

# **Summary of the BEREC Stakeholder Workshop on Combating Fraud**

---

21 May 2026

1 October 2026

## Contents

|                                                                                                                                                                      |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Introduction and Aim of the Workshop .....</b>                                                                                                                 | <b>2</b>  |
| <b>2. Opening of the Workshop and Keynote Speeches .....</b>                                                                                                         | <b>3</b>  |
| 2.1. Martin KÄHL, Specialist at 'Expertise and Stakeholder Management Unit' - European Union Agency for Law Enforcement Cooperation (Europol) .....                  | 3         |
| 2.2. Gyula BARA, Project Leader in the Unit 'Electronic Communications Policy, Implementation and Enforcement' - DG CNECT, European Commission .....                 | 4         |
| 2.3. Sharon BRENNAN, Manager of Network Trust, Commission for Communications Regulation Ireland (ComReg) .....                                                       | 5         |
| <b>3. Panel 1: Global Regulatory Best Practices .....</b>                                                                                                            | <b>7</b>  |
| 3.1. Eduard BARTHOLME, Bureau Chief Consumer & Governmental Affairs - Federal Communications Commission (FCC), United States of America (USA) .....                  | 7         |
| 3.2. Javier GUTIÉRREZ AFANADOR, Communications Commissioner - Communications Regulatory Commission (CRC), Colombia .....                                             | 7         |
| 3.3. Sanjay KUMAR, Joint Advisor - Telecom Regulatory Authority of India (TRAI), India.....                                                                          | 8         |
| 3.4. Will PINKNEY, Principal Infrastructure and Communications Group and Programme Director for Ofcom's Scams Programme - Office of Communications (Ofcom), UK ..... | 9         |
| 3.5. Freddie MCBRIDE, Chair of Working Group NaN (WG NaN) - ComReg, Ireland .....                                                                                    | 10        |
| <b>4. Panel 2: Industry Solutions.....</b>                                                                                                                           | <b>12</b> |
| 4.1. Lorik SEKIRAKA, Senior Counsel, Government, Policy & Regulatory Affairs, EMEA, Twilio Inc.....                                                                  | 12        |
| 4.2. Antongiulio LOMBARDI, Regulatory Affairs Director Giovanni BROCCATELLI, Head of Core and Beyond the Core regulated Markets, Wind Tre S.p.A. ....                | 13        |
| 4.3. Justen DAVIS, Senior Director Industry Relations and Global Public Policy, SOMOS Inc.....                                                                       | 14        |
| 4.4. Arturs ALKSNIS, Vice President - Public Policy, Proximus Global.....                                                                                            | 15        |
| 4.5. Haude LANNON, Policy Director, GSM Association (GSMA) .....                                                                                                     | 16        |
| <b>5. Main takeaways.....</b>                                                                                                                                        | <b>18</b> |
| <b>Annex .....</b>                                                                                                                                                   | <b>20</b> |

## 1. Introduction and Aim of the Workshop

On 21 May 2026, BEREC held an external stakeholder workshop on combating fraud, organised by the BEREC Cybersecurity and Resilience Working Group and co-chaired by Katja Kmet Vrčko (AKOS, Slovenia) and Zdravko Jukić (HAKOM, Croatia). The workshop brought together BEREC members, other relevant national authorities, electronic communications networks and services providers, equipment, technology and solution vendors, as well as representatives of key European and international institutions, including the European Commission, Europol and competent authorities from Colombia, India, the United Kingdom and the United States of America, to exchange views on the growing threat of fraud in the electronic communications sector.

The workshop took place against the background of a rapidly evolving fraud landscape, in which the increasing digitalisation of services has been accompanied by a significant rise in fraudulent activities targeting end users across the European Union. In particular, smishing and vishing have become increasingly prevalent, while malicious actors continue to adapt their methods and exploit both communications networks and digital services. Against this backdrop, the workshop marked an important step in BEREC's work to assess the current state of fraud in the electronic communications sector, identify key trends, and determine the most pressing challenges requiring coordinated action.

Structured around two panels, the workshop examined both global regulatory best practices and industry solutions. The discussions provided valuable insights into existing regulatory frameworks, technical and operational measures, and the need for stronger cooperation across sectors and across borders. The outcomes of the workshop will feed into BEREC's forthcoming analytical work in this area and are expected to provide a foundation for the preparation of a possible best practices report on combating fraud in 2027, in cooperation with the European Union Agency for Cybersecurity (ENISA), Europol, and other relevant partners from both the public and private sectors.

## 2. Opening of the Workshop and Keynote Speeches

In his welcome address, BEREC Chair 2026 Marko Mišmaš underlined that, while digital communications are a critical infrastructure for society and the economy, rapid digitalisation has also been accompanied by a significant increase in fraud targeting end users. He noted that smishing is only one element of a broader and rapidly evolving fraud landscape and highlighted that BEREC needs to widen its focus to other forms of fraud affecting electronic communications networks and services. He emphasised that the workshop was an important step in helping BEREC better understand the challenges and possible responses, and stressed the need for coordinated action across borders, sectors and institutions.

### **2.1. Martin KÄHL, Specialist at ‘Expertise and Stakeholder Management Unit’ - European Union Agency for Law Enforcement Cooperation (Europol)**

The presentation delivered by Mr. Martin Kahl, representing Europol and the European Cybercrime Centre (EC3), focused on the European anti-spoofing initiative and the development of a coordinated international approach to combating fraud in electronic communications.

