combatting scam calls and texts**

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

**ComReg Document 23/52**



**31 August 2023**

**DOCUMENT CONTROL**

<b>Document name</b>	eir response to ComReg 23/52
<b>Document Owner</b>	eir
<b>Status</b>	Non-Confidential

The comments submitted in response to this consultation document are those of eircom Limited and Meteor Mobile Communications Limited (trading as 'eir' and 'open eir'), collectively referred to as 'eir Group' or 'eir'.

## Executive Summary

1. eir acknowledges the importance of seeking to combat nuisance and scam calls which have a detrimental impact on society. As such eir is an active member of the Nuisance Communications Industry Taskforce (NCIT) and is proactively implementing a number of tactical measures that have been developed by the NCIT.
2. eir agrees that it is appropriate to codify the tactical solutions in order to ensure consistent implementation across Irish operators. eir notes that ComReg must give further consideration to the burden imposed on operators both in terms of financial cost recovery and mandating implementation deadlines in the context of limited skilled resources and 'competing' regulatory requirements alongside planned commercial developments.
3. eir is disappointed that ComReg is seeking, in this consultation, to codify technical measures that have not been discussed or developed by the NCIT (Voice Firewall), and measures where development discussions have not yet been concluded by the NCIT (Roaming Checker and SMS Content Filter). The technical specifications of these potential interventions are insufficiently developed to be codified at this time or to inform mandated implementation deadlines.
4. Voice Firewall and SMS Content Filter (subject to changes to data protection legislation) are potential strategic solutions which if designed and implemented correctly will be more effective than the current package of tactical measures.
5. Consequently eir calls on ComReg not to codify Voice Firewall, Roaming Checker, and SMS Content Filter at this time. The NCIT should be allowed to consider and develop these potential interventions further, taking a strategic perspective in order to ensure any developed solutions are effective, efficient, and can be implemented consistently. It would then be appropriate for ComReg to consult on proposals to codify strategic measures when sufficiently developed. Taking this approach will not be lost time, but rather ensuring that solutions are effective and resources are not wasted.
6. eir looks forward to further constructive engagement with ComReg and Industry in the NCIT.

## Response to consultation

8. eir welcomes the opportunity to engage in the consultation process. eir acknowledges the importance of tackling the issue of nuisance and scam communications and has been an active participant in the Nuisance Communications Industry Taskforce (NCIT) since its inception. eir has proactively implemented some of the proposed fixed voice interventions and is in the process of advancing Mobile CLI call blocking.
9. The primary purpose of this consultation is to codify and put measures on a statutory footing to ensure all parties are clear on their obligations. eir agrees it is important to codify measures that have been discussed and developed by the NCIT. However, as we discuss later in this response, proposals in respect of Voice Firewall and SMS Filter are at too nascent a stage to be codified in the current consultation. Rather they should be subject to further discussion and development by NCIT and subject to a subsequent consultation process, as required, to codify the work of NCIT.
10. eir notes ComReg's statement (para. 1.4) that "*Ireland, as an English speaking country with a developed economy, is disproportionately targeted compared with our EU neighbours*". However an industry source<sup>1</sup> suggests that Ireland is well down the league table in terms of scam and fraud call rates in Europe. Whilst acknowledging the need to address nuisance and scam communications this should be done in a measured way. Spending time now to further consider and develop longer term solutions will result in a more effective overall outcome in addressing nuisance and scam calls.
11. eir welcomes ComReg's willingness to engage in a clarification process following a request by Industry. eir believes this process has been helpful and has considered the output of the process, ComReg 23/75, in developing this response to consultation.
12. eir notes the primary subject matters of this consultation is on network based interventions to reduce the harm from Nuisance Communications. However the consultation questions are focussed on some related and non-related changes to the Numbering Conventions. As such we will consider the proposed interventions before responding to the questions.

## General comments on implementing the proposed technical interventions

13. eir notes that network based interventions are one aspect of combatting scam communications. End users also have the power to help protect themselves by using trusted third party Apps and / or enabling security features in their smart phones. Handset manufacturers appear to be taking considerable effort to integrate intelligent protective features in their devices akin to firewalls and filters. Currently Apps and handset features are available to end users on an opt-in basis. eir believes ComReg should establish a separate taskforce with handset manufacturers and App developers to promote the availability of these protective tools to end users and to consider whether handset features should be made available on an opt-out basis.
14. Before commenting on the proposed interventions eir would like to make general comments regarding cost recovery, implementation deadlines, and periodic review.
15. With regard to cost recovery ComReg proposes that each operator bears its own costs. ComReg proposes a number of interventions each of which will have a cost to each network operator to implement and maintain. It is ComReg's view (Para 1.31) "*When combined, ComReg's proposed interventions should bring €50 euros in economic and social benefit for*

---

<sup>1</sup> See page 19, Hiya Global Threat Report Q2 2023, available at [www.hiya.com/global-call-threat-report](http://www.hiya.com/global-call-threat-report)

every €1 spent securing networks”. Whilst this ‘benefit’ may justify regulatory intervention it does not of itself justify the costs should be borne solely by the network operators.

16. ComReg states (Para. 1.18) that it “*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.***” [emphasis added]
17. The principles of cost causation would therefore suggest that other parties in the value chain, who stand to benefit from the proposed interventions, such as those in the financial and logistics sectors, should contribute to the cost of tackling the menace of nuisance communications. eir therefore requests that a fund be established to contribute to the costs incurred in implementing and maintaining any technical interventions arising from Decisions made at the end of this consultation process.
18. With regard to implementation deadlines. eir has commented below on the reasonableness of proposed implementation deadlines in respect of each proposed intervention. This is based on an assessment of the individual interventions. What we have not done is to consider the reasonableness of multiple coincident deadlines. This is in part because eir has already voluntarily commenced implementation of a number of the proposed measures. However those operators that have not yet commenced implementation may find it challenging to implement multiple interventions within 6 months and as a general principle staggered implementation dates should apply.
19. In any event we request that ComReg does not consider implementation deadlines in isolation of other regulatory requirements and recognises that operator resources, both financial and human, are finite. Over the proposed period covered by the draft decisions mobile operators are likely to be required to implement Public Warning Systems for Ireland to be compliant with the European Electronic Communications Code. All operators are likely to be required to review and implement, as required, Electronic Communications Security Measures as legislated for in the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023. Operators will already have annual plans of development works for which resources are required. This means that ComReg should take a flexible approach to establishing implementation deadlines with operators.
20. ComReg proposes that each technical intervention be the subject of a dedicated Decision Instrument. eir has no objection to this approach, however the Decision Instruments are open ended and do not cater for changing circumstances that may render a technical measure ineffective or obsolete. Consequently mechanisms for periodic review of the effectiveness of the technical interventions (singly and collectively) should be incorporated into the Decision instruments. eir requests that the review mechanism should require a formal review every three years and allow for an ad hoc review at the request of NCIT in light of prevailing circumstances.

## Consideration of proposed technical interventions

21. ComReg has proposed to mandate the implementation of the following network interventions in respect of fixed voice calls – **Do Not Originate (DN)**, **Protected Numbers (PN)**, and **Fixed CLI Blocking**. eir has proactively commenced implementation of the three measures on a voluntary basis recognising the importance of taking action to try and mitigate against scam and nuisance calls using fixed originating CLI. As such eir can see merit in mandating these three measures requiring all relevant operators have them in place to ensure there are no back door routes for such calls to enter the national networks.
22. ComReg proposes that these measures should be implemented within 6 months of a Decision being issued<sup>2</sup>. eir agrees that this may be a reasonable timeframe for operators who have not yet commenced implementation to implement one of the measures. As noted above, ComReg needs to give due consideration to the interaction of multiple regulatory initiatives on operator resources when setting implementation deadlines.
23. eir has reviewed the draft Technical Specifications for these interventions which have been drafted with Industry collaboration in the NCIT. eir generally agrees with the proposed specifications however with respect to reporting we are unable to commit to providing detailed reporting for each intervention. Our fixed network systems are capable of identifying the total number of calls blocked but do not capture which of the three interventions resulted in the block. Consequently we request that the technical specifications are amended such that reporting the number of blocked call attempts at the aggregate level is permissible. We also request that reporting be placed on a quarterly basis rather than monthly in line with other regular regulatory reporting requirements and to minimise the administrative overhead on operators.
24. eir has the following comments with regard to the proposal to mandate the implementation of **Mobile CLI call blocking plus Roaming Checker**. eir acknowledges Mobile CLI call blocking has a role to play in seeking to mitigate against spam and nuisance calls, however further consideration is required by NCIT on practical aspects of implementation.
25. The InterWorking Function (IWF) outlined in the Technical Specifications, i.e., relay and interrogate the roaming validation requests and responses should be facilitated by the Fixed/Transit Operator, not the MNO.
26. eir notes the additional proposal in the technical specification, paragraph 9, that “Blocked calls should be terminated in the IGO’s equipment to a tone.” This is not a requirement outlined at NCIT for inclusion in the Mobile CLI Specifications. Each Operator should be allowed to determine how blocked calls should be handled. It should not be mandated. TDM interconnect calls should terminate to a tone and SIP interconnect calls should be handled in the appropriate manner. Backward SIP signalling 6xx message etc. allowing the originating network to deal with the call rejection appropriately.
27. ComReg proposes that phase 1 be implemented within 6 months of the Decision. There are significant data protection issues that will prevent Mobile CLI Checker from being implemented in any form before the Decision is formalised. Absent this legal mandate MNOs cannot share personal information about their customers to third parties (IGOs) i.e. about whether they are roaming or not. As such IGOs cannot implement access to the

---

<sup>2</sup> Consideration may have to be given to network freeze periods depending on when the Decision is made and consequently when the 6 month deadline actually falls.

mobile Number Portability Database (NPD) to know who owns the mobile number until the Decision is made.

28. With this in mind, there will be a significant amount of work including integration with the NPD, connecting networks, testing etc between MNOs and IGOs with MNO. Consequently eir believes that the implementation deadline should be increased to 12 months after the Decision given that preparatory works are constrained absent a formal Decision being in place.
29. eir notes that Part V of the draft decision instrument for Mobile CLI Call Blocking requires *“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”*. However it is our understanding that Decision 2 is for MNOs. Can ComReg please confirm if the text in the draft decision instrument is correct?
30. ComReg proposes that the intervention should be subject to a second phase of implementation within 2 years of the date of the Decision. The proposed second phase proposes to require MSPs to implement Roaming proxy Server and upgrade Roaming Checker to include VoLTE within 2 years of Decision.
31. The roaming check function outlined in the Mobile CLI Specification is based on standardised 3GPP specifications. Each Fixed/Transit operator will need to develop their own Roaming Proxy server based on their network signalling architecture. Implementing roaming proxy servers is likely to be complex and costly for operators. It is questionable whether cost and disruption can be justified for a solution that may be short lived due to technical evolution of VoLTE roaming and / or the implementation of other measures such as Voice Firewalls in similar timeframes which may be more effective
32. The proposed requirement for Roaming Checker for VoLTE should be removed as it is not necessary. When VoLTE roaming evolves it will be based on home routing (S8HR) architecture. Voice traffic from Irish VoLTE roamers abroad will route directly to the MNO network (never via Fixed/Transit Operators).
33. eir also considers that the Roaming Checker will become redundant if Mobile Voice Firewalls are mandated and implemented. A Voice Firewall solution should supersede any requirement for Mobile CLI Roamer check function. The Mobile CLI Roamer check is a basic, tactical solution that is not future proof. The Voice Firewall is a strategic solution that is adaptive, road-mapped, and utilises machine learning from worldwide nuisance communication threats. In parallel VoLTE Roaming is being rolled out and It is expected there will be a continued reduction in Mobile calls routing through International to Fixed/Transit. Technical interventions should only be mandated for so long as they have an effective role in tackling scam and nuisance communications and this should be reflected in the Decision Instruments.
34. With regard to **Voice Firewalls**, ComReg proposes MSPs or FSPs with over 330,000 Voice Capable Subscribers implement and use a Voice Firewall to block all calls that have the highest probability of being a Scam Call within 18 months of a Decision.
35. Whilst we can see potential merit in implementing a Mobile Voice Firewall (see preceding paragraphs), eir is disappointed that ComReg has brought forward this proposed intervention to be mandated in a Decision Instrument without first engaging in discussion at the NCIT.

36. The proposed Voice Firewall Technical Specification is a high level description of what a Voice Firewall may be and is not sufficiently detailed to ensure relevant operators can implement Voice Firewalls with sufficient consistency to provide an effective national solution. This is particularly important as firewall technology is at the early adopted stage and expensive to procure. Mistakes at implementation due to underdeveloped specifications will be costly for operators and should be avoided by facilitating further discussion and development at NCIT.
37. eir does not consider a Fixed Voice Firewall is necessary given the other measures that will be in place and believes there is no justification to mandate Fixed Voice Firewall.
38. eir believes Industry engagement is required before seeking to codify a Voice Firewall intervention and requests that this proposed intervention is not progressed in this consultation process. Voice Firewall should be remitted to the NCIT for detailed review and discussion to define and agree an appropriate Technical Specification. The Technical Specification may then be codified in a subsequent consultation exercise.
39. ComReg's proposal that Voice Firewalls should only be mandated on operators with over 330,000 customers also requires further discussion. It is not clear why the customers of smaller operators should be left more exposed to scam and nuisance calls. Nor is it clear why 330,000 customers is an appropriate threshold. eir does not believe there should be a threshold.
40. eir notes ComReg's assessment of **Stir/Shaken** and agrees it would not be appropriate to mandate this potential technical intervention at the current time.
41. We now consider the potential SMS Interventions.
42. ComReg proposes that a **Sender ID Registry** be implemented on a phased basis within 18 months of the Decision by Mobile Service Providers with over 270,000 subscribers (excluding M2M and MBB).
43. ComReg's proposal that Sender ID Registry should only be mandated on mobile operators with over 270,000 customers<sup>3</sup> requires further consideration. It is not clear why the customers of smaller operators should be left more exposed to scam and nuisance calls. Nor is it clear why 270,000 customers is an appropriate threshold. eir does not believe there should be a threshold.
44. [X<X]
45. eir notes ComReg's consideration of **Shortening the Chain** and ComReg's proposal not to proceed with this measure due to the 'underwhelming' response of the businesses originating the messages. This is disappointing and, as noted above, it is not acceptable for ComReg to abandon this initiative solely due to a lack of engagement by certain stakeholders. Operators cannot be expected to bear all of the costs in seeking to mitigate this multi-stakeholder issue while others are not required to follow through on far less taxing initiatives.
46. eir notes ComReg's consideration of **Origination-Destination verification** and agrees with ComReg's proposal not to pursue this intervention.

---

<sup>3</sup> eir notes that Part III of the draft decision instrument in section 7.6 refers to 270,000,000 which we assume is a typo.



47. ComReg proposes that **SMS Content Filter** will be implemented in addition to Full Sender ID register. However this requires a change to legislation. ComReg proposes, assuming change in legislation, a 12 month lead time would be reasonable.
48. Absent sight of the proposed legislation it is not possible for eir to comment on the reasonableness of the proposed implementation deadline. The legislation may contain requirements that would impact on the nature of the technical solution.
49. eir notes that ComReg has included the draft SMS Scam Filter Technical Specification in this consultation. eir strongly believes that it is too early in the process to codify a Technical Specification particularly as the Technical Specification “*is intended to provide an early view of future high level requirements*”.
50. eir believes Industry engagement is required before seeking to codify a SMS Scam Filter Technical Specification taking into account legislative requirements and requests that this proposed Technical Specification is not progressed in the current consultation process. The Technical Specification may then be codified in a subsequent consultation exercise when it has been more fully developed by NCIT taking into account any relevant legislative requirements. This should not unduly impact on implementation dates as it should prove more constructive to implement an agreed developed technical specification.

## Changes to the Numbering Conventions

### Q.1 Do you agree with ComReg’s proposal to amend the text in the Numbering Conditions as set out above?

51. eir has no objection to the proposed changes to the Numbering Conventions to support the introduction of the proposed technical interventions with the exception of the proposal (para. 6.26) to maintain a Mobile Station Roaming Number list. This matter is still under discussion at the NCIT and should only be mandated when those discussions have concluded and the nature of the solution is understood.
52. It is disappointing to note that Irish Language Sender IDs will not be supported. eir also notes that the proposed sender ID registration requirements will exclude charities / voluntary organisations / schools etc. This could effectively leave those organisations more vulnerable to being impersonated by an Irish mobile number and needs to be corrected.

### Q. 2 Do you agree with ComReg’s general updates to the CLI Conditions as set out above?

53. eir has no objection to the proposed changes to the Numbering Conventions to preserve MNAs. With regard to limiting the issue of NGNs to entities carrying out businesses in Ireland, the proposed approach may exclude charities and voluntary organisations etc.
54. With regard to the proposal to 999/112 as presentation numbers, eir agrees with ComReg’s recommendation (Para. 6.59) “*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.*” The use of non E.164 numbers as presentation numbers between networks is a novel concept. The technical assessment should be undertaken and concluded before any changes are made to the Numbering Conditions.

### Q. 3 Do you agree with ComReg’s general updates to provide CLI Guidance as set out above?

55. eir agrees with ComReg's proposed updates.

**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.**

56. eir notes ComReg's view (Para. 6.94) that "*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.*" However eir does not consider that the introduction of eSIM alone will lead to the registration of Prepay users.

57. eir has reviewed ComReg's proposed KYC Guidance and has the following comments. eir agrees it is important for KYC to operate effectively where it is required.

58. With regard to the Guidance in respect of Business customers:

- '*Nature of business*' and '*Information about the business customer's network and services provided*'. These seem to be the same requirement, i.e. the nature of the customer's business. It is not clear what an operator is meant to do on foot of this information. Can ComReg please provide further guidance on what forms of business, trades and professions should be prohibited and on the implications of an access seeker providing limited information about the nature of their business?
- "*Existing phone numbers and business websites*". The provision of the website(s) is a matter for the Business customer. Can ComReg please advise if it is expected that operators should perform an audit of the Business' website(s)?
- "*Volume of the request for numbers does not match the intended use of numbers*". This seems to be a somewhat subjective consideration. ComReg provides an example, "*(e.g., volume of numbers requested is not consistent with the intended use)*", however this is just a restatement of the requirement. Can ComReg please provide further guidance on how intended use and volume of requests should be considered?
- "*Previous complaints about numbers provided to the business customer*" and "*Consumers and organisations should be able to notify operators quickly and easily of suspected number misuse incidents.*" Previous complaints may not be known to the current operator providing service to the Business. Consumers and organisations suspecting number misuse incidents may not be aware of the identity of the operator providing service to the Business under suspicion. It would seem to be more effective if complaints are recorded at a central level and a list of suspect business maintained and circulated to operators. eir has no objection to working with the central body to assist in investigating complaints. Will ComReg assume this central coordinating role?

**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.**

59. eir notes ComReg's view on future NCIT focus at paragraph 6.144. ComReg appears to suggest that the NCIT should move towards developing an industry solution provided by third parties. eir does not agree that this is appropriate. Such an approach would be complex to implement and unwieldy to adapt to changing behaviour of scammers. Operators are best placed to manage technical interventions within their networks based upon agreed standards. In eir's view, as already highlighted in this response, the NCIT focus should move away from short term tactical solutions towards developing more strategic solutions such as Voice Firewall and SMS Content Filter. Once these have been developed the NCIT should become a quarterly or half yearly forum to monitor the issue of nuisance and scam calls in Ireland and review the effectiveness of technical interventions.

## 8 Ericsson

# Ericsson response to the ComReg consultation - Combatting scam calls and texts

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



## ABOUT ERICSSON:

Ericsson enables communications service providers and enterprises to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses. It is designed to help our customers go digital, increase efficiency, and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York. [www.ericsson.com](http://www.ericsson.com)



## Summary

Ericsson welcomes the opportunity to respond to the ComReg consultation on network based interventions to reduce the harm from Nuisance Communications. Ericsson is supportive of the proposed measures and interventions to reduce harm and restore trust in voice communications and reduce harms associated with scam SMS messages.

Ericsson recommends that implementation does not require the consumer to take action to activate the interventions and measures. Selection of a solution that does not require action by the consumer will result in a significantly higher success rate in blocking nuisance calls. It is equally important to secure that the solutions are capable of blocking nuisance calls on the widest range of devices, particularly ones that might not be capable of hosting apps or downloading the device vendors latest OS.

Ericsson believes that in the medium term the voice firewall solution will cater for all network users as operators migrate circuit-switched based consumers to IMS. This means all technologies (e.g., 2G, 3G, 4G and 5G) and all devices will be managed on IMS. The IMS based voice firewall can then be the single solution to manage nuisance voice calls. The voice firewall solution should ideally be able to implement DNO, PN and CLI call blocking in addition to its voice firewall functionality.

In the case of the voice firewall solution, Ericsson recommends an implementation where the decision to block a call is done by the network rather than via an app on the device. This avoids a scenario where the consumer is required to take action to activate the measures and interventions.

Taking a network approach will ensure the measures and interventions are implemented at the point of launch and that all device types and technologies are supported as the consumers are migrated to IMS.

With a network based solution it will be possible for individual consumers to opt out of the voice call blocking measures and interventions if they so wish.

## 9 Hiya

# Combating scam calls and texts Hiya:

## Consultation Response

31 August 2023

<b>Consultation title</b>	Combating scam calls and texts
---------------------------	--------------------------------

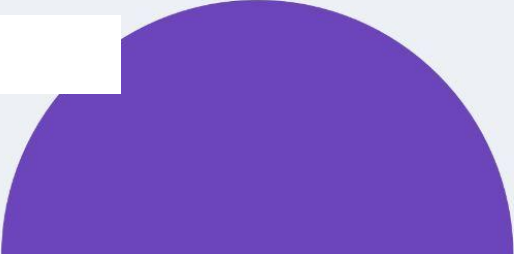
<b>Full name</b>	Nisha Malhan
------------------	--------------

<b>Contact phone number</b>	+44 (0)7500083578
-----------------------------	-------------------

<b>Representing</b>	Organisation
---------------------	--------------

<b>Organisation name</b>	Hiya Inc
--------------------------	----------

<b>Email address</b>	Nisha.malhan@hiya.com
----------------------	-----------------------

A large, solid purple semi-circle graphic located on the right side of the page, partially overlapping the contact information table.



<b>Introduction and overview</b>	<b>4</b>
<b>Consultation response</b>	<b>6</b>
<b>Beyond DNO lists: Benefits of a future-proof network-based technology</b>	<b>11</b>
<b>Hiya Protect product overview (Confidential)</b>	<b>14</b>
<b>A. Introduction to the Hiya Voice Security Platform</b>	<b>15</b>
<b>B. A foundation of data</b>	<b>16</b>
<b>C. Adaptive AI spam protection system</b>	<b>21</b>
<b>D. Continuous learning, continuous development</b>	<b>29</b>
<b>E. Flexible deployment</b>	<b>31</b>
<b>E. Reporting and monitoring: the Hiya Carrier Console</b>	<b>34</b>
<b>F. Privacy impact and data security requirements</b>	<b>40</b>
<b>Hiya Protect in Practice</b>	<b>41</b>

## Introduction and overview

Hiya is pleased to respond to Comreg's consultation on combating scam calls and texts. Securing the voice call is our purpose. Hiya is uniquely placed to consult with Comreg to establish the equivalent position on the voice call experience.

Scams are a blight on Irish society and cause significant financial and economic damage to all sectors of society including consumers, business, and public bodies. Scams also diminish the trust placed by consumers and businesses. Captured in this document are responses to the solution proposals presented by ComReg (in document 'ComReg 23/52e') as part of the consultation process. The response also provides an overview of AI solutions to spam, a product overview of Hiya Protect, and case studies for other global Voice Firewall implementations.

Hiya is a proven voice security solution that has been tested repeatedly against peer solutions. We've been protecting consumers from unwanted calls for over 10 years and we have a growing global data footprint of over 40 countries, reaching more than 450 million subscribers including 150 million Samsung devices.

*As this submission is rich in content it is worth additionally commenting on some key proposals made by Comreg in the consultation.*

- **Regarding Network vs App solutions:** As a business capable of delivering both solutions, we can speak from experience that only a network solution can deliver a comprehensive solution across an entire subscriber base, especially for susceptible demographics. Even if application uptake was 100% (it is not) there are serious limits on what is achievable due to iPhone restrictions and the lack of timely network signals.
- **Regarding Implementation Timelines:** Hiya notes that some Comreg proposed solutions (i.e. DNO list / Protected Number lists) form part of most Voice Firewall solutions. The proposed implementation timeline for DNO/Protected number list solutions is 6 months, and for a voice firewall it is 18 months. Combining the number list proposal into the Voice Firewall proposal and bringing forward the Voice Firewall timeline would form a more efficient solution.
- **A Voice Firewall that responds to evolving scammer tactics is the most viable, long-term solution.** Industry consultation and regulation can take time; and many scammer methods can be combated in a more agile way, especially by spam/scam specialists that have designed processes to deploy new models quickly and safely.

## Meet the team

In 2012, Alex Algard, then CEO of Whitepages, began developing the first-ever caller ID mobile app for spam blocking. After successfully bringing the app to market in 2016, he spun Hiya off as a separate company, bringing a

founding team that was already industry innovators in its understanding of illegal callers — and how to use data science to fight them.

Hiya recognized that while most networks, such as social media and payment applications, depend critically on trust and identity layers to function, the voice call had no trust or identity layer — leading to skyrocketing unwanted call rates and plummeting consumer trust in the channel. So the Hiya team set out to add trust and identity to the voice call with Hiya Protect, a voice security solution powered by advanced analytics and data science.

Hiya has built a world-class team in Europe, representing the very best talent across the tech and telecommunications industries. Hiya team members offer diverse and extensive experience across mobile network carriers, telecommunications providers, SaaS technology enterprises, and more.



**Alex Algard**

**Founder & CEO**

PAST:

Ekata, Whitepages



**Nisha Malhan**

**Regional Director, Business Development**

PAST:

Samsung, IBM, Mozilla, Nokia



**Mat Rees**

**Senior Data Scientist, MEng**

PAST:

Capgemini, GlaxoSmithKline



**Rob Mackinnon**

**Head of Architecture & Delivery, Business Development**

PAST:

Vodafone, NETGEAR



**Patrick Boyle**

**Senior Director Carrier Sales, Business Development**

PAST:

First Orion, Syniverse



**Scott Downie**

**Partnership Manager, Business Development**

PAST:

Check Point Software Technologies, British Telecom



**David King**

**Solution Architect, Business Development**

PAST:

Amdocs, Siemens, Digitalk, Nortel.



**Ram Rao**

**Lead Product Manager in Product - Protect & Distribution**

PAST:

Tesco, Skype, Microsoft

## Consultation response

Hiya understands that an email address and contact number will be kept on record. For confidential responses, ComReg can publish a reference to the contents of this response. The confidential information included in the response is clearly indicated.

Question	Your response
<p>Fixed CLI<sup>1</sup> Blocking: To stop fraudsters abroad spoofing Irish geographic numbers (e.g., 01-xx) to make scam voice calls.</p> <p><i>1 CLI means 'calling line identification'. Calling line identification allows the person receiving the call to see the caller's number.</i></p>	<p>Is this response confidential? – No</p> <p>Hiya agrees with ComReg assessment and the direction of the consultation.</p> <p>Hiya understands the risk and damage associated with call spoofing and we only wish to emphasise that call spoofing is only a tactic used to create some of these damaging calls. Scammers will find ways to circumvent any new solution, or find new ways to scam.</p> <p>Voice Firewall providers are able to react to evolving tactics and strategies more quickly than regulatory directives, and therefore offer a more robust long term solution against unwanted calls.</p> <p><a href="#">Please see more information on the Hiya Protect capabilities to prevent spoofing and other scams.</a></p> <p>Other regulators have required this blocking to be performed when the foreign traffic ingresses onto the domestic network. This is partly due to different location-signifying signals about the origin of the call being available at the point of ingress. If this information about the call was retained throughout the call's network journey it would enable a greater range of solutions at different integration points to block the call.</p> <p>Potential network-level partnerships with fixed-line carriers in Ireland using solutions such as Hiya Protect, will be able to detect</p>

	<p>spam calls based on shifting tactics instead of relying on phone numbers and historical data.</p> <p>Hiya Protect is powered by global call data from the Hiya Voice Security Network. This data spans the entire call ecosystem including enterprise callers, network providers, and consumers via app and device integrations providing real time insights to spam trends and tactics. <a href="#">More information can be found here.</a></p> <p>Everything about Hiya Protect has been designed to adapt to each carrier partner individually. Hiya Protect can be deployed in a variety of integration paths e.g. Support for legacy CS and IMS architecture, and the specific behaviour of the service is adjustable to the goals of a new partner. <a href="#">Hiya Protect flexible deployment,</a></p>
<p>Mobile CLI Blocking: To stop fraudsters abroad spoofing Irish mobile numbers (e.g., 087-xx) to make scam voice calls.</p>	<p>Is this response confidential? – No</p> <p>Hiya approaches the CLI blocking in Mobile in the same way as Fixed (noted this is potentially with different signalling)</p> <p>Hiya agrees with ComReg assessment and the direction of the consultation.</p> <p>Hiya wishes to note that spoofing of mobile calls from overseas providers comes with the additional analytical burden to consider if the mobile subscriber is currently roaming overseas. Fraudsters learn to find and exploit these types of exceptions, moving their traffic as necessary to continue success on their campaigns.</p> <p><a href="#">Please see more information on the Hiya Protect capabilities to prevent spoofing and other scams.</a></p>

A Protected number list: To stop fraudsters using numbers that are not yet in service or have yet to be allocated to a telecoms operator prior to entering service.

Is this response confidential? – No

Hiya agrees with ComReg's assessment, to help combat spam voice calls a Protect Number list is a method to prevent fraudsters using numbers not yet in service. A number list will be ingested by Hiya as and when the list changes.

Protected number lists are effective tools that are used in spam detection. However spam analytics e.g. traffic-based analysis, using user feedback and call duration to understand the nature of the calls, is an important part of the solution to reduce spam content. As scams are getting more sophisticated, spam analytics that employ machine learning across recipient reactions and call trends to detect spam call activity.

In Hiya's experience around the globe in providing spam protection services, we consistently see that unwanted calls using phone numbers not yet in service accounts for barely 0.1% of unwanted call traffic.

Furthermore Hiya notes a 6 month timeline proposed to implement this Protected Number List solution, and an 18 month timeline to implement a voice firewall. Given that most voice firewalls include Protected Number Lists as part of their solution; a more productive approach would be to require a voice firewall implemented within a shorter time frame.

[Please see more information on the Hiya Protect capabilities to protect the subscriber and improve carrier's performance on managing Spam.](#)

Do-Not-Originate list: Allows businesses / organisations to secure their numbers by blocking those numbers not used to contact consumers.

Is this response confidential? – No

Hiya agrees with ComReg's assessment, to help combat spam voice calls a Do-Not-Originate (DNO) list is a good way to secure numbers. Hiya already periodically ingests a number of different international DNO lists and can easily add new lists if Comreg chooses to maintain one.

DNO and Protected number lists are effective tools that are used in spam detection. However, spam analytics e.g. traffic-based analysis, using user feedback and call duration to understand the nature of the calls, is an important part of the solution to reduced spam content. Overall, very few of unwanted calls will originate from DNO or not-assigned phone numbers.

Furthermore Hiya notes a 6 month timeline proposed to implement this DNO number solution, and an 18 month timeline to implement a voice firewall. Given that most voice firewalls include DNO number solutions as part of their Voice Firewall; a more productive approach would be to require a voice firewall implemented within a shorter time frame.

As Hiya is an API solution, existing on the Ericsson MTAS infrastructure, the deployment timelines could be accelerated. Hiya's strong partnership with Ericsson has enabled Hiya to perform substantial testing over the years providing real proof points to the technology's effectiveness.

Hiya's API integration flexibility allows for integration to other TAS vendors.

<p>A SMS ID Registry: Allows businesses/organisations to register a SMS Sender ID<sup>2</sup> while blocking those that are not on the Register</p> <p>2 The SMS sender ID is the text display that you see at the top of your phone's screen and is typically used to identify who sent the message.</p>	<p>Is this response confidential? – No</p> <p>Hiya agrees with ComReg's assessment related to SMS messaging. However the solution would not prevent risky SMS from reaching customers; only that they would not be able to send unregistered Sender IDs.</p> <p>Hiya provides trust and security for global carrier voice networks. Hiya is also pursuing robust carrier-grade solutions that address messaging (SMS) related fraud and spam.</p>
<p>Voice-firewall: To block spam calls wherever they arise (i.e., Ireland or abroad) and protect against future more sophisticated scams.</p>	<p>Is this response confidential? – No</p> <p>Hiya agrees with ComReg's assessment that scams are getting more sophisticated, which is where spam analytics that employ machine learning across recipient reactions and call trends to detect spam call activity - whether associated with spoofing or not - is required to stop the scourge of spam and fraud calls. It has been proven in the US that STIR/SHAKEN is not enough as all 3 major US mobile carriers have employed an additional form of spam analytics to protect their subscribers from the potential danger associated with merely answering an unlabelled phone call.</p> <p><a href="#">Please see more information on the Hiya Protect capabilities to protect the subscriber and improve carrier's performance on managing Spam.</a></p> <p>The illegal caller industry is not static. Scammers are continuously adapting and evolving for maximum call success, which includes avoiding detection by spam analytics services like Hiya Protect. For this reason, Hiya Protect is architected for both automatic and team-driven continuous improvement through multiple layers. <a href="#">Please see here for further details.</a></p>



## **Beyond DNO lists: Benefits of a future-proof network-based technology**

As highlighted in the main body of the consultation response, scammers are constantly adapting their tactics to circumvent any new solution. Hence, protection and response to such challenges cannot be static. In our opinion, network-based voice firewall solutions, which are adaptive to evolving scammer tactics, are the most viable and long-term solution against unwanted calls. Captured below are a summary of the key benefits offered by network-based protection, for both carriers and consumers.

### **Data Science and AI**

Data science and AI are the core elements that enable Hiya to stay a step ahead of scammers. More specifically, an Adaptive AI system analyses every available facet of a phone call on the network in real time. As threats emerge, the system learns and adapts in order to apply the right protection to every call. Other solutions rely on basic protections such as number history analytics and validity checks, which are relevant signals but certainly not sufficient alone. Since mid-2021, Hiya has deployed multiple new layers of protection within Adaptive AI, powering the system to consider both terminating and originating call data.

### **Network integration and flexibility**

Network-based solutions provide certain advantages and flexibility (against DNO lists and app-based offerings) for both the carrier and consumers. Most notably, the solution does not require consumers to take any action. Once a network-based solution is live all subscribers are automatically protected.

### **Deployment Capability with Ericsson MTAS - pre-built APIs**

Hiya is the exclusive provider of call analytics for the Ericsson MTAS (v1.24+). The Hiya and Ericsson partnership offers a joint solution worldwide with the service name of Call Qualification. Call Qualification uses two standardised APIs to connect an Ericsson MTAS with Hiya Protect. Enabling these APIs is a simple matter of a licence upgrade and some basic configuration code written for the carrier's specific use cases. Hiya and Ericsson know each carrier has its own unique brand value, and the pre-built MTAS integration can bring these services to market faster, and at lower costs than other solutions.

### **Provisioning and management API support for network-based voice firewall solutions**

While many carriers may utilise the same TAS vendors, every carrier has an entirely unique service provisioning environment. Hiya approaches service provisioning according to how a carrier has designed its offering. For a carrier introducing a run-of-network service, Hiya can operate in a "provision-less" mode where each subscriber MSISDN

receives identical service (either call protection, branded caller ID, or both) and Hiya does not require advance notice. For a carrier choosing to implement a tiered service with a premium service level, Hiya can consume SOC or feature code changes as exposed by a SOAP or RESTful API from a carrier's orchestration system.

Hiya has experience managing trial periods of arbitrary length, as well as pushing service state changes back up to a profile if a subscriber downgrades or upgrades their service. To minimise customization, subscriber authentication and authorization gets delegated to the native carrier ecosystem. Hiya will consider the carrier's OSS/BSS subscriber profile as the ultimate source of truth for service levels and can support a regular auditing cadence.

Hiya has its own service management APIs for a carrier to consume if they choose. These RESTful APIs are available from a web or a mobile app context, and they cover the following:

- **List management:** Enabling a subscriber to add or remove numbers from block and allow lists.
- **Call treatment preferences:** Enabling a subscriber to choose how a call category is handled, such as sending all spam calls to voicemail.
- **Spam reporting:** Enabling a subscriber to identify a call as spam or not spam.
- **Call log:** Enabling a subscriber to see the most recent calls analysed, including if a call was blocked at the network level without a device ring.
- **Push notification:** Enabling subscribers to know a fraud call had been automatically blocked.
- **Service state:** Enabling subscribers to know if and how Hiya Protect will handle their calls.

The above enables simple, speedy and implementation.

## Network Solutions vs. Applications

As stated above, network-based solutions provide advantages over other protection solutions, with app-based solutions being a case in point. At the highest level, a network-based solution provides universal coverage, and does not require any action on the part of the consumer. Simply put, the customer does not have to download an application, activate a solution or see the results within the app. The network solution provides baseline protection for vulnerable sections of the population who tend to be targets for spam and fraud. It is worth noting that a subscriber will have the option to opt-out of this service if they desire.

We have summarised the key differences between a network-based solution and an application in the table below:

## Network integration

Advanced, adaptive call protection system that stays a step ahead of fraudsters and spammers

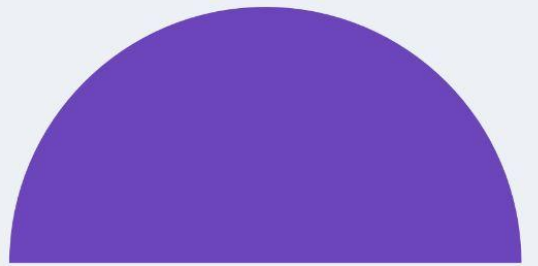
## SDK / App solution

Diverging user experience on Android and iOS with no adaptive features

Protection	<b>Highest level of fraud and spam detection</b> thanks to richer data in signalling and Adaptive AI to adapt to evolving scams	<b>Limited protection</b> due to limited data (only exposed to handset) and lack of adaptation to evolving scams
Latency	Call protection and context provided <b>at the exact time</b> the phone rings	Call protection and context provided after phone rings, which <b>can add latency</b>
UX	<b>Consistent user experience and limited friction</b> for subscribers	<b>Diverging experience</b> between Android and iOS Poor iOS UX (App Store ratings ~25% below Play Store's)
Uptake	<b>Instant activation</b> of subscribers with no need for local device app to activate the service	<b>Slow adoption rate lumpy</b> and there's a limit to percentage of active users (~5-15% of total base)
Analytics & reporting	Console provides rich, SaaS-based call <b>insights &amp; performance analytics plus reporting suite</b>	<b>Limited analytics &amp; reporting capabilities</b>
Data Security	<b>Data is stored securely</b>	Potential for 3rd party data harvesting and malware attacks
Overall	<b>"instant"</b> users' activation, <b>best protection</b> , and consistent user experience	Varying experience, user difficulty in adoption, no device dependency

In this section, we have highlighted the key benefits network-based technology offers over an app based solution. Furthermore, how investment in innovative, constantly evolving solutions will benefit the carrier in the long run, from a cost, speed to market, deployment perspective. Ultimately, providing protection against spam/scam for the Irish consumer.

hiya



# 10 i3forum

## Response to ComReg's Combatting scam calls and texts (ComReg 23/52). Consultation on network based interventions to reduce the harm from Nuisance Communications

i3forum welcomes the opportunity to respond to this consultation. We support ComReg's broad approach to evaluating the numerous solutions available to the telecommunications industry, especially including international origination, which will enable authentication and validation to reduce the opportunities for unsolicited communications.

### Introduction

The i3forum<sup>1</sup> established in 2007, is a not-for-profit organisation of International Telecommunications ecosystem that brings together all stakeholders (International Voice and Messaging Carriers, Vendors and Enterprise Service Providers) to help define best practices, promote and foster adoption of industry transformation and encourage innovation and competition.

i3forum membership is open and inclusive and the forum is driving the creation of an agile, adaptable and sustainable carrier business of the future. The aim is collaboration with a diverse and dynamic model with a mission to shape the future of the telecommunications industry.

The membership means our focus is targeted on the international aspects of call and messaging validation and authentication which will have a bearing / overlap with national call and messaging treatment.

### The Current Environment

It is our opinion we are in the midst of an international communications crisis on a global scale, caused by the proliferation of unwanted / illegal communications (e.g. spamming, spoofing, robocalling etc...), a significant portion of which originates from abroad. This has an impact across all levels of society, businesses and citizens which is creating an unprecedented burden on national regulators and the international communications environment.

i3forum believes the different approaches being adopted by NRAs across the world, with multiple variants, to try and eliminate unwanted / illegal communications with an international origination, only creates confusion, complexity and inefficiencies thereby allowing loopholes to develop and allowing opportunities for future exploitation. Our research regarding the fragmented approach being investigated and adopted is demonstrated in Annex 1, which highlights the continued increase in unwanted and illegal communications.

This fragmented approach creates a considerable cost burden for the NRAs and the international industry (cost and complexity of having to comply with multiple, often inconsistent requirements from various NRAs) and provides limited impact internationally thus resulting in suboptimal efficiencies and slow adoption by industry, particularly impacting those carriers who are active in the global marketplace. This in turn results in negative outcomes for genuine international communications which present as high-risk traffic. We fully support ComReg's broad and multi solution approach including considering the international origination.

### Lessons Learnt

ComReg, we are sure, are following the developments in the USA and are aware of the varying results from the initiatives to date. Youmail<sup>2</sup>, for example, although they may not be particularly accurate, shows that:

<sup>1</sup><https://www.i3forum.org>

<sup>2</sup> <https://robocallindex.com/>

- a) the trend shows stability at best
- b) consumers continue to be spammed
- c) international service providers still see significant amounts of traffic needing to be blocked regularly and
- d) figures suggest the trend continues to grow (5.1Bn in May 2023).

Even if we leave aside these numbers, end users are still spammed regularly and their experience remains very poor.

The implementation of STIR/SHAKEN in USA has been focused on the networks and not the end user experience. The FCC, by not issuing guidance on how calls are to be presented, failed to provide the end user with informed choice (based on network and technology-led solutions). i3forum would argue that regulators must take a holistic approach to spoofing and robocalling.

i3forum believe coordination is key and must include international carriers as well a local initiatives versus a localised disparate approach which has inherent limitations and will further exacerbate “whack-a-mole”, where the improvement in one area only displaces the issue elsewhere, TDM versus IP, for example.

Today, in trying to eliminate international inbound illegal/unwanted communications, many NRAs focus on termination, but little seems to be done to address the root cause of the problem, that of the origination side, which the terminating NRA alone cannot address. i3forum proposes that collaboration, coordination and inclusivity are the key. Regulators must aim towards creating a global environment which fosters innovation but will not leave international operators isolated and left to interpret and build individual solutions.

Inclusivity will enable international carriers to provide the “link” between terminating and originating NRAs by building on their experience of working together to combat fraudulent activity. Inclusivity will enable solutions such as CLI sanity & validation checks, Branded Calling, national & international Traceback. The application of a variety of solutions, such as these, will not be limited to either TDM or IP, therefore promoting a holistic approach and preventing further avenues of “whack-a-mole” developing.

Also critical is the “adoptability” and “affordability” of the requirements on international players. i3forum believes that the cost of complying with new requirements should not be so prohibitive as to de-facto exclude the smaller players.

## Mixed Approach

To achieve the aim of eradicating illegitimate international calls we believe it is vital to adopt a new mindset. As an industry we must tackle the issue of public trust by enabling solutions to be agile and to shift as soon as the fraud shifts and we welcome ComReg’s approach to this end. All industry stakeholders must work together with strong engagement from the regulators, as international carriers are not in a position to implement this on their own yet alone enforce any agreed measures.

An approach could be for any of the elements highlighted below be implemented at any time, in any order. These additional solutions to those already proposed by ComReg would further combat unsolicited communications.

### Option 1 – Basic Validation on International Calls

We note ComReg’s implementation of the DNO list<sup>3</sup> however, we would suggest that CLI validation for both national and international calls is required against National and Global Number Plans. To support this i3Forum has developed and launched the Numbering Plan Community platform<sup>4</sup> which

<sup>3</sup> <https://www.comreg.ie/industry/licensing/numbering/do-not-originate-list/>

<sup>4</sup> <https://i3forum.org/numbering-plan-community-platform/>

to date has 15 carriers participating and is open to all who wish to utilise the information.

The Number Plan checks need to work in conjunction with a comprehensive national Do-Not-Originate list (DNO) and we note that the Irish DNO list has few limitations regarding the numbers which can be added. However, in order for the DNO list to be as effective as possible, we would advocate that ComReg should consider ensuring the broadest scope possible and suggest that data is made available to international CPs and numbering information service providers to support blocking at source.

### **Option 2 – National CLI on International Trunk**

i3forum is developing solutions, architectures and governance which would support the implementation of 'Mobile Call blocking'. For example, "IsRoaming" a check on roaming calls, coupled with Trusted Trunks would be one way to ensure legitimate calls are handled correctly. Elements of these solutions may develop from the i3Forum activities where calls or trunks meet i3Forum standards, governance, approval (including 'Know Your Customer ("KYC") and "Know Your Traffic ("KYT") requirements) and viable technology solutions for Trusted CLI, then it would be recommended that these calls are not blocked.

### **Option 3 - International Traceback**

It is vital to be able to trace fraud, spam and spoof calls back to the originating call source, even for international calls and messages. i3Forum, with other industry associations, is developing a worldwide registry of carriers & operators who demonstrably meet high standards in ethical operations and which can facilitate traceback solutions. In addition, there will need to be a joint agreement on how to implement, operate and enforce international traceback. We note ComReg's identification of the "anglosphere" and that, if Ireland does not keep in step with other English speaking countries, there is the possibility of Ireland becoming a gateway to Europe for text-based scams. We believe that international traceback would act as a further deterrent to these scams along with the other measures being proposed.

### **Option 4 - International Trusted CLI solutions – Interworking between national solutions.**

This option remains technology neutral but recognises "Trusted Calls".

This solution requires the originating operator to carry out the basic validation checks against National and Global Number Plans and national DNO lists. It would then be reasonable to apply a policy to block all calls with national CLI on international trunks. However, it is essential to first implement industry viable solutions for the legitimate use cases of national CLIs on international trunks and we fully support the solutions ComReg is considering for mobile roaming, however, we would suggest that outsourced call centres located abroad and international DIDs for business should also be included.

### **Trusted Communications**

Practical solutions to enable verified CLI, for example - StirShaken, Trusted Trunks, Out of Band AB Match, CLI SafeZone, all of which are being actively developed by the i3Forum. These solutions can be used for national or international traffic, TDM or IP and can be implemented in any combination as is appropriate.

To enable "trusted calls" requires delivery of the call with a trusted CLI indicator (e.g. green tick calls) to display to the end user, that this call is verified, the CLI is attested and can confidently be answered. This solution is further supported by Branded calls and Branded Logo both of which identify the caller and could include a call reason text.

Utilising a variety of approved technology and contractual solutions, as highlighted above, for attesting trusted calls, introduces the concept of regulated "Trusted Call (or SMS) Indicator"



whereby the terminating operator is, for example, “beyond reasonable doubt” that a CLI is valid then the terminating operator can display the regulator approved trusted called indicator i.e. Green Tick or for alphanumeric CLI displays, such as “\*\*\*” or a “\*V\*” before or after the CLI. This can be applied for national or international calls and all network types (IP or TDM). We believe this will significantly improve consumer and business trust in calls / CallerID and empowers the communications industry to identify viable and practical solutions.

Once the concept of Trusted Calls and Trusted Call indicator(s) has been adopted, then the capability of Branded Calls and Branded Logo can be introduced. Branded calls display to the end user the brand name of the calling organisation, a reason text can also be added to the Trusted CLI. This is a powerful development in the services available which will drive greater value and usage of communications for Irish citizen consumers. These services are already being launched world wide.

## In Conclusion

i3forum firstly support the holistic and varied approach ComReg are proposing. By including international calls and messages this will lead to a genuine “end to end” approach. This will allow for a variety of technology neutral and industry viable approaches which in turn need to be supported with unified global guidance, we believe this starts with national CLIs on international trunks.

Secondly, we believe two areas of collaboration need to be explored jointly. One to agree global guidance and industry solutions. The second to look at joint governance and a joint regulatory framework to enforce unified guidance & solutions, this can comprise of:

- an opt-in framework for Carriers, NRAs,
- compliance at Carrier or trunk level
- compliance monitoring and enforcement
- compliance may bring “Trusted Carrier” benefits from participating NRAs & fellow Industry players.

Please see Annex 2 which explains our thinking.

Finally, we would propose that any and all regulations relating to stopping fraud must be enforced in order to ensure that any national rules actually deter fraudsters.

# Annex 1 - Various National Approaches to Robocall Protection for International Incoming Calls (and Messages)

## Survey of National Approaches to enabling Trusted Communications for Voice and Messaging

	1. Trusted CLI National Solutions		2. CLI Validating Solutions				3. Roaming Status Checks		4. SMS compliance	5. Vetting Process Traffic Statistics
	Voice	SMS	CLI Sanity Checks	DNO	CLI Removal	Call Blocking Policies	National	International	CLI and DNO	
US	US STIR/SHAKEN	TCR	Yes	Yes	N.a.	No	N.a.	N.a.	CLI Validation and DNO in 2023	N.a.
Canada	Canadian STIR/SHAKEN	N.a.	Yes		N.a.	No	N.a.	N.a.		N.a.
France	French version	N.a.	N.a.		N.a.	Yes	N.a.	N.a.	DNO	N.a.
Australia	On international inbound	N.a.	Industry Code C661		N.a.	Yes	N.a.	N.a.	CLI Validation and DNO	N.a.
Belgium	N.a.	N.a.	CLI guidelines BIPT		N.a.	Yes	N.a.	N.a.		N.a.
Latvia	N.a.	N.a.	CLI guidelines NRA		N.a.	Yes	N.a.	N.a.		N.a.
Norway	N.a.	N.a.	Regulation and Nkom Operator agreement 01.09.22		N.a.	Yes	N.a.	N.a.		N.a.
UK	Consultation 23.06.23	MEF SenderID	CLI guidelines Ofcom National CLI (except mobile)	Yes	Under study	Yes	Under study	Ofcom recommended		N.a.
Finland	N.a.	N.a.	Guidelines Traficom National CLI (except mobile)		If CLI not trusted	Yes	Based on API call	Via SS7 SRI-SM access		N.a.
Poland	Under study	N.a.	CLI guidelines UKE		N.a.	Yes	Based on API call	CAMEL triggering		N.a.
Germany	N.a.	N.a.	For specific CLI ranges		If CLI not trusted	No	N.a.	CAMEL triggering		N.a.
Saudi Arabia	N.a.	N.a.	N.a.		N.a.	Yes	Based on SS7 ATI	N.a.		N.a.
Oman	N.a.	N.a.	N.a.		N.a.	Yes	Based on SS7 SRI-SM	N.a.		N.a.
China	N.a.	N.a.	N.a.		N.a.	Yes	N.a.	N.a.		Realtime monitoring
Ireland	Under study	MEF SenderID	Fixed line	In progress >75% complete in operators	Under study	??	Under study	Under study		N.a.
India	N.a.	Blockchain registry	AI/ML-based filtering May 2023		N.a.	No	N.a.	N.a.	CLI validation AI/ML-based filtering May 2023	N.a.
Malaysia	N.a.								May 23 – block SMS from local and int. mobile no	
Spain		MEF SenderID								
Sweden								Under discussion		

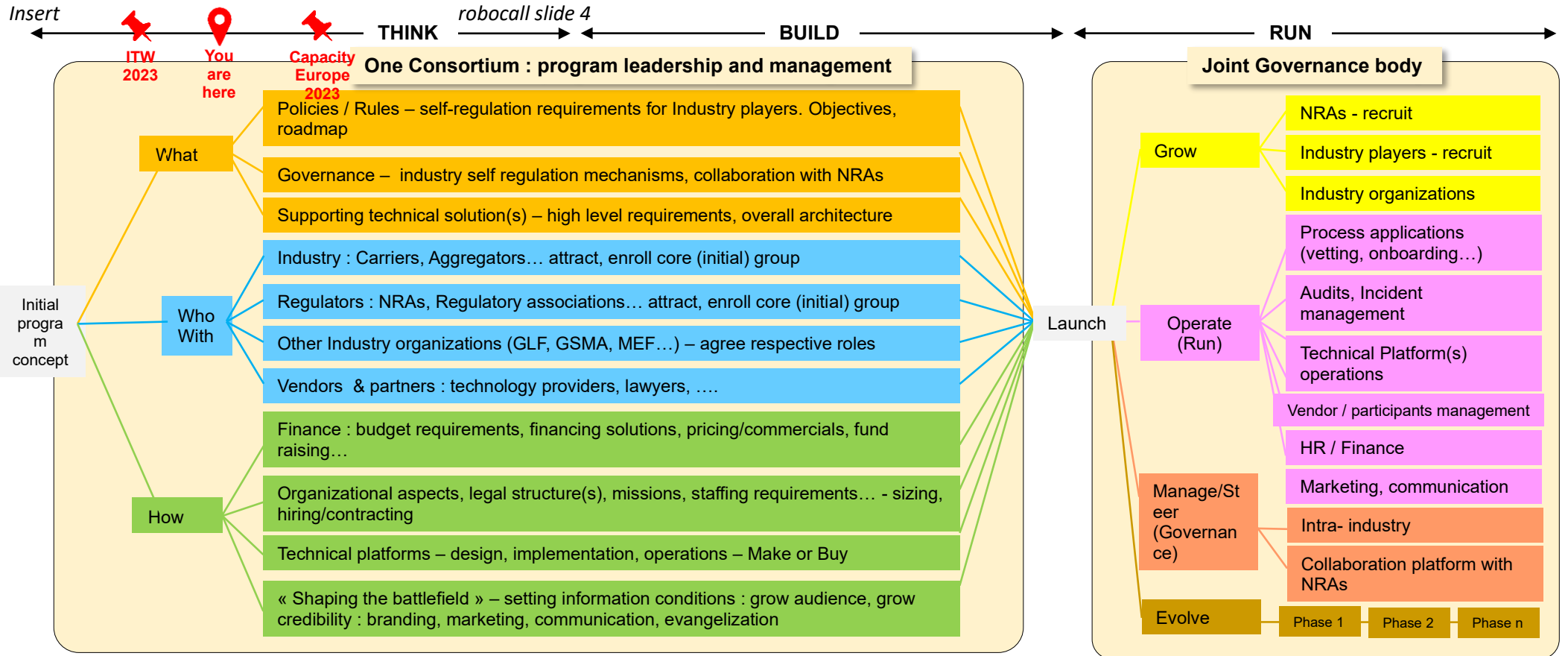


Updated June 2023

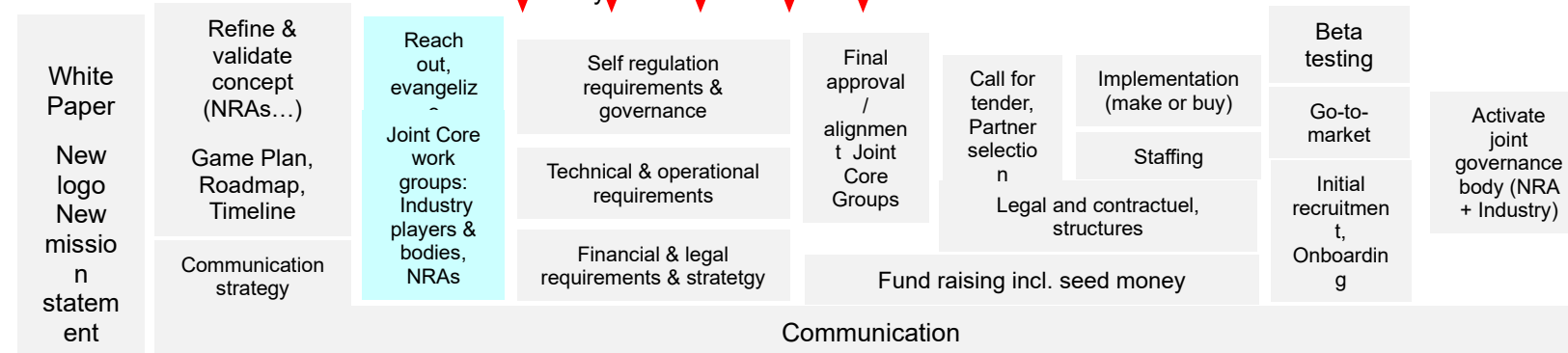
Source : i3forum, including industry input led by



# Annex 2 - Various National Approaches to Robocall Protection for International Incoming Calls (and Messages)



## Some key milestones / activities:



# 11 IBEC - Telecommunications Industry Ireland

## **Telecommunications Industry Ireland submission to ComReg Consultation Document 23/52 Combatting Scam Calls and Texts**

**31 August 2023**

Telecommunications Industry Ireland (TII) welcomes the opportunity to respond to ComReg Consultation Document 23/52 Combatting Scam Calls and Texts: Network Based Interventions to Reduce the Harm from Nuisance Communications. It also acknowledges the extended timeframe for responses and the clarification questions and answers provided by ComReg in Information Notice 23/75.

The members of TII take scam calls and texts very seriously and at a meeting on 1 November 2022 recommended to Minister Ossian Smyth the establishment of what became the Nuisance Communications Industry Taskforce facilitated by ComReg to devise and oversee implementation of an action plan to address the problem. Since its subsequent establishment, operators have worked collaboratively with ComReg on this matter through extensive collective engagement at the Taskforce and through bilateral monthly meetings. Both have involved direct and indirect input by numerous expert technical and network staff. Operators are currently working to implement the measures discussed and jointly developed at the Nuisance Communications Industry Taskforce as soon as possible.

Industry understands the economic, societal and reputational significance of this issue and remains committed to working collaboratively with ComReg to address the challenges posed by scam calls and texts. In this regard the number and sheer complexity of the measures envisaged make this set of proposals collectively particularly challenging. It is in effect 6 very detailed technical consultations rolled into one. It is critical to obtaining the best possible outcome that ComReg considers all the evidence, gathering more where necessary, and only mandates solutions when adequate time has been taken to fully consider all the alternatives as well as the overall industry context.

### **New proposals**

The consultation document contains several proposals based on detailed collaborative discussions between industry and ComReg at the Nuisance Communications Industry Taskforce. While they require significant capital investment, such proposals are welcome because they have the potential to make a significant contribution to addressing some of the challenges posed by nuisance calls and texts. Unfortunately, the document also contains some new proposals for specific measures that did not receive consideration by the Taskforce (e.g. voice firewall) or where considerations were not sufficiently developed or concluded (e.g. roaming checker and SMS content filter). These novel proposals are particularly problematic because they risk imposing disproportionate additional costs, structural changes to current operations and resource diversion for very small incremental benefits. Some proposals involve significant complexity because they will require the negotiation of multiple contracts and agreements with suppliers or industry. For these reasons, they should not be proceeded with until they are discussed collaboratively in detail by the Taskforce, and *inter alia* their effectiveness assessed through evaluating the

experience from other jurisdictions where such measures have been implemented. It would be inappropriate to make decisions on matters such as the proposed voice firewall, with associated implementation deadlines, before a full discussion with the operators takes place at the Taskforce to assess what has been done so far and what is most suitable for the Irish market.

#### Implementation costs

The members of TII are of the opinion that ComReg has significantly underestimated the cost of implementing its various new proposals. Before any of these proposals become mandatory, industry requests detailed engagement to ensure a comprehensive and accurate understanding of the costs involved in each case is reached. In this regard industry is willing to provide ComReg with any necessary information and assistance to help arrive at a shared understanding of these potentially very significant costs. Otherwise, the danger is that decisions will be taken without full knowledge of the relevant facts, which in turn risks that the amount of capital investment available for service and network improvement will be diminished.

#### Investment context

The consultation document does not take adequate account of the wider context of the time frames and overall level of investment required by a range of sector specific regulatory obligations. These time frames are overlapping, and industry has no discretion regarding the deadlines, which in some cases are mandatory under Irish or European legislation. These include but are not limited to the following.

- The Department of Environment, Climate and Communications' plans for the introduction of a public warning system by end 2024 so that Ireland will be compliant with the European Electronic Communications Code.
- The introduction of a new system for the secure and confidential retention of telecoms data for criminal investigations and national security as required under the recently commenced Communications (Retention of Data) Amendment Act. An independently chaired Department of Justice working group involving industry, An Garda Síochána and army intelligence is currently devising an operational memorandum of understanding (MOU) to govern data retrieval. This will in turn determine what is required of the operators and the system specification will flow from this. It is anticipated that the MOU will be concluded during Q4 2023, and the associated project IT will commence in 2024. The Department of Justice has informed industry that further data retention legislation is envisaged. This will in all probability require an additional IT project.
- Rollout commitments under new licences.

It is imperative that ComReg makes a value judgement on the quantum and phasing of investment required by the proposals under consideration in this consultation. A rigorous and transparent cost benefit analysis must be performed in each case and shared with industry. It is also of relevance that industry profitability is in long term decline, thereby reducing the amount of capital available for investment. The first call on this limited pool of investment capital is what is required to meet regulatory obligations, the remainder being left for network and service improvement, including enhanced cyber security.

## Clarity of obligations

The proposed obligations, should they come into force in their current form, are not sufficiently defined so that operators can know if they are compliant or not. What is proposed is inadequately specified, particularly those proposals that have not been discussed at the Taskforce. Further detailed consultation and discussion with industry is essential, ideally at the Taskforce.

ComReg should engage with industry over the next three to four months to develop more precise specifications on the proposed new obligations. Some of the proposed solutions are about two years off being ready to implement, so allocating additional time to improve the specification should not affect the timeframe for implementation but will greatly improve the end result.

## Number independent services

Industry believes that if operators succeed in making their networks even more secure against scam calls and texts, they will likely migrate to other forms of communications, which means that other types of providers will also be impacted. The consultation document does not discuss the role of number independent services notwithstanding the fact that ComReg regulates them in this context. There is a significant risk that scam calls and texts could well migrate to these services. This is an important omission that should be addressed given that the public make extensive use of such services. It should be clarified whether or not the obligations proposed for telecoms operators under Section 6 of the consultation also apply to operators of number independent services. If it is intended that these obligations do not apply, the reasoning should be explained as this would appear to leave a potential regulatory loophole for fraudsters to exploit.

## Privacy

Industry believes that some of the interventions have the potential to encroach on privacy rights. For example, there could be challenges under the European Charter of Fundamental Rights. Therefore, ComReg is urged to carry out a full assessment to establish if the proposed interventions are compatible with the Charter and any other relevant legislation. This assessment should involve engagement with the Department of the Environment, Climate and Communications and the Data Protection Commission. It is not appropriate for either ComReg or industry to spend time and resources on proposals with a major privacy component until the legal and regulatory issues have been clarified and fully resolved.

## Implications for market

If implemented, the proposals in Consultation Document 23/52 will have significant implications for the operation of the market as they entail significant structural changes affecting the entire value chain. It is assumed that ComReg is assessing the competition aspect of this, and it is noted that the matter is not addressed in the consultation document.

## Mitigation not elimination

It is important that it is understood by all stakeholders that the implementation of a full suite of highly effective measures will not eliminate the incidence of scam texts and calls. It will certainly significantly reduce the volume, but it is most likely that the problem will continue to manifest itself in other mutations, particularly on number independent services.

## Industry commitment

An uninformed reader of the consultation document would be forgiven for concluding that operators are to blame for the problem because they did not do more or act quickly enough. It is very relevant that these fraudsters became much more active when the world was hit by

a global pandemic and telecommunications providers invested substantially to reconfigure their networks to ensure their customers could work and study from home and could communicate with family and friends. The consultation document misses the opportunity to explain that it is a mistake to think that telecom providers did not respond to scam calls and texts; and to also explain that they had to devote major resources to keeping Irish families, students, employees, government bodies and businesses connected during the pandemic.

For the avoidance of doubt, the members of TII would like to put on the record that they are and have all times been fully committed to combating scam calls and texts with every means at their disposal. They remain committed to working collaboratively with ComReg on this very important matter both through the Taskforce and bilaterally.

#### Conclusion

TII calls for further analysis and discussion at the Nuisance Communications Industry Taskforce of ComReg's proposals, in particular those that have not been considered before. For its part industry will provide every assistance and all relevant information to ComReg to help ensure that the measures ultimately implemented are the most effective in protecting Irish consumers and businesses from scam calls and texts.

END



# 12 Imagine

31 August, 2023

Re: **Consultation on combatting Nuisance Communications (23/52)  
Draft Numbering Conditions of Use and Application Process(23/52d)**

Please find below Imagine's response to the above

On document (23/52)

Imagine has considered the content of the consultation document and in general agrees with, and understands, the need for interception actions by operators on certain calls to its end-users. However, there is concern that operators may be viewed to be, or deemed to be, 'responsible' or 'negligent', by their compliance with the regulations associated with Nuisance Call Interception, for instances where a call to an end-user results in an unfavourable outcome - either for the caller or the callee. It should be made clear, that it is not appropriate for operators to be expected to be 'call police' in this context (for clarity this means voice calls only, not SMS or other non-voice messaging). It is our view that it is the end-user who is always empowered to decide to accept a call, reject or block calls, and that must be reinforced to end-users by the regulator.

Imagine would like to comment on the Mobile CLI aspect of the document:

Mobile CLI blocking

On the mobile CLI blocking, as acknowledged in the document, not all operators have direct agreements with the Irish network MNO's, by which they can carry out mobile CLI screening on their ingress traffic. The document makes reference to a Phase 1 element, whereby a non-direct to MNO operator will have to enter into an agreement with another operator to carry out a 'lookup' of an ingress mobile-CLI on their behalf. Having examined the operational, commercial and technical viability of such a method, considering the date for Phase 1 deployment, and the current status of operators to offer such a method, we don't see this Phase 1 implementation date as being achievable, and would propose that the Phase 1 stage is removed as an obligation for non-direct operators, pending Phase 2. Notwithstanding, and, in recognition of the benefits of mobile CLI screening, any non-direct operator that can implement mobile CLI screening by whatever means should be permitted until Phase 2 is implementable.

On document (23/52d)

The proposed updates are noted, and are in line with Imagine's understanding. Based on our customers experience and requirements, we make the following suggestions:

Allowance should be made for a class of CLI Presentation Numbers that is permitted to be presented by a sub-contracted party (End-User), to a contracting party (End-User) to allow for representation on behalf of the contracting party, to which the number is assigned.

*Use case example: call-centre service provider, contracted to provide customer services help-line on behalf of an Irish located service company, calling to Irish PSTN end-users.*

Also, in the same context as above, item 9 is considered too restrictive and should be expanded to permit uses cases on behalf of other undertakings end-users.

If you have any further questions please do not hesitate to contact us.

Yours sincerely,

Imagine Communications Group

## 13 Joe Sheerin

## Submissions to ComReg 23/52



Joe Sheerin >  
To Market Framework Consult

[Reply](#) [Reply All](#) [Forward](#) [...](#)

Wed 19/07/2023 20:18

**i** Follow up. Completed on 22 July 2023.  
You replied to this message on 24/07/2023 19:36.  
If there are problems with how this message is displayed, [click here to view it in a web browser.](#)

**CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and believe the content is safe.**

I suspect that Telecom operators have started to make changgrd to reduce spam calls. I use the hotvoip service for my outgoing calls, and previously I was able to use my landline callerid when making the calls. (Hotvoip verify all callerids on each account through call backs). Now these calls are being blocked. Whatever soultion you agree for blocking spam calls/txts should still allow legitimate use of verified callerids on voip services based outside Ireland.

# 14 Johnny Bugler



Johnny Bugler [redacted]  
To: Market Framework Consult


Reply

Reply All

Forward




Mon 03/07/2023 11:20

 You replied to this message on 10/07/2023 09:47.  
If there are problems with how this message is displayed, click here to view it in a web browser.

**CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and believe the content is safe.**

Hi. I am writing in relation to the consultation on interventions by Telecoms network operators to reduce the harm from scam calls and texts.

When I receive a scam text I should be able to forward a screenshot of the number and message to Comreg. Comreg should then force the Telecom network responsible for that number to put a stay on it immediately, shutting it down or until it can be proven that the number is safe.

Johnny Bugler,  


# 15 Magrathea



Mr Donnacha Hennessy  
Commission for Communications Regulation

29<sup>th</sup> August 2023

### **Response to “ComReg 23/52 – Combatting scam calls and texts”**

Magrathea welcomes the opportunity to respond to this consultation which forms part of Comreg’s work to tackle scam and nuisance calls. In the UK we are a very active participant in this area, fully engaged with a number of key groups including the NICC CLI Task Group, Ofcom, ICO and Trading Standards and copy all of our efforts here across to our Irish client base.

The majority of this consultation relates to the proposed ‘voice interventions’ and we generally agree with the position Comreg is proposing. In fact, we have already implemented some of the measures being considered.

We are particularly pleased to note that you consider CLI attestation (STIR/SHAKEN) is not proportionate at this time, something with which we strongly agree, particularly when other simpler measures have not yet been fully implemented.

We have requested details separately relating to how mobile CLI blocking might work and cannot offer any specific comments on implementation issues until that has been analysed by our technical team.

We offer no opinion on the SMS interventions or the Voice Firewall as we have very little relevant experience in these areas, in addition the proposals included in the consultation exclude Magrathea from these requirements.

Our response focusses on Section 6 of the consultation – Updating the Numbering Conditions - specifically we would like to address the proposals made in 6.6 – Future Number Management.

#### **Inappropriate form of consultation**

First of all, we would like to express how disappointing it is to see the topic of future number management slotted in towards the end of a consultation focussed on scam calls and texts.

This is a topic of major significance with considerable implications and, in our opinion, must be the subject of its own consultation. By having this added almost as an afterthought, appearing only towards the end of a document without any mention in the title or in the

first 200 or so pages, it would be fair to assume that many interested parties will be unaware that this is even under discussion.

Particularly when you take into account previous consultations on the Numbering Conditions, it would be fair to assume that few Service Providers will be anticipating this content. The 2019 consultations on the Numbering Conditions makes no mention of sub-allocation or reseller rules and the 2021 document, which was used to transpose the EEC regulations, noted that Comreg may choose to assign numbers to other entities under certain conditions and Comreg concluded that no changes were needed to the Numbering Conditions at that time.