The main focus of the presentation was the challenge faced by law enforcement authorities in investigating and prosecuting spoofing-related fraud. Although spoofing is relatively easy to deploy from a technical perspective, tracing fraudulent calls and identifying perpetrators remains extremely difficult, particularly due to the cross-border nature of telecommunications and the limited availability of relevant operational data. In response to these challenges, Europol launched a strategic initiative dedicated to caller ID spoofing, including the publication of a position paper outlining the scale of the threat, possible regulatory and technical responses, pilot projects on cross-border traceback mechanisms and call validation models, and the stakeholders that should be involved in future solutions.

The speaker also presented the role of European Multidisciplinary Platform Against Criminal Threats (EMPACT), which serves both as a cooperation framework and a funding mechanism for joint operational activities involving law enforcement agencies, regulators, and industry stakeholders. Another important aspect of the presentation concerned cooperation with international standardization bodies and regulatory authorities.

Europol is currently working together with the European Telecommunications Standards Institute (ETSI), Office of Communications (Ofcom, UK), BEREC and the Federal Communications Commission (FCC, USA) on the development of technical recommendations and traceback-related standards, that consist in identifying and tracing the origin and route of fraudulent communications, especially spoofed calls or scam messages, across networks and across countries.

The presentation also highlighted the importance of aligning European initiatives with broader global efforts, including cooperation with the Global Informal Regulatory Antifraud Forum (GIRAF) and FCC-led international taskforces, to avoid fragmentation and duplication of standards and regulatory approaches.

Overall, the presentation demonstrated that caller ID spoofing has evolved into a major global cybersecurity and trust challenge affecting both telecommunications infrastructures and end users. Europol stressed that effective mitigation would require a combination of technical standards, regulatory convergence, cross-border cooperation, and stronger collaboration between law enforcement authorities, regulators, standardization bodies, and industry stakeholders. The intervention provided a comprehensive overview of the ongoing European efforts to establish coordinated and scalable anti-spoofing mechanisms at both European and international level.

#### **Key messages:**

Europol highlighted caller ID spoofing as a major enabler of fraud and stressed the need for coordinated international action.

Effective mitigation requires stronger cooperation between law enforcement authorities, regulators, standardization bodies and industry stakeholders, supported by amending the current ETSI technical specification and approving new common technical standards and cross-border frameworks.

## **2.2. Gyula BARA, Project Leader in the Unit ‘Electronic Communications Policy, Implementation and Enforcement’ - DG CNECT, European Commission**

In his opening remarks, Mr. Gyula Bara expressed his satisfaction that BEREC is addressing the topic of fraud from both end-user protection and a cybersecurity perspective. He noted that the workshop was highly timely for three main reasons: the persistence and duration of fraud, the continuous technological evolution of fraudulent schemes, and the ongoing negotiations regarding the draft Regulation for the *Digital Networks Act* (DNA) proposal published in January 2026.

He highlighted that the DNA provides a specific framework to combat fraud, particularly through Article 103, which, among other things, assigns a crucial role to BEREC. He observed that while various Member States have implemented national measures to address specific fraud techniques – such as those relying on CLI spoofing, *smishing*, and *vishing* – these measures remain uncoordinated. He emphasized that these efforts often reflect narrow national perspectives, dictated by differing implementations of data protection rules and the ePrivacy Directive. More importantly, because not all Member States have adopted such measures, fraudsters are able to shift their activities to jurisdictions where these practices are not effectively addressed.

To bridge these gaps, the Commission's proposal aims to create a framework for cooperation between electronic communications service providers and national competent authorities, which will bring an added value where this cooperation is weak. Data gathered at the national level will be collected by the new BEREC Office (Office for Digital Networks – ODN – in the DNA), which will serve as a platform for cooperation and for aggregating information on fraud schemes in partnership with European and global organizations, particularly EUROPOL and ENISA. It is expected that this information, combined with shared best practices, will enable BEREC to adopt guidelines that include both technical and legal measures.

Mr. Bara stressed that the technical nature of these guidelines will allow operators to implement effective countermeasures, while their legal framework will ensure consistency with Union data protection legislation. For this reason, the proposal suggests that BEREC consult the European Data Protection Board and ENISA before issuing such guidelines. The expectation is that the adoption of these measures by Member States will be effective, coordinated, and complementary. Finally, he noted that if this goal is not achieved, there remains the possibility for the European Commission to intervene and adopt relevant delegated acts.

#### **Key messages:**

Current anti-fraud measures across Member States are fragmented.

Not all Member States have implemented anti-fraud measures, which can inadvertently create "safe havens" for fraudsters to exploit jurisdictional gaps.

The DNA proposal aims to:

- Move beyond fragmented national measures, creating harmonized anti-fraud measures among Member States.
- Establish a critical role for BEREC and for the new Office (ODN) by collecting information at national level and issuing guidelines that will ensure compliance with EU data protection standards and will leverage synergies with EUROPOL and ENISA.
- If the guidelines are not sufficient to combat fraud the European Commission can intervene and adopt relevant delegated acts.

### **2.3. Sharon BRENNAN, Manager of Network Trust, Commission for Communications Regulation Ireland (ComReg)**

Ms. Sharon Brennan delivered a presentation based on the responses to 2 surveys, one sent to National Regulatory Authorities (NRAs) and another to Mobile Service Provider (MSPs) across 28 countries (EU members and the United Kingdom – UK). Responses were received

from all the NRAs as well as 83 MSPs, giving a broad picture of the views of both across the EU.

The main points from the survey responses were:

- There are legal and regulatory instruments against fraud in place in 23 countries, but only in three countries did the respondents consider the instruments sufficient.
- Regulation must quickly adapt to successfully combat an ever-evolving scam ecosystem. In particular data protection and privacy laws (such as the General Data Protection Regulation (GDPR), the ePrivacy Directive, and national data protection legislation) are viewed as a barrier for data sharing between MSPs in country, between different sectors in country and across borders.
- In 22 countries, calls considered to be scams are blocked, however the granularity of reasons for blocking vary so it cannot be considered that citizens are fully protected across the EU.
- In 9 countries a Sender ID registry is in place.
- In 5 countries, the instruments allow for checking the content of the SMS, e.g. if it includes a potentially fraudulent link.
- For MSPs, blocking calls is the primary intervention implemented. In contrast, scanning/analysis of SMS content/structure is the least used intervention. MSPs called for both type of interventions to be authorised in national legal and regulatory instruments, and viewed the lack of ability to protect their customers as having negative effects on both business operations and their relationships with end users.

Ms. Brennan mentioned, for example, that ComReg cannot currently mandate a content scan for SMS in the absence of an appropriate legal basis.

She also raised the issue of over-the-top (OTT) communication services, which tend to fall outside the scope of regulation. Fraudsters frequently initiate contact via SMS, before directing the victim to an OTT platform, such as WhatsApp. The need for firmer regulation of these services was highlighted.

#### **Key messages:**

Regulation is not adapting quickly enough to deal with the rapidly evolving highly sophisticated scam business.

Data privacy regulation hampers data sharing which is crucial to timely interventions to scams.

MSPs across the EU would like the ability to better protect their customers but need regulation to support them.

### 3. Panel 1: Global Regulatory Best Practices

#### 3.1. **Eduard BARTHOLME, Bureau Chief Consumer & Governmental Affairs - Federal Communications Commission (FCC), United States of America (USA)**

Mr. Bartholme stated that there are over 11,000 telecom providers in the USA, and they also have multiple administrators of the numbering plans, which makes the ecosystem extremely complex.

Regulation has historically been focused on obligations on carriers to complete calls. However Do Not Originate (DNO) lists are now in place to allow some blocking.

STIR/SHAKEN was introduced to provide a Caller ID Authentication Framework, however this only works on IP networks. The Robocall Mitigation Database was introduced to identify providers who are repeatedly facilitating bad traffic. Operators must upload their scam prevention methods. 1,400 providers who have either deficiency in filing reports or were shown to be carrying bad traffic have been blocked from operation in the US.

Industry Traceback Group (ITG) is the official traceback consortium, and are used by the FCC, law enforcement and banks. Providers are required to cooperate but traceback stops at the border in general, so the FCC is interested in global traceback initiatives.

FCC are also tightening Know Your Customer (KYC) and numbering rules among other initiatives.

#### **Key messages:**

International cooperation is needed to ensure that traceback is effective.

A multi-layer approach is crucial, starting with good KYC, MSPs doing all possible to ensure they are not carrying bad traffic, and a functional global traceback process.

#### 3.2. **Javier GUTIÉRREZ AFANADOR, Communications Commissioner - Communications Regulatory Commission (CRC), Colombia**

Mr. Javier Gutiérrez opened his intervention emphasizing that Colombia, and the wider region, urgently need skilled professionals to tackle the growing threat of cybercrime. He highlighted the critical need to improve institutional and business coordination to establish a primary cybersecurity centre, which must take a proactive approach, as the country cannot afford to wait for attacks to occur before taking all the necessary actions.

In Colombia, SMS remains the primary entry point for fraud, with one in three companies experiencing an incident in the last three years. Consequently, it is essential to enhance reporting mechanisms, focus on prevention, and improve recovery times following an attack. Furthermore, modern scams are increasingly difficult to detect, which erodes end-user trust in digital communications (calls and SMS). Mr. Gutiérrez noted that a key challenge identified by the Colombian regulator is that rules are often established only after fraudulent incidents take place.

To shift from a reactive to a proactive stance, a three-step prevention plan was established: verified centres, monitoring traffic, and educating end-users. The core objectives include strengthening the verification of communications and reducing the risk of spoofing and fraudulent communications. Possible measures mentioned for consideration include the use of caller authentication solutions, such as STIR/SHAKEN, and enhanced sender verification to block spoofed numbers and implement text message controls to verify senders and blocking of suspicious traffic routes. However, additional measures – such as monitoring operator reports and conducting public awareness campaigns – were also considered necessary.

Ultimately, regulators, telecommunications operators, banks, and authorities must work collaboratively to restore security to voice and messaging services, with the overarching goal of intercepting fraud before end-users are exposed.

#### **Key messages:**

Shift from reactive to proactive, move away from implementing regulations only after fraud occurs.

Three-step prevention strategy, verify the origin of the communication, active traffic monitoring and end-user education.

Technical and operational controls, through measures for caller authentication solutions, such as the use of STIR/SHAKEN, and sender verification to detect and block spoofed numbers and implement text message controls and traffic monitoring mechanisms to block suspicious traffic routes.

Cross-sector collaboration, securing communication channels requires a coordinated, multi-stakeholder approach involving regulators, operators, the banking sector, and authorities.

### **3.3. Sanjay KUMAR, Joint Advisor - Telecom Regulatory Authority of India (TRAI), India**

Mr. Sanjay Kumar started by outlining the scale of the digital communications in India with 1.3 billion telco subscribers, with daily traffic comprising 8 billion calls made and 6.64 billion messages exchanged. Furthermore, 241 billion digital payments are transacted annually.