In fact, in consultation *Comreg21/28*, Comreg proposed adding words to the Numbering Conditions to clarify that resellers were active in the market, resulting in a new paragraph (12, section 3.1) along with a new definition of reseller.<sup>1</sup>

This conflicts with references made in this current consultation. For example, you quote Regulation 79(4) of S.I 444<sup>2</sup> which implies it is an offence to resell numbers, however in Regulation 79(5) it states a regulator may grant the rights if a number of conditions are met. It is our belief that Comreg is not compelled to withdraw resale or multi-level number provision and to do so, either retrospectively or in the future, would be deeply detrimental to the Irish telecoms market.

It seems that this view is shared too. The EEC report<sup>3</sup> referenced by Comreg in consultation 23/52, explicitly mentions that any regulator wishing to move from the existing multi-level resale model must have careful consideration for the change. The report recognises that there are benefits to sub-allocation (i.e., efficient number management and increased competition) and any withdrawal could have a considerable impact.

Part 2 of the S.I. 444<sup>2</sup> lays out the tasks and objectives for the regulator and this states that any conditions must be necessary and proportionate; promote access and take up of networks; promote competition, develop internal markets by removing obstacles, ensure widespread connectivity, promote investment and innovation and must not discriminate in the treatment of ECN and ECS. Again, it is our opinion that by preventing the multi-level business model Comreg would not be able to meet the above tasks and objectives and we hope to explain below how the opposite is true by leaving the market as it is today.

### **Impact of individual number management**

If Comreg were to restrict the reseller model it has a number of knock-on impacts which we have attempted to briefly summarise here.

#### *Call routing efficiency*

Ireland, like the UK, has no central database currently. There is of course a form of 'exception' routing in place via PXS which allows networks to check if an alternative route should be applied. But in the main calls are routed at a network level to the range holder of the number. This makes for efficient routing and has the benefit of an incumbent (OpenEir) which acts as the network of last resort – ensuring all end users can be reached when no direct interconnect is available.

If we were to move to individual number allocations as proposed, every number would have to be added to the database – at a cost to the provider – and every network would have to do real time look ups for all calls, again adding cost. Not to mention the cost of scaling the existing number management system to cope with the additional requirements and load. Adding this capability would be expensive and require time and resource to implement. In our opinion it would be difficult to claim this model is efficient and encourages competition, it would in fact add a major barrier to entry for many smaller telecommunication providers.

As well as increasing cost and reducing competition, this option would favour any major or integrated vertical network by supporting their business model above others (i.e., discrimination).

### **Impact of removing multi-level allocations**

#### *Number hosting*

If we stick with range allocations, at present OpenEir will only databuild numbers that are assigned to the network they are interconnected with. They will not accept a service provider with their own number allocation from Comreg utilising a switch partition on another network. This forces the service provider to transfer their allocation to their network of choice, immediately putting them in the position of having numbers sub-allocated to them.

If sub-allocation is banned and this databuild challenge isn't solved it is clear to see there is a significant barrier to entry here. Number hosting is an extremely cost effective, efficient and technically prudent way for smaller networks to establish themselves in the market. In the UK we have a very healthy market for this service which not only benefits competition but also reduces the workload on the larger networks as they can deal with fewer partners and rely on the host network to manage interconnect issues.

The fact this model is not supported by OpenEir is restricting access to the market. If Comreg do determine that networks should only be allowed to supply direct to end users, to avoid anti-competitive affects you should enforce network partitions to allow consumption of this model.

Without intervention we would also expect to see existing 'white label' distribution chains and MVNOs disappear as they are also utilising sub-allocated numbers. Something that becomes perhaps even more of an issue as the legacy telecom's infrastructure is phased out and the desire for innovative and flexible new solutions gain significance.

#### *Number management*

Our understanding is that your key motivations at seeking to eradicate the reseller models is to have greater visibility of the user to help reduce scam calls but also to protect number resource. And of course, Regulation 79(5) of S.I 444 specifically says that Comreg must be confident that there are adequate number resource to satisfy demand in order to allow sub-allocation, but also be confident that the parties involved can suitably manage that resource too.

Based on our experience in the UK and Ireland, a numbering market we have been involved in for over 20 years now, we strongly believe that our business model contributes to efficient resource management and through proper handling of this responsibility we have the added benefit of managing scam and nuisance calls to a greater level than perhaps we could do otherwise.

When Magrathea is the range holder we are able to ensure consistent call routing, reliable and resilient network management, pricing controls compliant with regulation and network billing standards. All of this means that interconnected networks, and the regulators, only have us to deal with on these key high-level issues.

Magrathea provide a tool to our clients, the service providers or resellers, who can then allocate individual (or small batches) of numbers from any of the area codes required. They have real time controls to manage how calls are routed from us to the end user and are able to choose small quantities of numbers from areas that otherwise they may have to not serve or risk holding a huge range of numbers. Because Magrathea handle all calls to the numbers we are able to monitor usage and automatically recycle unused numbers and also manage new range requests responsibly through greater visibility and anticipation of our clients' needs.

#### *Fraud controls*

Alongside the efficiencies that having us manage numbers brings, we are also able to help with due diligence activity and apply monitoring to our clients and their end users. Each of our clients goes through a comprehensive KYC process, and in turn they are required to do the same for their customer or end user. We provide tools to store details such as end-user address information and of course we provide guidance and support on how to comply with all current regulation in regard to number use and management.

By providing these services to a number of clients we reduce considerably the number of small providers who are having to engage directly with the networks and the regulator. We are pre-screening many potential undesirable number holders and also ensuring numbering resource is carefully managed. The advantage for our clients is lower barrier to entry, great cost efficiencies and the support and knowledge that they get by dealing with a well-established carrier network.

#### **Reducing scam calls**

It is a generally accepted fact that there is no 'silver bullet' to address scam calls, instead it's an ongoing process of making it more challenging for the perpetrators by introducing a variety of measures to interrupt the schemes. Therefore, it is even more important to ensure that any measures are proportionate. Magrathea do not believe that such a drastic change to the business model being proposed will have enough of the desired effect to be considered proportionate.

Instead, the problem is likely to shift from where we are today with the range holder being to a great extent responsible for managing issues, to Comreg dealing with end users to

investigate breaches. With a vast amount of CLI spoofing and false identity, these types of calls will be unaffected, but the tracing of source may become much more challenging.

A more sensible approach would appear to be to formalise which providers in the supply chain are responsible for each part of the process. For example, in the UK it is clearly defined what is the responsibility of the entity contracting with the user versus the carrier network/range holder.

If Comreg were to keep a register of all service providers and/or retailers this would ensure a highly visible chain and support an appropriate level of accountability.

## Summary

To summarise, in this document we have highlighted our support for action to combat scam calls and texts. We already mirror the work we have done in the UK to comply with regulation, both in spirit as well as action, in our Irish operations.

We are however concerned that proposed, significant restrictions to the Irish reseller market have been introduced as part of this consultation as a possible solution to protect consumers. There are three key drivers to our concern: Firstly we believe the proposed changes have potential to actually work against some of Comreg's key tasks and responsibilities. Secondly the proposals have potential negative impact to the currently accepted and effective business model operating in Ireland, which go beyond a proportionate response. Thirdly we believe the title and main focus of this consultation inhibits a full response from our industry on these proposals.

Our current view is that the proposed change to the reseller model cannot be justified for the reasons explained in this response and that there are better ways – some, of which are included in the consultation – to achieve the end result that Comreg is seeking in relation to scam calls.

We therefore urgently request that Comreg create a separate and dedicated consultation on the proposed changes to the reseller market, so all impacted parties have an opportunity to express their opinions. Any such consultation should also include market analysis and look to understand the risk to competition, discrimination and reduced efficiencies within the wider telecoms network.

We remain available to discuss any of these points further if Comreg should wish to do so.

Yours sincerely,



Tracey Wright  
Magrathea Telecommunications Ltd

<sup>1</sup> <https://www.comreg.ie/media/2021/07/ComReg-15136R3.pdf>

<sup>2</sup> <https://www.irishstatutebook.ie/eli/2022/si/444/made/en/pdf>

<sup>3</sup> <https://docdb.cept.org/download/1420>

# 16 Mobile Ecosystem Forum (MEF)

## Consultation response form

Please complete this form in full and return to Mr. Donnacha Hennessy  
Commission for Communications Regulation Email: [marketframeworkconsult@comreg.ie](mailto:marketframeworkconsult@comreg.ie)

<b>Consultation title</b>	<b>Combatting scam calls and texts Submissions to ComReg 23/52</b>
<b>Full name</b>	Mike Round
<b>Contact phone number</b>	+44(0)7802 220171
<b>Representing (delete as appropriate)</b>	Mobile Ecosystem Forum
<b>Organisation name</b>	Mobile Ecosystem Forum (MEF)
<b>Email address</b>	mike@mobileecosystemforum.com

## Confidentiality

<b>Your details: We will keep your contact number and email address confidential. Is there anything else you want to keep confidential? Delete as appropriate.</b>	Nothing
<b>Your response: Please indicate how much of your response you want to keep confidential. Delete as appropriate.</b>	None
<b>For confidential responses, can COMREG publish a reference to the contents of your response?</b>	Not Applicable. There are no confidential responses

### General Remarks:

The Mobile Ecosystem Forum (MEF) is a global not-for profit association established in the year 2001 to advance and protect the potential of mobile communications. Our members offer multiple perspectives in the ecosystem including mobile network operators, connectivity providers, wholesale vendors, security solutions, system integrators, content providers, financial players, and retailers. MEF headquartered in London, UK, with subsidiaries Brazil and Ireland.

- **The Mobile Ecosystem Forum (MEF) supports and welcome all efforts to limit fraud and protect the end consumer. The industry can limit threats, but it should do more and increase speed of its responses.**
- **MEF believes that there is no single technology that can deal with text and call spoofing. MEF supports CLI authentication, especially to protect consumers from fraud.** Focussing on a single solution is potentially detrimental for the end user. A concerted effort to react and respond quickly to threats is more likely to fend off the multiple systemic attacks attempted by fraudsters.
- **The implementation of STIR alone would not stop spoofed calls. STIR is a valuable tool for building trust in Caller ID for voice calls,** but it is not a silver bullet for reducing scam calls. It is still important to be vigilant and use other tools to protect yourself from fraud, see the U.S.A.

data. In addition, STIR would not cover text-based threats, allowing for displacement of fraud from one channel to another. The regulatory response should articulate the problem across the channels, and not with reference to one only.

- **If STIR were to be rolled out, we could suggest adding further elements to the CLI authentication solution such as:**
  - Increasing focus on establishing identity of callers, not just authenticating transport carriers
  - Actual meta data on calling party.
  - The use of a central numbering data base since the ability to traceback is important to fight bad actors.
- **Blocking or disrupting calls is not the only potential answer to spoofing. ‘User Guidance Indicators’ could provide an important defence mechanism, and trust enhancing feature. This is a long-term solution to be developed with the wider telecom ecosystem, but one that could qualitatively improve the customer experience** It is possible to increase user confidence on the authenticity of the caller by first establishing identity and sharing identity attributes with the end users.
- MEF encourages COMREG to establish goals and outcomes for the industry to work towards, rather determining tools to be applied. **We encourage COMREG to establish accountability in the industry and establish the positive outcomes it wants to see in the market. These should reflect the user experience and not just the roll out of a single specific technology – which might not by itself have an impact.**
- **We recommend an approach including more flexibility to responds and plan to threats as they develop over time.** We believe Ireland needs a forum for the industry to consult and respond in near real time to the emerging threats, sharing information, proposing responses. The Irish Sender ID Protection Registry is a positive example for SMS spoofing, and it has now been copied globally. For disclosure, MEF chairs this forum in its role of secretariat, but the overall model could be used in this context.



## Your response

	Your response
Number Spoofing	<p><b>The threat of number spoofing is real and troubling for the entire industry, as it erodes trust in the whole telecom service.</b> Unfortunately spoofing has already resulted in significant damage to the market. Short-term action is essential to address the challenges we face (2024). A long-term plan may be too late, as the situation may have changed by then. We need to be agile and responsive to the needs of the moment.</p> <p>Consumer Trust in telecommunication services is threatened by the volume of fraud. In the <b>2023 MEF Consumer Trust Survey</b>, British smartphone users reported receiving unsolicited text (44% of them, vs. global average of 49%), unsolicited calls (43% vs. global average of 48%), reported receiving fraudulent text messages (37% vs. global average of 39%). Despite the challenges, UK consumers are more confident in their ability to stay safe. The consumer trust index showed a (+4% p.p. year on year) increase in confidence with consumers believing safety from threats is improving. In the United Kingdom, incidence of unsolicited texts remained stable year on year, but unsolicited calls dropped year on year by 2 percentage points, incidence of fraudulent text messages dropped year on year by 7 percentage points. The improving trend is consistent with the previous year benchmarks.</p> <p><b>The Irish and UK telecom industry has made significant progress in limiting threats to consumers.</b> This is a testament to the actions and successes of the industry, which should be encouraged and supported.</p> <p>The Irish Sender ID Registry has significantly reduced the success rate of fraudsters attempting to use alphanumeric aliases in the SMS network. This UK development has been exported to other countries including Ireland, and its approach could provide important learning for spoofing prevention efforts around the world.</p>
	MEF agrees that more needs to be done to tackle number spoofing. This is a complex problem that requires shared accountability and clear lines of action. A single solution is unlikely to be effective, and no single decision will significantly limit the actions of fraudsters. Fraudsters are becoming increasingly adept at adapting to new challenges, so

	<p>the industry needs to be able to manage both long-term solutions and short-term tactical responses. Coordination, responsiveness, and information sharing are essential principles that should drive all activity in this area. Attestation by itself is not likely to reduce the volume of fraud calls.</p> <p>STIR is a valuable tool for limiting CLI spoofing in parts of the networks, but it is not a panacea. It is important to consider the empirical results in other markets such as the USA and Canada where volumes of fraud were displaced from purely domestic routes to international ones, or from ‘protected routes’ to ‘non-protected routes.’</p> <p>Unless STIR is mandated universally in telecom networks it is likely that fraudsters will find weaker points to exploit.</p> <p>There are several complementary solutions to STIR, such as in-band and out-of-band implementation of additional header data, a central phone number registry, and phone number verification solutions based on existing data sets. Multiple types of solutions are currently offered or used by MEF members. The industry should not limit itself to STIR alone but should continue to deploy and devise new solutions to tackle number spoofing. DNO lists and CLI validation against numbering plans are good foundational requirements. CLI attestation and validation using STIR are also valuable tools. However, MEF recommends extending validation requirements to include additional data sets, such as assignment or fraud reports.</p> <p>An industry forum to align and orchestrate different fraud responses is more likely to have an impact. Fraudster strategically attempt to change their attacks. The positive experience of the Ireland (&amp; UK) Sender ID Protection Registries, anti-smishing registries set up by BPFI, MNO’s, Aggregators Cyber Security Centres, and the Mobile Ecosystem Forum provides a reference for such a platform. Originally aimed at managing a registry it developed into a forum for information sharing, joint activities, and rapid escalations.</p>
	<p>STIR is not likely to reduce spam or unwanted calls.</p> <p>The USA example is a good reference point. Since the introduction of STIR the consumer experience has decreased. YouMail robocall index (<a href="https://robocallindex.com/">https://robocallindex.com/</a>) has reported the USA number of robocalls (i.e., SPAM calls). This index has increased from less than 4 billion a month in 2021 to over 5 billion in May 2023. STIR/SHAKEN has not been able to limit the impact to consumer</p>

	<p>in the USA, the volumes of calls have significantly increased.</p> <p>This is not to say that STIR is not a valuable tool, but it shows how fraudsters could be using the implicit vulnerability and predictability of the solution to implement successful strategies.</p> <p>CLI authentication is a critical step in building trust in phone calls by helping terminating service providers and consumers identify authentic calls. It is important to note that STIR/SHAKEN has been extended to non-IP networks to further this goal, the solution is evolving for better support.</p> <p>MEF supports the suggestion of creating in UK a common numbering database could play a role in CLI authentication among other services. This is line to international experiences.</p> <p>International traceability of calls from gateway would represent a challenge and potentially eroding real connectivity. This area seems particularly at risk for fraudsters attacks, increasing complexity for good industry players. The “Openness of Communications” should not be at risk.</p>
<p><b>Administrative steps required to implement CLI authentication</b></p>	<p>MEF supports the idea of the Administrator role, however we believe that the nature of the work of the administrators will require the separation withing the Administration of two separate functions:</p> <ol style="list-style-type: none"> <li>1- Solution. Managing of the Operational Activities and underlying platform the running and functional implementation of the solution.</li> <li>2- Secretariat – an industry body/forum to manage governance and reporting, including: <ol style="list-style-type: none"> <li>a. The awarding of contracts for the operational activity to a solution management organisation</li> <li>b. Creation, discussion, and improvement of rules and regulation</li> <li>c. Sharing of information to industry players</li> <li>d. Reviewing of operational activities performance and KPIs</li> <li>e. First escalation of infringements or irregularities</li> </ol> </li> <li>3- Supervisory reporting – the controlling the overall effectiveness of the solution and potential final escalation.</li> </ol> <p>This would allow to separate functionality of the technical solution vs the industry, and the role of the regulatory input. Such a model has been used in the setting up of the UK Sender ID Protection Registry, and it has provided a good governance model.</p>

	<p>SMS spoofing is mitigated in the United States by the industry's adoption of a common numbering database (CNDB). This database distributes unequivocal and transparent information on the allocation of phone numbers to service providers, allowing all messaging ecosystem participants to block sender IDs from unauthorized connections and bad actors.</p> <p>The regulator should set up the CMDB framework as an essential part of the activity of consumer protection, even outside the planned STIR solution. The establishing of the rules, operators, and solution of this are important to be managed by Ofcom directly - a view to support transparency, accountability, and fair competition in the market.</p>
<p><b>Executive summary 1.8</b>  <i>'Around half of consumers now require confirmation of message legitimacy/40% consumers have lost trust in SMS service.'</i></p>	<p>Over recent months/years there has been significant industry/media focus/education on the issue of scams calls and text with consumers constantly advised to question the validity of communications they receive. Lunchtime radio phone-ins featured almost daily updates on the problems related to banks. It is therefore not surprising that consumers are now more questioning. This is probably a testament to the effectiveness of media/industry education rather than evidence of a worsening situation.</p>
<p><b>SMS Interventions 1.25</b></p>	<p>It should be noted that an SMS Protection Registry – an industry collaboration run by MEF – has operated in Ireland for over 2 years and has achieved positive results for the participating merchants/brands. All Irish MNO's and most aggregators have participated in the initiative which has supported 10 major merchants to date – but is available for much greater expansion as has been the case with the UK MEF Registry.</p> <p><b>A recent new MEF registry merchant (a bank) reported a 70% reduction in smishing in less than 6 months engagement.</b></p>
	<p>This approach is best described as 'partial' as it is only necessary for the 'most-smished brands' to register. Telecoms providers are encouraged <i>not</i> to block traffic using protected senderIDs if they believe it comes from another legitimate brand with a similar name – thus over-blocking is eliminated.</p> <p>Unlike URL's, SenderIDs are not 'owned' by anyone and there are many instances where</p>

brands with identical or similar sounding names legitimately send messages to consumers. Where a 'partial' Registry is operated these identical/similar names can be catered for with pragmatic processes operated by the telecoms providers.

SenderIDs are territory/country specific and vary between countries – even for the same international merchants.

Arguably, given the senderID character length constraints there are not enough unique senderIDs within country to allow every merchant to specify their own brand name under a fully mandated solution. I.e Nationwide Building Society, Nationwide windows, Nationwide Tyres, Nationwide windscreens, Nationwide kitchens, Nationwide Bathrooms – may all want to use the senderID 'Nationwide'. So who decides who gets it? There are many, many examples similar to this. Brands with short names - often just using 3 or so letters - are impacted even more.

The vast majority of brands will never be targeted by random opportunist smishing attacks – as consumers just won't be convinced them to be valid. By removing the need for these brands unlikely to be targeted from the registry solution frees up senderID for those brands that need protection.

A mandatory SenderID for all merchants would present a massive overhead for **All** merchants big and small as well telecoms providers (MNO's and aggregators). Most merchants do not know how their messaging is routed from end-to-end and to define this process presents a huge overhead. Most messaging providers have redundancy in their routing to allow for the necessary alternative routing required to ensure continuity of critical services. All these alternate routes would need to be registered and approved in advance to avoid over-blocking of legitimate messaging.

A mandatory Registry solution requiring participation of all merchants would potentially lead to consolidation in the messaging industry with smaller players being disadvantaged – resulting in a less competitive market.

<p><b>SMS Scam Filters</b></p>	<p>To date privacy concerns have hampered the efforts of industry players regarding investigations into suspect messages. The ability for messaging providers to look at message content in the pursuit of fraud prevention – is a massive barrier – even when consumers have made a complaint. There needs to be much greater clarity for those involved in investigating and preventing smishing attacks regarding examination of messaging .</p>
<p>4.3 7 shortening the chain</p>	<p>Most merchants don't understand the routing of their messaging and as such are not able to shorten chains. As previously stated this measure would adversely impact smaller messaging entities and drive market consolidation of the bigger aggregators – reducing market choice and competition.</p>
<p><b>4.75 full or partial SenderID registry</b></p>	<p>MEF have run a 'partial' registry as part of an industry collaboration on behalf of industry in Ireland for over 2 years – with good results. However more merchants need to be engaged for it to achieve its potential – particularly the 'most-smished brands' such as couriers.</p> <p>Regulatory encouragement from COMREG would make a significant difference.</p> <p>Whilst the banks suffer financial loss through smishing (by compensating consumers and covering the admin involved) many other merchants just suffer 'brand damage' and don't feel the need to engage. There is also an education issue.</p> <p>Bizarrely some Government agencies (such as Revenue) don't believe they need to participate in an SMS registry as they don't send out any SMS messages to consumers. Clearly this argument is flawed as fraudsters have adopted the 'Revenues' digital identity and send out thousands of scam messages using the SenderID 'Revenue'.</p> <p>Whilst couriers are the most smished brands they are also reluctant to engage despite the significant consumer harm carried out in their name.</p> <p><b>It is proposed that a list of the 'most smished brands' is established and COMREG should strongly encourage the brand owners to participate in a partial registry – such as the ongoing MEF SMS Protection Registry – to ensure consumer protection.</b></p> <p><b>Option of this simple proposal will drive significant smishing reduction in weeks – without further development.</b></p>
<p><b>Impersonation – denied list</b></p>	<p>Brand Impersonation through the use of mis-spelt senderID variants can easily be controlled with</p>

	<p>the use of a 'denied list' as used by the MEF Registry.</p>
<p><b>Impersonation – reducing the allowable character sets</b></p>	<p>Most MNO wholesale services support an extensive extended GSM character set. These extended special characters are used by fraudsters to impersonate legitimate brands.</p> <p>By reducing the MNO supported character sets – the options for fraud are significantly reduced. This is the approach currently being rolled out in the UK</p>
<p><b>Impersonation – handset autocorrection of senderIDs</b></p>	<p>Some handsets have s/w to auto correct misspelled senderIDs. Fraudsters exploit this function to evade controls. Ie the frauster uses a misspelled senderID which is delivered to the h/s where the h/s auto-corrects the misspelled senderID to a (for example) a bank name where the message is inserted into a legitimate message thread.</p>
<p><b>SIM Farms</b></p>	<p>MEF agrees the sale of SIM farms should be banned</p>
<p><b>5.5.2 Regulatory options</b></p>	<p><b>Option 2 ban SIDs</b>  Banning senderIDS would lead to a significant reduction in consumers ability to identify the sender. Consumers would be forced to rely solely on the message content in order to decide if genuine or scam</p> <p>There is no evidence from markets that don't currently support Alpha senderIDs that this leads to a reduction in scam/fraud. In fact the opposite is true. A large number of legitimate messages are in immediate response to an action the consumer is carrying out – ie consumer accesses banking app and receives a OTP using the banks name. As the consumer is expecting the message – the ability to use a brand name is very helpful and promotes confidence. Consumer education needs to focus on 'unexpected' messages from brands.</p> <p><b>Option 3 full senderID</b>  Fraudsters rely on indiscriminate targeting of consumers. They virtually never have lists of consumer mobile numbers associated with a specific brand. Therefore fraudsters target the 'most plausible' or 'most smished brands', such as courier/postal services, major banks, tax authorities, utility companies etc. These scam messages resonate with consumers who often go on to click fraudulent links within messages.</p> <p>Therefore only a very small proportion of A2P messaging will ever be associated with scam</p>

	<p>texts. ie no fraudster is ever likely to target smaller brands/local companies sending out appointment reminders or marketing messages to subscribers</p> <p>Hence it is unnecessary to require industry/every brand to be required to use a full SenderID registry. if the top 150-350 'most smished' brands were protected by a registry the fraudsters would be almost completely disrupted.</p> <p>Option 4 partial senderID register</p> <p>Some brands never send any messages out to consumers – but still need to be protected by a registry. ie Visa &amp; Mastercard are not 'card issuers' in their own right and may not send out messages – however this doesn't stop fraudsters impersonating the bands as they are clearly extremely plausible (everyone has a card with visa or Mastercard on it). MEF therefore encourage merchants/brands to take control of their digital identity and protect senderIDs in their name – even if they don't send any message.</p>
<p><b>Single-click (7726) SCAM reporting</b></p>	<p>The Irish market/COMREG should implement a single click fraud reporting solution such as the UK 7726 solution. Since the adoption of Android single click reporting was implemented around 2 years ago – significant data on SCAM messages has been reported and acted upon. This includes the identification of additional URL's to be taken down.</p> <p>MEF would be happy to facilitate this solution for the Irish market.</p>

Please complete this form in full and return to: [marketframeworkconsult@comreg.ie](mailto:marketframeworkconsult@comreg.ie)



# 17 Microsoft



## MICROSOFT IRELAND OPERATIONS LIMITED

### Comments on ComReg's Consultation on network based interventions to reduce the harm from Nuisance Communications

31 August 2023

Microsoft Ireland Operations Limited ("Microsoft") appreciates the opportunity to provide its views on the proposals of the Commission for Communications Regulation ("ComReg") to combat fraudulent and nuisance calls and texts to persons in Ireland.

As ComReg has outlined in its Consultation, the problem of nuisance and fraudulent calls is significant. In particular, there is a rising concern regarding criminal schemes that involve fraudulent "spoofing" of the number displayed to the receiving party in order to deceive the recipient into believing that the call is from a known or familiar call source. Microsoft appreciates the time and effort ComReg has invested in studying the issues and proposing solutions to reduce these harmful calls, and Microsoft fully agrees that actions must be taken to address them. In these comments, Microsoft provides an additional perspective on the types of calls – legitimate calls routed to customers in Ireland – that would be blocked by some of the proposals in the Consultation. Microsoft, moreover, offers herein alternative approaches that can protect Irish consumers and businesses from nuisance and fraudulent calls while also ensuring that legitimate calls reach their intended recipients.

#### **Distinguishing Legitimate Calls from Fraudulent Calls**

At the outset, it is important to highlight that not all number "spoofing" or Calling Line Identification (CLI) number manipulation is fraudulent or performed with malicious intent. Therefore, solutions should be designed to prevent illegitimate calls while allowing legitimate ones. There are several reasons why an alternative number that is not directly tied to the calling line may be displayed as caller ID to the receiving party, as well as numerous situations in which legitimate calls are routed over international trunks displaying domestic CLI. Below are several examples:

- Cloud-based conferencing services, such as Microsoft Teams Meetings, are global in nature and may, for legitimate reasons, display an Irish CLI on calls routed into Ireland over international trunks. This can happen because Teams enables meeting participants to dial a phone number – in this example, an Irish phone number – from the bridge to add a user, on her mobile or landline, to the conference call. The outbound call, which originates from the Teams conference bridge which may not be in Ireland, will display an Irish phone number. Importantly, this is an Irish phone number that has been issued to Microsoft and has been assigned to the Teams conference bridge. Due to the characteristics of our cloud architecture, Irish network operators are likely to perceive such calls as international traffic, even though the call, in fact, originated and terminated in Ireland. As a result, it's likely that such a call would be blocked. Unfortunately, in countries where CLI blocking on inbound international calls has been implemented, we have encountered this scenario and it has caused significant disruption to government agencies and large enterprises because they suffer degradation to their cloud conferencing services.

- In the enterprise context, a user may dial out from their individual direct line, but the enterprise's general number will be displayed as caller ID so that the employee's direct line is not shared with the receiving party.
- There are growing numbers of scenarios in which phone numbers are temporarily assigned to an outbound call for privacy, security or other reasons, such as in ride-share app scenarios.
- As ComReg acknowledges in the Consultation, global call centers often legitimately modify the CLI that appears on outbound calls to ensure their customers answer inbound calls from a familiar number (i.e., the company's local number).
- In the consumer context, Skype to Phone is a one-way outbound VoIP-to-PSTN calling service that does not have inbound calling capabilities and therefore does not assign dialable phone numbers to the user that could be used as CLI by default. However, Skype allows users to assign their authenticated Irish mobile number as displayed CLI on outbound calls. This enables Skype users to display CLI using their mobile number that their friends and family can recognize, thus vastly increasing the chances that the call will be answered. Skype to Phone partners with several global telephone network operators to convert these IP calls to the PSTN for delivery to the recipient's terminating carrier. Many of Skype's partners use international trunks to deliver Skype to Phone calls to terminating carriers in Ireland. In these cases, a call made from an Irish Skype to Phone user to another person in Ireland may nevertheless be delivered to the Irish telephone network over international trunks and would be blocked as international traffic carrying local CLI.

All of the examples above ensure that: (1) the displayed number is a legitimate, assigned number that the calling party has the authority to use; and (2) the displayed number uniquely identifies the caller and originating carrier in a manner that enables the source of the call to be traced. These examples further demonstrate that the increasingly cloud-based telecommunications marketplace, with infrastructure in a single country supporting calling services across the globe that necessitates the legitimate manipulation of CLI, requires precise solutions to combat fraudulent and nuisance calls/texts. Otherwise, these legitimate business models will be unintentionally and adversely impacted, in derogation of EU single market goals. Below, Microsoft offers solutions that properly balance the need to protect consumers while simultaneously enabling emerging and legitimate pan-European business models.

### **Protecting Consumers While Enabling Diverse Business Models and Innovative Communications**

Restrictions designed to target number spoofing should undertake significant efforts to avoid degrading legitimate traffic, and should focus with precision on fraudulent spoofing, i.e., displaying a number that is either illegitimate or that the calling party does not have the right to use. In addition to deceiving call recipients about the source of the call, fraudulent spoofing also prevents the ability to trace the source of the call, making it difficult or impossible for law enforcement agencies to track down criminal enterprises engaged in this conduct. This is not the case, of course, with legitimate forms of CLI modification. As such, Microsoft recommends that any new regulations should be designed to protect against these distinct features of fraudulent spoofing, without inadvertently blocking legitimate use cases.

In its Consultation, ComReg makes several proposals to combat nuisance calls. While some of these proposals protect consumers without harming legitimate businesses, there are other proposals – specifically, the proposal to block calls with Irish mobile or fixed line numbers routing into Ireland over international trunks – that should be reconsidered by ComReg. Moreover, Microsoft urges ComReg to reconsider the STIR/SHAKEN solution and proposes herein a phased-in approach.

Microsoft supports ComReg’s proposals to block calls from numbers that are either “Do Not Originate” (DNO) or have not been allocated by ComReg to any provider (“Prohibited Number” or “PN”) and the formalization of the related DNO and PN lists. In both scenarios, there is no legitimate basis for making outbound calls using these numbers. Therefore, blocking all such calls will protect consumers from harmful, fraudulent calls while not putting legitimate business models at risk.

Similarly, ComReg’s proposal that carriers implement a voice firewall, using Machine Learning and Artificial Intelligence (AI) techniques to identify fraudulent calls, is a potentially useful tool that – if implemented successfully – could be used to combat fraud while preserving and protecting legitimate business operations. Microsoft itself is currently developing products that will deploy AI as a powerful tool to combat illegitimate scam calls. The risk with firewalls, however, is rushing them to market, before they are fully tested and proven. This will result in overreach and blocking of legitimate calls. Based on Microsoft’s experience studying these types of tools, we believe 18 months is not enough time to develop, test, and deploy appropriate firewalls. More time will be necessary to ensure only the blocking of illegitimate calls. In addition, procedures need to be established to enable operators to discuss any actual blocking prior to its implementation, and to immediately undo blocking where applied erroneously. Microsoft would be happy to work with ComReg to further study and test the use of AI tools in the context of fraudulent spoofing.

Regarding the proliferation of fraudulent SMS, Microsoft believes it is important to acknowledge the differences between voice and text communications when combatting nuisance communications. A ringing incoming voice call requires the recipient to make an immediate determination to answer the call before they know the “contents” of the call – what the caller is likely to say. By contrast, a text message can more easily be temporarily ignored by the recipient, particularly until they see the contents of the message. Moreover, by merely tapping their mobile phone screen a couple of times, users can block future texts from the offending number. Both iOS and Android mobile phone operating systems enable users to identify an inbound text as “junk” and ask their carriers to block future messages on a number-specific basis.

For these reasons, Microsoft does not support the use of SMS registries that block SMS messages or blunt instruments such as blocks on entire categories of SMS messages such as all messages sent using a Sender ID. A better solution is one to which ComReg points in its Consultation: the Singapore SMS Sender ID Registry (SSIR) established and overseen by the Infocomm Media Development Authority (IMDA). Rather than blocking text messages not properly registered in the SSIR, Singapore labels such messages with “LIKELY-SCAM,” thus allowing the end-user to determine whether to open, read, and/or respond to the message. This approach gives end-users the ability to control what messages they receive, while protecting them from fraudulent and nefarious actors. ComReg should modify its proposal to label non-registered Sender ID messages rather than blocking them. Moreover, the SSIR in Singapore is operated by the IMDA, rather than an industry body. Microsoft supports the Consultation’s proposal that ComReg manage the registry because that will better ensure technological and business model neutrality. Creating a registry that is managed by participants in the telecom industry risks favoring some business models over others, resulting in blocking or degradation of legitimate texts.

Regarding the use of a Scam Filter to block certain SMS messages by relying on the scanning of SMS message contents and application of AI tools, Microsoft believes that it has the potential to be helpful insofar as it is premised upon a sufficiently robust analytics model that does not block legitimate text messages. Indeed, the spam folder in most electronic mail services offers a potential model for handling texts of dubious legitimacy. Most people have found a legitimate mail in their spam folder – notwithstanding the best intentions of the email service – and it can be useful to have the capability to retrieve it and reclassify it as legitimate. If instead of diverting texts, a filter blocks them entirely and they are not visible to the intended recipient, the potential for harm to the user increases. Whether to make a filter requirement mandatory, opt-in, or opt-out would likely depend on its potential to inconvenience or harm the intended recipient of the message. SMS messages are interpersonal communications, as are e-mail services. It is expected that e-mail service providers will take measures to protect account holders from fraud and unwanted mail, and will categorize some messages as spam or junk accordingly.<sup>1</sup> This requires some form of analysis, including algorithmic analysis of metadata relating to the e-mail message. Insofar as the text message data reviewed is not disclosed or used for other purposes, the justification applicable to e-mail spam filtering should apply here.<sup>2</sup>

### **Blocking Calls Inbound on International Trunks Will Inadvertently Block Legitimate Calls**

ComReg’s proposal to block all such calls will harm users in Ireland. As described above, there are numerous legitimate business models that result in the routing of calls, with Irish CLI, over international trunks. To prevent malicious spoofing while also accounting for these legitimate use-cases, Microsoft recommends an alternative approach that leverages the advanced capabilities of Session Initiated Protocol (SIP) fields that are communicated between operators in the delivery of VoIP calls. There are two SIP fields for CLI that don’t necessarily need to provide the same number. First, the P-Asserted Identity (PAID) field conveys the “Network Number,” a unique network identifier associated with the call that is communicated from operator to operator, but not displayed to the called party. The second SIP field is the FROM field, often thought of as traditional Caller ID, which communicates the “Presentation Number” that should be displayed to the called party. For example, as described above, when a user makes a call from Teams, the number associated with their individual direct line might be the Network Number in the PAID field, but their enterprise’s general number might be used as the Presentation Number in the FROM field.

The UK’s Ofcom implements blocking of international inbound calls with a local Network Number in the PAID field but permits local CLI to be used as the Presentation Number in the FROM field.<sup>3</sup> Although Ofcom issued this approach as a guideline rather than a requirement, we understand that it was requested by incumbent network operators in the UK to afford regulatory authority to block certain forms of inbound international traffic. Thus, in practice, it has become the *de facto* approach in the UK.

---

<sup>1</sup> See Directive 2009/136/EC of the European Parliament and of the Council, 25 Nov. 2009, Recital 68 (Stating that ECS providers “make substantial investments in order to combat unsolicited commercial communications (spam),” and “possess the knowledge and resources necessary to detect and identify spammers,” and also acknowledging that spam detection and prevention is a legitimate business interest of e-mail service providers.)

<sup>2</sup> See *id.* at Recital 67 (“Safeguards provided for subscribers against intrusion into their privacy by unsolicited communications for direct marketing purposes by means of electronic mail should also be applicable to SMS, MMS and other kinds of similar applications.”)

<sup>3</sup> Ofcom, [Guidance on the provision of Calling Line Identification facilities and other related services](#) (Nov. 15, 2022).

It just as easily could be implemented as a mandatory requirement in other countries. The advantage of this approach is that Microsoft's Teams Meeting traffic can continue to display UK CLI to the called party and avoid blocking insofar as Microsoft modifies the PAID field to include a non-UK telephone number *issued to Microsoft*. An inferior approach, but one that is still better than the blocking proposal being considered here, would be the approach taken by Germany which requires carriers that receive inbound international calls with domestic CLI to change the display number to ANONYMOUS before delivering the call.<sup>4</sup> This approach at least permits the option for the called party to answer the call, albeit with caution.

### **Deploy STIR/SHAKEN Protections Sooner Rather than Later**

Efforts to combat illegal spoofing through CLI rules, such as those proposed by ComReg, will either be only partially effective or will harm legitimate calls or both. In the longer term, Microsoft recommends that ComReg combat fraudulent spoofing by adopting industry standards-based, technological measures to authenticate CLI. In the US, Canada, and France, regulators have implemented the STIR/SHAKEN<sup>5</sup> framework for authenticating the accuracy and integrity of CLI data communicated between operators. Microsoft appreciates the challenge STIR/SHAKEN poses for Ireland's current telecom infrastructure, given that many providers continue to operate TDM networks. However, this is not a reason to postpone STIR/SHAKEN implementation indefinitely. As described below, work is ongoing to develop a cross-border STIR/SHAKEN authentication framework that would enable providers to authenticate calls even in countries where there is no national STIR/SHAKEN deployment. ComReg should encourage Irish service providers operating networks that are capable of reading STIR/SHAKEN tokens to participate in these cross-border CLI authentication programs so fraudulent calls into Ireland can be more effectively stopped.

To accelerate the availability of STIR/SHAKEN in the absence of national deployments in Ireland and elsewhere, Microsoft has joined other global service providers to create a new STIR/SHAKEN governance authority that, with the support of the telecoms standards body ATIS, has developed a CLI authentication framework designed to operate across international borders. As it is not tied to a particular country, this new framework will allow STIR/SHAKEN to be available to voice service providers in countries where token-based CLI authentication has not been implemented on a national basis. It will also allow voice service providers that have IP networks to exchange authenticated traffic with other voice service providers that have implemented STIR/SHAKEN in their networks.

Specifically, a Cross Border Call Authentication Governance Authority (CBCA-GA) has been created by an initial group of international voice service providers to develop the policies and architecture for the STIR/SHAKEN deployment. National governing authorities, like ComReg, will be able to evaluate the CBCA-GA's policies, and it is our hope that they will be able to treat the CBCA-GA as a trusted partner and make national systems interoperable to facilitate information sharing for cross-border CLI authentication in the future. The CBCA-GA has put in place processes to ensure that voice service providers meet strict requirements for membership in the CBCA. The CBCA-GA has selected iconectiv as its policy administrator,

---

<sup>4</sup> German Telecommunications Act (TKG) § 120 (4), and further details provided [here](#).

<sup>5</sup> STIR, or "Secure Telephone Identity Revisited," is a set of standards established by the Internet Exchange Task Force (IETF) describing the mechanics of CLI authentication signaling. SHAKEN, or "Signature based Handling of Asserted information using toKENS," is a framework that defines the use of STIR and other elements to make up a complete ecosystem, as defined by the Alliance for Telecommunications Industry Solutions (ATIS) in a number of standards.

which will be responsible for approving service providers and certification authorities, issuing tokens, verifying originating providers for terminating and gateway providers, and enforcing CBCA-GA policies.

Each service provider must provide the policy administrator with information necessary to authenticate the provider and determine they are legitimate and trustworthy. This includes evidence of the provider's legal status, contact details, authorization to provide communications services, and other information concerning their compliance and service history. Service providers are required to have processes in place to identify problem users and support traceback requests. The policy administrator will also make an evaluation of whether the service provider is technically capable of deploying SHAKEN. Once accepted, registered as a member, and issued a token, an originating service provider can obtain a certificate for signing calls from a certification authority approved by the CBCA policy administrator. Originating service providers will be suspended or removed from membership if they provide attestations for customers that do not have the right to use a particular telephone number or engage in other activities inconsistent with the CBCA-GA's policies.

In the future, we hope that there will be interoperability between national SHAKEN frameworks (such as the STI-GA in the U.S. and the STI-CA in Canada) and the CBCA-GA so that attestations from the CBCA-GA will be recognized by the governance authority in the terminating country, and vice versa. This would require interconnection between the two policy administrators to share read-only access to their lists of registered service providers and approved certification authorities. Such exchange of information will be based on ATIS's standard for cross-border use of SHAKEN (ATIS-1000087).

Cross border STIR/SHAKEN is expected to launch on a limited basis in September 2023. A small number of voice service providers, including Microsoft, will provide attestations when sending traffic to each other that originates in countries without a SHAKEN framework already established.

ComReg should encourage Irish voice service providers with IP networks to implement STIR/SHAKEN on a voluntary basis so they can leverage this newly developed cross-border authentication framework. This would allow terminating providers in Ireland who are completing their transition to IP to use call attestation information to help shield their subscribers from illegally spoofed calls. Similarly, when originating calls these providers could use STIR/SHAKEN to mitigate the increasing risk that their customers' calls will be blocked by terminating providers. Even if a solution is only temporary until a national framework is developed, these providers can leverage the use of CLI authentication among a selected group of domestic and foreign carriers to ensure the delivery of legitimate calls to both national and international destinations.

Initial interest in the project has been positive and additional voice service providers are expected to become members in the coming months. Microsoft would be pleased to work with ComReg to discuss accessing the benefits of the non-jurisdictional governance authority so Ireland's consumers are protected from scam calls while ensuring they receive legitimate calls that may originate outside of Ireland.

## **Conclusion**

Microsoft applauds ComReg's work to protect residents and businesses in Ireland from harmful and fraudulent calls and text messages. This is a critical issue that must be addressed using a number of tools that are currently – and prospectively – available to regulators and industry participants. As discussed herein, however, some of these currently available tools can inadvertently harm Irish users by disrupting legitimate business models. Microsoft encourages ComReg to implement solutions that protect

consumers and businesses from harmful illegitimate calls and texts while also protecting legitimate businesses and their innovative communications solutions. Using STIR/SHAKEN to authenticate calls on a call-by-call basis is the most effective solution to combatting fraudulent activities, and Microsoft encourages ComReg to begin the transition to STIR/SHAKEN now, as carriers become capable of authenticating calls, by opting into the non-jurisdictional STIR/SHAKEN governance authority.



# 18 Netnumber



# **Response of netnumber to ComReg's Consultation on Combating Scam Calls and Texts**

NetNumber, Inc. (“netnumber”), a global provider of data solutions that guides messaging and voice traffic, hereby provides comments in response to the Consultation issued by ComReg called “Combatting scam calls and texts”.

## Background

netnumber was founded over 15 years ago with a mission to equip every telecom operator and enterprise in the world with critical phone number routing and intelligence data to streamline their operations, reduce costs and combat fraud. netnumber offers a broad set of solutions that solve complex ecosystem challenges and reduce both costs and operational complexity for its customers. netnumber’s solutions are designed to support a service provider’s day to day operations – providing the data that drives their routing, rating, billing, authentication, and fraud prevention initiatives.

netnumber does this by collecting and organizing detailed network and services attributes for telephone numbers globally, including enhanced, high resolution network identification capabilities that are unique to netnumber. The solutions include information about all types of services offered today, including Voice over Internet Protocol (VoIP), Mobile Virtual Network Operator (MVNO), Application-to-Person (A2P) and Rich Communication Services (RCS) information. netnumber combines this data with global number plan information, global title data, global number portability and carrier identification data to enable operators to identify, rate and route telephone calls and text messages. netnumber offers information about any of the telephone numbers in the world (approximately 10 billion), based on several hundred data sets that span countries and networks globally, many of which are updated in real time, eliminating the complexity that operators would face if they sourced these disparate datasets (with different formats) on their own.

We are a global company with customers all over the world. These include mobile and fixed line operators, messaging and voice service providers, fraud prevention vendors, enterprises and many others.

Fifteen years ago, the predominant use cases for netnumber’s solutions involved the routing of voice traffic to fixed-line numbers, mobile numbers, and IP-based numbers. However, netnumber’s solutions have been designed to enable new use cases to emerge, provided they are consistent with industry best practices. Increasingly, a variety of attributes and service types associated with telephone numbers are emerging which are not native to the underlying voice network provider. For example, a service provider may route voice traffic over one network but messaging traffic over another provider’s network. As these attributes are established, netnumber provides a central platform where the telephone number and such attributes can be published globally, for use cases that comply with policies established by stakeholders (including tier 1 carriers, CLECs, and messaging hubs) in the voice and messaging markets.

With the introduction of STIR/SHAKEN in the United States and Canada, netnumber expanded its product portfolio to help service providers achieve compliance with the FCC and CRTC regulations while reducing time to market and minimizing cost. netnumber’s **Guaranteed Caller** product family covers the full spectrum of STIR/SHAKEN requirements, from certificate issuance and signing / verification of calls to specialty capabilities that support international service providers and enterprises participate in STIR/SHAKEN. netnumber is one of the few entities approved as an STI-CA in the United States.

Fraud prevention is a core element of netnumber’s solutions. netnumber customers across the globe reduce risk, achieve compliance, save cost and run better processes by using one or several of the following services:

- **NumeriCheck** brings in real-time phone number intelligence to help prevent a multitude of fraud types. NumeriCheck evaluates the likelihood of a phone number anywhere in the world being valid or invalid, enabling brands, enterprises and communications service providers to enhance their phone number verification processes.
- **NumeriView** helps identify account takeover fraud by determining when a phone number has been moved between service providers.
- **NumeriRisk** evaluates the risk of calls being scam in real time, protecting subscribers and service providers alike.

## Do Not Originate

netnumber agrees with ComReg's assessment that DNO data is a powerful tool in stopping fraudulent calls and in avoiding the consumer scams perpetrated using phone numbers that are on the DNO list. We consider ComReg's intervention of defining Protected Numbers as positive, because DNO protection goes beyond a list that relies on being populated voluntarily by the industry participants. In addition to ComReg's proposal, netnumber considers that the same concept can and should be applied to texting services (SMS/MMS). We would also like to suggest that ComReg considers alternative mechanisms for collecting and distributing the DNO data to the industry. The proposed approach, based on email transmission and the consolidation of data in a file that gets distributed monthly, appears effort intensive and slow. A real-time API-based solution appears better suited to effectively consolidating the DNO numbers and distributing them immediately to the industry, therefore achieving the goal of stopping fraud and scam calls quickly.

## Protected Numbers

netnumber agrees that numbers that are not assigned by ComReg should not be used to originate voice calls or messages and appreciates ComReg's proposal to aggregate and distribute these numbers to the industry. We would like to note that unused numbers, if added to this intervention, will increase its success. Obtaining the unused numbers likely requires the collaboration of mobile and fixed-line carriers.

## Fixed CLI Call Blocking

In netnumber's opinion, this intervention appears to be effective at addressing the type of fraud identified in the ComReg consultation.

## Mobile CLI Call Blocking

In netnumber's opinion, this intervention appears to be effective at addressing the type of fraud identified in the ComReg consultation.

## Voice Firewall

In netnumber's opinion, this intervention appears to be effective at addressing the type of fraud identified in the ComReg consultation. We would like to point out however that voice firewalls are only as effective as the data used to implement the filtering rules. Phone number intelligence, as provided by netnumber's many services for different use cases, is essential for proper configuration of firewalls and therefore to their operational success.

## Sender ID Ban

netnumber considers that instead of blocking alphanumeric sender IDs, ComReg should consider mandating their protection using the Sender ID Registry intervention. While it's true that alphanumeric sender IDs are a prime target for fraudsters who attempt to spoof them in order to impersonate the message sender, they are also valuable to consumers to recognize the brand sending them the respective text messages. Given the limited options for branding of SMS, alphanumeric sender IDs are an important tool for brand recognition and, if properly secured, for trust.

## Sender ID Registry

netnumber agrees that the Sender ID Registry, as proposed by ComReg, is a powerful and effective tool at protecting sender IDs used for texting. We further believe such a Sender ID Registry should be applied to all permissible sender ID types in Ireland, i.e. alphanumeric, short code and long code. We also agree with ComReg's proposal that after a transition time the Sender ID Registry should become mandatory and text messages that do not meet the Sender ID Registry criteria should be blocked. Sender ID spoofing is a big issue that facilitates significant consumer harm, often times beyond just nuisance. For example, a fraudster impersonating a bank may be able to successfully run smishing campaigns and also retrieve SMS one-time passwords via social engineering, leading to high financial losses to the victims.

We applaud ComReg's proposal of a short message delivery chain, where the Sender ID Owner needs to work directly with a Participating Aggregator, who in turn connects to the MNOs directly. This approach ensures robust sender ID registration, usage, tracking and troubleshooting.

## SMS Scam Filter

Similar to the Voice Firewall, the SMS Scam Filter will very likely be effective at addressing the type of messaging fraud contemplated in the ComReg consultation. As we noted above, empowering the SMS Scam Filter with the right data is key to its success. As an example of how netnumber helps the industry address messaging fraud, our NumeriCheck service enables customers to perform phone number verification. Numbers that have a high likelihood of being invalid or inappropriate for the given use case (e.g. fixed-line numbers used for SMS or phone numbers involved in telecom fraud) can be blocked.

## Conclusion

We believe that ComReg has put together a set of interventions that is comprehensive yet realistic. The ComReg analysis of feasibility and impact is well informed and considers implementations in other geographies and the resulting best practices. If implemented, such interventions are very likely to mitigate the types of fraud described by ComReg. netnumber has significant experience operating such services in other geographies. We would welcome the opportunity to further discuss with ComReg how our technology and expertise could be of help in supporting ComReg's goals.

# 19 Openmind

## Executive Comments

Openmind Networks response to the documentation received on SMS Sender ID Registry and SMS Scam Filter. We believe that the Sender ID Registry may result in a small group of preferred aggregators being given too much prominence in the system as a whole. We believe that verifying Sender ID at the MNO level would be preferable.

The SMS Scam Filter as outlined in documentation may result in fraudsters using it to essentially test and probe the system for weaknesses. It is important that this Filter operates in the background and treats each message as if it was fully terminated so fraudsters are not given any information on whether their messages are getting through or not. The issue of how exactly to apply screening on urls contained in messages is the one that needs to be addressed.

Zero trust is a principle that could and perhaps should be applied to this legislation. The safest approach to take here is all urls contained in SMS messages should be considered guilty until proven otherwise.

Considering how to treat url links embedded in SMS messages. Url messages can be allowed through and checked as they go but this will result in a certain percentage of end users being caught out by fraudulent links before they can be checked. Alternatively all urls links could be effectively quarantined and remain unclickable until the fraud detection tools have done their job and checked the links to threat assess. ComReg could apply a standard url shortener to all messages in Ireland which would then be understood to have a layer of protection built-in.

## SMS Sender ID Registry

1. The SMS Sender ID registry faces the problem of a small group of preferred aggregators having an unnatural prominence as they **must** be used for sending messages in Ireland.

2. Each individual enterprise that wants to send A2P messages will be tied to a specific aggregator and must apply to ComReg to switch.
3. The lack of simplicity in switching from one aggregator to another may lead to higher prices and could be considered anti-competitive.
4. An alternative approach is to remove aggregators from the Sender ID registry loop and verify Sender ID at the MNO (Mobile Network Operator) level.

## **SMS Scam Filter**

1. The SMS scam filter actions described create a feedback loop for fraudsters testing message delivery.
2. All suspicious messages in principle should be blocked before reaching the end user. The removal of suspicious URLs and delivery of the stripped down message to the targeted device will also provide a feedback loop for fraudsters. Any warnings provided to end-receiving subscriber might provide an indication to fraudsters. It is important that the sender is charged for the message even if it is quarantined so the fraudster has as little information as possible, preventing fraudsters from testing message sending while also reducing their profits from such activities. Test phones are a key part of the fraudsters arsenal of tactics.
3. If a receiving operator blocks a message, they should have the ability to charge the sender to offset the negative impact on their revenue resulting from their efforts to protect subscribers.
4. Longer format messages that need to be split into multiple parts can create an opportunity for fraudsters to insert URLs across message breaks thereby evading detection. Message reassembly needs to be clarified.

## **Further information**

If you would like to discuss our feedback in more detail or require clarification on any points please reach out to us through  
[brendan.tobin@openmindnetworks.com](mailto:brendan.tobin@openmindnetworks.com)



## 20 Risk & Assurance Group (RAG)



# RISK & ASSURANCE GROUP

Risk & Assurance Group  
10 The Serpentine  
Aylesbury  
HP19 8HJ  
United Kingdom

26<sup>th</sup> June 2023

Mr. Donnacha Hennessy  
Commission for Communications Regulation  
One Dockland Central  
Guild Street  
Dublin  
D01 E4X0  
Ireland

Dear Mr. Hennessy,

Re: **Comreg Consultation 23/52 on Combatting Scam Calls and SMS Messages**

You and your colleagues deserve thanks for the thorough research that has gone into developing an action plan to protect Irish phone users from scam voice calls and SMS messages. Your conclusions about the best practices being followed in other countries are consistent with my own. As a consequence, you have distilled this research into the most sensible, cost-effective and actionable plan for tackling scam calls and messages that I have seen any national regulator produce.

You have also done others a service by providing a balanced rationale for each mitigation you propose, and those you do not recommend. Expressing the reasoning in plain language, within a single document, means you have provided a template that others can copy from.

Implementing the six mitigations that you would like to pursue without delay, and the seventh recommendation that first requires a change of law, should be treated as a priority in every country. When these mitigations have all been implemented in Ireland it will then be appropriate to allow some time to assess their impact before considering what further action may be needed. You have seemingly avoided the trap of pondering and debating an endless series of hypothetical steps that might be required in future, by identifying the seven consumer protection controls that are most likely to deliver measurable results in the shortest possible timeframe. That is why I hope you will encourage the regulators of other countries to follow your lead. I certainly will be.

Yours sincerely,

A handwritten signature in dark ink, appearing to read 'Eric Priekalns', written in a cursive style.

Eric Priekalns, RAG Chief Executive

# 21 Revolut

# Revolut

**27/07/2023**

## **Revolut response to ComReg consultation 23/52**

### **Introduction**

Revolut Bank UAB is a licensed credit institution with more than 20m customers across Europe, and more than 2.2m in Ireland. Since March 2023, payments services for Irish Revolut customers have been offered by the Irish branch of Revolut Bank, which is supervised for the conduct of business by the Central Bank of Ireland.

### **Key ComReg Proposals:**

#### **Fake calls**

a) A Do Not Originate (“DNO”) list. This 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).

e) ComReg also proposes to introduce a Voice Firewall over a period of 18 months. 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

# Revolut

upon unusual patterns of call signalling data and traffic volumes.

## Fake texts

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<sup>2</sup> 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.

## Consultation response

Revolut would like to express its gratitude to ComReg for carrying out such extensive work in this critical area. The detailed research undertaken in support of proposed measures will be extremely valuable to all those involved in the fight against fraud. It is critical that cross-sectoral efforts to tackle fraud are carried out on a data-led basis: ComReg's insights into fraud levels, typologies and causes are therefore a very significant addition in this regard.

Revolut also welcomes the detailed, powerful and forward-looking proposals set out by ComReg to tackle fake texts and phone calls, which it correctly describes as a "scourge" causing immense harm - financial as well as emotional - to huge numbers of our citizens.

In particular, Revolut welcomes the clear assessment by ComReg that 365,000 annual cases of fraud it identified occur "*as result of scam calls and texts*". [Emphasis added]. This recognition that scam calls and texts are the direct cause of such frauds is a critical step towards a holistic national approach to tackling fraud.

In this regard, Revolut also notes evidence given to the Oireachtas Finance Committee by An Garda Síochána that most frauds do not occur as a result of "complicated hacks, spam or computer viruses" targeted at financial institutions themselves: rather they are targeted at customers directly. "The deception creates the willing participation of the victim, *which bypasses any security measures put in place by the financial institution*" stated Mr Justin Kelly, Assistant Commissioner of An Garda Síochána. [Emphasis added].

Revolut also notes comments by Chief Superintendent Pat Lordan of the Garda National Economic Crime Bureau in the Sunday Independent, 18/06/23: "If we can shut down the text messaging and the voice messaging... it really is the lifeblood, the embryo, that sows the seeds for all these types of crime."

# Revolut

It is a matter of public record that Revolut has made the case to governments and regulators that payments firms are the last link in the fraud chain: effectively, by the time a payment is made, the fraud has already occurred. To protect citizens and businesses from criminals, digital fraud needs to be tackled at source. Revolut therefore supports the proposals put forward by ComReg (highlighted above) specifically on measures to address both fake calls and fake texts.

With particular regard to the SMS registry, the Revolut team has suggested extending this proposal, stating: “It would be useful to see a feedback loop of cases where the attempt has been made (i.e. if the registry blocks an attempt to send a scam SMS via the Revolut thread, then they notify Revolut of the number the criminals were attempting to send the SMS to, so that we can take more protective action on that account).”

Revolut also suggest that Irish customers be offered one simple and easy way to report scam texts or calls. A version of the 7726 system available in the UK <https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls> could prove beneficial both to consumers and also to all those engaged in the fight against digital fraud. (Though perhaps a more memorable number might be of value).

Overall, it is vital that the important measures set out by ComReg are introduced quickly and in full. The longer the timeframe required for implementation, the more people will be the victim of such fraud attacks; and the longer criminals will have to attempt to devise new ways around these measures. As Chief Superintendent Lordan also noted in his recent interview, while welcoming ComReg’s efforts in this area, “it needs to progress more rapidly”.

However Revolut notes that while the proposed suite of measures constitutes a powerful and forward-looking response to fraud prevention, the question of liability for frauds engendered through fake texts and calls is not addressed. If we accept that these frauds are occurring as a result of scam calls and texts, then the question of liability for losses caused by them should surely follow.

Ensuring that liability lies with the firms which enable fraud would ensure that such firms are incentivised to take swift action to combat new typologies as they emerge, rather than having to wait for specific proposals from regulators. While creating such a legal liability may fall outside of the remit of ComReg, recommending such a provision would have a significant bearing on the potential for any required legislative changes to be put forward by legislators.

Revolut is already working with industry peers, with government and with An Garda Síochána and other relevant stakeholders to tackle digital fraud. We would be happy to engage directly with telcos - as well as tech firms - either directly or via the offices of ComReg or other relevant

# Revolut

regulators to widen this coalition and ensure that customers are able to enjoy all the benefits of digital banking without having to be subjected to the scourge of attempted frauds.

## 22 Sky





**Sky's Response to ComReg's Consultation  
on network based interventions to  
reduce the harm from Nuisance  
Communications**

Reference: ComReg 23/52

31<sup>st</sup> August 2023

Sky Ireland welcomes the opportunity to provide feedback on the draft measures outlined to tackle nuisance communications and some of which stem from ongoing discussions within the Nuisance Communications Industry Taskforce (NCIT) which Sky Ireland has actively been engaging with.

As ComReg will be aware, Sky Ireland is not yet a mobile provider but will launch a mobile service in Ireland at some point in 2024, as such some of the measures outlined, due to the various market subscription thresholds, will not apply to Sky Ireland in the short to medium term.

Sky Ireland welcomes these market subscription thresholds and agrees with ComReg that such an *'approach is proportionate as it only includes sufficiently large operators'*<sup>1</sup>. It is important that the measures balance the challenges that new entrants to the mobile market face while taking into account their entry improves the overall levels of competition within the market.

With this in mind, Sky Ireland would like to highlight that the measure for blocking international origination of an Irish mobile CLI will apply to Sky, with the scope defined as exposing and offering the "roamer check" capability, once we launch as a mobile provider.

Sky Ireland highlights the complexity of certain aspects of this measure in terms of the delivery effort, the inter-operator network designs covering the "roamer check" signalling dialogue as part of the inbound international call setup procedure, and the need to negotiate and enter into up to 14 bilateral contracts with the International Gateway Operators (IGOs). This is a significant additional burden for an operator launching in the Irish mobile market, and it is important that ComReg takes into account the significant investment that is required to launch in the market already.

- ENDS -

---

<sup>1</sup> S.5.53, P110, ComReg consultation 23/52

## 23 Tanla



Commission for Communications Regulation  
One Dockland Central, Guild Street,  
Dublin, D01 E4X0  
Ireland

Monday, 28 August 2023

**Subject: Submission to ComReg Document 23/52 – Tanla Platforms Private Limited's Response to "Combatting Scam Calls and Texts" Consultation**

Tanla Platforms Private Limited, India's largest Communication Platform as a Service (CPaaS) provider, values this opportunity to contribute to the discussion initiated by the Commission for Communication Regulation vide Document 23/52 titled "Combatting scam calls and texts".

We commend ComReg for its proactive stance against nuisance communications and its commitment to restoring user confidence in voice and SMS communication. Tanla is proud to contribute to this consultation, drawing from our extensive experience in India.

Some of the interventions proposed by the Commission are very similar to the ones adopted by Telecom Regulatory Authority of India in 2018. We believe that the insights derived from the Indian experience would be useful in your deliberations.

## **Background**

In 2018, the Telecom Regulatory Authority of India (TRAI) established the Telecom Commercial Communication Customer Preference Regulations (TCCCPR)<sup>1</sup>. These regulations introduced or streamlined the following:

1. Registration of Senders.  
The senders are called Principal Entities in the regulation and refer to the business that initiate the communication, either directly or through an intermediary.
2. Registration of Headers.  
These are the alphanumeric strings with which the sender wishes to be identified to the recipient.
3. Registration of templates  
Commercial messages can be templated because they are sent to many subscribers (recipients), with some details tailored to each individual or transaction mentioned in the message.

The 2018 regulations involved telecom operators as co-regulators and implemented permissioned distributed ledger technology for managing the registries and ensuring compliance with regulatory requirements.

This approach anticipated following benefits, which were substantially obtained in its implementation:

1. The Regulator did not have the burden of hosting the registries or carrying out the registration function.
2. The operators had the agility to address client (sender) grievance related to strict operating procedures while also responding to the strategy of spammers and scammers.
3. Working together generated trust among the operators and between the operators and other stakeholders in the communication.

Tanla took the lead in developing and implementing this solution (our product called Trubloq) in collaboration with several large telecom operators in India. An impact assessment of how the solution improves subscriber experience and the efficacy of regulatory processes is captured in an academic paper published by the Paul G. Allen School of Computer Science and Engineering at the University of Washington.<sup>2</sup>

Very recently, Tanla introduced Wisely ATP (Anti-phishing Technology Platform), that utilizes AI/ML models to proactively identify, prevent, and eliminate SMS scams. This platform has undergone successful testing in a regulatory sandbox provisioned by TRAI, where it demonstrated excellent capability in identifying phishing message with a high degree of recall. As part of the sandbox, we have also concluded a successful proof-of-concept (PoC) with three large banks in India.

---

<sup>1</sup> Telecom Commercial Communication Preference Regulations Tcccpr, 2018 | Telecom Regulatory Authority of India.  
Available at: <https://traigov.in/tcccpr>

<sup>2</sup> Singanamalla, Sudheesh. "Telechain: Bridging Telecom Policy and Blockchain Practice." arXiv.Org, 24 May 2022, Available at: [arxiv.org/abs/2205.12350](https://arxiv.org/abs/2205.12350)

<sup>3</sup> Mobile Spam Policy | Telecommunications Regulatory Authority. Available at: [https://www.tobeprecisesms.com/downloads/TRA\\_Unsolicited\\_Electronic\\_Communications\\_Regulatory\\_Policy.pdf](https://www.tobeprecisesms.com/downloads/TRA_Unsolicited_Electronic_Communications_Regulatory_Policy.pdf)

Following the sandbox test, TRAI issued an official directive in June 2023<sup>4</sup>, mandating operators to deploy solutions that prevent scam across their networks using the AI/ML based detection technology.

---

<sup>4</sup> *Trai issues direction for deploying Artificial Intelligence and machine learning based UCC detect system under TCCCPR, 2018 (2023) Telecom Regulatory Authority of India.* Available at: <https://www.trai.gov.in/notifications/press-release/trai-issues-direction-deploying-artificial-intelligence-and-machine>.

## Tanla's Comments on Document 23/52

### Interventions 8 - 10 – The regulation of Sender ID

**Sender ID Registry:** Among the options proposed by ComReg, Tanla supports the idea of establishing a **full sender ID Registry** which shall include the 11-character alphanumeric sender ID, Sender ID Owner (SIDO), Participating Aggregator (PA).

Tanla further recommends introduction of a **private and permissioned DLT network** operated by telecom service providers to manage and enforce the rules. Such a registry has several useful characteristics like high-availability, high-security, and tamper resistance. Furthermore, it supports competition among operators based on price and quality of services, with negligible switching costs for the customers.

In addition to registering, sender IDs, SIDOs and PAs, we also suggest registration of **message content templates** for all commercial message, whether used for promotion or to deliver information related to transactions of the subscribers.

One lesson from India is that registrations should not be free of cost. And continuation of registration should also be periodically charged. These charges, even if small, would prevent unnecessary registration, such as the registration of millions of templates that happened in India.

**Enforcement mechanism.** We also urge that the Commission consider an enforcement mechanism with the telco for 100% precheck to ensure compliance with the rules. This mechanism by the name of scrubbing function is already operative in India and handles over a billion messages every day.

With robust registration of senders, headers and templates, the probability of fraudster being able to evade the sentries is low.

#### **Co-regulatory approach can unburden ComReg from maintaining the Registry.**

As per ComReg's proposal, the regulator shall be responsible for (i) setting up and running the registry (ii) verifying authenticity of SIDO applicants.

While Tanla agrees that the costs of developing and implementing this kind of registry are non-trivial, we believe that that its scope of operations is quite large, and the regulator may not be burdened with these responsibilities.

Therefore, Tanla suggests that ComReg provides for a co-regulatory approach where telecom operators are responsible for the following:

- Developing, implementing and operating the registry
- Performing KYC of SIDO/PA applicants and maintain records
- Assigning sender IDs and rule out proximity match
- Registering and approving message content templates relevant to SIDOs area of business
- Flagging non-compliance and deactivating defaulting sender IDs
- Detecting and penalizing the offenders
- Resolving customer complaints

The above objectives could be most effectively achieved through a decentralised system that we recommend.

The regulator must act as a watchdog and pass on the operational responsibilities to the telecom operators while giving them flexibility to devise their own code of practice for adhering to the regulations. This will allow the operators to respond to the changing needs of the sector without constantly seeking regulator's intervention.

If required, one node of the distributed ledger can be hosted by the regulator for monitoring the system.

### **A Rigorous KYC Process Acts as a Deterrent for Fraudsters**

ComReg acknowledges the significance of KYC verification in protecting a company's brand and thwarting attempts by fraudsters to impersonate it.

A comprehensive KYC procedure not only allows telecom operators to authenticate an entity but also ensures that its message content (via template registration, as suggested above) is appropriate for its business.

Tanla concurs with ComReg's approach for SIDOs and further advocates for the validation of a business's official documents, such as incorporation papers, tax filings, relevant licenses, and physical address. Such measures have been instrumental in enhancing the KYC verification process for medium and small businesses in India.

### **Efficient Resource Utilization through Sender ID Namespace Allocation**

Tanla supports ComReg's strategy to encode Sender IDs using the GSM 7-bit default character set and using the full length of 11 characters in the Standard to accommodate a broad range of entities with distinct headers.

Sender ID registration and filtering should be case-neutral, like internet domain names, so that same header cannot be registered by two entities and the same entity is not required to register all variants by mixing up the case. Introducing more characters prevents sender IDs from resembling well-known entities because of constraints of length. However, providers or the regulator would also need to provide rules for avoiding lookalike headers.

Reserved suffix or prefix in the available namespace can be used to enhance trust in the header by allowing their allocation only with the approval of the sector regulators. For instance, .BNK could be reserved for the banking sector and any header ending in this suffix would only be registered by the banking regulator.

Allocation rights should be based on a "first come, first served" principle, with open auction where the contention cannot be resolved by the laid down policy. For instance, "BestPrice", "DealAlert" "Buy1Get2" and numerous such headers could be auctioned to the highest bidder, with the proceeds being credited to an account for appropriate use of the funds by the regulator or the licensor.



## Enhanced Oversight through Template Registration

While the introduction of a sender ID registry, as seen in Singapore, has significantly bolstered trust in the IDs of reputable organizations, it doesn't fully address the issue of content authenticity.

Malicious entities can still masquerade as small businesses, secure an ID from the registry, and then misuse it to disseminate deceptive content.

To address this, Tanla recommends incorporating message content template registration in tandem with sender IDs. This would allow for closer scrutiny of the communications from registered SIDOs and enable the interception of any fraudulent content.

For example:

Sender ID	Content Template registered on DLT	Actual message
Bank of Ireland	Dear <#var>,  <#var> is the one-time password to verify your credentials for bank account number ending <#var>.	Dear Edward,  12469 is the one-time password to verify your credentials for bank account number ending 4122.

A template should be registered with two components: i) static content segments that remain the same for all messages, and ii) variable segments that change with each message. During the filtering process, the static content will be scrutinized.

It's imperative for operators to meticulously vet and approve templates that align with the SIDO's business domain. As illustrated, the template above should be allocated exclusively to a validated banking entity.