The sheer size of the market and scams has motivated the NRA to automate as far as possible scam mitigation measures, using Artificial Intelligence (AI) and machine learning. 3.5% of calls (280M) and 0.21% of SMS (159M) are flagged as Spam each day by the AI systems. TRAI use a co-regulatory approach whereby the NRA lays down the rules for the MSPs and empowers the MSPs to make further rules for telemarketers.

TRAI have been using a blockchain platform for the last 7 years mandating each entity to register themselves and then each SMS and call is verified as coming from the correct source and along the correct route. Traceability is then guaranteed. All Application-to-Person (A2P) SMS are scanned and can only contain whitelisted URLs, APKs, OTT links and callback numbers.

TRAI concluded by remarking that efforts are underway to move from a reactive approach to preventative scam controls, and stronger co-ordination between the involved sectors.

#### **Key messages:**

AI is needed to fight the sheer volume of scam communications.

Collaboration between the various sectors is vital to move to a more preventative, rather than reactive, controls.

### **3.4. Will PINKNEY, Principal Infrastructure and Communications Group and Programme Director for Ofcom's Scams Programme - Office of Communications (Ofcom), UK**

Mr. Will Pinkney from Ofcom presented the UK's integrated approach to combating fraud and scams across regulated services, with a strong focus on telecommunications and an expanding role in online fraud. Since 2023, Ofcom's remit has included online fraud such as fraudulent search ads, social media content, OTT messaging, and social advertising, supported by guidance on scam content and upcoming consultations on online advertising rules.

The UK mainly faces two threats: scam calls and scam SMS messages, most of which originate outside the country. Fraudsters often rely on UK phone numbers - either obtained temporarily or spoofed - to appear legitimate.

To counter scam calls, Ofcom has strengthened number allocation rules, increased operator due diligence, introduced a DNO list, and required blocking of clearly illegitimate calls, including spoofed fixed-lines. It has also proposed stricter controls on calls appearing to come from UK mobile users roaming abroad, requiring operators to withhold number presentation unless roaming status is verified by the home network.

UK operators currently block around 1% of incoming calls as suspicious or fraudulent.

For scam messages, fraudsters use both person-to-person (P2P) routes, often via SIM farms, and A2P routes by impersonating legitimate businesses. Initial measures focused on SMS firewalls, which now block over 2.5 billion scam messages annually, alongside victim reporting tools. Ofcom is now introducing stronger regulatory obligations, including blocking known fraud numbers, filtering messages in transit, limiting prepaid SIM use, and strengthening KYC and traffic monitoring requirements.

Measuring impact remains difficult, but indicators suggest improvement: reports of suspicious landline calls fell from 53% in 2022 to 39% in 2026, and overall reports of suspicious communications dropped from 68% to 40%, with the DNO list contributing significantly. Despite progress, fraud remains a major issue.

Future priorities focus on improving data collection and analysis, including better measurement of scam reach, stronger links between communications fraud and financial harm, enhanced cooperation with the financial sector, improved traceback and number usage transparency, and greater information sharing across the ecosystem. The overarching goal is to better evaluate regulatory effectiveness as fraud increasingly shifts from telecom networks to online environments.

#### **Key messages:**

Numbering integrity and traceability are critical: improving verification, allocation controls, and traceback mechanisms is essential to disrupt scam operations.

Cross-sector cooperation is essential, particularly between telecom operators, online platforms, and financial services, to track and disrupt end-to-end fraud chains.

As telecom defences strengthen, fraud is shifting online, so regulatory approaches must evolve to extend comparable “friction” and enforcement in digital advertising and platform ecosystems.

A key future priority is improving data quality and analytics, including better measurement of scam reach, financial harm linkage, traceback capabilities, and cross-sector information sharing.

### **3.5. Freddie MCBRIDE, Chair of Working Group NaN (WG NaN) - ComReg, Ireland**

Mr. Freddie McBride from ComReg gave a presentation outlining the interventions put in place in Ireland. In 2024 ComReg published a Response to Consultation (ComReg 24/24) which mandated 6 interventions to mitigate scam calls and SMS.

For voice calls, the interventions included a DNO list, Protected Numbers (PN) list, Mobile Calling Line Identification (CLI) Call Blocking, Fixed CLI Call Blocking, Voice Firewall. These interventions give good layered levels of protection to end users and have resulted in large volumes of blocked scam calls in Ireland, mainly due to the Mobile CLI blocking intervention. It was clarified that a roamer status check is in place to verify if a number is actually in roaming status and to determine whether the call should be blocked or otherwise).

For SMS, a further intervention was mandated, namely an SMS SenderID Registry. This Registry is solely for A2P SMS, which involves a complex ecosystem of SMS providers. There are over 20,000 SenderIDs registered from in excess of 15,000 entities. However, this leaves the gap of P2P SMS messages which scammers are now moving to. ComReg noted that there is currently no legal basis empowering them to mandate content scanning.

ComReg run a monthly forum with Industry which is very useful to get understanding between all parties involved. After the SenderID Registry was introduced, scammers moved to using short codes (5xxxx) and this shift was identified through such forum and subsequently shut down with great speed.

ComReg are now consulting on various SMS interventions that do not use content scanning but mitigate in other ways (SMS cap, Domain Name System (DNS) filter, metadata analysis).