## Message Filtering through the Scrubbing Platform

In the suggested framework, the scrubbing—or more straightforwardly, filtering—platform enables enforcement of rules based on criteria imposed by the regulator or telcos.

Such a solution can provide high throughput and low latency while examining the sender ID, template, and SIDO of every message prior to transmission. A malicious actor trying to inject non-conforming messages would thus be prevented in the effort.

Tanla's scrubbing system, operational with three of India's four primary operators, processes nearly 1 billion SMS messages daily.

## Decentralized Ledgers Eliminate the Need for Sender ID Portability

Tanla concurs with ComReg's perspective that, in the interest of fostering competition, SIDOs should have the flexibility to transition between their PAs within a reasonable duration. However, our stance is that SIDOs should be able to engage with multiple PAs without resorting to portability requests.

Embracing the DLT framework streamlines this process, relieving the service provider of the tasks of documenting, authenticating, and orchestrating the transition. Owing to the system's decentralized

nature, any SIDO can avail the services of any registered PA, as the entire delivery pathway is delineated by capturing the audit trail on blockchain.

### **Ensuring Authenticity in Commercial Voice Calls through Scrubbing**

The DLT framework, currently employed for verifying SMS sender IDs, can be similarly applied to commercial voice calls. To enable businesses and aggregators to make legitimate voice calls for valid reasons, regulators could designate distinct series or registration for calling numbers, which can then be associated with the caller's name.

Entities aiming to make promotional, transactional, or service-related calls to mobile users would need to register. For example, in India, service providers are mandated to assign distinct calling line identities from the 140-level numbering series to each registered entity, marking them as commercial. The voice message content for such calls must be scripted, at least for the initial exchange with the recipient and include the purpose of the call.

Commercial voice calls captured by honeypots or donated by the recipient may be used to confirm compliance with the registered script.

To display the entity's name in a verified manner, technologies like Calling Name Display or enhanced CNAME (in line with 3GPP standards) can be utilized.

The existing infrastructure for DNO and PN list blocking, set up by operators in Ireland, can be seamlessly integrated with such a system. This ensures calls from these numbers undergo rigorous scrutiny and are filtered appropriately.

While the regulations in India prescribe such a system for voice calls, it is only partially implemented so far.

### **Technical Viability and Efficacy**

Using DLT to curb unsolicited commercial SMS communications represents a novel application of blockchain technology, arguably the largest one in the telecommunications realm. When TRAI introduced this pioneering approach in 2018, it was met with some scepticism from industry stakeholders.

However, Tanla is proud to have been associated with this challenging project which was successfully developed and deployed within 9 months. The following stages were involved:

1. **Design Stage:** The foundational phase involved consensus-building among telecom companies and the regulator regarding the Code of Practices (CoPs) to be implemented. This was followed by the finalization of an IT architecture that ensured interoperability.
2. **IT Readiness:** After endorsing the CoPs, the subsequent steps encompassed the establishment of ledgers, settling on commercial terms, determining hardware ownership, system sizing, designing workflows, outlining processes, and selecting vendors.
3. **Deployment:** This phase entailed the integration of pre-existing IT systems, data migration, onboarding of entities, and testing the scrubbing functionalities.

Tanla's successful rollout of DLT in India is a testament to the technical viability of these of distributed ledgers in building a comprehensive registry and enforcement mechanism.

The effectiveness of the solution is documented in the academic paper referred to earlier in this submission.

Tanla believes the solution can be up and running within 12 months in Ireland: 9 months for development and 3 months for onboarding businesses.

In Summary,

- Tanla supports the idea of establishing a **full sender ID Registry** which shall include the 11-character alphanumeric sender ID, Sender ID Owner (SIDO), Participating Aggregator (PA)
- Tanla further recommends introduction of a **private and permissioned DLT network**—a distributed database operated by telecom service providers.
- Tanla suggests that ComReg opts for some form of a **co-regulatory approach** where telecom operators are given freedom to establish practices and fulfil the responsibilities of developing, deploying, operating, monitoring the registry.
- Tanla agrees with ComReg’s application process for SIDOs and further recommends verification of official papers of a business such
- Tanla agrees with ComReg’s approach to encode Sender IDs according to the GSM 7-bit default set of characters and allow the maximum limit of 11 characters for covering maximum entities with unique headers. Sender IDs would need to be governed by a set of rules and may need an auction mechanism where rules cannot guide the allocation.
- In addition to registering sender IDs, SIDOs and PAs, we also recommend registration of **message content templates** for commercial (transactional/promotional) messages that business wish to send. This will enable greater controls over who is sending what.
- Tanla suggests that sender ID portability or switching PA is not required. Adopting the DLT framework, shall automate this process and unburden the service provider from recording, verifying and configuring the switch.
- The DLT infrastructure for authenticating SMS sender IDs can also be extended to commercial voice calling by assigning separate series or registration of calling numbers which can be presented with name of calling line.
- Tanla believes the solution can be up and running within 12 months in Ireland: 9 months for development and 3 months for onboarding businesses.

## **Intervention 11 – SMS Scam Filter**

As scammers globally refine their tactics, their methods of deception have seen constant innovation. From mimicking a bank's website to executing theft via a missed WhatsApp call, their strategies are both sophisticated and alarming. Addressing such advanced threats necessitates solutions that not only counteract scams in real-time but also target their underlying causes.

In light of this, Tanla wholeheartedly backs ComReg's initiative to implement an SMS scam filter powered by artificial intelligence and machine learning. This technology scrutinizes message content, offering a more nuanced approach than the traditional methods. ComReg's assertion that the conventional method of filtering messages based on metadata falls short is accurate, especially given its limitations in detecting fraudulent URLs and other emerging scam techniques. TRAI reached a similar conclusion and has directed that AI/ML based solutions should be adopted vide their communication dated June 13, 2023.

Tanla suggests that the SMS scam filtering functionality must be offered by default to all telecom users ("All-in" approach) because we believe subscribers would be willing to seek such protection. However, an opt-out can be offered to the subscribers who do not want the protection for any reason. In Australia, Telstra has starting offer such protection to all customers, with an "Opt-out" that they can exercise.

As mentioned in the introduction of this document, Tanla has recently revealed Wisely ATP (Anti-Phishing Technology Platform), a dedicated platform that utilizes AI/ML technology to proactively identify, prevent, and eliminate SMS scams. This platform has undergone successful testing in a regulatory sandbox provisioned by TRAI, where it met various performance metrics. We have also concluded a successful proof-of-concept (PoC) with three large banks in India.

The following modules conceptually explain the features of Wisely ATP:

### **1. CTA Engine:**

SMS scams often involve urging the recipient to perform a specific action, serving as the critical step in the fraudster's machinations. The platform recognizes these prompts as "call-to-action" or CTAs. These CTAs can encompass callback numbers, WhatsApp links, URLs, email IDs, short codes, or APKs. The engine's primary function is to categorize these CTAs, determining whether they are safe or unsafe.

### **2. Semantics Engine:**

Phishing messages often employ emotional triggers, aiming to induce anxiety or excitement in the recipient to manipulate their actions. By leveraging the capabilities of an NLP engine, it's possible to discern these emotionally charged attempts.

The semantics engine can identify the underlying sentiments and intentions within the message content, offering an independent signal about the sender's motives, thus flagging malicious intent.

### **3. Sender Reputation Engine:**

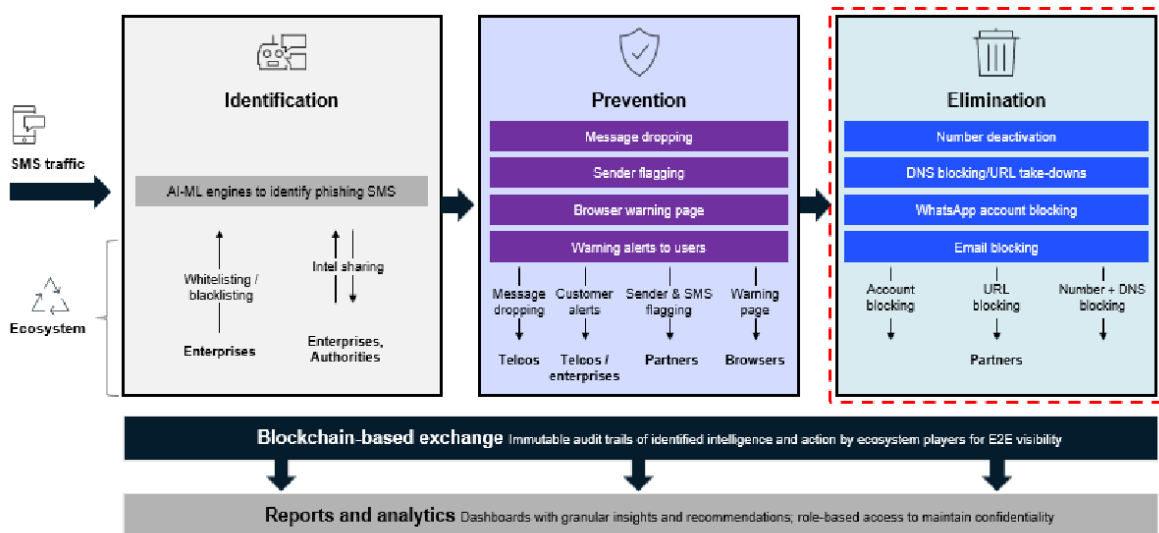
This engine evaluates the credibility of a sender, encompassing both Application-to-Person and Person-to-Person communication, by considering a range of factors. These include the nature of communication, average monthly message volumes, the frequency of complaints, and other relevant parameters. Based on this comprehensive assessment, a reputation score is assigned to the sender. If a sender's score falls below a specified threshold, the engine categorizes them as "bad senders."

#### 4. Evaluation Engine:

The Evaluation Engine synthesizes inputs from the three previously mentioned engines—CTA Engine, Semantics Engine, and Reputation Scoring Engine. By integrating these insights, it arrives at a classification for a message: either "good" or "bad." Should a message be deemed "bad," it is withheld from reaching the intended recipient. However, a record of this message is created, facilitating subsequent investigations by law enforcement agencies and other relevant stakeholders who might need to take appropriate actions based on the content and metadata of the message.

#### 5. Blockchain Exchange:

The Blockchain Exchange serves as a centralized hub, uniting all key players in the ecosystem, including telecom operators, regulators, takedown partners, OTT platforms, law enforcement agencies, banks, and more. Its primary function is to facilitate the real-time exchange of evidence related to phishing attempts. By fostering seamless communication and collaboration among these stakeholders, the platform aims to swiftly identify and neutralize both the scam and its orchestrator.



## Technical Viability and Effectiveness

Our India experience suggests there are no technical barriers to developing a comprehensive AI/ML based solution which can identify SMS phishing in real-time. We have witnessed an exceptionally high accuracy in identifying scam during our trials in India.

## Timelines

An SMS scam filter can be developed within 3 months followed by easy deployment within the telecom operator's network.

In summary,

- Tanla supports ComReg's intervention to introduce an SMS scam filter based on artificial intelligence/machine learning technologies which scans messages for content.
- Tanla suggests that the SMS scam filtering functionality must be offered by default to all telecom users ("All-in" approach) because we believe subscribers would be more than willing to seek such protection, with option to choose otherwise.
- An SMS scam filter can be developed within 3 months followed by easy deployment within the telecom operator's network.

Tanla deeply appreciates this opportunity to share our perspectives and contribute to this policy-making consultation.

We trust that our insights will prove beneficial, and we stand ready to provide any further details as needed.

Yours Sincerely,



28/08/2023

Sunil Bajpai  
Chief Trust Officer, Tanla Platforms  
Former principal advisor, TRAI

## 24 Tesco Mobile





**Tesco Mobile Ireland Limited (“Tesco Mobile”)  
response to ComReg consultation**

**‘Combatting scam calls and texts’  
ComReg 23/52**

Tesco Mobile welcomes the opportunity to feed into ComReg's consultation regarding the proposed network-based interventions to reduce the harm from scam calls and texts.

Overall, Tesco Mobile agrees and supports ComReg on its proposal to mandate network-based interventions that will work towards combating fraudulent scam calls and texts i.e., nuisance communications. Nuisance communications are an issue and a menace to society that also negatively impact operators, operators do not benefit from such fraudulent activities. ComReg notes in its consultation that MNO's in very few countries have taken the initiative to implement measures and we would suggest, that is because there is no one silver bullet that could have been implemented, fraudsters evolve and the best approach to mitigate against such fraud is for all key stakeholders to work together to target the fraudsters in a co-ordinated manner. The interventions can only be successful if all key stakeholders are working together, including regulators, government bodies, public bodies and end-users.

Tesco Mobile believes ComReg's consultation unfairly lays the blame on operators for not doing more or acting fast enough. Tesco Mobile believes it prudent to remind ComReg that fraudsters became active in a time when the world was hit by a global pandemic and Irish telecom providers were under increased pressure to maintain services for their subscribers, to ensure they could communicate with family and friends. It is disingenuous to say that telecom providers didn't act. Telecom providers prioritised keeping Irish consumers, schools, government bodies and businesses connected during the pandemic. This point is lost in ComReg's consultation.

In addition, the telecoms industry has been working under the auspices of the Nuisance Communications Industry Taskforce ("NCIT") with ComReg since January 2022 to identify interventions to mitigate against nuisance communications. Tesco Mobile fully supports the work of the NCIT and has been participating in the taskforce since February 2022. The NCIT is a voluntary industry-led taskforce and Tesco Mobile believes the collaborative approach with ComReg was the best approach for Ireland, as it enabled key stakeholders to discuss potential interventions and work through them with their peers, while noting key learnings from other jurisdictions.

ComReg had outlined from the onset of the NCIT that the output from the NCIT would be underpinned by Regulation, hence the importance on getting the interventions right within the NCIT. Therefore, Tesco Mobile believes that having successfully provided detailed specifications for the short to medium term interventions, that ComReg should follow the same approach with the proposed long-term solutions before mandating the solutions now. The long-term proposed solutions, along with any proposed alternatives need to be fully considered and specifications defined to ensure the right solutions are mandated. The long-term proposed solutions are complex hence it would be a worthwhile exercise that the industry that must implement the interventions, validate the solutions chosen via the NCIT.

The NCIT provides a transparent process whereby the long-term solutions including proposed alternatives could all be assessed against defined timeframes so that there's complete focus on finding the right, fit for purpose solutions for Ireland and then ComReg can mandate the implementation of same. In line with the short-medium term solutions, the industry will have already commenced work on implementation and therefore no time would be lost.

Tesco Mobile as a Mobile Virtual Network Operator (MVNO) will be reliant on its host network to implement most of the network-based interventions as required. Notwithstanding our reliance on our host network, as we have our own HLR we will be required to support the implementation of the Mobile CLI intervention, specifically the roamer check element and proposed 'proxy server' solution. Tesco Mobile believes that the proposed long-term interventions need to be fully assessed and considered by the NCIT, similar to how the short to medium term interventions were established. ComReg should utilise the NCIT and allow for the opportunity to fully consider the proposed long-term solutions such as the Proxy Server, SMS ID registry and the Voice Firewall as it did with the short to medium term interventions.

Tesco Mobile notes that ComReg's research suggests that consumers are moving away from voice and SMS services for alternative applications because of the harms associated with these services, when the migration to OTT services has been evident for a number of years and not as a result of nuisance communications. The prevalence of nuisance communications has not helped but it's not wholly the reason behind the migration. The cost-of-living crisis is also attributable to the migration, given that subscribers can use the alternative applications using their mobile data service and or WIFI hence reducing their telecommunication costs.

In relation to the agencies that were impacted as a result of scam calls, specifically the HSE (note reference 130) Tesco Mobile does not think it is appropriate to include the HSE, given that it suffered greatly from a cybersecurity hack that completely took down its systems. It is unfair to include or even reference any costs incurred by the HSE to tackle the 'cost of certain cyber security measures' in this consultation document that impacts on the proposed interventions that must be implemented by the telecommunications industry.

With regard to KYC and ComReg's proposal to publish a standalone guideline document, Tesco Mobile believes that ComReg has contradicted itself by stating that '*ComReg expects that all operators, adopt a KYC process, as set out in the consultation, without delay*', yet confirms that it is a guideline only and not mandatory but as part of its compliance monitoring role, ComReg may audit the KYC processes in place. Tesco Mobile would welcome the publication of its guidelines as long as it does not impose unnecessary additional burdens on operators. ComReg also references the increase in fraudulent activity using prepay sims – yet ComReg is focusing on KYC requirements for bill pay sims. Operators are already invested in completing risk assessments when registering a bill pay customer on its network. Prepay is

the issue where registration is not mandatory. Furthermore, where a contract requires explicit reference to the numbering conventions as proposed, any such change should be permitted without invoking any right of exit right.

Finally, Tesco Mobile believes that ComReg should be cognisant of all of the areas that ComReg and or the EU are currently requiring investment by operators for example to ensure compliance with the Electronic Code, the Public Warning System and the Customer Charter to highlight a few. ComReg has the opportunity via the NCIT to ensure that the right interventions are invested in and that timeframes for compliance are fully considered.

## 25 Three

# Three

## Three's response to the Consultation by ComReg on Combatting scam calls and texts

31<sup>st</sup> August 2023



Three.ie

## **Introduction**

Three welcomes the opportunity to comment on this consultation. The issue is an important one affecting users, both those directly impacted by fraud and the wider pool of users of the telecoms services whose confidence in telecoms services might be eroded if the issue of scam and fraud calls is unaddressed.

In this regard it is important to recognise the efforts and achievement of the nuisance calls industry taskforce (NCIT) since its first meeting in early 2022.

These proposals seek to build on the foundations laid by the NCIT. In this regard three believes that in a number of instance better outcomes could be achieved by engagement with the NCIT to refine and to improve the proposals prior to imposing an obligation.

Three looks forward to continued collaboration with ComReg, other operators and wider industry stakeholders in address in the issue of scam and fraudulent calls.

NON-CONFIDENTIAL

## **Consultation Topic - Do Not Originate**

### **Summary of proposals**

Operators will block calls which use a presentation CLI which is contained on a “Do Not Originate” (DNO) list maintained and periodically circulate by ComReg.

### ***Three Response in relation to the draft Decision Instrument relating to “Do Not Originate”***

Three wishes to make a number of comments on operational aspects of the obligations proposed to be imposed.

The first of these relates to the fact that the proposed Decision requires that affected operators implement changes to the DNO list within 2 working days of being notified by ComReg. This obligation requires that operator intervene in their networks to block calls. In order to avoid errors which might result in the blocking of legitimate traffic implementation of these changes should follow the established internal change management processes used by operators. In Three’s case the standard leadtime for implementing network changes similar to implementing DNO changes is  $\times$  [REDACTED]. The proposed obligation does not take into account the fact that most operators usually have a freeze on network changes commencing in early December and spanning the Christmas period. These network freezes are to ensure the stability and integrity of services at a time of peak demand.

If operation implementation targets are to be framed as regulatory obligations, operators would require a much higher level of detail and certainty regarding the format and timing of the communication of the DNO list. At the moment the DNO intervention in place on foot of the NCIT activity means that updates are issued by ComReg email on an approximately monthly basis with the information contained in an excel workbook. While the format of the excel used by ComReg is currently consistent from iteration to iteration it is not guaranteed to be consistent. In order for any time bounded obligation to implement changes to the DNO List to be proportionate the Decision must also specify further detail on what must be implemented what must be implemented. This would include the frequency of the updates (For example a monthly updated issued on the Xth of the month and the format of the updates (for example the update will be by way of an excel workbook with the format set out in an appendix to the Decision). Absent this further specification operators would face having to build processes and procedures that could accommodate the full range of possible update scenarios from very frequent (perhaps with less than one day minimum interval), but irregular (with no certainty over the gap between successive updates) to infrequent but regular (with a long gap between updates that occur at a known specified time/date).

The more onerous the obligation the higher degree of specification required in the Decision Instrument.

Three notes that where there are no changes to the DNO list month to month ComReg does not currently reissue the DNO list but simply sends an email to say that there are no changes. Three is of the view that the full DNO list should issue each month with a separate section showing deltas (both addition to and subtractions from) to the previously issued full list.



In relation to the requirement to provide proposed obligation to provide reports regarding the volumes of calls blocked on foot of the DNO obligation is unduly onerous and that a period of 15 working days is more appropriate.

When assessing the potential impact of the DNO obligation Three reviewed its entire estate of services and customers.

✂ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Three recognises the wider need to deal with scam and nuisance calls, however we believe that this must be balanced against the adverse impact on this cohort of customers of the imposition on the requirements in the timelines set out in the Draft Decision.

In light of this we believe it is appropriate that the Draft Decision be modified to allow for ComReg to grant derogations from the obligation for existing services based on a combination of the technical difficulty of implementation and the risk profile of the services to which the derogation is given.

✂ [Redacted]

## **Consultation Topic - Protected Numbers**

### ***Three Response in relation to the draft Decision Instrument relating to “Protected Numbers”***

Three wishes to make a number of comments on operational aspects of the obligations proposed to be imposed in connection with Protected Numbers.

The first of these relates to the fact that the proposed Decision requires that affected operators implement changes to the Protected Numbers list within 2 working days of being notified by ComReg. This obligation requires that operator intervene in their networks to block calls. In order to avoid errors which might result in the blocking of legitimate traffic implementation of these changes should follow the established internal change management processes used by operators. In Three’s case the standard leadtime for implementing network changes similar to implementing Protected Numbers changes is  $\approx$  [REDACTED]. The proposed obligation does not take into account the fact that most operators usually have a freeze on network changes commencing in early December and spanning the Christmas period. These network freezes are to ensure the stability and integrity of services at a time of peak demand.

If operation implementation targets are to be framed as regulatory obligations, operators would require a much higher level of detail and certainty regarding the format and timing of the communication of the Protected Numbers list. At the moment the Protected Numbers intervention in place on foot of the NCIT activity means that updates are issued by ComReg email on an approximately monthly basis with the information contained in an excel workbook. While the format of the excel used by ComReg is currently consistent from iteration to iteration it is not guaranteed to be consistent. In order for any time bounded obligation to implement changes to the Protected Numbers List to be proportionate the Decision must also specify further detail on what must be implemented what must be implemented. This would include the frequency of the updates (For example a monthly updated issued on the Xth of the month and the format of the updates (for example the update will be by way of an excel workbook with the format set out in an appendix to the Decision). Absent this further specification operators would face having to build processes and procedures that could accommodate the full range of possible update scenarios from very frequent (perhaps with less than one day minimum interval), but irregular (with no certainty over the gap between successive updates) to infrequent but regular (with a long gap between updates that occur at a known specified time/date).

The more onerous the obligation the higher degree of specification required in the Decision Instrument.

Three notes that where there are no changes month to month ComReg does not currently reissue the Protected Numbers list but simply sends an email to say that there are no changes. Three is of the view that the full Protected Numbers list should issue each month with a

separate section showing deltas (both addition to and subtractions from) to the previously issued full list.

In relation to the requirement to provide proposed obligation to provide reports regarding the volumes of calls blocked on foot of the Protected Numbers obligation is unduly onerous and that a period of 15 working days is more appropriate.

When assessing the potential impact of the DNO obligation Three reviewed its entire estate of services and customers.

✂ [Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Three recognises the wider need to deal with scam and nuisance calls, however we believe that this must be balanced against the adverse impact on this cohort of customers of the imposition on the requirements in the timelines set out in the Draft Decision.

In light of this we believe it is appropriate that the Draft Decision be modified to allow for ComReg to grant derogations from the obligation for existing services based on a combination of the technical difficulty of implementation and the risk profile of the services to which the derogation is given.

✂ [REDACTED]

**Consultation Topic - Fixed CLI Call Blocking*****Three Response in relation to the draft Decision Instrument relating to “Fixed CLI Call Blocking”***

Three wishes to make a number of comments on operational aspects of the obligations proposed to be imposed in connection with Fixed CLI Call Blocking.

In relation to the requirement to provide proposed obligation to provide reports regarding the volumes of calls blocked on foot of the Fixed CLI Call Blocking obligation is unduly onerous and that a period of 15 working days is more appropriate.

Three notes that as part of the current NCIT intervention on Fixed CLI Blocking the non or partial whitelisting of MSRNs resulted in the blocking of large volumes of legitimate calls. In this regard Three also notes the proposed obligation on relevant Mobile Service Providers to advise ComReg of proposed changes to their pool of Mobile Station Roaming Numbers (MSRNs) at least three months before such changes become effective. Given that the obligation is on IGOs and not ComReg to use the list of MSRNs as part of the Fixed CLI Blocking Intervention there is a gap in the operational flow relating to the mechanism for communication of MSRN changes to IGOs and the maximum time permitted for IGOs to implement such changes. Three believes that in order to ensure the correct completion of legitimate calls the final Decision should address this gap.

### **Consultation Topic - Mobile CLI Call Blocking**

#### ***Three Response in relation to the draft Decision Instrument relating to “Mobile CLI Call Blocking”***

Three notes that there are three separate elements to the proposed intervention.

The first is the requirement for Mobile Serve Providers (MSPs) to offer a service whereby IGOs can query the roaming status of a mobile number in real time. There are a number of components to implementing this facility. These include the bypassing of “home-routing” signalling where MSPs have implemented this. Another element is the requirement for MSPs to modify the standard signalling responses to remove personal data which is superfluous to indicating the roaming status. This second element arises due to MSPs’ data protection obligations under the GDPR and in particular Articles 5(1)(c) and 5(1)(f).

While the NCIT members set an initial indicative target of 12 months for implementing the intervention this was before detailed design had commenced or vendors engaged in relation to their ability to deliver on the detailed design.

Three notes that as part of the consultation ComReg has only been able to reference one other market where the Mobile CLI blocking has been implemented. This is a clear indication that the intervention is not widespread nor has the solution been previously implemented by all network equipment suppliers.

The “newness” of the intervention and the lack of general industry experience (including by vendors) in implementing it is reflected in the fact that MSPs have been indicating to the NCIT that the initial indicative target date of end Sept 2023 was unrealistic.

✂

Three believes that, based on a Decision being issued in Q1 2024<sup>[1]</sup>, the effective date for the obligation can be no earlier than the 6 months after the Decision as has been consulted on.

Three notes that the Technical Specification for the Mobile CLI Blocking calls for an availability of 99.999% for the Roam Check facility. ComReg’s justification for setting this level of availability is that “ComReg understands that operators design and operate their voice traffic handling functions on a high availability basis (presumed to be 99.999%) and therefore by extension this would apply to the roamer check facility to ensure consistent treatment of traffic.” <sup>[2]</sup>

However there are a number of issues with this reasoning. The first is that the MAP signalling protocol being used relates to SMS and not voice. SMS is a store and forward service and not a real time service like voice. Imposing an obligation on MSPs requiring MSPs to operate their SMS platforms to the same availability as voice is disproportionate.

The disproportionate nature of the proposed requirement is further highlighted in the context that the unavailability of the Roamer Check facility would not prevent calls being successfully completed. In fact calls complete successfully today without this facility and the technical specification explicitly provides that *“In the event of the roamer check facility being unavailable due to temporary technical failure, resulting in no information being available to the IGO on the roaming status for the presentation CLI then the IGO should not block the call.”*

In these circumstances a target design criteria of 99.9% availability would be more appropriate.

The next element of the Draft Decision Instrument is the obligation on IGOs to implement blocking of inbound international calls which present an Irish mobile number as a CLI unless the result of the Roamer Check indicates that the number is roaming.

This obligation requires IGOs to modify their networks to recognise that an incoming international call has a CLI which purports to be an Irish mobile number and to use this fact to trigger the sending of a Roaming Status query to the home Irish mobile network associated with that CLI. If the response to the query is that the customer whose number is being queried is not roaming then the call should be blocked.

✂



Three notes that the proposed requirement on MSPs is to *“provide a Roamer Check facility based on use of MAP protocol to all requesting IGOs”*. In practical terms the provision of a Roamer Check facility involves establishing inter-network signalling connectivity where this does not already exist and the configuration and testing of the MSPs network based on the specific technical parameters agree bilaterally with a requesting IGO (for example configuration of signalling routing based on the specific Global Titles of the requesting IGO). Where multiple requests for Roamer Check Access are received there is a significant risk that these will not be capable of being delivered simultaneously and that they must instead be implemented in a sequence.

The proposal sets a backstop date for the availability of the Roamer Check facility from MSPs at six months after the date of the Decision. However the backstop date for IGOs to implement the Mobile CLI Blocking is on the same date. As an IGO if Three cannot obtain access to the Roamer Check facility from other MSP until their backstop date it will not be possible to implement the Mobile CLI Blocking on the same day. IGOs will require to carry out a Roamer Check with all MSPs that operate an outbound roaming service. The integration of the Roamer Check facility for each MSP cannot practically be carried out simultaneously



and some degree of sequential activity is required. In addition as this intervention will operate on live traffic it must be tested prior to activation in the network in order to ensure the integrity of the existing traffic flows.

Therefore, the backstop date for IGOs to implement the Mobile CLI Blocking must be after the backstop date for MSPs to make the Roamer Check facility available. Three believes that this offset in backstop dates must be at least three months.

As outlined at the NCIT forum Three does not believe that in its role as an IGO it can realistically implement the functionality to support Mobile CLI blocking before mid 2024. Our responses above set out the reasons for this.

The third element of the draft Decision Instrument relates to the obligation to implement a centralised common solution to provide Roamer Check.

ComReg has proposed a collective regulatory obligation that would oblige MSPs to jointly design, procure, and operate a platform to replace the initial MAP solution mandated by the Decision (2) of the draft Decision Instrument.

There appear to be two main strands to ComReg's reasoning for mandating the replacement of the MAP solution with the Proxy Server Solution. These are to accommodate a projected increase in the volume of VoLTE roamers and to allow smaller IGOs avoid the cost of investing in network support for MAP protocols.

Dealing with the issue of VoLTE roamers, the issue is not whether the outbound roamer is VoLTE or not, it is whether the Irish MSP which is the home network of an outbound roamer can correctly respond to a MAP Roaming Check query. While the initial NCIT specification for Mobile CLI Blocking only considered 2G/3G roamers this was because at that point in time the issue of VoLTE outbound roamers was not relevant to Irish MSPs and it was not necessary to delay the NCIT activity to fully research the issue of 5G outbund roamers. Since that time MSPs have activated VoLTE outbound roaming and have a clearer understanding of how this might impact the ability of the MAP solution to support Roamer Check for VoLTE roamers. Based on the practical experience gained in the past 12 months it is Three's belief that for the foreseeable future, and for a timeline which is multiples of the proposed two year implementation period for the Proxy Server solution, the roaming status of an outbound roamer will be held in the HLR Irish home network. This means that the home network will be able to correctly respond to a Roamer Check query based on MAP.

This means that there is no technical imperative relating to VoLTE which would require the replacement of the MAP solution within 18 months of its implementation.

Once the technical imperative to accommodate VoLTE using a proxy server solution to replace the initial MAP solution is removed then remaining reason set out by ComReg to replace the MAP solution is an economic one. It allows smaller IGOs to avoid the cost of investing in the network functionality to support MAP. Instead, it forces MSPs, including those who are not IGOs themselves to invest in the Proxy Server solution. Because the Proxy server would act as an intermediary between the IGOs and the MSPs the MSPs must in effect support Roamer

Checks originated towards them by the Proxy Server. In terms of cost causation, the upfront and ongoing costs of the Proxy Server are entirely attributable to the smaller IGOs which use it.

ComReg has specified that the Roamer Check should be a high availability service. Forcing MSPs and IGOs to insert an additional unnecessary platform into the end-to-end query flow for the Roamer Check appears to be at odds with this stated aim.

Three notes that the Finnish example referenced<sup>1</sup> by ComReg as part of its analysis justifying the proportionality of this obligation explicitly excludes VoLTE Roamers

*“This Recommendation does not apply to VoLTE roaming (S8HR) calls, because in these calls telecommunications operators can identify users and verify their right to use numbers.”*

Three believes that from a technical point of view this reasoning has wider application than just VoLTE calls. Where MSPs implement IMS Centralised Services (ICS) for VoLTE enabled outbound roamer then, even where they are not making VoLTE calls these will be “home routed” over the PSTN. The “home routing” will be effected by the visited foreign network routing the call back to the home network using a temporary routing number similar to MSRN. This means that once ICS is implemented by an Irish MSP IGOs should only see Irish Mobile CLIs associated with that MSP if they have a routing number as the destination number. In this scenario the Mobile CLI blocking intervention becomes very similar to the Fixed CLI blocking intervention, with no need for a Roamer Check for customers of that MSP whether using MAP or the Proxy Server. While there may be a need for a porting status check to identify if the number is homed on the MSP this is far simpler than the Roamer Check.

✂

Given that this functionality is part of the technology evolution roadmap solutions based on this would be future proof.

ComReg itself recognises that there is no short-term technology requirement for a replacement for the MAP based Roamer Check. As outlined above there are potentially far better medium to long term solutions than the Proxy Server solution. Because of this Three believes that it is inappropriate for ComReg to impose the Proxy Server Solution at this time.

As an alternative we would suggest deferring a decision on the longer-term solution until a substantive engagement with industry as regards other alternatives. We believe that this engagement can be carried out in a time bounded manner via the NCIT with a separate consultation on longer term solution based on the outcome of the engagement. This approach is likely to result in better outcomes for MSPs, IGOs and consumers.

---

<sup>1</sup> Traficom Publication 5/22 RECOMMENDATION TO TELECOMMUNICATIONS OPERATORS ON DETECTING AND PREVENTING CALLER ID SPOOFING

The engagement could start even in advance of the target date of Q1 2024 for a Decision on this topic and therefore the impact on the overall timelines would not be significant.

### **Consultation Topic - Voice Firewall Specification**

#### ***Three Response in relation to the draft Decision Instrument relating to “Voice Firewall Specification”***

Three has very significant concerns regarding the proposed Decision Instrument.

First and foremost, it is inadequately specified to give operators legal certainty as to what is required to achieve compliance.

It imposes an obligation to block calls with *“the highest probability of being a Scam Call.”* However, it does not set out what constitutes the threshold for “highest probability”.

It also imposes an obligation to modify calls *“...with a high probability of being a Scam Call that is other than the highest probability of being a scam call”*. Similarly, the draft Decision does not set out what constitutes the threshold for “high probability”.

The definition of “voice firewall” mentions a number of characteristics which must be included in the process of classifying calls. These include *“...signalling information for the call, patterns of traffic volumes and call durations, and phone number data.”* even where there is a probability rating applied to a call based on these parameters the classification process may be subject to errors. However, the draft Decision Instrument is entirely silent as to the requirements as to quality of the classification process. It does not set out targets in relation to false positives, false negatives.

The obligation to classify calls is based on probability of being a scam call. Even if the classification process was not prone to errors and correctly assigns a probability above the threshold there will be legitimate calls which are assigned a high or highest probability. The draft specification and the draft Decision give no indication of how to deal with these.

While the RIA takes account of the protection offered to call recipients from the successful screening out of scam calls, there is no assessment of the adverse impacts on either originators or recipients from the inadvertent screening out of legitimate calls.

This intervention is fundamentally different to the other call blocking interventions such as DNO, or Mobile CLI Blocking. These are based on criteria relating to the permitted uses of certain categories of numbers. Here what is required is an assessment of whether the originator of the call is making a scam call even where the CLI would otherwise be a permitted use. What is required is automated profiling of every terminating call. Where these calls are originated by individuals Three believes that this profile falls within the ambit of the GDPR.

Where the calls are originated from another EEA country, the profiling is carried out on the data subject located in that country. The impact assessment for this proposed intervention sets out no analysis of whether the imposition of an obligation to carry out automated profiling on a mass scale, and almost certainly involving cross border processing, is compatible with individuals' rights under the European Charter of Human Rights and the Charter of Fundamental Rights of the European Union.

Three notes that in advance of the proposed timescale for implementation of the Voice Firewall ComReg and other NRAs are developing interventions to address the issue of scam calls. Because of this we believe that the urgency for implementing this intervention is not as acute as is reflected in the proposed 18-month implementation timescale.

Because of this Three believes that it is inappropriate for ComReg to impose the Voice Firewall Solution at this time.

As an alternative we would suggest deferring a decision on this intervention until a substantive engagement with industry and other stakeholders with a view to further developing and refining the specification. We believe that the Industry engagement can be carried out in a time bounded manner via the NCIT.

We believe that a separate consultation should be held based on the outcome of the engagement. This approach is likely to result in better outcomes for MSPs, IGOs and consumers.

## **Consultation Topic – SMS Sender ID Registry**

### ***Three Response in relation to the draft Decision Instrument relating to “SMS Sender ID Registry”***

While in principle Three supports the introduction of a centralised SMS Sender ID Registry Three notes that this intervention represents perhaps the most fundamental change to market structure of all of the proposals being consulted on. It will result in a completely new commercial situation whereby Sender ID Owners (SIDOs) must contract with a single Aggregator. The intermediate wholesale market which currently allows for larger Aggregators to consolidate traffic from other smaller Aggregators will disappear and MSPs will not be able to limit the number of Aggregators to which they connect.

Given the radical changes to market structure that will arise from this draft decision Three has concerns regarding the specific proposals made by ComReg.

- In relation to the introduction to the Registry, all stakeholders, ComReg, MSPs, and Aggregators will require to develop interconnected IT systems to allow for the transfer of data relating to the entries in the Registry. The frequency of updates, the method of data transfer and the format of the transferred data must all be specified in detail before development work on systems can commence. The “Adoption Process” set out in Section 2.4 of the draft specification is entirely silent on this necessary preliminary activity.
- The ComReg has provided an estimate that the Registry will ultimately contain of the order of low tens of thousands of SenderIDs. While in the medium to long terms steady state there might be low volumes of change in the Registry month on month, in the initial stages there is likely to be a much higher level of change month-on-month. There will need to be a careful assessment of the IT systems capability to ensure that systems, interfaces, and processes dimensioned for the steady state will be able to accommodate the likely higher throughput rates as the new commercial environment beds in.
- Based on the current proposal each registered SenderID must be unique and will be assigned on a “first come first served basis”. The draft Decision Instrument and the associated changes to the Number Conditions of Use do not deal with the initial set-up phase in respect of situations where multiple legitimate senders are currently using the same Sender IDs.
- Related to this initial implementation issue are longer-term, steady issues of intellectual property relating to Sender IDs. The first issue is the SMS Sender ID equivalent of “cyber-squatting” whereby parties apply for the assignment of SenderIDs that may be more appropriate to be assigned to other users, and in particular trademark owners. While the current proposals allow ComReg to refuse a registration which would “lead to confusion; to facilitate fraud or misuse; to incorrectly suggest state sponsorship; or cause offence” However unless ComReg was aware of the potential conflict the current proposals would not prevent this Sender ID squatting and there is no mechanism set out to address it if it occurs.

The second issue relates to trademark holders who wish to register Sender IDs for which they hold intellectual property rights. The current proposals require that the SenderIDs be activated within three months. While there is scope for ComReg to agree to a longer period on a case-by-case basis there is no structured provision allowing rights holders to register SenderIDs related to their trademarks in order to protect the mark or to preserve it for future use.

- ComReg has proposed to impose an access obligation on MSPs by requiring them to accept new direct connection requests from PAs. Three notes that the indirect routing option set out in the draft specification means that direct connections are not required to ensure end-to-end connectivity or to ensure the correct operation of the Sender ID Registry framework.

- ✂ [REDACTED]

[REDACTED] Based on the fact that the indirect routing option set out in the draft specification means that direct connections are not required to ensure end-to-end connectivity or to ensure the correct operation of the Sender ID Registry framework Three does not believe that it is necessary or proportionate that ComReg imposes the access obligation.

In its response to requests for clarifications in relation to the consultation ComReg has invited input on a number of these topics these topics. It has outlined that these inputs will be “... will be reflected in its Response to Consultation ...”.

Three believes that it would be procedurally and operationally flawed for ComReg to impose obligations with strict implementation timeframes without properly consulting on its proposed approach in respect of these fundamental issues.

In light of this Three believes that that it is inappropriate for ComReg to impose the obligations in respect of the SMS Sender ID Registry at this time.

As an alternative we would suggest deferring a decision on this intervention until a substantive engagement with industry and other stakeholders with a view to further developing and refining the specification and associated processes. We believe that the Industry engagement can be carried out in a time bounded manner via the NCIT.

We believe that a separate consultation should be held based on the outcome of the engagement. This approach is likely to result in better outcomes for MSPs, Aggregators and consumers.

Even if ComReg is minded to proceed in imposing an obligation, when Three considers the range of technical and operational issues (some of which have been outlined above) that require to be resolved before the proposed SMS Sender ID regime can be successfully implemented then the proposed implementation frame in the draft Decision is unrealistically short. Three notes that even though ComReg will be responsible for the development and hosting of the Registry, its published workplan covering the period until end Q2 2024 shows no activity on this item.

NON-CONFIDENTIAL

**Consultation Topic – Changes to Numbering Conditions of Use*****Three Response in relation to the draft Decision Instrument relating to “Numbering Conditions of Use”.******Implementation timeframes***

The proposal that the obligations become effective immediately on the date of the Decision is unreasonable and unachievable. Some of the proposed obligations will require changes to operational and commercial processes, with potential for linked changes to OSS and BSS systems. Others will require changes to network functionality. Until the final decision is issued the detail of the required changes cannot be assessed and the related implementation projects commenced. Based on project lifecycle requirements and a high-level assessment of the proposed changes Three believes that a minimum of 9 months is required for implementation.

***Provisions to establish the framework for the SMS SenderID Registry***

Three’s position in relation to the SMS Sender ID Registry is set out in its response to the Draft Decision Instrument relating to this topic.

***Requirement that operators only assign numbers to their own end users – sub-assignment is not allowed.***

Where retail Service Providers rely on wholesale voice inputs with an associated number allocation (for example WLR, wholesale IP voice services, etc.), the wholesale provider has the assignment of the numbers from ComReg but has no direct relationship with the end users. The proposed wording of Section 7.1.(2) of the Numbering Conditions of Use explicitly requires such wholesale providers to “*only use their assigned numbers for their own end-users*”. This obligation as formulated would not be compatible with the continued supply of wholesale voice services which have a number allocation associated with them.

Three suggests rewording the restriction on sub-assignment to explicitly exclude the supply of wholesale voice services.

***Originating operators must perform a CLI check on all originating calls******Three position***

When assessing the potential impact of the obligation to perform a CLI check on all originating calls Three reviewed its entire estate of services and customers.

✂

A large black rectangular redaction box covers the majority of the page content below the 'Three position' section. The redaction is complete, obscuring all text and graphics underneath.



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

[REDACTED] As outlined above the customers using this service have embedded it in their own internal business processes and this is a significant part of the reason why it is proving difficult to withdraw from the market.

Three recognises the wider need to deal with scam and nuisance calls, however we believe that this must be balanced against the adverse impact on this cohort of customers of the imposition of the requirements set out in the Draft Decision.

In light of this we believe it is appropriate that the Draft Decision be modified to allow for ComReg to grant derogations from the obligation for existing services based on a combination of the technical difficulty of implementation and the risk profile of the services to which the derogation is given.

✂ [REDACTED]

#### ***Long-lining only permitted for operators own end users***

*Three position*

✂ [REDACTED] While we acknowledge the issue that this is trying to address we have no views on the topic.

#### ***Additional KYC requirements for freephone and 0818 numbers***

*Three position*

The proposed additional KYC requirements will impose some operational overhead at point of sale

✂ [REDACTED]

#### ***Requirement that the operators ensure that the CLI for the calling party is a number assigned to the caller***

*Three position*

From a technical perspective this requirement is linked to the requirement to check the CLI for all originating calls. It effectively specifies what should be checked. As set out in our response to the requirement to check the CLI for all originating calls we believe it is

appropriate that the Draft Decision be modified to allow for ComReg to grant derogations from the obligation for existing services based on a combination of the technical difficulty of implementation and the risk profile of the services to which the derogation is given.

✂ [REDACTED]

In these scenarios a separate issue arises in situations where  
✂ [REDACTED] Validation must be performed to verify that any CLIs associated with the originated calls are numbers which have been assigned to the caller by a third party operator. Three believes that in order to ensure consistency of application of the obligation and to provide legal certainty ComReg should provide guidance as to acceptable forms of validation. Three suggests that one form of validation could be a copy of a bill from the Service Provider who assigned the number and which details the number assignment.

A similar issue arises in the case of outsourced call centres which may be originating calls on behalf of a customer and displaying that customer's number as a CLI (as opposed to the call centre's own assigned number). Three believes that in order to ensure consistency of application of the obligation and to provide legal certainty ComReg should provide guidance as to acceptable forms of validation Three suggests that a letter of authorisation from the call centre customer authorising the origination of the CLI in question. This letter of authorisation would be in addition to the validation carried on in respect of the assignment of the number to the customer.

### ***Requirement that CLI for geographic numbers be tied to the appropriate MNA***

#### *Three position*

✂ [REDACTED]

For a number of reasons, the CLI for geographic numbers allocated to customers  
✂ [REDACTED] may not always be tied to the appropriate MNA.

These reasons include the fact that historically Address validation was not always carried out in a consistent manner when allocating geographic numbers to new customers. Address validation was not historically performed for ported in numbers or the customer may have moved to a different MNA.

Three believes that these issues will also affect other providers of OTT VOIP based services.

The proposed obligation would require revalidation of Proof of Address for all existing customers along with changes to numbers for any customer not able to provide proof of address. This is likely to have significant impacts both on services providers and end-users.

Three ✂ [REDACTED]

[REDACTED] believes that the fraud risk from the embedded base of customers making calls with “out of area” CLIs is low.

Three suggests that this this issue can be addressed by splitting the obligation so that the MNA validation is on a “where practical” basis. This should be combined with an explicit requirement to carry out address validation for new number assignments. This address validation requirement would substantially address the issue on a going forward basis.

NON-CONFIDENTIAL

## ***Other Considerations***

### **Data Protection considerations**

Three notes that any intervention which involves examination of the calling number potentially involves the processing of personal data. In fact, the proposed set of voice interventions require operators to examine the calling number for every call to assess whether it should be blocked according to the rule set specified in the various draft Decision Instruments for Protected Numbers, DNO, and Fixed CLI blocking. The interventions for Mobile CLI blocking and Voice firewall require even higher levels of data processing.

These calling parties are likely to include individuals both domestic and EEA based and ComReg now proposes to impose an obligation to carry out a new class of data processing on the personal data of the originators of these calls.

For the voice firewall intervention, the level of intrusion into data subject's privacy is even higher with what is automated profiling being mandated.

It is notable that the RIA is entirely silent on ComReg's analysis of the impact that these new forms of processing would have on the privacy rights of individuals. Three believes that this is a significant omission and that data subjects and wider civil society have not been given an adequate opportunity to provide input on this topic.

### **RIA**

It is Three's view that the RIA significantly underestimates the financial and resource costs of these interventions.

✂ [REDACTED]

The estimates of time and expenditure set out in the consultation do not reflect this complexity.

ComReg has set out a cost benefit analysis which would appear to justify the interventions even at higher cost for industry. However, this is not the central impact of the underestimates. The issue is the temporal stacking and overlapping of the interventions and whether the current proposed phasing of these is proportionate. Industry has capex constraints and, in most cases, will have already planned its capital programs well into 2024 and perhaps into 2025. While prudent operators will have made some provision for the evolution of the NCIT initiatives, activities such as the Proxy Server Roamer Check, the Voice Firewall, the SMS

Sender ID registry will not have been fully provided for based on the information to hand when Budget planning commenced.

Increases in the level of budget required and clustering of these requirements will necessitate diversion of resources (both capital and human) from programed projects aimed at improving the underlying service and the care levels that are offered.

The RIA does not take account of other sector specific regulatory projects. These include implementation of the Public Warning System and the implement effort required to meet our obligations under the new retention of data regulations. Other initiatives are within ComReg's control such as the timing of obligation in respect of the proposed Customer Charter. The consultation does not address the migration of scams to Number Independent Interpersonal Communications Services also regulated by ComReg (e.g. WhatsApp).

The RIA doesn't take account of the other sector specific regulatory obligations due to be implemented in the same time period (including Public Warning System and Data Retention) and the impact that Capex limitations and these stacked obligations will have on operators' ability to deploy service improvements and to meet roll-out obligations.

For some of the interventions (such as voice firewall) ComReg has significant discretion to modify the proposed implementation dates in order to level the resource demands over a longer period. We would urge ComReg to reassess the overall regulatory implementation burden that the industry faces over the next 12 to 24 months and to reconsider the timing and phasing of the proposed interventions in the light of this reassessment.

### **Content Scanning and Filtering**

Three does not believe that it is possible to offer substantive views on the ComReg proposals until such time as there is clarity on the exact legal framework in which these proposals will operate.

### **Responses to Specific Consultation Questions**

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.

#### ***Three Response***

Three's views on the proposed changes to the Numbering Conditions of Use are set out in its assessment of the draft Decision Instrument.

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.

#### ***Three Response***

Three's views on the proposed changes to the Numbering Conditions of Use are set out in its assessment of the draft Decision Instrument.

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.

#### ***Three Response***

Three's believes that the CLI Guidance is a useful consolidation of ComReg's views on the issues relating to CLI and should be issued as a standalone document.

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.

#### ***Three Response***

Three agrees with ComReg's assessment that it is not appropriate to mandate SIM registration in Ireland at this time.

Three's position in relation to the issues regarding the proposed changes to prohibit sub-allocation are set out in its assessment of the draft Decision Instrument.

In terms of the proposed KYC guidelines Three is of the view that the binary distinction between KYC checks for Individual Customers and KYC checks for Organisation/Business Customers is overly simplistic. To apply what ComReg describes as the "*minimum KYC checks*" to all business customers regardless of size is disproportionate. Different services also have different levels of risk as there may be technical features inherent in the service that either lend themselves to or mitigate against their use for fraud.

The situation is more nuanced than is suggested by the guidelines. Three believes that it is more appropriate that this topic be explored more fully at the NCIT before any guidelines are finalised.

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.

While Three believes that further refinement of the existing suite of interventions (DNO, Protected Numbers, etc.) could further enhance the quality of the detection and blocking of scam calls we have some reservations regarding the suggestion that industry should move to an outsourced model to profile and block scam calls. Consideration of any such evolution must be carried out in parallel with a consideration of the legal framework it would exist within. In this context the EU AI Act would be one such legal aspect to be considered.

<sup>[1]</sup> ComReg Document 23/75

<sup>[2]</sup> ComReg Document 23/75



-End-

NON-CONFIDENTIAL

## 26 Twilio



*Non Confidential version*

*Combating scam calls and texts  
Consultation on network based interventions to reduce the harm from Nuisance  
Communications*

*Twilio's Response to ComReg Consultation 23/52*

31 August 2023



## 1. About Twilio

- 1.1. Twilio Ireland Limited (hereafter 'Twilio') is a provider of electronic communications services in Ireland. Twilio does not provide services directly to consumers, and is not an International Gateway Operator (IGO).
- 1.2. As a leading global Communications Platform as a Service (CPaaS) provider, Twilio provides services to more than 285,000 enterprises globally and powers more than 1 trillion interactions between them and their customers every year.
- 1.3. Twilio's software allows customers to communicate with their customers over voice, SMS, messaging, or email thanks to the communications feature that companies have added into applications across a range of industries, from financial services and retail to healthcare and non-profits.
- 1.4. Twilio serves a number of global customers as well as Government organisations. Many of Twilio's customers are also small and medium-sized enterprises. Twilio's nonprofit arm, Twilio.org, supports charitable organisations to deliver their communications, such as the Norwegian Refugee Council, a global NGO supporting refugees worldwide. Twilio is also a technology partner and supporter of the United Nation's Vaccine Alliance GAVI.

## 2. Key comments on ComReg Consultation 23/52

- 2.1. Twilio welcomes ComReg's consultation entitled *Combating scam calls and texts. Consultation on network based interventions to reduce the harm from Nuisance Communications*, published on 16 June 2023<sup>1</sup>.
- 2.2. An overarching key comment on the part of Twilio is to urge ComReg to pursue as much clarity as possible in the envisaged ruleset for network based interventions, and as much international harmonisation as possible, in particular with other European countries. This is especially necessary where it concerns blocking of calls/texts, know your customer requirements, in order to avoid obligations that contradict one-another. This comment is made because, whilst being a quasi-global operator, Twilio is a comparatively very small

---

<sup>1</sup> ComReg 23/52: <https://www.comreg.ie/publication/consultation-on-combating-nuisance-communications>



operator in the EU jurisdictions including Ireland. The lack of harmonisation of national regulatory approaches creates a disproportionate burden on multi-country operators.

- 2.3. Hereafter, Twilio provides its key comments on ComReg’s consultation, taking into account the answers to questions provided by ComReg on 10 August 2023<sup>2</sup>, presented in the following sections and sub-sections:

Section 2a: Potential Voice Interventions

Section 2b: Geographic Numbers, Non-Geographic Numbers and CLI

Section 2c: Sub-Assignment of Numbers

Section 2d: Potential SMS Interventions

Section 2e: Know Your Customer (KYC)

Section 2f: Draft Regulatory Impact Assessments (RIAs) and draft Decision Instruments

Section 3: Answers to ComReg’s Consultation Questions (cross-referenced to Section 2)

Section 4: Concluding Remarks

### **2a. Potential Voice Interventions**

- 2.4. Twilio takes note of the fact that ComReg’s proposals relating to voice calls entail, to some extent, the codification of initiatives and interventions agreed by the Nuisance Communications Industry Task Force (NCIT) established in 2022 (paragraph 2.4.1). Twilio is an active member of the NCIT.
- 2.5. Twilio has already implemented agreed NCIT processes relating to fixed voice (the Do Not Originate List (DNO List), the Protected Numbers List (PN List), and fixed number blocking).





330,000 voice capable subscribers (paragraph 5.59 and draft Decision Instrument, Part III), Twilio urges ComReg to be keenly aware of risks relating to Type 1 errors in the form of false positives (referred to in footnote 160).

- 2.7. From Twilio's perspective, it is essential for ComReg to explicitly acknowledge and address the risk of false positives in the formal regulatory measures it will ultimately decide to take, as well as in the technical and governance arrangements that will result from these formal regulatory measures. An agreed efficient process must be in place to deal with the situation where blocking proves to be unjustified or accidentally impedes a legitimate use case, in order to provide for blocking to be undone immediately. An agreed fair process must also include a set of procedures for going after the entity conducting harmful activity (harmful use may involve numbers that are also used for legitimate purposes, and may well go through multiple operators) rather than to block number ranges or even the traffic of a given operator. Specifically as regards voice firewalls, the procedures to enable blocking need to be agreed and trialled prior to implementation.
- 2.8. ComReg proposes to conclude that STIR/SHAKEN is not likely to be effective in Ireland as long as there is substantial use of non-EU networks (paragraph 4.49), and that STIR/SHAKEN could become relevant as a European solution (paragraph 4.54 and paragraph 6.146.142) in the future. Twilio broadly agrees with these findings, at this point in time, particularly given the costs involved in introducing a fully fledged STIR/SHAKEN system in Ireland, even if closely aligned to the implementation in other countries. ComReg should nevertheless continue to monitor the extent to which the implementation of STIR/SHAKEN in other jurisdictions (and on a voluntary basis by operators) is producing positive outcomes, as well as progress towards standardisation leading to easier deployment. A key reason for this is that blocking calls at the point of origin, if effective, (e.g. based on STIR/SHAKEN) is preferable to blocking calls at the termination end, which will surely lead to cases of unjustified blocking of legitimate communications.
- 2.9. Overall, as regards the set of measures needed to effectively combat scam calls (and also texts), Twilio's experience shows that the ability to rapidly and reliably perform a traceback to the entity that is in reality originating a call/text is crucial to effectively combating harmful



activity, regardless of whether the call/text originates from an entity that uses a spoofed number, or from an entity that has legitimately been given a number in use. This is the case because harmful activity, including automated calling/text, can and does occur not only by entities spoofing numbers, but also by entities that are given numbers to use on a bona fide basis.

- 2.10. Vigorous law enforcement against the actual scammers (which are abusing not only citizens and businesses as end-users, but also operators of electronic communications services), also, needs to be part of the package of measures, in addition to the technical measures imposed on operators of electronic communications networks and services.

### **2b. Geographic numbers, Non-Geographic numbers, and CLI**

- 2.11. At paragraphs 6.46-6.44, ComReg puts forward that geographic numbers must remain subject to the so-called “*physical location*” condition, and provides a draft amendment to Section 3.1(5)(a) of the Numbering Conditions, specifying explicitly that the presentation CLI for the call shall be a Geographic Number appropriate to the designated MNA for that number.
- 2.12. ComReg provides only the most minimal justification, referring to the need to maintain trust in numbers and combating nuisance communications. A stronger articulation of the need for maintaining this restrictive approach would be expected, and ideally ComReg refraining from it, on account of the increasing legitimate use cases of cloud communications, which are barely recognised in this consultation document (minimally at paragraph 6.62, with all other references to cloud being of negative connotation). The way in which cloud communications is referred to stands in contrast with an earlier ComReg consultation document, which set out in detail the increasing relevance of legitimate use cases of cloud communications<sup>3</sup>, even if that document also did not lead to more flexible usage conditions for geographic numbers. Overall, Twilio considers that ComReg’s stance does not come as a surprise, but Twilio emphasises that it does not agree with the restrictive approach to geographic numbers maintained by ComReg, because many business end-users express legitimate demand for

---

<sup>3</sup> ComReg 21/ 18, Section 4.1– Numbering Resources for Cloud Communications Service Providers: [https://www.comreg.ie/media/2021/03/Review-of-the-Numbering-Conditions\\_Consultation\\_doc-21\\_28.pdf](https://www.comreg.ie/media/2021/03/Review-of-the-Numbering-Conditions_Consultation_doc-21_28.pdf)



more flexibility. Such flexibility is provided for in a number of regimes including the UK regime which recognises and allows for out of area allocation.

2.13. Non-Geographic Numbers: In the consultation document, ComReg proposes to restrict eligibility to freephone numbers (1800) and standard rate numbers (0818) to Irish companies/registered sole traders (paragraph 6.48). In its answers to stakeholders' question 23<sup>4</sup>, ComReg usefully clarified that governmental organisations, non-profit organisations, charities, etc. would continue to be able to use non-geographic numbers. Whilst being thankful for this response, Twilio nevertheless seeks reassurance from ComReg that European Union-based<sup>5</sup> businesses, governments, agencies and NGOs will be able to continue to use Irish non-geographic numbers. In addition, in Twilio's view, this should also extend to others who can demonstrate a relevant link to Ireland whilst not being present in Ireland (for instance those selling products and services in Ireland from abroad, providing warranty, technical support etc.). There are further questions relating to applicable international treaties with non-EU/EEA third countries in this regard. Twilio wishes to emphasise that non-Irish/non-EU businesses and organisations generally do not wish to rely on 00800 international freephone and other global numbering ranges, because: (i) the high cost to them, and (ii) the reluctance of citizens and businesses to dial these numbers, with which few are familiar. ComReg will recall that the nomadic VoIP number range (076) failed to gain traction in Ireland, because of implementation delays, high interconnection costs and reluctance on the part of users to dial this unfamiliar number. In the proposed equivalent rules for SMS Sender IDs, ComReg includes in the eligible entities those holding a trademark enforceable in Ireland (paragraph 6.40). Twilio is pleased to note that, in response to stakeholder question 24, ComReg committed to look into the discrepancy in approaches taken in paragraphs 6.40 and 6.48.

2.14. CLI: At paragraph 6.12, ComReg proposes to amend the Numbering Conventions (Section 3.1 (5)) to the effect that:“(a) *the undertaking which originates a call shall ensure: i that the CLI*

---

<sup>4</sup> ComReg 23/75: See footnote 2 above.

<sup>5</sup> Operating under the EU Treaties' provisions on the free movement of goods, capital, services, and people, known collectively as the "four freedoms".





*shall be the assigned number for the calling party* Whilst this is a condition which makes sense to combat scams, there are legitimate use cases for modifying the CLI, and for using temporary CLIs, for instance to ensure that subsequent calls are properly answered, to protect the identity of both the caller and callee etc. Examples include: a doctor setting the number of the hospital as the CLI, rather than their personal mobile number as the CLI, so that the patient is able to call back even when the doctor is not available; a delivery person or driver exchanging messages about an impending delivery or cab ride, but where neither party wants to be called or texted subsequently. Twilio therefore believes that exemptions from the rule should be possible, to support legitimate use cases (some such cases described in ComReg 21/18, Section 4.1 Numbering Resources for Cloud Communications Service Providers, referred to in footnote 3 above). Twilio also notes that recent CLI guidance published by Ofcom allows for specific presentation CLI in cases where customer has the right to use that CLI.

- 2.15. CLI: At paragraph 6.58, ComReg proposes to amend the Numbering Conventions (Section 3.1 (5)(a)(ii)) to permit the use of emergency numbers 112 and 999 as CLI. The manner in which this is drafted, by combining it with CLI rules for other types of numbers, itself create potential sources of misuse, e.g. an emergency CLI being presented by another entity than an emergency service. It would probably be safer for ComReg to introduce a separate paragraph dedicated to CLI for emergency services.

### **2c. SubAssignment of Numbers**

- 2.16. At paragraphs 6.96-6.106, ComReg suggests that subassignment of numbers, which it acknowledges explicitly as a practice currently in existence in Ireland (paragraphs 6.100 and 6.101) would be *irregular use* (paragraph 6.100). ComReg proposes to prohibit subassignment going forward, by means of an amendment to Section 7.1. of the Numbering Conditions (paragraph 6.105).
- 2.17. Twilio wishes to express its surprise and disagreement, with ComReg's analysis, as well as with the proposed intervention. Twilio is concerned that what amounts to a major policy issue on number management is not accorded its own consultation process but briefly included at the very end of a 313 page consultation on other topics related to combatting scams. This



proposed change is not called out in the summary of the document and it is not unreasonable to think that many parties who may have a view on this would have been unaware of its inclusion.

- 2.18. The interpretative reference made by ComReg is to Consultation 15/60, which is not a decision. The interpretation is also not consistent with decades of practice, which was deemed compliant with the National Numbering Conventions and subsequently the Numbering Conditions. █



- 2.19. In essence, Twilio considers that ComReg's proposals, amounting to prohibiting sub assignment, are not proportionate, impede legitimate and beneficial use cases, run counter to the objective of promoting competition, are not consistent with relevant practice in other EU Member States and elsewhere, and have not been appropriately justified by ComReg.
- 2.20. Based on the elements outlined in the paragraph above, and in order to enable smaller operators in Ireland to continue to compete, promote innovative services and in particular enable software-based innovations in telephony (CPaaS is basically the only growing segment of an otherwise declining telephony market), Twilio proposes that ComReg refrains from taking measures amounting to prohibiting sub assignment of numbers. Instead of pushing all operators to apply for their own number blocks (paragraph 6.102), potentially restricting market development and flexibility needed for legitimate use cases, ComReg could provide an enabling framework for at least a stage number sub assignment.
- 2.21. If deemed needed, this could possibly (as in Portugal and Spain) be done in the form of a simple notification system to ComReg, resulting in clarity on the identity of both the assignee and the sub assignee, and the number ranges involved. ComReg managing a database of this type is not complicated, and not more complicated than the various databases ComReg already runs and proposes to introduce as part of this consultation.
- 2.22. Finally, and for the avoidance of doubt, number transfers are relevant, and need to remain possible, but are not a substitute for sub assignment, because they imply that the entire administrative and technical burden of number management and implementation would be imposed on even the smallest operators and IT systems integrators, some of which may need very few numbers.

#### **2d. Potential SMS Interventions**

- 2.23. Twilio considers that ComReg's proposals relating to interventions to address scam texts appear less thought through than those proposed for voice calls. This is a matter for concern, in particular in terms of the administrative processes proposed (some of which could be avoided), and in terms of risks to competition.



2.24. As an overarching point, Twilio considers that a Sender ID Registry, managed by the independent regulatory authority (as opposed to being managed by the Mobile Network Operators (MNOs), or unilateral SMS blocking by the MNOs), is a relevant and sensible way forward for Ireland.

2.25. That being stated, Twilio has serious doubts about ComReg's proposed approach to Sender ID, and the articulation of responsibilities between Sender ID Owners (SIDOs), Participating Aggregators (PAs), and ComReg, at least in the following respects:

(a) In the consultation document, ComReg proposed to restrict eligibility to SIDOs to Irish companies/registered sole traders, and those holding a trademark enforceable in Ireland (paragraph 6.40). In its answers to stakeholders' question 23<sup>10</sup>, ComReg usefully clarified that governmental organisations, non-profit organisations, charities, etc. would be able to use SMS Sender IDs. Whilst being thankful for this response, Twilio nevertheless seeks reassurance from ComReg that European Union-based<sup>11</sup> businesses, governments, agencies and NGOs will be able to use SMS Sender IDs. In addition, in Twilio's view, this should also extend to others who can demonstrate a relevant link to Ireland whilst not being present in Ireland (for instance those selling products and services in Ireland from abroad, providing warranty, technical support etc.). There are further questions relating to applicable international treaties with non-EU/EEA third countries in this regard.

(b) ComReg proposes that it will manage the Sender ID Registry (paragraph 6.33), which Twilio agrees with, but ComReg also proposes that PAs will apply for Sender IDs to ComReg on behalf of SIDOs (involving the filing of forms, a declaration validating the existence of a contract – paragraph 6.39), and a proposed SMS Sender-ID portability concept (paragraph 6.36) ostensibly aimed at preserving competition. The result is a proposed one-to-one relationship between PAs and SIDOs, and a first-come-first-served system (paragraph 6.38) with PAs rushing to sign-up and file. Not only does this seem unduly complex, it could also cause a land-rush in which some (for instance the MNOs or their affiliates acting as PAs) may have competitive advantages over

---

<sup>10</sup> ComReg 23/75: See footnote 2 above.

<sup>11</sup> Operating under the EU Treaties' provisions on the free movement of goods, capital, services, and people, known collectively as the "four freedoms".



others. It also negates the fact that many businesses and organisations see benefit in using more than one SMS aggregator, multifactor authentication provider etc. Being able to use more than one messaging service provider enables them to issue tenders to select the best specialist messaging provider for a given task, or for a given communications channel/campaign, while also using other messaging providers for other tasks, etc.

(c) In the draft Decision Instrument, it is stated that *the relevant Undertakings that are PAs shall:*  
*a. Implement direct connections to SMS infrastructure of one or more Participating MSPs*" (page 280, point 5). In the Technical specification it also states that valid messages must not traverse more than one aggregator.

- 2.26. Twilio considers that it should not be necessary to have direct connections to the MNOs but if a decision to that effect is taken by ComReg, then it is essential to place an explicit obligation on each of the MNOs (ComReg uses the term MSPs) to ensure that connections are made available, tested, and fully operational 3 months before the effective date (which is 12 months after the date of the making of the Decision Instrument) and that any disputes about technical and financial terms are settled by ComReg 2 months before the effective date.
- 2.27. Based on the above, Twilio considers that it would be far simpler if ComReg would manage the qualification process for Sender IDs directly (i.e. those Sender ID owners interested in being assigned a Sender ID would apply directly to ComReg rather than through a Participating Aggregator), if ComReg would manage the list of qualified Sender IDs, and publish periodic updates of the list, enabling SIDOs to enter into (exclusive) contracts with messaging providers. Importantly, therefore, this would enable businesses/organisations to give their Sender ID in use to more than one messaging provider (or Qualified Aggregator if qualification is deemed necessary, which Twilio would support) at the same time, thus meeting users' needs, providing a much stronger impetus for competition, and removing the need for a SMS Sender ID portability system.
- 2.28. In addition, Twilio advocates that not only individual businesses and organisations meeting a reasonable set of qualification requirements should be entitled to an Irish Sender ID, but that aggregators should also be entitled to register a Sender ID in their own name. This would enable companies such as Twilio to develop and deploy their own trusted Irish/EU/global



Sender ID, and give it in use to those of their customers who choose to use that solution in Ireland (i.e. a combination of a known trusted sender, with their own brand or identity).

2.29. Singapore provides a relevant example of a functioning Sender ID regime, as acknowledged by ComReg (paragraph 4.77), and also in its answer to question 22<sup>12</sup>. Twilio is a participant in the Singaporean system. We are available to discuss it with ComReg, and we encourage ComReg to further engage directly with its Singaporean counterpart, IMDA, to understand the exact functioning and latest developments of its Sender ID regime<sup>13</sup>. Twilio notes that Singapore's IMDA however has neither found it necessary or proportionate to restrict the use of Sender IDs by a Sender ID owner to one Participating Aggregator, nor has it found it necessary to specify that such valid messages must not traverse more than one aggregator as set out in the SMS Sender ID Registry Functional Specification. Twilio is concerned that ComReg is attempting to shorten the chain intervention through the mechanism of its Sender ID registry and has neither justified why there is the need for a Sender ID to be linked to one aggregator nor why a message when being sent should not traverse more than one aggregator.

2.30. Two notable features of the Singapore regime are as follows:

(a) In Singapore, the registration of the Sender ID is subject to the agreement of the Internet domain name registry (SGNIC) which has set up a SMS Sender ID Registry<sup>14</sup>. SGNIC will need to be satisfied that there is a nexus between the Sender ID and the sender ID owner seeking to register the said Sender ID. Importantly Sender ID owners can also provide a list of the Participating Aggregators that they work with to deliver their SMS messages as part of their application.

(b) IMDA has clarified its Sender ID Registry rules, with a Notification of Variation of Direction of Full Singapore SMS Sender ID Registry Regime (SSIR) dated 2 August 2023. In essence, this clarifies that Participating Aggregators are able to use a Common Sender ID, of their own

---

<sup>12</sup> ComReg 23/75: See footnote 2 above.

<sup>13</sup> Singapore IMDA: <https://www.imda.gov.sg/how-we-can-help/anti-scam-measures>

<sup>14</sup> SGNIC SMS Registry: <https://www.sgnic.sg/smsregistry/overview>



choosing (subject to the same SGNIC agreement requirement as a single organisation Sender ID), to enable multiple foreign merchants (those which do not have a Singapore local unique entity number (“UEN”) issued by relevant Singapore government agencies) to communicate through this Common Sender ID. Of course, Participating Aggregators will be held responsible for all SMS sent under that Common Sender ID. By way of example, this enables companies such as Twilio to determine and develop their own unique alphanumeric ID, create a trusted brand identity around this ID, and convince companies and organisations not present in Singapore that it is in their best interest to use this trusted system. Clearly, this is more flexible than the restrictive approach put forward by ComReg in paragraph 6.40.