**Key messages:**

A layered approach is needed to have maximum protection, so blocking of calls for various reasons (DNO, PN, Roamer status check, firewalls) is effective.

While a SenderID registry is very effective for A2P SMS, the gap left in other messaging channels (P2P) will be exploited by scammers, leaving the end users vulnerable.

## 4. Panel 2: Industry Solutions

### 4.1. Lorik SEKIRAQA, Senior Counsel, Government, Policy & Regulatory Affairs, EMEA, Twilio Inc.

The first speaker on the second panel was Mr. Lorik Sekiraqa, working for the EMEA (Europe, the Middle East and Africa) unit of Twilio, a US-based cloud communications platform, who described general fraud trends such as fraudsters exploiting KYC weaknesses, creating openings for impersonation. Free-text forms, avoiding flagged keywords and malicious URLs are increasingly used by fraudsters to bypass filters and checks. Fraudsters sometimes establish initial contact with a phone call, as this is the least monitored channel, before moving on to messages or emails to complete the scam. He explained that fraudsters now request One-Time Passcode (OTP) fulfilment messages to generate Artificially Inflated Traffic (AIT)<sup>1</sup>. Such techniques, sometimes referred to as SMS pumping, are made to appear more legitimate by the fraudsters nowadays, as the OTPs requested are actually being used to lower the risk of arousing suspicion. Alongside this, fraudsters are randomizing their fraudulent calling behaviour. Mr Sekiraqa also presented examples of Twilio's measures to combat fraud, both offered as services to clients and implemented within its own network.

Twilio outlines that its internal protection measures against fraudsters can be structured in three stages, namely "Prevent", "Attest" and "Act". Prevention involves checking the identity and legitimacy of an applicant before they come onto the Twilio network through robust KYC or Know Your Business Customer (KYBC). Attestation happens next, once an identity and use case have been verified, Twilio ensures that trust (in the sender) can travel down the value chain (e.g. through STIR/SHAKEN, Sender ID Registry measures, etc.). Lastly, the "Act" stage covers how Twilio gathers intelligence and responds quickly, acting where required.

Since there is a need for a baseline on what providers should do to protect against fraud and scams, Twilio identifies three areas where harmonisation would deliver results:

- Harmonisation of the operational rules of communications, such as for numbering assignment and sub-assignment, coupled with a technology-neutral approach to use cases,
- A single, pan-European rulebook implementation for alphanumeric Sender ID (SMS and Rich Communication Services (RCS)), and Branded Calling framework,
- Simplified and harmonised KYC/KYBC requirements across Member States.

---

<sup>1</sup> Which traffic is typically directed towards premium-rate numbers or international numbers under the control of the fraudster to extract routing, termination and/or premium-rate fees.

The advantages of harmonizing baseline regulatory standards and the operational rules of communication could eliminate "weakest-link" exploitation, protect responsible providers, secure the ecosystem, and foster regulatory trust to unlock the Single Market.

Twilio highlights the EU Digital Identity and Business Wallet as an important tool in combating fraud. If designed effectively, it could simplify the process for providers of verifying the identity of those coming onto their network.

**Key messages:**

Effective fraud prevention requires a harmonised European approach based on consistent KYC/KYBC requirements, common operational rules, and trusted digital identities.

Combining preventive identity verification, trusted authentication, and rapid intelligence-based response would reduce opportunities for fraudsters to exploit regulatory and operational gaps.

#### **4.2. Antongiulio LOMBARDI, Regulatory Affairs Director Giovanni BROCCATELLI, Head of Core and Beyond the Core regulated Markets, Wind Tre S.p.A.**

The presentation delivered by Mr. Antongiulio Lombardi and Mr. Giovanni Broccatelli from Wind Tre, an Italian telecom operator, focused on the Italian regulatory model developed by Autorità per le Garanzie nelle Comunicazioni (AGCOM) to combat telecom fraud, particularly spoofing calls and SIM-swap fraud. The speakers emphasized that the presentation was not intended to promote the company itself, but rather to explain the collaborative approach adopted in Italy between the national regulatory authority, telecom operators, consumer associations, and other institutions.

A central idea throughout the presentation was the methodology developed by AGCOM to address complex telecom security issues. The process begins with identifying a specific problem, followed by the creation of technical working groups involving operators and other stakeholders. These groups analyse technical constraints, operational realities, and possible solutions before AGCOM takes a final regulatory decision. The speakers stressed that this model preserves the independence of the regulator while ensuring that decisions are informed by practical industry knowledge.

A major part of the presentation focused on CLI spoofing, which involves falsifying the caller ID in order to hide the real origin of calls. The speakers explained that spoofing was initially used to avoid international termination fees, but later evolved into a large-scale fraud mechanism involving robocalls and scam calls targeting consumers.

AGCOM developed a "border protection" approach requiring international carriers operating in Italy to block suspicious incoming calls from abroad that use Italian numbers unlawfully. Special mechanisms were introduced to verify whether mobile users were actually roaming abroad before allowing calls with Italian mobile numbers to pass through the network.

The final section addressed SIM-swap fraud, which occurs when criminals abuse of weaknesses in the process for SIM issue and/or number portability and request a replacement SIM for an active user without that user's knowledge, in order to gain access to the user's assigned number and subsequently also to the user's banking services, personal data, and other digital accounts. AGCOM addressed this issue through a similar collaborative process involving operators and financial institutions. The adopted measures strengthened customer identification procedures during SIM replacement and mobile number portability requests. The speakers concluded that these measures have practically eliminated SIM-swap fraud cases in Italy and demonstrated the effectiveness of AGCOM's cooperative governance model. However, they also noted that telecom operators currently bear the costs of implementing these public-interest security measures without compensation, and argued that future legislation should recognize and reimburse these operational burdens.

**Key messages:**

AGCOM's cooperative regulatory model enabled the development of effective anti-spoofing and SIM-swap measures.

By combining regulatory oversight with operators' technical expertise, Italy significantly reduced telecom fraud and enhanced consumer protection.

### **4.3. Justen DAVIS, Senior Director Industry Relations and Global Public Policy, SOMOS Inc.**

Mr. Justen Davis presented the Comprehensive DNO and Telephone Number Intelligence Framework. SOMOS Inc. is a US-based nonprofit-adjacent organization that administers North American telecom numbering resources.

The presentation showed a use case for the North American Numbering Plan (+1 Country Code), covering resource allocation and the RealNumber® DNO breakdown. This was presented in the context of fraud prevention, and as a solution for blocking calls and text messages at origin before they enter the network. The Comprehensive DNO categorised the 10 billion numbers in the +1 Country Code into groups such as non-US allocated numbers, unallocated numbers, invalid numbers, customer-set DNO list of numbers, unassigned inventory pending assignment, and IoT numbers used for machine-to-machine services. After this mapping, only 21% (~2.1 billion) remained as the stock of US numbers allocated to service providers, toll-free and non-geographic numbers, for assignment of service. The purpose of this mapping was to establish how many numbers are allocated to services that can originate legitimate telephony traffic (e.g. voice calls) and in active use, so that traffic originating from all other numbers (79% in this case) can be blocked at origin, before it enters the network.

The next example showed a similar deployment working with Ofcom in the UK. For the UK Numbering Plan (+44 Country Code), the resource allocation and DNO breakdown categorised the 10 billion numbers into groups. After this mapping, only 8% (~824 million) remained as numbers allocated to UK communications providers for assignment of service.

The presentation concluded with examples demonstrating the operational benefits of implementing comprehensive telephone number intelligence. The most notable included a 3% daily reduction in fraudulent traffic for a US Tier 1 provider, a 90% reduction in reported robocalls for a leading US mobile provider, and 3x ROI with a 4% revenue increase for a US communications provider. A major softswitch vendor also blocked 296.8 million calls in its first 45 days.

#### **Key messages:**

A DNO list approach is an effective measure for blocking illegitimate calls and text messages at origin, before they enter the network.

Calls and messages originating from numbers that are unallocated, unassigned, invalid, used for incoming-only communications, or used for non-telephony services, such as Internet of Things/Machine-to-Machine (IoT/M2M) should be blocked.

Real-world deployments show measurable results, with major reductions in robocalls and fraudulent origination. The same intelligence can also help with number suballocation and traceback.

#### **4.4. Arturs ALKSNIS, Vice President - Public Policy, Proximus Global**

Mr. Arturs Alksnis from Proximus Global the international wholesale carrier part of Belgian telecom group Proximus highlighted in his presentation the scale of global fraud, driven by organized crime and accelerated by artificial intelligence. In 2025, global scam losses reached \$442 billion, with 57% of adults worldwide encountering scams and 23% losing money. Phone calls and SMS remain leading attack vectors.

AI has industrialized impersonation fraud, with deepfakes and voice cloning now common tools. Over €1.3 billion in losses have been linked to deepfake scams. One in four adults has experienced or knows someone affected by a voice-cloning scam.

Proximus Global is deploying advanced anti-fraud solutions. These include FraudGuard, 365guard, the Fraud Management Suite and the Telesign Trust Engine, which are AI-driven, alongside the Recycled Number Fraud Prevention API (with EnStream) and CAMARA-based Network APIs (in partnership with Nokia) targeting the developer ecosystem.

Despite these tools being effective and widely deployed, their impact is limited by fragmented national regulations. Two-thirds of fraud losses are tied to international traffic, but national

measures stop at the border. Multiple authorities, conflicting obligations, and slow regulatory adaptation further hinder effective defence.

Industry and regulatory bodies are beginning to organize globally, with initiatives like the One Consortium and GIRAF bringing together stakeholders across continents. However, the key bottleneck remains the legal framework, which restricts the use of available tools and intelligence across borders.

#### **Key messages:**

The tools and intelligence to fight global fraud exist and are delivering results, but what is missing is the regulatory permission to use them together across borders. Cross-border fraud defence should be a clear, named workstream in the EU regulatory framework.

#### **4.5. Haude LANNON, Policy Director, GSM Association (GSMA)**

GSMA, a global organisation with a membership of over 800 operators and 300 ecosystem partners, was represented by Ms. Haude Lannon. GSMA's mission is to unlock all the power of connectivity and tackle a big social challenge, which is fighting fraud and scammers. Fraud is global, cross-border and rapidly evolving. Operators are seeing that scammers are increasingly using AI and developing very sophisticated techniques. Hundreds of millions of people are impacted globally, and no one is immune regardless of age, income and education. GSMA is seeing that AI is truly a force multiplier and it is on the side of scammers. It increases their success rate and the profitability of their operations. It is logical that fraud is a top international priority requiring a joint united global response.