## **2e. Know Your Customer (KYC)**

- 2.31. Twilio takes note of the fact that ComReg’s proposals relating to Know Your Customer (KYC) (Section 6.5) take the form of a guide to KYC processes, that the guidelines are not mandatory, that ComReg proposes to publish the guidelines as a ~~stand~~ document (paragraph 6.84), and that ComReg expects all operators, including cloud service providers, to adopt a KYC process, as set out in Section 6.5, without delay (paragraph 6.98).
- 2.32. We congratulate ComReg for proposing KYC guidance which appears very closely aligned with established practice in the UK, as contained in Ofcom’s Good practice guide to help prevent misuse of sub-allocated and assigned numbers<sup>15</sup>. Clarity and alignment is most welcome from Twilio’s perspective, given that we face particular challenges as a consequence of being subject to the application of different regulatory obligations in different jurisdictions, including – unfortunately – discrepancies if not outright contradictions between regulatory obligations, even where they are aimed at meeting the same objective. Twilio calls on ComReg to work proactively with its counterparts (e.g. for the EU/EEA through BEREC which also has members without voting rights from non-EU/EEA countries), in CEPT ECC, and more widely, to aim for, and maintain, maximum harmonisation of KYC requirements for

---

<sup>15</sup> Ofcom Statement published on 15 November 2022:

[https://www.ofcom.org.uk/\\_data/assets/pdf\\_file/0019/24750/statement-good-practice-guide.pdf](https://www.ofcom.org.uk/_data/assets/pdf_file/0019/24750/statement-good-practice-guide.pdf)



telecommunications operators with specific attention to the challenges faced by multi-country providers of cloud-based communications services.

## **Section 2f. Draft Regulatory Impact Assessments (RIAs) and draft Decision Instruments**

2.33. Twilio has carefully examined the RIA Framework (Section 5.1) and the four draft RIAs put forward by ComReg (Section 5.2), as well as the draft Decision Instruments (Chapter 7). It would take us too long to repeat all our key substantive comments in ~~total~~ each of these in this response. Our key comments apply mutatis mutandis to each of the draft RIA conclusions and the overall conclusion (the options proposed by ComReg to be selected), and to the draft Decision Instruments.

2.34. This being stated, Twilio requests that ComReg modify paragraph 5.42, ~~which~~ *lists several key industry stakeholders in relation to the matters considered*. Types of operators are listed, which are all clearly relevant. However, Twilio considers it imperative that providers of cloud communications and Communications Platform as a Service (CPaaS) are explicitly recognised by ComReg, and are added as ~~a~~ *a* category. The impact of ComReg's proposals on this additional category of providers must then be assessed by ComReg in each draft RIA. This is especially important given that ComReg invokes the existence of Cloud Services among the motivation to address ~~and~~ modify CLI principles and conditions (paragraph 6.62). Please allow us also to emphasise in this context that: (a) Twilio is very favourable to international harmonisation, because in its absence it has to implement sometimes substantially different, ~~and~~ in some cases contradictory, decisions taken by regulatory authorities, and, (b) whilst Twilio is active globally, it is a comparatively very small operator in Ireland, and indeed is very small in each individual jurisdiction.

## **3. Answers to ComReg's Consultation Questions (cross-referenced to Section 2)**

3.1. Please find Twilio's answers to ComReg's concrete consultation questions below. These should be read in conjunction with the entirety of this response, which contains Twilio's reactions to the full set of proposals made by ComReg in this very wide-ranging consultation. This is important, because the 5 consultation questions only address a subset of what ComReg is in fact proposing.





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.

- 3.2. Twilio agrees with ComReg's proposals to amend the Numbering Conditions as they relate to the introduction of the DNO list (paragraph 6.14), the introduction of the PN list (paragraph 6.16), and the carve out from fixed number blocking in the form of "long-lining" and its definition (paragraph 6.17). These are sensible proposals, codifying NCIT work, in which we have participated. We have already implemented these measures. Please also refer to our key comments in Section 2a above on Proposed Voice Interventions (in particular our point 2.5 above).
- 3.3. We have no comments on the Mobile CLI Blocking proposals (paragraphs 6.26 and 6.27).
- 3.4. Twilio has serious concerns about ComReg's proposals to amend the Numbering Conditions in light of the proposed SMS interventions. In particular, we believe that the close relationship ComReg creates between a SIDO and a Participating Aggregator will not satisfy user needs for relying on more than one messaging provider, is not conducive to promoting competition (and may create advantages for MNOs and their affiliated PAs), and creates unnecessary administrative burdens, for both ComReg and operators, relating to portability for SMS Sender IDs. We therefore disagree with the related proposals (paragraphs 6.32, 6.36, 6.38, 6.39 in particular) and we have formulated what we believe to be a superior alternative in Section 2d above (in particular our point 2.27 above). We provide supporting information, notably as regards the latest developments in Singapore (our points 2.29 and 2.30). Please study our Section 2d above in full, as it contains further supportive information and arguments. As regards the eligibility criteria (paragraph 6.40), please refer to our specific comments in Section 2d (our point 2.25 above).

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.

- 3.5. Twilio disagrees with ComReg's proposal to amend the Numbering Conditions relating to Geographic Numbers, confirming the "physical location" requirement (paragraph 6.44). Our



arguments in favour of introducing more flexibility, in response to legitimate use cases and usage scenarios, and supporting information are provided in Section 2b above (our point 2.11).

- 3.6. As regards the eligibility criteria for Non-Geographic Numbers (paragraph 6.48), please refer to our specific comments in Section 2d (our point 2.13 above).
- 3.7. For emergency numbers, we believe that it would be advisable to create a separate paragraph in the Numbering Conditions (our point 2.14 above).

Q.4: 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.

- 3.8. Twilio has limited comments on ComReg's proposed general updates to provide CLI Guidance. However, where *long-lining* is discussed (paragraph 6.70), it would be preferable for ComReg to not only mention *Irish customers that have international branches or call centres that wish to use their Irish number as presentation number* but also to maintain an opening for other legitimate use cases, for which *long-lining* provides the necessary safeguards. This comment is made with reference to ComReg's Answer to Question 12 in document 23/75.

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.

- 3.9. Twilio agrees with ComReg's proposed *binding* guidance. Please refer to section 2e above. It is very important that KYC guidance remains as aligned as possible with its equivalents in other jurisdictions.

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.

- 3.10. The section on Future Number Management Needs and Developments is very brief. Twilio evidently agrees that *national numbering management should be based on increasing effectiveness and efficiency and must also address the evolving nature of nuisance communications* (paragraph 6.132) and that *ComReg will continue to improve the systems*



and processes for managing the national numbering resources (paragraph 6.136). Twilio would like to see added to this that numbering policy and management should also reflect the evolving technology landscape, including innovative services which meet users' needs, and are welfare-enhancing. The points made on STRAKEN are relevant, and consistent with Twilio's views (our point 2.8 above). In addition, we believe that the ability to perform a traceback on harmful calls to the actual origin (i.e. the actual scammer, of which the ECN/ECS operator is also a victim) will be an essential part of future additional measures, and that vigorous law enforcement against the actual scammers, needs to be part of the package, in addition to the technical measures imposed on operators of electronic communications networks and services (see our points 2.9 and 2.10 above).

- 3.11. ComReg's consultation document makes numerous references to dynamic (rather than static) interventions, which amount to blocking calls/texts, and in the section on Future Number Management, reference is made to Artificial Intelligence for pattern detection, as well as crowd-sourced information. Twilio clearly recognises the potential of existing and developing technological approaches, but also wishes to caution that such solutions entail risks of over reach. In particular, the risk of false positives should explicitly be acknowledged and addressed in any near term or longer term formal regulatory measure considered by ComReg. In addition, where blocking proves to be unjustified or accidentally impedes a legitimate use case, it should be possible for blocking to be undone immediately, and for more effective arrangements to be pursued, in particular going after the entity conducting harmful activity (harmful use may involve numbers that are also used for legitimate purposes, and may well go through multiple operators) rather than to block number ranges or even the traffic of a given operator.

#### 4. Concluding Remarks

- 4.1. Whilst use of electronic communications to cause harm is an unfortunate reality and should be actively combatted, legitimate innovative use cases of numbers, including Communications Platform as a Service – CPaaS – exist and are growing. CPaaS use cases are appreciated by businesses, government, and end-users. Introducing measures, be they



industry agreed, regulatory in nature, or even legislative in nature, should not result in hampering innovation or restricting competition on telecommunications markets. In addition, conflicts with electronic communications legislation should be excluded in particular as regards the provisions ensuring end-to-end connectivity.

- 4.2. Placing the totality of responsibility for combating harmful activity on ECN/ECS operators is neither appropriate nor realistic. Harmful actors and the persons and organisations which are at the origin of nuisance communications are sophisticated and constantly adapt their practices. Several of ComReg's proposals are likely part of mitigating actions and real solutions in some cases, but do not replace law enforcement in cases of criminal activity. Ultimately, criminal activity is a matter of law enforcement.
- 4.3. Twilio is aware that the CEPT ECC NaN working groups (in particular *NaN2* *Portability and Switching*, *Trust in Numbering*, *Network Technology Regulatory Issues* and *NaN1 future of numbering issues*) have in the past addressed CLI spoofing, and are currently working on deliverables such as:

- draft ECC Recommendation on incoming international voice traffic with suspected spoofed national E.164 numbers (NaN2 working group)

<https://cept.org/ecc/groups/ecc/wg-nan/nan2/client/meeting-calendar/>

The NaN2 working group also has a meeting scheduled on SMS Sender ID.

- draft ECC Report on Numbering for cloud-based communication services (NaN1 working group)

<https://cept.org/ecc/groups/ecc/wg-nan/nan1/client/meeting-calendar/>

This work is actively being pursued, with meetings scheduled, and a consultation ongoing. It would be unfortunate if individual authorities, such as ComReg, would take radical decisions that will render a coordinated international approach impossible. Twilio appreciates that ComReg is actively engaged in relevant discussions at CEPT ECC level and would welcome its continued efforts in ensuring that a common approach is taken in such a critical area.



- 4.4. Twilio looks forward to studying the elements that will be provided by other respondents to this consultation, and therefore requests that ComReg publishes the ~~confidential~~ responses as soon as possible, well in advance of ComReg's decision (in line with ComReg's usual practice to publish the responses only when it has reached its decision).
- 4.5. Twilio is available to discuss the matters at hand directly with ComReg, to clarify its concerns, explain the legitimate use cases of its customers, jointly identify practicable solutions, etc. Please do not hesitate to reach out to:

Twilio Ireland Limited

Address: 3 Dublin Landings, North Wall Quay, Dublin 1, Dublin, Ireland D01 C4E0

Attention: Twilio Global Regulatory Affairs

Email: [regulatorynotices@twilio.com](mailto:regulatorynotices@twilio.com)

## 27 Verizon

# Verizon Response to ComReg's consultation on measures to reduce the harm from Nuisance Communications

31 August 2023

## I. Introduction

Verizon Ireland Limited ("Verizon")<sup>1</sup> welcomes the consultation<sup>2</sup> by the Commission for Communication Regulation ("ComReg") on measures to reduce harm and restore trust in voice communications.

Verizon supports the overall objective of ComReg and we are fully committed to implement measures that have proven to be efficient to tackle nuisance calls and restore customer trust in voice communication. The views expressed are specific to the Irish market and its regulatory regime and should not be considered as an expression of the views of Verizon in other jurisdictions where the market and regulatory environments may differ from those of Ireland.

### I. Technical interventions

Verizon continually evaluates the risk for our customers and we took a very active position in implementing voluntary network-based interventions that have been identified by the Nuisance Communications Industry Taskforce, when technically possible. As such, we have already implemented the Do Not Originate and Protected Numbers lists, as well as the international Fixed CLI blocking.

Verizon welcomes ComReg's approach considering that Stir Shaken is not a viable intervention at this point of time, proposing instead a set of measures for the fixed market that have the potential to bring positive impact in the short term.

Nonetheless, Verizon is very concerned with the complexity and the challenges that would be faced by fixed communication providers for the design and implementation of the International Mobile CLI blocking as proposed by ComReg. Indeed, both interventions identified in phase 1 and 2 are very costly and burdensome. We believe it is disproportionate to require the industry to make an important investment twice; first for the design and implementation of a MAP protocol-based roamer check solution, and then for the design and implementation of an industry database solution.

<sup>1</sup> Verizon Ireland Limited is part of Verizon Communications, one of the world's leading providers of technology and communications services. Outside of the United States, the company provides a broad range of global communications products and enterprise solutions predominantly to large business customers.

<sup>2</sup> ComReg consultation on network based interventions to reduce the harm from Nuisance Communications - ComReg 23/52 dated 16.06.2023 - <https://www.comreg.ie/media/2023/06/Consultation.pdf>

Furthermore, Verizon is not aware of any fixed provider who has developed a mobile call query functionality on their switch and who intends to offer a wholesale service to smaller providers; nor is there any regulatory compulsion to do so. If any operators were to offer a wholesale solution, we would like to be offered assurances that the costs of buying into their solution would be minimal. Otherwise, we face the risk that carrying this traffic may not be commercially viable for us.

The implementation of a network-based solution as proposed by ComReg in Phase 1 is very challenging. There is still a considerable amount of legacy network equipment that does not (and will not) have the technical capability to interface with a mobile carrier's roaming database. Choosing a network-based solution would create counterproductive results as terminating providers might be in a position where they have no other choice than to block all legitimate internationally originated calls in order to be compliant with their obligations, i.e. to ensure that no spoofed mobile CLIs are allowed to pass.

There is also a risk of large call blockages if any such "roamer check" functionality was to have an outage or service issue. At this time there is also no legal requirement on the mobile providers to share their roaming data with fixed line operators, and any such solution would need unrestricted near real-time access to all the mobile operators roaming database.

As such, we would urge ComReg to ensure that a wholesale solution is available, and that the terms and conditions to access this solution are discussed and agreed amongst the industry stakeholders. This would ensure that there is the possibility for those smaller players for whom the costs of implementing a solution themselves is prohibitive to become compliant through a wholesale solution. Alternatively, we would invite ComReg to consider an industry database solution instead of a network-based solution.

Separately, Verizon considers that it would be disproportionate to require communications providers who are not able to report on the relevant information due to the legacy system they have in place, to invest in a new system for the sole purpose of reporting. We would suggest that ComReg changes the reporting requirement for any interventions into a voluntary arrangement, following a similar approach as in the UK.<sup>3</sup>

## **II. Know Your Customers**

Know your customer (KYC) is fundamental to ensure communications providers are confident on how their customers use valid numbers.

Verizon believes the guide includes some helpful suggestions for those communications providers who have yet to fully implement processes to ensure they know their business customers and how numbers will be used by them before numbers are transferred.

Verizon considers the guide can be used to help plan and focus the development of suitable processes. However, communications providers such as Verizon who have already implemented robust and efficient processes should not be required to implement new processes.

By definition, the measures mentioned in the guide are only suggestions and we would urge ComReg not to be prescriptive on measures providers are expected to implement to ensure their compliance with their regulatory obligations. Rather, ComReg should focus its guidance on encouraging communications providers to support the principle of assigning numbers to low risk and/or reputable customers, while allowing them flexibility to define the relevant measures for their customer base and service offerings.

---

<sup>3</sup> See paragraph 7 of the Nuisance Calls tech MoU, Ofcom, [https://www.ofcom.org.uk/data/assets/pdf\\_file/0026/31859/nuisance\\_calls-tech-mou.pdf](https://www.ofcom.org.uk/data/assets/pdf_file/0026/31859/nuisance_calls-tech-mou.pdf)



Amongst other things the risk profile of business customers should be considered. For example, it is not proportionate to require communication providers to implement new and highly prescriptive processes for corporate and enterprise customers. These types of customers will have low risk profiles with regard to number misuse.

### **III. Updated the Numbering Conditions**

Verizon would suggest the following additions to the new Section 3.1(5)(d) proposed by ComReg :

*"That the CLI on inbound international calls shall be in international E164 format. Trusted international calls not in such format may be modified with appropriate prefixes including "00", "+" and the relevant country code, or setting the correct ISUP "Nature Of Address" flag". If the international call is untrusted and the CLI not in ~~E164~~ a correct format, an operator may mark the presentation CLI as "Caller ID unknown" or equivalent".*

## 28 Viatel



## Viatel Response to Comreg Consultation Document 23/52

30/08/23

## 6 Updating the Numbering Conditions

Related Question:

**Q.1 Do you agree with ComReg’s proposal to amend the text in the Numbering Conditions as set out above? Please explain the basis for your response in full and provide supporting information.**

6.1 This Chapter proposes changes to ComReg’s Numbering Conditions of Use and Application Process document (“the Numbering Conditions”)<sup>340</sup> 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.

### Section: CLI Conditions - Assigned Number

6.12 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;

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;~~

**ANSWER: Viatel has no issue with the proposed change above**

### Section: Do Not Originate

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

**ANSWER: Viatel has no issue with the proposed change above**



### Section: Protected Numbers

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

**ANSWER: Viatel has no issue with the proposed change above**

### Section: Fixed CLI Call Blocking

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;*

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;*

**ANSWER: Viatel recently engaged with Comreg regarding a potential scenario where Long-Lining was not setup directly to an end user but involved a SIP Trunk Long Lined from end user to a Reseller who would then route traffic to the Operator over standard National Interconnect. After some discussion and further information provided by Viatel, including call flow diagram - Comreg agreed that this practice would meet the definition of Long-Lining - therefore the proposed wording should be changed to reflect this.**



6.19

"ComReg has concerns regarding the use of Irish geographic numbers as CLI on these calls..."

"ComReg sees the use of NGNs by Irish overseas branch offices or call centres as a possible alternative"

**ANSWER/COMMENT: Although the use of NGN numbers is valid for CLI as per the current numbering conditions, Viatel does not see this as an alternative solution currently - primarily due to the unreliable nature and inconsistent results of such methods.**

**In our experience, the attempted use of NGN numbers for CLI in recent years produces unreliable results and have worked with other Operators to try to remedy this.**

**The fact 1800 NGN numbers start with 1 and 0818 NGN starts with 0 compounds this. As a result, we have discouraged customers from attempting this to date and advise the practice is best effort only.**

#### **Section: Mobile CLI Call Blocking**

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

**ANSWER: Viatel has no issue with the proposed change above**



## Section: 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."

**ANSWER: If the numbering conditions will change to specifically include the requirement for CLI-analysis on all calls we propose that more detail will be required to state what actions Operators should take if calls fail the CLI-analysis. Should they be blocked? Or CLI Supressed/Changed but call allowed to flow? Should there be exceptions? i.e., in the case of ECAS calls for e.g., if CLI-analysis fails should those calls be blocked? – Keeping in mind that ECAS calls are allowed when billing/suspension issues are present.**

We note 5.e in 3.1 General Authorisation Conditions of the Numbering Conditions where it is specified CLI "may" be marked as unknown if the operator "cannot ensure" the CLI info is "valid." The proposed terminology is stronger in the consultation document and more specific than checking if it is "valid." Therefore, removing the ambiguity around "may" and confirming specific consequence would be better in our opinion.

In later sections below, we have referred to the presence of Resellers in the market where the Operator is not directly connected to the end user and this can add difficulties and complexities in relation to numbering conditions, however clearly specified consequences would go a long way to assist Operators in enforcing the conditions.



## 6.3 General updates to CLI Conditions

Related Question:

**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.**

### Section: Geographic Numbers

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 appropriate to the designated MNA for that number, a Harmonised Code of Social Value, a Mobile Number or a Standard Rate Number;

**ANSWER: Viatel agrees with the statement in 6.19 where a consumer survey is referenced: "*consumers have concerns regarding fraud if the link between area codes and geographic areas is removed*". However, the proposed wording specifically deals with the MNA and not area code.**

**We agree in general that there is a level of trust and familiarity with area codes linked to physical locations, however in our experience there is little public knowledge of these areas being broken down further into MNAs.**

**Furthermore, the quoted Comreg Consumer Survey appears to deal specifically with public knowledge of the 50 Area Codes - not the much larger number of MNAs.**

**Viatel does not agree in general that the use of MNA should continue and believe this legacy concept provides no benefit in today's modern Telephony Networks. A simplification in the numbering scheme by removing MNAs but retaining Area Codes would drive efficiencies in the number portfolio by allowing Operators to use all assigned number blocks in an Area Code regardless of MNA and would in turn reduce the number of new block requests.**





**Section: Non-Geographic Numbers (“NGN”)**

Add the following underlined text to paragraph 2 of Section 4.3;

Furthermore, as 1800 Freephone numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 1800 Freephone number, a business end-user shall be required to provide the following:

- i. A company’s Irish CRO number, Revenue VAT or business number, [and/or]
- ii. A partnership/sole trader’s Irish VAT number in their name(s) or proof of their business or Irish income tax registration.

And add the following underlined text to proposed paragraph 2 of Section 4.4;

Furthermore, as 0818 Standard Rate numbers are only provided to businesses, to demonstrate its eligibility to be assigned an 0818 Standard Rate number, a business end-user shall be required to provide the following:

- i. A company’s Irish CRO number, Revenue VAT or business number, [and/or]
- ii. A partnership/sole trader’s Irish VAT number in their name(s) or proof of their business or Irish income tax registration.

For reference here is paragraph in question:

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.

**ANSWER: Viatel agrees with the proposed addition.**



### Section: Emergency Numbers

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;

**ANSWER: Viatel agrees in principal that the use of 112 or 999 as presentation CLI for call backs from the Emergency Services would encourage the emergency caller to answer a returned call. However, we can also see the technical difficulties of such action so believe clarification would be required around the origination of the calls, call flow/route, number format etc This will likely require interop testing between Operators so this would need to be taken into consideration including if this should be formal or informal testing and agreements.**



## 6.4 General updates to provide CLI Guidance

Related Question:

**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.**

**ANSWER: Viatel welcomes any attempt to clarify or provide more detailed information regarding CLI in general. In reference to the following point:**

**6.68 (i) "The presentation and network CLI must be authenticated".**

The prevalence of Resellers in the market would make this proposal difficult to implement and police where the Operator is not directly connected to and servicing the end customer/user.

We feel the Reseller should take some level of responsibility here and any requirements under "CLI Guidance" which include "must" will have to apply to the providers of the end service – not necessarily the Undertaking who have been assigned the original number blocks i.e., the Operator.

Furthermore section 6.71 refers to the "originator" of the call who "must ensure that the CLI is the calling party's assigned number." This does not go far enough to take into consideration the Operator – Reseller – End User relationship and the wording should be further explored.



## 6.5 Know Your Customer

Related Question:

**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.**

6.105 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.*

**ANSWER: Viatel does not agree with the wording of this proposed change as it does not take into consideration the Operator - Reseller relationship which by its very nature does not result in an Undertaking assigning numbers to its own end users.**

We acknowledge that previous Numbering Consultations have dealt with the concept of Resellers at length and it is widely accepted in the industry that Resellers play an important role in delivering services to end customers.

We also note Comreg's specific mention of Resellers in section 3.1 General Authorisation Conditions as well as the inclusion of the definition of Reseller.

Viatel also acknowledge after recent discussions with Comreg it was confirmed that the intention was to address Operator to Operator sub allocations only and not in any way hinder the existing Operator to Reseller relationships. Therefore, we believe the wording should be improved to reflect this. As it stands the proposed wording "*Undertakings are obliged to only use their assigned numbers for their own end-users*" is problematic.

The following line "*Sub-assignment to other undertakings is not permitted*" goes a little way to clarify but the working could still be improved to remove any ambiguity and confusion.

In relation to KYC in general we note the wording in section 6.114: "*Therefore, operators and cloud providers shall establish the location of their customers before providing Geographic numbers.*" And in section 6.98: "*ComReg expects that all operators, including cloud service providers, adopt a KYC process, as set out in this section of the consultation, without delay*".

Bringing this back to our previous mentions of the Operator – Reseller relationship, it appears that the use of term "cloud provider" and Reseller are interchangeable here for the purpose of this subject in question and we welcome any changes that enable/assist Operators to ensure numbering condition compliance by emphasising all parties have a role to play here and are responsible whether they are Operators, Resellers, Cloud Providers etc. The section 6.109 appears to confirm this as the wording refers to operators who "*provide Irish phone numbers to customers*" and not Undertakings who are assigned numbers. (i.e. number blocks from Comreg)



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.

**ANSWER: Viatel suggests that KYC is not mandated but rather an outline of future suggested improvements.**



## 6.6 Future Number Management – Needs and Developments

Related Question

**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.

**ANSWER:** Viatel welcomes any improvement to the current geographic number application process and the possible integration with the INA system especially if this reduces the time between the number application and being live on all networks as is the case now with NGN applications. The current manual process is outdated and often difficult to track/manage etc and any efficiencies here would be helpful.

In relation to STIR/SHAKEN we are following developments with interest and defer to subject experts in the NCIT forum who have had direct experience with the deployment and development of this technology in other jurisdictions. We welcome the continued monitoring of this but agree it should not be considered further at this time based on what we have seen and heard from other NCIT members in the various meetings.

In relation to the proposal that NCIT should progress from static interventions to outsourcing to third party specialist firewall providers – although technically this might be a better solution in the long run this would effectively replace the current interventions which have required a lot of investment by NCIT members in terms of financial/time/resources etc so it would seem this plan is inefficient overall.

## 29 Virgin Media



## **Virgin Media response to:**

ComReg “Consultation on network based interventions to reduce the harm from Nuisance Communications.”

Non-Confidential

31 August 2023



## Introduction

Virgin Media Ireland Limited (“Virgin Media”) welcomes the opportunity to respond to the ComReg document 23/52 “Consultation on network based interventions to reduce the harm from Nuisance Communications.”

This response is non-confidential.

## Executive Summary

Virgin Media strongly supports the aim of ComReg’s consultation document (“the consultation”), which is to reduce as far as possible the impact of scam calls and texts. This is the right thing to do and will be of benefit to a broad set of stakeholders in Ireland.

Virgin Media’s summary views on the ComReg consultation are:

- Several of the proposed interventions have already been discussed in depth at the Nuisance Communications Industry Taskforce (“NCIT”). It is right that industry should proceed with the implementation of these interventions.
- ComReg then goes on to propose several additional interventions. Virgin Media considers that further assessment by industry is needed in relation to these interventions before they are mandated. The NCIT can serve as the body to lead on conducting those further assessments.
- All the interventions need to be fully compliant with relevant data protection legislation ahead of them being mandated by ComReg. This is not presently the case with the “SMS Scam Filter” proposed intervention – the legal issues need to be fully addressed before industry does more work on this proposal.
- The consultation doesn’t at this stage discuss the role of number independent services. This is an omission that needs to be investigated by ComReg. If this gap isn’t addressed, the risk is that scam calls and texts migrate to this environment (with other areas being better protected given the various interventions being taken).

Virgin Media is committed to doing further collaborative work with industry and ComReg, via the NCIT and other bodies as needed, to ensure continued progress in this space in future.

## Virgin Media General Comments on ComReg's proposed interventions

The questions raised in the consultation are quite narrow in nature relating as they do solely to numbering conditions and management.

Virgin Media has a number of comments to make regarding ComReg's proposed interventions and the proposed timing for those interventions, which it sets out below.

As noted above, Virgin Media strongly supports ComReg's overall aim in the consultation – which is to reduce the impact of scam / nuisance calls and texts where possible. Delivering this ambition will be of benefit to a broad set of stakeholders and to the communications industry in Ireland.

Virgin Media has played a constructive role, with other industry players, in improving our understanding of scam calls / texts, along with developing measures to tackle the same. For example, Virgin Media has played an active role in the industry body the NCIT, including helping to design several of the fixed interventions being proposed by ComReg in the consultation.

Virgin Media will continue to play a constructive role through the NCIT, which is doing important work, and which must remain in place for the foreseeable future as there is more to be done. For example, the NCIT can (and should) play a lead role in monitoring the effectiveness of the interventions once implemented, and in specifying if additional interventions are required in future.

ComReg has set out a three-stage approach for assessing potential interventions, which is: (1) providing a description of the proposed intervention including how it would reduce harm; (2) assessing whether the intervention is technically feasible and effective in relation to its intended purpose; and (3) assessing whether the intervention is implementable over a reasonable period.<sup>1</sup> Virgin Media considers that these are sensible high level assessment principles provided that they are applied thoroughly where all relevant information is taken account of.

Having made its assessment, using the principles discussed above, ComReg is proposing several interventions and has also ruled out some other interventions. Virgin Media provides below its high-level comments on each of the interventions considered by ComReg, including those that it is proposing not to implement at this stage.

Taken overall, Virgin Media considers that the interventions that were specified by the NCIT following a period of collaborative discussion, which involved ComReg, are right and that industry should proceed with their implementation. However, ComReg is also proposing in the consultation some additional interventions that have not been subject to the same (if any) level of scrutiny at the NCIT. For these additional proposed interventions Virgin Media considers that these proposals need further consideration – including *inter alia* whether

---

<sup>1</sup> See [Consultation.pdf \(comreg.ie\)](#) paragraph 4.5.

they are necessary, their specification, and the cost / benefit analysis – ahead of them being mandated by ComReg. The NCIT should act as the industry body to conduct such further examination of the new proposed interventions. Virgin Media therefore suggests that for the additional proposed interventions, rather than proposing to mandate them in the consultation, ComReg should instead specify a time-bound period enabling further examination led by the NCIT (and involving ComReg) after which a decision be made of whether the interventions are needed, and if so on what timescales.

### **Preliminary comments on privacy and data protection legislation**

Virgin Media also has some preliminary comments to make regarding the implications of ComReg’s proposed interventions for relevant data protection legislation. These comments apply to all the proposed interventions.

ComReg needs to ensure that all proposed interventions are fully compliant with existing data protection legislation and consulted on with the Data Protection Commission / other relevant statutory bodies as appropriate.

Getting confirmation on this point is needed to ensure that the interventions are technically feasible and can be implemented within a reasonable timescale (i.e. involving parts (2) and (3) of ComReg’s 3-stage assessment approach as discussed above).

As noted in the Telecoms Industry Ireland submission to the ComReg consultation, which Virgin Media endorses, *“It is not appropriate for either ComReg or industry to spend time and resources on proposals with a major privacy component until the legal and regulatory issues have been clarified and fully resolved.”*

### **Voice interventions**

#### **Do not originate (“DNO”) list**

Virgin Media supports the proposed DNO intervention. In Virgin Media’s view, this proposed intervention is likely to assist in reducing harm, is technically feasible and, from Virgin Media’s perspective, is capable of being implemented in a reasonable timescale. This intervention has now been implemented in Virgin Media’s network.

#### **Protected Numbers (“PN”) list**

Virgin Media supports the proposed PN intervention. In Virgin Media’s view, this proposed intervention is likely to assist in reducing harm, is technically feasible and, from Virgin Media’s perspective, is capable of being implemented in a reasonable timescale. This intervention has now been implemented in Virgin Media’s network.

#### **Mobile CLI Call Blocking**

Virgin Media supports phase 1 of the proposed Mobile CLI Call blocking intervention. In Virgin Media’s view, this proposed intervention is likely to assist in reducing harm and is

technically feasible. Virgin Media supports the concept of phase 2 but considers that more thought is needed in specifying the detailed requirements ahead of it being mandated.

Virgin Media has concerns regarding the proposed implementation timeline proposed by ComReg. Specifically, Virgin Media considers that it will not be possible for it to implement all aspects of the phase 1 intervention within 6 months of the Final Statement being published.<sup>2</sup>

These concerns are based on real, practical considerations that are bound up with ✂

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

---

<sup>2</sup> The working assumption is that the Final Statement will be published between end of 2023 – early 2024.

✂ [Redacted] ✂

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### Fixed CLI Call Blocking

Virgin Media supports the proposed Fixed CLI Call Blocking intervention. In Virgin Media's view, this proposed intervention is likely to assist in reducing harm, is technically feasible and, from Virgin Media's perspective, is capable of being implemented in a reasonable timescale. This intervention has now been implemented in Virgin Media's network.

#### Voice Firewall

Virgin Media does not support – at this stage – the proposed Voice Firewall intervention. In Virgin Media's view, the case has not been sufficiently made that this intervention is necessary now, while the implementation of the intervention is also likely to be onerous and costly and could use up resources better deployed delivering other interventions that have better cost-benefit credentials and that will have a greater impact on Nuisance calls in the short-medium term.

Further, Virgin Media considers that the intervention is not currently well defined, and that further consideration on this – which should include an assessment on how other fixed interventions are performing – is needed at an industry level before next steps are proposed. This further discussion could, as noted above, take place at the NCIT.

This is essentially a timing and evidence question – Virgin Media is not definitively rejecting the concept of - at some stage - having an intervention that is dynamic in nature. However, Virgin Media does consider that industry will be better served considering such an intervention after other interventions have been implemented and their effectiveness properly assessed, at which point there should be better evidence showing if an additional

dynamic intervention is required (and if so, of what specification). Better evidence needs to be gathered showing that the other interventions are insufficient in of themselves to address the problems identified and that an additional Voice Firewall intervention (or some other type of additional dynamic intervention) is needed.

Virgin Media considers that by waiting a short time to allow other voice interventions to bed in will enable industry and ComReg to better devise the technical specification of a Voice Firewall intervention, should evidence show that such an intervention was warranted. In this regard, ComReg rightly notes that the Voice Firewall workstream is “*..not as advanced as other proposals discussed in NCIT as part of the NCIT layered approach to implementing interventions.*”<sup>4</sup>

*There is not clear evidence that a Voice Firewall intervention is necessary at this stage*

Virgin Media does not consider that ComReg has presented a clear case that this intervention is required at this stage. Virgin Media is not convinced that this intervention will offer clear benefits above and beyond those already conferred by the other proposed voice interventions in the near term.

ComReg’s rationale for implementing the Voice Firewall intervention now is that the other voice interventions proposed are essentially “static” in nature and will not be well placed to address 3 sources of risk, namely: (1) scam calls that originate in Ireland; (2) spoofed numbers that originate from, or spoof, numbers of a foreign country trusted by Irish consumers such as the UK; and (3) future scams, for example associated with Artificial Intelligence (“AI”).<sup>5</sup>

In relation to item (1) above, Virgin Media is not itself seeing evidence that scam calls that originate in Ireland are either a material issue or increasing at this stage. Our own experience therefore suggests to us this is not a material issue (or set to become a material issue soon). On item (2) above, Virgin Media already has processes in place that we consider can address this issue. For example, under existing fraud management systems, Virgin Media can identify issues with traffic from the UK and intervene with IGOs where necessary to address suspicious / harmful traffic. It is therefore not clear to us that an additional intervention is required at this stage to address this issue. On item (3) Virgin Media agrees that there is a risk of AI driven scams increasing, but for the AI risks on the immediate horizon such as using AI software to spoof voices, it is not clear to us how significant such a risk is, or that a voice firewall as specified would even be effective in combating such an issue. This reinforces the need to further consider the correct specification of the measure given available evidence.

In support of its position that scam calls in Ireland are increasing, ComReg has said, in response to a supplementary question from industry, that “*This view was expressed by An Garda Síochána in a stakeholder meeting with ComReg and Europe Economics which was conducted as part of the many stakeholder interviews that informed the Consultation.*”<sup>6</sup>

---

<sup>4</sup> See [Consultation.pdf \(comreg.ie\)](#) paragraph 4.40.

<sup>5</sup> See [Consultation.pdf \(comreg.ie\)](#) paragraph 5.152.