Europe is developing its own set of recommendations, guidelines and measures. The Global Fraud Summit in March 2026, held in Vienna, was deemed to be very important, as it was convened by the UN Office on Drugs and Crime and Interpol, and the message was very clear, because it served as the springboard for launching the 'Global Public-Private Partnership Framework Against Fraud'<sup>2</sup>. At this proposal, GSMA is taking a very comprehensive holistic approach with their members to combat rising numbers of scams that affects individuals, businesses and is eroding trust that is fundamental in the global mobile industries. Mobile operators are committed to protecting their customers and taking decisive actions against fraud and scams. Solutions vary significantly because there is no one size fits all approach. So, operators are deploying diverse anti-fraud measures independently and through cross-sector partnerships and at varying stages of maturity and sophistication.

The *first pillar* of the tools that GSMA is deploying is *expertise and intelligence sharing*. This collaboration helps to generate crucial insights, and the Fraud and Security Group (FASG)

---

<sup>2</sup> <https://www.unodc.org/unodc/en/organized-crime/global-fraud-summit/endorsements.html>

plays a central industry coordination role by bringing together worldwide operators, vendors and security experts, and helps to increase the protection of mobile operations and technology and infrastructure to protect the customer identity security and privacy. GSMA also hosts the so called *Telecommunication Information Sharing and Analysis Centre* (T-ISAC), which is a central hub for information sharing for the telecommunication industry. There, they have 160 operators sharing high risk number intelligence in real-time.

The *second pillar* is around *innovation and industry collaboration*. GSMA had the great chance to develop a tool, which is the GSMA scam signal, where GSMA and UK Finance came together to deliver solutions that enable banks to better identify and stop fraudulent transfers, by analysing real-time network data, identifying correlation between phone calls and fraudulent bank transfers. It is now extended to other geographies including South Africa.

The *last pillar* is *education*. GSMA has been developing awareness of the danger of scams, campaigns and information tools. It encourages the development of government-led, industry-wide awareness campaigns and the development of those tools.

**Key messages:**

Scam prevention cannot be achieved by a single sector, so cross-sector and cross-border collaboration is at the very heart of this and cannot be addressed by isolated and prescriptive measures.

## 5. Main takeaways

The workshop confirmed that fraud in electronic communications has become a fast-evolving and increasingly sophisticated threat, affecting end users, and business, undermining trust in communications services, and generating wider economic and societal harm. While smishing and vishing remain particularly visible manifestations, the discussions showed that the fraud landscape is broader and constantly adapting across voice, SMS and online channels. A recurring message throughout the workshop was that fraudsters are quick to exploit technological change, operational gaps and regulatory inconsistencies, while regulatory and institutional responses often remain fragmented and slower to adapt.

### **From reactive detection to proactive prevention**

A first key takeaway was the need to move from reactive to more preventive and coordinated approaches. Several speakers highlighted that fraud measures are still too often introduced only after specific fraud schemes have already become widespread. Effective action therefore requires earlier intervention, better anticipation of emerging patterns, and stronger monitoring capabilities. In practice, this means combining preventive measures such as robust KYC procedures, sender or caller verification, traffic monitoring, and number usage controls with swift operational responses when suspicious activity is detected.

### **Layered approach**

A second clear message was that a layered approach is necessary and important. No single intervention can address all fraud scenarios, and effective protection depends on combining different technical and operational measures. Across the presentations, these included DNO lists, caller ID authentication and verification, blocking cross-border calls with national calling party numbers with roaming status checks (for mobile CLIs), voice firewalls, SMS Sender ID registries, filtering and metadata analysis, route validation, traffic monitoring, content or link controls where legally permitted, and traceback mechanisms. The workshop also showed that interventions may be effective in one part of the ecosystem, while fraudsters rapidly shift to less protected channels or routes, underlining the importance of addressing vulnerabilities holistically.

### **Integrity and traceability**

A third major takeaway concerned the importance of numbering integrity, identity verification and traceability. A number of speakers stressed that fraud prevention begins with stronger controls on access to communications networks and numbering resources, including improved KYC and KYBC requirements, stricter numbering assignment and sub-assignment rules, better verification of the legitimacy of users and use cases, and clearer accountability throughout the value chain. Related to this, many contributions highlighted the importance of traceback capabilities and of greater transparency regarding number use and traffic origination, particularly in light of the cross-border nature of a large share of fraudulent communications.

### **Cross-border and cross-sector cooperation**

The workshop also highlighted the importance of cross-border and cross-sector cooperation. Fraud does not stop at national borders, and several speakers noted that national measures alone cannot sufficiently address international traffic or prevent fraudsters from exploiting weaker jurisdictions. Equally, fraud often spans multiple sectors, involving not only telecom operators but also online platforms, messaging providers, banks, law enforcement authorities, regulators and standardisation bodies. Effective mitigation therefore depends on timely information sharing, clearer cooperation frameworks, and a more coordinated approach between public authorities and private actors at national, European and international level.

### **Legal streamlining and convergence**

A further important lesson concerned the current regulatory framework. While many speakers pointed to promising operational and technical tools already available to mitigate fraud, they also noted that fragmented legal frameworks, uneven national implementation and constraints related to data screening and information sharing that limits their effectiveness. Several interventions stressed that operators and other stakeholders need clearer legal basis and more harmonised rules in order to implement effective anti-fraud measures, share relevant intelligence, and protect end users consistently across jurisdictions. In this respect, the discussions underlined the value of greater regulatory convergence and of possible future guidance at European level.