<sup>6</sup> See [ComReg-2375.pdf](#)

Virgin Media respectfully submits that this is not strong evidence, and would request (again) that ComReg provide further detail as to what evidence there is that such calls are increasing, and if so to what level. There is presently nothing to show empirically that this is happening, or how significant it is. If this evidence is not presently available in a robust form, Virgin Media again suggests that industry will be better served gathering further evidence and looking again when the other voice interventions have been implemented.

*Implementation is likely to be costly and time consuming*

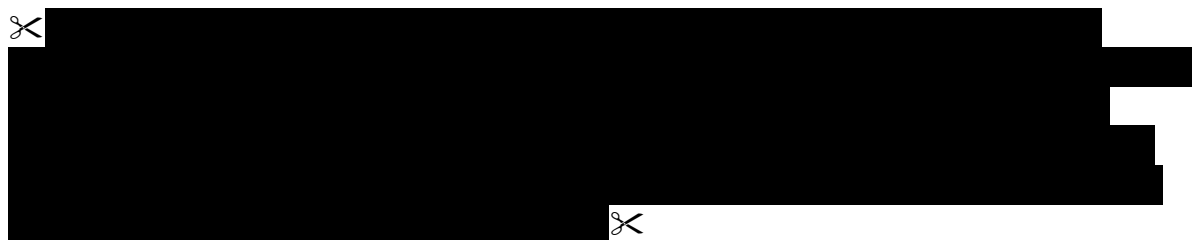
ComReg goes on to argue that Voice Firewall solutions are already readily available in the market and so are likely to be technically feasible to implement and not unduly expensive. In Virgin Media's view, the present Voice Firewall intervention is not well specified, and so it is premature at this stage to refer to other available products that could be purchased "off the shelf" – it is far from clear that such products are needed at this stage, let alone whether they will be effective in addressing issues not already addressed when other fixed interventions have been implemented.

Stir / Shaken

ComReg is not proposing to require implementation of this intervention at this stage. ComReg is right – the available international evidence, which is well summarised in the consultation, shows that there are several dependencies, some rather large and outside of Ireland's agency to control, that would need to be in place for a Stir / Shaken intervention to be effective as a remedy. Industry will therefore be better served at this stage focussing its attention and resources on interventions that we can be confident will deliver benefits in the near to medium term.

Potential SMS interventions

✂



✂

Shortening the chain

ComReg is not proposing to require implementation of this intervention at this stage. ComReg is right – as pointed out in the consultation, the success of this measure is reliant on engagement and action by certain businesses, such as banks, and to date those businesses have shown no interest in taking any requisite actions. Unless and until there is a radical change in this situation, it would therefore be pointless and wasteful for the communications industry to expend resources on developing this intervention.



### Sender ID Registry

ComReg is proposing to require implementation of this intervention between 12-24 months after the Final Statement (depending on whether a partial or full scheme).

Virgin Media considers that this looks like a potentially promising intervention and commends ComReg for the breadth of its international research.

That said, the intervention is quite novel and the ComReg specification currently lacks detail. Virgin Media therefore considers that it would be useful to discuss the specification of this intervention further at an industry level (via NCIT) so that the need, likely effectiveness and implementation requirements can be better understood.

After a preliminary review, it appears to Virgin Media that the effectiveness of this intervention plus the “heavy lifting” within its implementation are very much bound up with getting corporate organisations to adopt the system by making full use of the registry. In other words, to be effective this needs the involvement of third parties in addition to operators and ComReg. Given this, it would be useful to give more thought to how such implementation will be managed, including the role to be played by ComReg in facilitating implementation.

The intervention has, in theory, the potential to be very effective, but only if adopted broadly by corporate third parties – how achievable this is therefore a key question and should help to inform the potential treatment of this intervention. Virgin Media suggests that ComReg engage in further review on this intervention at an industry level, ahead of formalising whether the intervention is needed plus its specification and implementation timelines.

### SMS origination-destination verification

ComReg is not proposing to require implementation of this intervention at this stage. ComReg is right – as pointed out in the consultation, this intervention has not been implemented anywhere globally, and so is a theoretical solution only at this stage. ComReg rightly proposes to continue to monitor this area but take no other action at this point. Virgin Media agrees – the communications industry is best served not expending resources on this, as yet wholly untested, idea at this point in time.

### SMS Scam Filter

ComReg is proposing to require implementation of this intervention, with intervention proposed 1 year after the Final Statement.

In Virgin Media’s view, from a reducing nuisance / scam texts perspective, the approach that would work most effectively would be an all-in based solution. Virgin Media considers that the other approaches would be less ineffective because they would either leave gaps / would enable parties engaged in sending scam texts to simply opt-out.

However, there is also a major legal issue with this proposed intervention which needs to be fully resolved before industry should do any further work on it. Specifically, there is a question about whether implementing an SMS Scam Filter as proposed by ComReg in the consultation would be legal under relevant Data Protection Legislation presently in place in Ireland.

This legal problem is acknowledged by ComReg, with ComReg saying *“It is ComReg’s understanding that a change to current legislation to allow for such scanning is necessary.”*<sup>7</sup>

Presently, the legal issue identified is not resolved, nor is there any certainty that the issue will be resolved. Further, there is not even a timetable setting out when we will know whether the issue can be resolved. In the most recent update, following a supplementary question from industry, ComReg simply said *“Discussions are ongoing between ComReg staff and senior officials from the Department for the Environment, Climate Change and Communications in relation to the request from industry and ComReg for targeted legislation to permit SMS content filtering in the State.”*<sup>8</sup>

It is Virgin Media’s position that no further work should take place on this proposal unless and until the legal issues discussed above are fully resolved. It would not be acceptable for ComReg to direct industry to do further work developing a solution that would in practice be illegal, and so unusable (or where the legal status was seen as high risk / uncertain). As well as being legally questionable (at best), such an approach would also be wasteful. Industry will be better served focussing its energies and resources delivering the proposals already examined in depth at the NCIT.

Virgin Media therefore suggests that industry does not undertake any further work on this intervention until a point when the legal issues have been resolved. If it turns out that the legal issues cannot be resolved (which is a possibility), then the proposed intervention should be formally withdrawn.

## Virgin Media Response to The Consultation Questions

Q1. 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.

Virgin Media has no further comments at this stage.

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

Virgin Media has no further comments at this stage.

<sup>7</sup> See [Consultation.pdf \(comreg.ie\)](#) paragraph 5.297.

<sup>8</sup> See [ComReg-2375.pdf](#) paragraph 2.67.

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

Virgin Media notes that it can only authenticate its directly connected customers. Virgin Media cannot authenticate numbers from other providers or wholesale operators. Consideration therefore needs to be given to how comprehensive authentication will happen.

*Q4. 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.*

Virgin Media has no further comments at this stage.

*Q5. Do you have any views on ComReg's assessment of future number management as described? Please explain the basis for your response in full and provide supporting information.*

Virgin Media has no further comments at this stage.

## 30 Vodafone



Vodafone Response to Consultation

Combating Scam Calls and Texts

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

Public Consultation

Reference: ComReg Doc 23/52

Version: Non-Confidential

Date: 31/08/23

## Introduction

Vodafone welcomes the opportunity to respond to the Commission for Communications Regulation (ComReg)'s consultation on network-based interventions to reduce the harm from Nuisance Communications. The consumer, business and societal harms that arise from nuisance communications require ongoing collaboration by all stakeholders. Vodafone invests significant resource in Ireland and at a group level to combat fraudsters on networks and have fully supported initiatives through the Nuisance Communications Industry taskforce ('NCIT'). At the outset of NCIT in February 2022 there was general acknowledgement of the importance for ComReg and industry to collaborate and identify what could be done to impede the fraudsters that are clearly causing serious financial and emotional harm to consumers and who are damaging Irish business and public services.

### **Vodafone has demonstrated its commitment to addressing such harms.**

This was evidenced long before the level of nuisance communications escalated in recent years when Vodafone took action to combat compliance for premium rate services through the imposition of restrictions to address poor practice. The outcomes for Irish consumers are positive demonstrated by level of complaints going in to ComReg from Vodafone customers regarding premium services. Vodafone is also fully committed to the Nuisance Communications Industry Taskforce. The taskforce has already delivered results and the solution roadmap agreed in the forum is expected to have significant further impact.

### **The existing action plan must remain the priority focus.**

Vodafone are actively participating in all NCIT workstreams and was one of the first operators to run the initial trials to test and implement Do Not Originate "DNO" and Protected Numbers lists. This initiative has prevented millions of potential scam calls reaching Irish consumers. Vodafone also implemented Fixed CLI blocking on its network and calls are now being blocked, and further developments are planned. Further enhancements on Mobile CLI Roamer check and SMS workstreams are also ongoing.

This consultation now proposes to put the defined NCIT initiatives on a legislative footing. This will make the requirements clear to all current and future market participants. It will also provide an end date for activation of measures. The need to address the harms is the priority for all and the solution design, resource allocation and deliverable dates have been a point of considerable debate within the NCIT and in bilateral discussions with ComReg. This level of tension within the NCIT is understandable, nonetheless the direction of travel for the NCIT initiatives is clear and results are being realised. The challenge arising relates to the some of the additional resource intensive and more complex solutions that are now being proposed.

### **Too many complex initiatives will divert important resource**

Vodafone believe the introduction, via Decision, of new and as yet undefined, somewhat conceptual, complex solutions such as the Voice Firewall and Mobile CLI proxy server are unjustified and will only serve to divert attention from the already ambitious NCIT programme. The primary concern now arising from this consultation is that ComReg propose to put obligations in place for operators to implement additional complex solutions and specifications and in particular the Voice Firewall and Mobile Proxy Server proposals.

### **Sender ID may be the exception.**

When looking at new proposals the Sender ID proposals warrant further discussion to ensure advancement of the SMS workstream. Several actions already developed and agreed at the NCIT have progressed. There has been considerable resource allocated to SMS controls and ComReg and industry have attempted to address SMS scams in the absence of a legislative framework that facilitates advanced network A2P filtering capabilities. The shorten the chain initiatives have proven challenging however it is acknowledged the latest

proposal from ComReg on Sender ID may have the potential to address challenges. Vodafone highlight below some of the complexities that arise around Sender ID however it does make sense to have a more focused evaluation of this proposal through NCIT following closure of the consultation commentary period. We would urge ComReg to hold on a formal decision until the end-to-end process is clearly defined.

#### **ComReg need to prioritise demand.**

ComReg, in collaboration with the NCIT, must choose the priority project to implement. The situation is that the capex resource to meet obligations on regulation related initiatives is already over allocated.

- The delayed spectrum auction completed in 2023 means capex is urgently being channelled towards meeting the rollout obligations for 5G services. This is also consistent with ensuring Ireland can meet its national Digital targets.
- In addition important cross industry projects are also in progress or commencing including initiatives on Internet Access Switching system implementation and support for government initiatives on Public Alert messaging.
- Added to this the forthcoming Electronic Communications Security Measures ECSMs will also place considerable demands on the industry and some of these measures have potential crossover with proposals from ComReg in this consultation.

#### **There are limits to the demand/resource capacity.**

The programmes which are now being actioned require specialist technical network skills and demand for such resource is carefully managed. To do thorough scoping, requirements gathering, and solution design also requires access to limited project and IT resource. At the same time the IT and networks teams are also running many programmes in parallel to rollout network, maintain network quality, to ensure continuity of operations, to serve our customers and to develop the solutions that customers need. This does not mean the NCIT workstreams have not been prioritised – these projects all have high priority. The fundamental issue is that the programme once agreed needs to be implemented and evaluated and it is not possible to continue to implement 'potential' solutions on a rolling basis as seems to be the aspiration with some of the proposals in this paper. The rationale is understood but the approach needs to be less specific i.e. hold on implementing requirements (Firewall and Proxy Server) by legal decision until there is an understanding of the impacts on measures being implemented.

#### **It goes without saying that in addition to resource constraints – capex is a factor in the telecoms sector.**

It is acknowledged that the telco sector is challenged in Ireland and across Europe. Since 2015 we have lost almost 40% of our share price as an industry. Large EU telcos have lost EUR 23bn in equity value just over the last 12 months. Our ROCE is well below the cost of capital and even negative in some markets across Europe. ComReg point to operator revenue as the indicator of the low impact on operators when the reality is the true measure of impact is profitability. In addition investment challenges are magnified at the peak of the current 5G and fibre investment cycle. This cannot be discounted as part of the ComReg Regulatory Impact Assessment of the measures proposed in this consultation.

A broader range of non-telco technology company, business stakeholders and policy makers have a part to play in the collective effort to address nuisance communication. Nonetheless the telecoms sector has put solid NCIT plans into action and has also sought legislative change to support future SMS initiatives. The measures that are being actioned will deliver results however a collective stakeholder response will be required moving forward.

The responses to the specific questions raised in the consultation are set out below.

The broader comments including the general points above and commentary on specific initiatives are also put forward for consideration by ComReg as part of this process. The summary of the Vodafone position is as follows:

#### SUMMARY OF POSITION

- Vodafone support implementation of the NCIT initiatives as developed through NCIT.
- The priorities should be
  - Voice – the implementation of the current NCIT Fixed and Mobile CLI programme
  - SMS – to progress on ComRegs proposal on Sender ID registration.
- ComReg’s proposal on Sender ID warrants further investigation. This should be prioritised for NCIT to clearly define the process and set a realistic implementation timeframe. We would recommend this is now prioritised to inform any potential ComReg Decision timeframes.
- It is important ComReg take account of actual lead times communicated via the NCIT and bilateral meetings when setting any formal Decision.
- It is not appropriate to set further measures by ComReg Decision at this time including proposals on Voice Firewall and the Mobile CLI proxy server at least until existing measures are fully implemented and assessed.
- In addition Vodafone would urge ComReg to complete appropriate privacy level assessments of all initiatives in particular those where sharing of roaming location is being directed.



## PROPOSALS TO IMPLEMENT A VOICE FIREWALL

Vodafone engaged local and group experts on the Voice Firewall technical specification as proposed. The general view was that more detail needs to be provided. This concept of a Voice Firewall has been referred to at a very high level in NCIT however it has not been part of the implementation plan. The technical specification is not sufficiently detailed to understand what ComReg have costed. In addition there has been no engagement in relation to operator implementation and operational maintenance and support costs for any voice firewall solution.

Vodafone will engage in further discussion through NCIT on future advanced initiatives incremental to the programme of work that has been established. We expect over the next year that more centralised solutions will become available as all countries in Europe are impacted and given Irelands scale it would be more efficient to invest in central solutions rather than individually replicate solutions rolled out in larger EU countries. Our view is that ComReg must prioritise the key workstreams and assess effectiveness before imposing additional requirements. More complex programmes will only divert attention at this critical time in the NCIT work programme.

It is also not appropriate at this point to impose Voice Firewall requirements via formal ComReg Decision without having assessed the full impact of industry resourced and funded initiatives to date; without consideration of centralised, group or industry solutions and without having engaged operators directly or as a taskforce on impacts assessment. It is also worth noting that further legislation around Electronic Communications Security Measures is pending which includes individual workstreams to ensure security of networks (including signalling) all of which will require significant parallel commitment from industry and potentially crossover with what ComReg is suggesting is now required in NCIT. The list of potential solutions that 'could' be effective to address nuisance communications is long however there must now be prioritisation.

## PROPOSALS TO EXTEND MOBILE CLI REQUIREMENTS

Vodafone have commenced implementation of mobile CLI blocking on a voluntary basis as we believe it will provide an important protection for consumers. This has been prioritised on the Vodafone 2023 IT and networks capital programme and resources are allocated. ComReg are now putting the NCIT programme on a legislative basis. The timelines proposed remain extremely challenging. Vodafone has communicated clear timelines to ComReg for delivery of this programme and we would urge ComReg to reflect the realistic timelines in their formal decision. The programme has commenced, it has a defined vendor development timeframe which is then followed by operator implementation on the network with testing.

This programme has remained a consistent point of debate within NCIT, in particular around the initial timeline which all operators have advised was not possible. Nonetheless the direction of travel is clear to all. Vodafone is of the view that the programme as agreed should now have a priority focus. Vodafone would strongly urge ComReg to avoid placing additional new demand into the programme through formal decisions on other voice requirements. The plan should be to implement and evaluate the effectiveness of the measure. It is important to note:

- **VoLTE roaming requirements may not be needed.** Many operators are expected to implement home routing for VoLTE roaming and as a result MO calls will be originated from the home network and Roamer check will not be required.

- **The proxy server proposal** is a new proposal and has not been discussed to date in NCIT. It is not appropriate to formalise such a requirement via a Decision instrument at this time. The proposal on a proxy server is complex to implement. The technical implementation aside, it raises important the questions regarding centralised industry ownership, service management and accountability. It would require central project management to implement from ComReg. It is also highly likely that it may not be required with the evolution of VoLTE home routing negating the need for roamer check.

The only focus at this time should be on the Phase 1 implementation. As stated above the NCIT has set the priorities for implementation and the focus should now be on completing those objectives rather than introducing further new discussion that will divert resource from the main programme.

### PROPOSALS ON SENDER ID

The functional requirement for Sender ID (SMS Sender ID Registry Functional Spec V1.0) is a new specification that has not been considered by the NCIT. It has been signalled by ComReg and some of the detail is now provided and we welcome this detail. The logic for the ComReg proposal is clear.

The proposal for new full SMS Sender ID registration scheme requires the Sender ID owner to register their Sender ID with ComReg. There is a broad range of companies using Sender ID including banks, credit unions, doctors, medical centres, dentists, delivery companies (parcels, home heating, food etc) retail outlets and veterinary services. Under the proposed approach all such companies would need to become aware of the new requirement make arrangements to register their Sender ID and this can then can only be sent by a participating aggregator.

The proposal where the Sender ID is not registered that there would be an initial phase where the Sender ID would be modified and presented as “likelyscam”. In the subsequent phase the message will be blocked and will not be delivered to the targeted individual. The requirement also prohibits Irish operators from delivering messages routed via the so-called ‘grey routes’.

Vodafone have developed a technology plan to support Sender ID and we have also engaged proactively with ComReg to try to advance on shorten the chain initiatives. ComReg had flagged to NCIT that it was assessing this other option around Sender ID registry and the proposed approach now is to focus on this initiative. In paragraph 4.76 ComReg state the costs of setting up and running the Sender ID registry are non-trivial – this also applies for an MNO and it is fair to say it would also apply to participating aggregators.

Flexibility is needed on dates as there is a design process that needs to be discussed and finalised at industry level and the lead times as prescribed are overly ambitious. Vodafone would strongly urge ComReg to engage now to agree the end-to-end project implementation plan. Ideally this would become the priority SMS initiative for NCIT.

Vodafone consider this proposal from ComReg is pragmatic however the set-up process will not be without complexity which in our view is best addressed via broader industry operational engagement. It is not appropriate, in our view, to prescribe a definitive date via Decision now in the absence of further detailed operational engagement. A 12-month date for implementation from the Decision date, in the absence of a defined and clear end to end solution will result in a less than ideal solution and will have impacts on the wider business community. We acknowledge there must be a balance and some targets are required. Vodafone would propose therefore that Sender ID Registry becomes the priority next SMS project for NCIT,

and all resource is now committed to defining, designing, and planning this project so we can set a clear implementation date.

Several considerations arise in relation to ComReg proposals

1. **The number of Sender IDs active:** Vodafone note the Singapore model on which ComReg has based its proposal was applied to 2000<sup>1</sup> Sender IDs. It is likely in Ireland that many more corporate and smaller to medium enterprises would be in scope. The end-to-end process from registration with ComReg through to network activation has not been discussed at this stage. This solution constitutes a fundamental overhaul of the operation of the current market arrangements whereby end-customers (the message senders) first need to understand the process, then engage with a participating aggregator and adjust their own internal operational processes to ensure their messages are not blocked.
2. **Transition Phase:** ComReg are proposing a transition phase to apply 12 months from date of publication of a final decision. During the transition phase from month 12 the proposal is that a mobile operator would Modify the Sender ID. Modify is defined in the draft Decision instrument as meaning that the Sender ID is replaced with “LikelyScam”. The NCIT working group undertook a detailed assessment of the legal basis for filtering action on messages. Vodafone would seek confirmation that a detailed assessment of this proposal has included checks against key pieces of Irish law that regulate the permissibility (or otherwise) of filtering interventions including the Postal and Telecommunications Services Act, 1983 (1983 Act), the Interception of Postal Packets and Telecommunications Messages (Regulation) Act and European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (2011 Regulations). It should be noted, looking at the technology roadmap that modification capability is a feature of filtering solutions which, do not currently have legal basis in Ireland.
3. **The project plan:** As outlined above Vodafone have designed its technology roadmap to ensure it has the capability to support Sender ID initiatives through NCIT. The proposal is for ComReg to develop a web portal that distributes information to aggregators and networks upon registration of a new Sender ID. The workings of that process require very clear definition. This enables the networks and IT teams to assess the solution design and predict the resource demand, cost, and timelines. The Sender ID proposal while conceptually clear is missing the detail and it is likely all would agree that further engagement is required, ideally through NCIT to develop the end-to-end solution. This will help operators to dimension their own end solution. The participating aggregators would also need to be involved in this workstream. The scope of the detailed design needs to be clear on
  - a. The overall architecture and comms flow
  - b. The hosting of the central list/database of permitted sender IDs
  - c. The updates/integration process and what level of automation is possible
  - d. Connectivity requirements
  - e. SLAs for update of lists and troubleshooting processes
4. **The operational model:** If this proposal is to progress then the NCIT also need to engage on operational process design. This will include

---

<sup>1</sup> [Almost 2,000 organisations registered with SMS registry that will roll out 'likely scam' alerts from Jan 31 | The Straits Times](#)

- a. clarity on how, operators and aggregators direct Sender ID customers through the process in a consistent and clear way.
- b. how to decide on allocation rules, copyright, aging of Sender IDs etc
- c. how to resolve queries, complaints, and disputes

## Consultation Questions

**Question 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.**

The question relates to specific changes in the numbering conditions.

**Assigned number:** Vodafone agree that clarity on use of the number is important. ComReg need to ensure that important customer use cases are not unintentionally restricted. As set out in the ComReg paper large companies operating call centres will choose a CLI for their outbound calls so that the telephone number used enhances the ability of the call recipient to identify the company.

A customer, in this case the large company, will often be assigned multiple numbers across several operators. For business operations the customer will choose which assigned numbers to present. For example where a customer is assigned a block of numbers from Operator A and a block from Operator B, the customer may use Operator A to originate calls and for operational reasons chooses to present CLIs it is assigned through Operator B. Operator A will need to satisfy itself that the numbers are validly assigned however this is a valid and required customer application.

**Do Not Originate and Protected Numbers:** Vodafone are supporting DNO and Protected number lists and have no comments in relation to changes to numbering conditions regarding updates to the numbering conditions.

**Fixed CLI Blocking:** Vodafone have implemented Fixed CLI blocking on its network and calls are now being blocked. Further enhancements are also in development. Paragraph 6.17(ii) sets out proposed text for Long-Lining:

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

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

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

**Sender ID number updates text changes:** Please note comments above in relation to Sender ID and Vodafone suggestions on implementation. In relation to the text in the numbering conventions further considerations are necessary on particular aspects.

- Par 6.35 sets a 3-month deadline which could be amended with ComReg consent. Vodafone suggest it may be clarified what is meant by activated. Some Sender IDs may be configured on the PA and may lie dormant and will only be used as needed if for example a service issue or other unexpected event occurs that requires a communication.

- Par 6.38 proposes that Sender ID's will be allocated on a "first come, first served" basis. There will be challenges around ownership of specific Sender ID as and ComReg will need to have provisions in place to avoid hoarding or potential misrepresentation or misleading allocations. This will need to be clarified as part of the operational process. Text is proposed in Par 6.40 (a)(iii) however more detail is required.

**Question 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.**

The general updates relate to CLI Conditions for geographic numbers non-geographic numbers (NGN); 1800 freephone; and emergency numbers.

- **Physical Location Condition:** ComReg notes that the physical location condition remains an essential tool in combatting nuisance communications. It is important to note there are some important use cases where customers require calls that originate outside the MNA (the physical location) to present the geographic number from that MNA. For example a remote worker for a company in Dublin, residing in Meath will make a call on the company network and present the company 01 number as opposed to an 041 number when originating calls. The CLI presented by the remote worker is appropriate to the physical location/ MNA of the company. This is very similar to the permitted use case for international offices who long line. It is not clear however if this use case is constrained when referring to Par 6.77(ii) of the consultation. This may not be ComReg's intention as it would unfairly constrain innovation in business unified comms within the regulated sector. The numbering conditions need to take account of developing legitimate use cases. As more companies start to look at breakout using unified comms such as teams and other solutions key workers will need to present their company DDI while working remotely.

**Question 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.**

Please refer to comments on Physical location above.

**Question 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.**

**Sub-Allocation:** The position outlined by ComReg in Figure 40 and in Par 6.101 and the applicability to reseller type arrangements warrants clarification. This also applies to the text in Par 6.105

(2) Undertakings are obliged to only use their assigned numbers for their own end-users. Sub-assignment to other undertakings is not permitted.

This has not been discussed to date. Vodafone request ComReg to clarify proposals for all the existing scenarios where an operator resells other operator services or virtual operators exist on a network using a sub-range of the network operator's allocation.

In addition the approach on sub-allocation requires engagement of subject matter experts across industry to avoid any unintended consequences. Vodafone would propose re-establishment of the Numbering Advisory Panel (NAP) as an appropriate forum to further discuss. We also note there are learnings from other Vodafone markets. For example in Portugal sub-allocation is possible where a contract is agreed between the assignee and the sub-assignee.<sup>1</sup>

**KYC Guidelines:** Vodafone agrees with ComReg's views regarding the approach for Pay as you go SIM registration. It is pragmatic to assess the impacts of the current NCIT work programme before imposing further levels of process and system change that would essentially amount to a complete overhaul the Pay as you go customer journey. Unintended consequences would also need to be considered. For example, a simple fact is that Pay as you go services are very popular with many consumers as gifts where the purchaser will not be the end-user.

It is appropriate to collect customer details and other company information such as a company's Irish CRO number, Revenue VAT, or business number, as required by the proposed amendments in Sections 4.3 and 4.4 of the numbering conditions. However we consider it disproportionate to require some of the other detail set out in the proposed KYC guidelines. Several the categories of data may be considered intrusive and impose an unnecessary obstacle to commercial engagement. This includes the nature of business, existing phone numbers and business websites, contact details of the senior manager with responsibility for numbering, information about the business customers network and services provided, volume of number requests versus intended use of numbers. Clearly when large amounts of numbers are sought further detail can be obtained but as a norm this would not be appropriate.

Vodafone already collect considerable data that is necessary when allocating services/numbers to business customers and to other bill pay customers. As above certain details are not practical to require and moreover will be considered as unnecessary by customers requesting number allocations. It is important to note also that checks are in place to prevent fraudulent activity for new service applications. Vodafone also have ongoing processes in place to manage anomalous and potentially fraudulent usage on the network.

In paragraph 6.130 ComReg are stating an intention to audit KYC processes. This seems quite interventionist in terms of a ComReg 'guideline'. As part of this process ComReg should provide clarity on the basis for audit in respect of guidelines issued.

In paragraph 6.127 (Operators) should also provide support and information to any affected customers, cooperate with ComReg, other regulators, law enforcement and other relevant organisations. Vodafone will always cooperate fully to resolve incidents affecting our customers.

Paragraph 6.128 states where 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.

---

<sup>1</sup> [ANACOM 2021 decision on sub-allocation of numbers](#)

This reporting obligation requires definitive reporting thresholds such as those provided for network security and integrity reporting. The terms “significant” and “timely or appropriate” are important as are how an operator would submit any report.

**Question 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.**

Vodafone agree the ever-evolving threat requires ongoing collaboration and engagement across industry and across the broader stakeholders to ensure Irish consumers and business are protected from evolving scams. This telecoms industry in Ireland has engaged on the current challenge through the NCIT taskforce however broader collaboration will be required as scams become more sophisticated and move away from traditional voice and SMS on to other applications including OTT services.

The current approach through the NCIT has required significant investment and resource commitment from several telecommunications operators in particular those investing in Fixed & Mobile CLI blocking and Sender ID filtering. Multiple operators are rolling out separate solutions to support the programme. The understandable priority has been to address the immediate harm and Vodafone is of the view that the programmes set out at NCIT should have the fullest priority. This will ensure Ireland locks down calls using Irish CLI from international locations and place controls on SMS.

Additional highly complex and resource intensive initiatives, such as the proxy server and the voice firewall will only service to derail the focus at this time. There may well be synergies that can be realised through, for example, centralised group solutions, through a common approach at EU level, through programmes of work on signalling that will be actioned through the ECSM workstream and through more centralised industry collaboration in Ireland.

**ENDS**



## 31 XConnect

## Response to ComReg’s consultation - Combatting scam calls and texts (ComReg 23/52). Consultation on network-based interventions to reduce the harm from Nuisance Communications.

XConnect welcomes the opportunity to respond to this consultation. We support the proposals as set out by ComReg and the open approach to understanding the various steps which can be taken towards implementing authentication and validation of call traffic and messages in Ireland.

### Introduction to XConnect

XConnect<sup>1</sup> provides a trusted global registry of network and subscriber information, based on privacy compliant phone number data, including global number portability, global number ranges/prefixes and mobile phone subscriber status.

Established in the UK in 2005, XConnect delivers mission critical carrier-grade numbering information services to over 200 operators globally, including MNOs, business messaging (“A2P”) hubs, aggregators, carriers and interconnect providers. XConnect is an ISO 27001 certified company and annually processes nearly 50bn queries.

Our number information services are used for voice and message routing, fraud protection, phone number validation as well as fraud mitigation and risk scoring. XConnect also supports the deployment and evolution of next-generation communications, such as VoLTE<sup>2</sup> and RCS<sup>3</sup>. Our Number Information Services<sup>4</sup> are accessed through our global distributed hybrid cloud platform using simple, secure, scalable real-time protocols and APIs.

In 2020, XConnect was acquired by Somos, Inc., a USA-based company providing number information and services to over 1,400 organisations, and the trusted USA telecom sector administrator for over 3 billion numbers throughout the USA and North America. Somos helps to enable seamless communications between enterprises and consumers through the management of the USA regulatory agency’s (“FCC”) mandated databases including North American Numbering Plan (“NANP”), Toll-Free Number Administrator (“TFNA”) and the Reassigned Numbers Database (“RND”). In addition, Somos administers the USA’s largest Do Not Originate (“DNO”) list.

### Comments on Current Regulations

The checks which have recently come into force in Ireland must be the basic minimum treatment that the number being used is validated against. In addition to these steps, we strongly recommend international validation be carried out against Global Number Plans, according to publicly available information from NRAs. This information is also commercially available from a number of providers, such as XConnect, and can be easily enabled, therefore providing cost effective support to all parts of the value chain in order to block unsolicited calls and texts.

### DNO List

We fully support the steps taken to date by ComReg to utilise this information and would urge ComReg to expand the list to include mobile numbers including [REDACTED]

<sup>1</sup>About Xconnect: <https://www.xconnect.net/about-xconnect/>

<sup>2</sup>VoLTE - Voice over Long-Term Evolution (VoLTE) is LTE high-speed wireless communication standard for mobile phones and data terminals.

<sup>3</sup>RCS - Rich Communication Services protocol is designed as a modern take on texting that rolls features from Facebook Messenger, iMessage, and WhatsApp into one platform.

<sup>4</sup>About XConnect Number Information Services: <https://www.xconnect.net/services>

<sup>5</sup>MSNRs, Mobile Station Roaming Number, used by mobile operators to facilitate roaming services.

<sup>6</sup>Global Title, (GT) is an address used for routing messages within Signalling System Number 7 (SS7)

[REDACTED]

In the USA, the Somos DNO database includes approximately 3.2m numbers provided by enterprise and end-users (manual number sets which are provided directly by end-users) which are registered as Do-Not-Originate. As we understand it, ComReg has not limited the numbers which can be submitted to the DNO list to any particular subset. We would suggest, however, that the DNO could be substantially more effective if the list included a broader set of information. For example, it could include Government departments, old banking numbers and Communications Providers unallocated numbers or numbers only allocated for internal use. In the USA, conferencing and numbers used for internet advertising which are in-bound only take advantage of DNO.

### **Enabling Controlled Access**

In reviewing the DNO Guidance<sup>7</sup>, we note that ComReg instructs operators to use the DNO list and ComReg does not, as such, restrict access to the DNO list to operators only. However, the guidance is not clear in terms of which parties beyond operators should have access to the DNO list. We respectfully urge ComReg to allow both international operators and approved providers of Numbering Information Services (“NIS”) access to the DNO list to enable information to be more broadly implemented and utilised.

Companies such as XConnect and others, who provide Numbering Information Services, enable both voice and messaging operators efficient and simple access to global routing and validation data sets to identify spamming and spoofing. These services bring together numbering information from number plans from around the world, DNO data sets and information from the fraud industry into one easily accessible aggregated data set.

We note that in October 2022, ComReg<sup>8</sup> met with the Canadian, Australian, Hong Kong and USA NRAs to discuss international collaboration with respect to nuisance calls and we believe broadening access to the DNO information will support this global approach to blocking unsolicited calls at source.

As referenced in our introduction, XConnect is part of Somos Inc., who in 2018 were awarded the contracts to serve as the North American Numbering Plan Administrator (NANPA) and Pooling Administrator (PA) including the Routing Number Administrator (RNA), by the FCC. [REDACTED]

<sup>7</sup> <https://www.comreg.ie/publication/do-not-originate-list-guidance-note-for-organisations-and-application-form>

<sup>8</sup> <https://www.comreg.ie/comreg-engages-in-international-forum-to-combat-nuisance-communications/>

<sup>9</sup> Analytics providers, similar to Number Information providers, provide adjunct services to support CPs with other, such as, monitoring information, for example, answer seizure rates, drive Least Cost Routing and other cost efficiencies.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Recognising there are a number of providers enabling fraud protection services today, we propose that ComReg develops legislation to allow fair, open, controlled access to the DNO data set.

### Conclusion

XConnect fully supports ComReg's proposed approach and urges ComReg to consider our suggestion for a wider use of the DNO list by allowing approved, legitimate, and trustworthy third parties access to the DNO.

## Annex 1

### **XConnect achieves recertification for ISO 27001 in 2023**

XConnect has successfully been recertified to ISO/IEC 27001, the globally recognised gold standard for Information Security Management Systems, by independent auditors accredited by the ANAB Management Systems Certification Body, the largest accreditation body in North America and serving more than 75 countries.

XConnect is committed to having security at the heart of its everyday working practices and, as well as this certification, it's a founding signatory of the Mobile Ecosystem Forum's A2P SMS Code of Conduct, Trust in Enterprise Messaging (TEM).

The ISO 27001 certificate is critical when partnering with Mobile Network Operators, Carrier and Messaging providers to manage sensitive network and subscriber information, especially for information subject to new data protection regulations. As XConnect expands its fraud, risk and advanced routing services to its global telecoms and identity customers, it is increasingly managing sensitive data with additional privacy and security requirements.

#### **About ISO27001:**

ISO/IEC 27001 is the world's best-known standard for information security management systems (ISMS). It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

With cyber-crime on the rise and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risks. ISO/IEC 27001 helps organisations become risk-aware and proactively identify and address weaknesses.

ISO/IEC 27001 promotes a holistic approach to information security: vetting people, policies and technology. An information security management system implemented according to this standard is a tool for risk management, cyber-resilience and operational excellence.