### **AI and other emerging technologies**

The workshop also showed that data, analytics and emerging technologies are becoming increasingly important in both fraud and fraud prevention. Fraudsters are making growing use of AI and automation, while operators and regulators are likewise deploying AI, machine learning and advanced analytics to identify suspicious patterns and act at scale. At the same time, several speakers stressed the need for better data collection, more accurate measurement of the scale and impact of fraud, and stronger analytical capabilities to assess the effectiveness of interventions and support evidence-based policy making.

### **Conclusion**

Overall, the workshop confirmed that combating fraud in electronic communications requires a comprehensive, collaborative and adaptable response. The main lessons emerging from the discussions point to the need for more preventive action, layered technical and operational measures, stronger identity and numbering controls, improved traceback and information sharing, and closer cross-border and cross-sector cooperation supported by an appropriate legal and regulatory framework. These insights provide an important basis for BEREC's further analytical work in this area and for possible future best practices on combating fraud, to be developed in cooperation with ENISA, Europol and other relevant partners from both the public and private sectors.

## Annex

# AGENDA

## BEREC Stakeholder Workshop on Combating Fraud

|                         |                                                         |
|-------------------------|---------------------------------------------------------|
| <b>Location:</b>        | Hybrid workshop<br>- IRG Secretariat Brussels and WebEx |
| <b>Date &amp; Time:</b> | 21 May 2026, 13:30 - 16:30 CEST                         |

### 21 May 2026

#### Background

In recent years, the rapid digitalisation of services has been accompanied by a significant rise in online fraud targeting end users across the European Union. As highlighted in the [NIS Cooperation Group's report of 21 February 2024 on the cybersecurity and resilience of the EU's communications infrastructure and networks](#), smishing and vishing attacks have become increasingly prevalent. These techniques are used by malicious actors to deceive individuals into visiting fraudulent websites that impersonate trusted entities such as government services, delivery providers or retailers, or to compromise sensitive data, including two-factor authentication codes sent via SMS.

While smishing represents a critical and highly visible threat vector, it is only one aspect of a broader and rapidly evolving fraud landscape. Attackers are continuously adapting their methods, leveraging both technological vulnerabilities and human factors so as to exploit communications networks and digital services. As part of its efforts, BEREC will assess the current state of fraud in the electronic communications sector, identify key trends and determine the most pressing challenges which require coordinated action.

#### Aim

This external workshop marks an important step in this process. Building on ongoing collaboration with ENISA and other important stakeholders, it will be a unique opportunity for dialogue among BEREC members, other relevant national authorities, electronic communications providers, equipment vendors and key European institutions, including the European Commission and Europol. The insights gathered will be important for further BEREC's forthcoming analytical work.

From 13:15 Getting connected in WebEx

### Start of Workshop

13:30 Welcome and introduction by the **Co-Chairs of the BEREC Cybersecurity Working Group**,  
**Katja KMET VRČKO** (AKOS/Slovenia) and **Zdravko JUKIĆ** (HAKOM/Croatia)  
 and

Opening of the Workshop: **Marko MIŠMAŠ**, **BEREC Chair 2026**

13:35 Keynote speeches:

**Martin KÄHL**, Specialist at 'Expertise and Stakeholder Management Unit'  
**European Union Agency for Law Enforcement Cooperation (Europol)**

**Gyula BARA**, Project Leader in the Unit 'Electronic Communications Policy, Implementation and Enforcement'  
**DG CNECT, European Commission**

**Sharon BRENNAN**, Manager of Network Trust  
**Commission for Communications Regulation Ireland (ComReg)**

### 14:00 Panel 1: Global Regulatory Best Practices

Introduction by the moderator (Katia GONZALEZ, SOMOS)

14:05 **Eduard BARTHOLME**, Bureau Chief Consumer & Governmental Affairs  
**Federal Communications Commission (FCC)**, United States of America

**Javier GUTIÉRREZ AFANADOR**, Communications Commissioner  
**Communications Regulatory Commission (CRC)**, Colombia

**Sanjay KUMAR**, Joint Advisor  
**Telecom Regulatory Authority of India (TRAI)**, India

**Will PINKNEY**, Principal Infrastructure and Communications Group and  
 Programme Director for Ofcom's Scams Programme  
**Office of Communications (Ofcom)**, United Kingdom

**Freddie MCBRIDE**, Chair of Working Group NaN (WG NaN)  
**Commission for Communications Regulation (ComReg)**, Ireland

**Q&A**

---

15:00 Coffee break

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15:15 | <b>Panel 2: Industry Solutions</b><br>Introduction by the moderators (CSR WG co-chairs)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 15:20 | <b>Lorik SEKIRAQA</b> , Senior Counsel, Government, Policy & Regulatory Affairs, EMEA<br><b>Twilio Inc.</b><br><br><b>Antongiulio LOMBARDI</b> , Regulatory Affairs Director<br><b>Giovanni BROCCATELLI</b> , Head of Core & Beyond the Core regulated Markets<br><b>Wind Tre S.p.A</b><br><br><b>Justen DAVIS</b> , Senior Director Industry Relations and Global Public Policy<br><b>SOMOS Inc.</b><br><br><b>Arturs ALKSNIS</b> , Vice President - Public Policy<br><b>Proximus Global</b><br><br><b>Haude LANNON</b> , Policy Director<br><b>GSM Association (GSMA)</b> |
| 16:10 | <b>Q&amp;A</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 16:25 | <b>Closing remarks</b><br><b>Katja KMET VRČKO</b> (AKOS/Slovenia) and <b>Zdravko JUKIĆ</b> (HAKOM/Croatia)                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 16:30 | <b>End of Workshop</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |