Ref. Ares(2025)8483729 - 07/10/2025

BoR (25) 129

Summary Report on the BEREC Workshop on practical issues preventing number misuse and possible fraudulent activities, 21 May 2025

2 October 2025

Contents

Introduction and aim of the Workshop

Connectivity and electronic communications services are now more relevant than ever to end-users. The efficiency of the end-user rights provisions of the European Electronic Communications Code (EECC) may be affected by changes in the use of different electronic communications services and their capability to ensure effective access to emergency services, by end-user use of communications services which is evolving over time, and by the prevalence of digital platforms as a substitute for traditional electronic communications services.

In recent years, fraudulent activities and misuse of numbering resources have increased significantly, impacting end-users and market players alike. This trend has also raised broader concerns about privacy, security, and the overall trustworthiness in digital interactions. Therefore, the workshop aimed to comprehensively address these challenges, reflect on their implications beyond the telecommunications sector and explore solutions to ensure end-users' confidence and trust in electronic communications services. The BEREC Opinion on the market and technological developments and on their impact on the application of rights of end-users in the EECC (Article 123)[1] highlighted that fraudulent activities in the digital space are among the most significant trends impacting end-users and their protection.

As the problem is increasing and the schemes established are becoming more complex, periodic experience exchange between national regulatory authorities (NRAs) is extremely important. The discussions with market players are organised to increase the knowledge and seek long-lasting and sustainable solutions, especially employing newly arising solutions (e.g. artificial intelligence). Due to the rapid pace of innovations and applications in the field of AI, and in order to keep up with these changes, BEREC needs to constantly monitor the evolution of this technology and how end-users are impacted in order to achieve a better understanding, transparency, and safety.

Workshop structure

The workshop was structured into four key sessions[2]:

1. Overview of the problem – Establishing the context by emphasising the impact on end-users and the end-user perspective.
2. Market players' measures and tools – this session was intended to explore technical solutions and strategies to combat fraud, also with a focus on AI-driven approaches.
3. The role and practices of NRAs – this session was dedicated to regulatory measures and other initiatives implemented by national regulators.
4. Panel discussion – bringing together regulators, market participants, and other stakeholders to address cross-sectoral and cross-border challenges, particularly in the context of the ongoing EECC review.

[1] BoR (24) 180, link: https://www.berec.europa.eu/en/all-documents/berec/opinions/berec-opinion-on-the-market-and-technological-developments-and-on-their-impact-on-the-application-of-rights-of-end-users-in-the-eecc-article-123

2 detailed agenda is in Annex I.

BEREC points out that the workshop was well attended, with more than 230 onsite and online participants and 20 speakers throughout the 4 sessions. The biographies of the speakers are included in Annex II.

BEREC takes the opportunity to thank the presenters and participants for their engagement and valuable contribution to the discussions on the topic. The slides from the workshop are available on the BEREC website[3].

During the workshop the participants were engaged via live polls and Q&A in order to understand their feedback and comprehension of the topics that were discussed during the workshop. Between 55 and 85 participants responded to the questions, depending on the poll. The poll results showed that most attendees were regulators or industry representatives, with primary goals of learning about fraud trends, understanding regulatory responses, and exploring best practices. Description of the collaboration between regulators and stakeholders was mixed with ratings from good/fair to poor, with poor coordination identified as the main obstacle to fraud prevention. Participants were most familiar with smishing, Calling Line Identification (CLI) spoofing, and Wangiri fraud, and almost all had been targeted by scams, though only a few suffered actual losses. Fraud in those cases was most commonly carried out via voice calls, email, and fake websites. The majority believed national regulators should take the lead in combating fraud, while coordination at the EU level was perceived as weak. Overall, the workshop was rated highly useful and well-organised, with excellent or good ratings from nearly all participants. For more information on the poll results please consult Annex III.

[3] https://www.berec.europa.eu/en/events/external-workshop-on-practical-issues-preventing-number-misuse-and-possible-fraudulent-activities-as-a-result-of-impact-of-new-technologies

Opening of the workshop

The Workshop started with an introductory speech provided by Mr. Tonko Obuljen, the BEREC Vice Chair for 2025, who stated that in recent years, we have witnessed a significant increase in the misuse of numbering resources and the emergence of increasingly complex fraud schemes. These activities not only harm end-users through financial loss, privacy breaches or disruption, but also undermine trust in our digital communications ecosystem. As new technologies evolve, so do the tactics of those exploiting them. This evolution demands equally sophisticated and collaborative responses. He emphasised that this workshop will look beyond the technical challenges and also reflect on broader implications for trust, security, and the rights of end-users, as set out in the European Electronic Communications Code (EECC). BEREC's recent Opinion under Article 123 of the EECC[4] identified fraudulent activity as one of the most serious issues facing end-users today. It is essential to hear different perspectives from market players deploying cutting-edge tools, including AI, and from regulators implementing new frameworks and enforcement strategies. He also referred to the importance of considering the cross-sectoral and cross-border nature of the problem, because collaboration is not an option here; it is essential. Ultimately, he emphasised the need for continuous dialogue, shared experiences, and coordinated action to create resilient, transparent, and user-centric solutions.

Session 1 – Overview of the problem

This session aimed to set the context by highlighting the impact on end-users, presenting their perspective, and showcasing global trends along with public and private initiatives.

Rens Grim, Global Anti-Scam Alliance (GASA)

The Global Anti Scam Alliance (GASA) is a non-profit organisation, bringing together policymakers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organisations to share insights and knowledge surrounding scams.
Mr. Rens Grim introduced the Global Signal Exchange (GSE), a cloud-based meta-aggregator launched in January 2025 by the GASA and the DNS Research Federation.
GSE acts as a global clearinghouse for real-time signals of cybercrime and scam-related activities. It brings together diverse stakeholders: ISPs, registrars, telecom providers, governments, platforms, and cybersecurity entities, that collaborate to share data and improve collective response to online threats. The GSE covers a wide range of cyber threats, including

[4] BoR (24) 180.

scams, fraud, IP violations, spam, ransomware, DDoS, hacking, illegal content, and cyberbullying. In the UK alone, 41% of reported crimes are related to online scams, yet underreporting remains a key challenge globally.
Operating as a neutral, cloud-based platform, the GSE aggregates about 230 million signals from both non-profit and commercial partners (e.g., Meta, Amazon, Microsoft, UNODC). It includes a feedback loop allowing trusted users to improve data quality and reduce false positives.
Given the experience in the format described, Mr. Grim highlighted the importance of collaboration and transparency. The goal is not to shame, but to show which actors are effective in combating abuse and where support is needed, ultimately aiming for a safer global internet environment. Hence, the list of participants in the initiative can serve as a proof for reliable partner.

Els Bruggeman, Euroconsumers

Ms. Els Bruggeman, representing Euroconsumers, which brings together national consumer organisations from Italy, Belgium, Spain, Portugal, and Brazil, shared insights into the victim perspective and the consumer impact of scams.

According to a Euroconsumers survey, 92% of people have experienced a scam in the past two years. She pointed out that while consumers often feel confident in managing risks, this changes quickly once a scam occurs, especially if there is a financial loss.

To illustrate, she shared several real-life examples:

- A man recently lost €100,000 to a scam involving a fake compliance service mimicking a well-known Belgian bank.
- Another individual lost €13,000 after receiving a fake call claiming their bank card had been stopped.
- A fraudulent email, impersonating another Belgian bank, requested a personal data update and financial loss was €4,000.
- An 80-year-old man lost his entire pension and life savings in a scam.

Ms. Bruggeman stressed that even scams involving small sums can have a major impact on financially vulnerable households. Victims rarely recover their losses: Euroconsumers' survey shows only 3% were reimbursed. While banks are legally obliged to refund fraud victims, they often invoke "gross negligence" to deny claims, especially when payments were authorised.
She highlighted that this overlooks how scams have evolved: modern fraudsters use advanced social engineering, often exploiting personal data from breaches and social media, and mimic bank interfaces with AI tools and deepfakes. Victims are manipulated into believing the transactions are legitimate.
She argued that authorisation does not equal informed consent, calling for a liability shift. Responsibility should not rest solely on victims; hence, in her opinion, banks, platforms, and telecom operators must do more to prevent and detect scams.
Beyond financial damage, she emphasised the emotional toll. Victims often feel shame, guilt, anger, stress, embarrassment and self-blame. Some even developed long-term issues,

including depression. Scams also erode trust in people, in digital platforms, and in the entire digital economy.

She criticised the practice of directing scam victims to ordinary call centre agents, stating that victims should never be blamed again or re-traumatised. Victims sometimes even claim that the post-scam journey was more traumatic than the scam itself due to constant blame and lack of support.

She also raised the issue of reporting. Surveys show:

- Half of the victims do not report scams, often out of shame;
- 22% believe nothing can be done;
- 90% did not even know where to report; and
- Only one-third report to the police or their bank.

Instead, most victims confide in family or friends. She pointed out a serious lack of clear procedures for reporting cybercrime and called for a centralised support system where police, law enforcement, victim support groups, consumer organisations, banks, telcos, and platforms work together, offering victims a single point of contact.

She concluded by stressing that while supporting victims is important, we must also do more to catch the perpetrators, noting that less than 1% of scammers are ever caught.

Marnix Dekker, ENISA

Mr. Marnix Dekker, representing ENISA, explained that the agency's goal in terms of resilience is to harmonise and align, promote best practices, and facilitate incident reporting across EU member states. He highlighted strong collaboration with BEREC in these efforts.
He introduced CIRAS, the Cybersecurity Incident Reporting and Analysis System, maintained by ENISA – a database that collects large-scale telecom incidents, enabling detailed analysis and reporting.
He described the telecom sector’s cybersecurity efforts as a success story and a model for cooperation. ENISA primarily focuses on network security and resilience, rather than on consumer scams or frauds. However, there are areas of overlap - such as the Nevers risk assessment developed in response to the Russia-Ukraine war.
Mr. Dekker raised concerns about threats, citing examples like cyber groups infiltrating networks for espionage, the SMS and SS7 signalling attacks that expose user location or intercept communications.
He gave an example involving voicemail security, where attackers bypassed authentication by calling from the user’s own number and accessing 2FA codes sent by voice call, thereby compromising accounts like Gmail.
He also discussed SIM swapping, where changes in telecom procedures make it easier for customers to obtain eSIMs or to replace stolen SIMs are misused by attackers. Banks and other companies often rely on these systems, assuming they are secure – when in fact, legacy telecom systems may have critical vulnerabilities.
He warned that attackers are now shifting their focus to smartphones, as PCs become harder to exploit. He noted a recent surge in phishing and smishing attacks and stressed that telecom

incident reporting thresholds are too high, meaning smaller but impactful attacks go unreported.
He agreed that even attacks affecting only a few users can have major consequences, including financial losses and reputational damage. For example, SS7 attacks have been used to track VIPs, politicians or dissidents.
He urged telecom operators to identify weak points in their systems and take full responsibility not just for their security, but also to ensure other sectors do not depend on less secure legacy infrastructure.
He noted that newer technologies like 4G and 5G are significantly more secure, as well as new smartphones. Apps like WhatsApp offer fully encrypted communication. However, even these platforms are not immune to scams.
The speaker concluded with a call for greater transparency in incident reporting, especially for smaller-scale attacks. He proposed introducing immunity measures for telecom operators to encourage more open reporting.

Session 2 – Stakeholders' perspective

The session aimed to facilitate the sharing of insights from different stakeholders regarding the main issues to be considered to prevent number misuse and potential fraudulent activities. The actors providing their views were the association encompassing mobile network operators, two telco operators, as well as a cloud communication provider and one of the main hyperscalers.

Rita de Castro (GSMA)

Ms. Rita De Castro, Director of Policy at GSMA Europe, presented a comprehensive overview of the growing impact of fraud in the mobile ecosystem[5], emphasising that fraud is not merely a technical issue but a societal threat that undermines trust in digital services and has become a critical concern for mobile operators.
Spoofing is one of the most prevalent and damaging practices employed by criminals through telecommunication channels. The Calling Line Identification (CLI) is illegally manipulated, making the call appear to originate from a trustworthy number, even though it would be originating from a different number, often from abroad. These attacks rely on social engineering tactics, are organised, persistent, and increasingly sophisticated.
To combat this threat, according to the speaker, mobile network operators are significantly investing in deploying fraud detection technologies to identify, filter, and block spoofing and scam calls. These include number registries with blocklists to verify caller identity, technical signalling controls to authenticate CLI, and traceback and reconciliation processes to detect and eliminate abusive traffic at its source. GSMA, through its Fraud and Security Group[6] (FASG), leads the mobile industry's efforts on fraud and security by raising awareness, developing guidelines, and fostering innovation.

[5] The global financial cost of cybercrime is projected to exceed 15,63 trillion USD by 2029 (Statista).
[6] https://www.gsma.com/get-involved/working-groups/fraud-security-group/

Ms. De Castro highlighted that mobile operators are only one part of the financial fraud chain, and that a coordinated response across the entire ecosystem is essential. She urged governments and regulators to remove barriers to cooperation, promote cross-sector and cross-border data sharing, empower consumers, and leverage regulatory sandboxes to test new fraud prevention technologies. She concluded with a call for collective action: operators must act swiftly, share intelligence, and train their staff; consumers must stay vigilant and secure their devices; and regulators must establish clear, harmonised legal frameworks to enable effective fraud prevention.

Katia Gonzalez Gutierrez (BICS)

Ms. Katia Gonzalez Gutierrez, Head of Public Policy at BICS, underscored the urgent need for a global, coordinated response to telecom fraud, which is becoming increasingly sophisticated and international. She illustrated how similar fraud schemes, such as SMS and voice phishing, are replicated across regions, sharing technical patterns like originating numbers rather than language or content, showing how fraudsters scale successful tactics internationally. Despite the availability of advanced tools like AI and real-time monitoring, the industry remains largely reactive, with fragmented and localised responses.
Ms. Gonzalez highlighted the importance of intelligence sharing and collaboration to improve fraud prevention efforts across borders. While many operators have internal fraud mitigation systems, collaboration is hindered by legal and regulatory fragmentation, especially in Europe. She highlighted Australia's model as a positive example, where both domestic and international traffic are subject to monitoring, blocking, and intelligence sharing requirements. In contrast, European operators often face legal uncertainty and conflicting obligations.
The speaker also emphasised the need to involve data protection authorities alongside telecom regulators, as privacy laws can conflict with fraud prevention and leave users exposed. She called for a regulatory environment that balances privacy with effective fraud protection and remains adaptable to evolving threats.
To address these challenges, the Restore Trust Initiative was launched, built on two pillars: One Consortium, a not-for-profit industry group developing vendor-neutral tools and best practices; and GIRAF (Global Informal Regulatory Anti-Fraud Forum), a multilateral platform promoting harmonised regulatory approaches. These groups are already collaborating on key issues like international traceback, CLI spoofing, and Know Your Customer (KYC) practices.
Ms. Gonzalez concluded by calling for flexible, future-proof regulations and a level playing field where all industry players meet minimum standards for secure and ethical operations.

Tomas Grinevičius (Telia Lietuva, AB)

Like previous speakers, Mr. Tomas Grinevičius, Lead Service Architect at Telia Lithuania, emphasised that while telecom fraud is a global issue, anti-fraud measures remain fragmented and mostly national. Without cross-border cooperation, their effectiveness is significantly limited. He shared data on fraud trends in Lithuania and within Telia's network, illustrating the scale of attempted fraud.
Despite Telia's layered anti-fraud ecosystem with tools aimed to detect and block fraudulent traffic in near real-time, DNS firewall, SMS sender ID protection, SMS scam filter, roaming

check and voice firewall, fraudsters adapt quickly, often within weeks of new countermeasures being deployed.
Mr. Grinevičius shared that scam traffic dropped by 80% after Europol dismantled 12 scam call centres in Europe but rebounded within two months as fraudsters adapted their tactics, using random numbers instead of numbers from stolen user database. This highlights the agility of fraud networks compared to the slower pace of regulatory and technical responses.
Among the key lessons learned was the importance of cross-border cooperation and shared practices across the five markets where Telia operates. However, development cycles for anti-scam solutions remain slow, taking up to nine months, while scammers evolve in weeks. National regulations often shift the burden entirely onto operators, expecting continuous improvement without broader systemic support.
Mr. Grinevičius called for an EU-wide regulatory framework to harmonize efforts, improve data sharing, and ensure consistent implementation of measures. He also urged financial institutions to take a more active role in stopping scams, as cutting off fraudulent transactions would be the most effective way to disrupt scam operations.
In conclusion, he stressed that operators alone cannot eliminate fraud. Collaboration with regulators, law enforcers, and financial institutions is essential to keep pace with evolving fraud and scam threats.

Filip Filković (Infobip)

Infobip is a global cloud messaging platform used by around 70 telecom providers, processing 42 billion messages monthly. Mr. Filip Filković highlighted the growing scale of fraud, estimated at $39 billion annually. In 2022, Belgium reported €40 million in phishing losses (a 60% increase), and €115 million losses were reported in Ireland from SMS fraud. Infobip blocked 96 million malicious SMSs by May 2025 and 185 million in 2024. Fraud impacts subscribers (identity theft, financial loss, privacy invasion), operators (reputation damage, revenue loss), and enterprises (business disruption, increased costs).
Filković emphasised regulatory barriers to fraud prevention. The ePrivacy Directive requires operators to manage network risks but also prohibits communication interception, complicating SMS content filtering. NIS2 supports filtering for security, but national implementation is inconsistent and often ambiguous. Some countries, like Poland, allow active content analysis. He compared this to email, where NIS2 regulation 2024/2690 mandates filters to reduce malicious content. He argued SMS should be treated similarly.
Despite the availability of advanced, EU-developed solutions like SMS firewalls and AI-driven fraud detection, few EU operators use them due to legal uncertainty and fear of fines. ENISA recommends these tools for harmonised telecom security. Poland is seen as a regulatory model, enabling automatic SMS filtering while balancing privacy and security. The speaker called for clearer, harmonised EU legislation, using Poland's approach as a best practice.

Tomas Jakimavičius (Microsoft)

Mr. Tomas Jakimavičius, representing Microsoft, shared a global view on anti-fraud strategies in modern telecom networks. He emphasised the shift to cloud-based communication and the need to support technologies that leverage cloud capabilities for fraud detection, while

minimising regulatory burdens and service disruption. Key tools include Know Your Customer (KYC) practices, AI analytics, and call authentication.
He stressed that automatic detection is effective but must be combined with KYC data. He cited Japan's strict KYC rules, such as requiring verified photo ID, which led to a 90% drop in fraudulent use of Japanese numbers. KYC should be proportionate and consider privacy implications.
AI analytics, including large language models (LLMs), can analyse calls and messages in real time, even pausing calls to warn users and offer options. On authentication, Microsoft is a founding Board Member of the Secure Telephone Identity Governance Authority (STI-GA) to develop cross-border standards for encrypted identity tokens. Rich call data, showing verified caller names and logos, builds user trust.
He warned against outdated, overly technical anti-fraud methods that may harm legitimate cloud-based services. Instead, regulation should avoid excessive blocking and respect net neutrality. AI-driven, real-time solutions offer a more flexible and innovation-friendly approach to fraud prevention.

Session 3 – NRAs' activities and regulatory measures

This session was dedicated to regulatory measures and other initiatives implemented by national regulators.

Laurence Nivot – Cullen International

Ms. Laurence Nivot presented recent findings on regulatory measures combating fraud in telecommunications across Europe. Nivot's research focused on measures adopted by National Regulatory Authorities (NRAs) or legislators in 15 European countries, including 14 EU member states and the UK, to address scams involving CLI spoofing. CLI spoofing is a fraudulent practice where the Calling Line Identification is illegally manipulated to show a trusted number even though the call originates from a different number, often from abroad.
She noted that 11 out of the 15 countries examined had implemented measures to combat illegal spoofing practices, with most key binding measures specifically targeting CLI spoofing being adopted in 2024. The regulatory landscape is rapidly evolving, with new national measures being introduced.
Ms. Nivot described various types of measures adopted or under discussion by NRAs.
Blocking incoming international calls using a national CLI: this common measure prevents calls from abroad from being associated with a national fixed number unless exceptions apply. It primarily targets fixed numbers, often with detailed exceptions for legitimate services. Blocking mobile numbers is more complex, with some NRAs requiring operators to check the roaming status of mobile users.
Do-not-originate registry: a national database listing numbers that should never be used for outgoing calls, ensuring that any call showing such numbers as the calling party number is blocked. Examples include premium and short numbers, emergency and directory services.
Protected numbers registry: like the do-not-originate registry, this is a list of phone numbers that the NRA has not assigned and therefore cannot be used to originate calls. In some

regulations, operators shall also block calls where the CLI field is left empty or contains a number that is not consistent with the national numbering plan.
SMS sender ID registry: this involves registering alphanumeric SMS sender IDs, with operators required to block messages from unregistered IDs.
STIR/SHAKEN: a technical solution requiring providers to authenticate and digitally sign the caller's identity. Its effectiveness depends on effective cross-jurisdictional deployment, and it is limited to all-IP networks.
Ms. Nivot also mentioned broader measures such as voice firewalls, SMS filtering solutions, and efforts to raise end-user awareness. She concluded by emphasising the dynamic nature of regulatory responses to fraud.

Alīna Stafecka – Latvian regulator (SPRK)

Ms. Alīna Stafecka outlined Latvia's strategy to address fraud and scams, emphasising persistent vulnerabilities to telephone scams despite public awareness, resulting in resource and loss of trust in communication services. Although successful fraud cases have decreased, the overall volume of scam attempts is on the rise. Fraudsters display high organizational levels, sometimes bypassing banking systems by directly collecting cash.
Frauds initially targeted operators but
Latvia's anti-fraud legislation mandates operators to include fraud-related clauses in interconnection agreements, adopt generalised measures against numbering fraud, and report monthly fraud data. Despite these steps, limitations persist, such as the national scope of legislation, unnoticed small fraud cases, and the exclusion of communication content from regulations.
Initially, operators were resistant, arguing about user responsibility and fraudsters' adaptability. A significant shift occurred when Estonian and Lithuanian operators implemented anti-fraud measures, causing fraud activities to concentrate in Latvia and prompting cooperative action by Latvian operators.
Looking ahead, SPRK plans new measures with a focus on a few key areas. First, the NRA is considering a decentralised anti-fraud API solution, which will initially be voluntary but may become mandatory for transit operators. This solution aims to enhance the verification of call-origin legitimacy. Additionally, SPRK has been seeking solutions to strengthen the legal requirements for transit operators who manage international traffic. Finally, SPRK aims to enhance cooperation at both national and international levels.
Key takeaways include the necessity of a unified solution to reduce fraud impact and volume. Latvia is trialling a solution used in Lithuania and Estonia, with cross-border potential. The human factor remains critical as individuals can still fall victim despite technical safeguards. Fraud is anticipated to shift towards OTT services and messaging platforms as traditional telephony declines. Involving broader market players beyond telecommunications is crucial.
Ms. Alīna Stafecka closed her intervention, stressing the importance of international collaboration, promoting cooperation and sharing experiences to combat fraud.

Darius Kuliešius – Lithuanian regulator (RRT)

Mr. Darius Kuliešius discussed Lithuania's strategic regulatory approach to safeguarding consumers from digital scams. He emphasised the shared responsibility among the entire

ecosystem, including regulators, service providers, law enforcement, media, and civil society, with a key role for regulators in setting standards and ensuring accountability. Mr. Kuliešius noted BEREC's importance as a platform for coordination and collective action.
Effective blocking measures are a cornerstone of RRT's anti-fraud strategy. The National Cybersecurity Center (NKSC) manages a central system for blocking harmful internet links, preventing users from accessing harmful links. Call blocking measures, implemented in phases from November 2023, include blocking calls from foreign operators using unauthorised numbers and filtering suspicious traffic in real-time. SMS blocking measures, effective from January 2024, target fraudulent messages containing links to harmful resources.
Mr. Kuliešius highlighted the impact of these measures, with millions of digital crimes blocked, including 8.5 million fake calls, 3.3 million fake SMS and 24 thousand daily blocked attempts to connect to malicious links in 2024. Despite these efforts, financial losses to individuals remain high, with €20 million lost in 2024 and over €9 million in the first quarter of 2025, underscoring the need for more effective measures. Collaboration and enforcement are vital, enabling real-time actions and partnerships with trusted flaggers, using AI and open-source techniques to combat online threats.
As a result of RRT leadership, a cross-institutional Memorandum on cooperation was signed on March 27, 2025, by key public sector institutions to facilitate cooperation and real-time data exchange. Lithuania has identified SIM card farms operating within the country, which are used for fraud, bypassing telecom filters. The response includes network analysis, prohibition of anonymous national prepaid SIM cards, and close cooperation with law enforcement.
Education and public awareness are essential components of RRT's strategy. A project led by RRT, named “No One Is Forgotten”, focused on raising digital literacy skills for older individuals and has reached 13,000 participants across 40 cities and rural areas, emphasising the importance of education to prevent fraud.
Mr. Kuliešius concluded by stating that the extent of digital losses will not decline on its own, and that leadership, smart laws, cooperation, and education are the four main elements needed to combat this challenge.

Sharon Brennan – Irish regulator (ComReg)

Ms. Sharon Brennan outlined ComReg’s multi-layered strategy to combat spoofing and telecom fraud, emphasising the critical need for coordinated action among regulators, telecom operators, digital platforms, and the financial sector.
ComReg launched its anti-scam initiative in 2022 in response to a significant rise in financial and societal harm caused by fraudulent calls and messages. Interestingly, younger individuals under 30 were found to be more susceptible due to their digital habits and quick engagement with suspicious content. Older users, though less likely to fall victim, often suffer greater psychological distress from scam attempts.
Initial efforts to work voluntarily with telecom operators proved insufficient, prompting ComReg to adopt mandatory measures formalised through regulatory decisions. These include blocking calls from “do not originate” and unassigned “protected” numbers, as well as improving international call routing, for instance, ensuring Irish fixed numbers don’t appear to come from abroad. A key mechanism is CLI roaming check: if a mobile number is not roaming abroad, calls from that number from abroad are blocked.
A major measure to be introduced by October 2025 is a voice firewall that uses real-time AI to detect and block suspicious calls dynamically, offering stronger protection than static filters.

Since CLI filtering began in October 2024, around 5.5 million scam calls have been blocked monthly, which is remarkable for a country of 5.5 million people.
To improve SMS security, ComReg has created a registry for SMS Sender IDs, allowing businesses to register official sender names. From 3 July 2025, unregistered IDs will be marked as “likely scam,” and from 3 October 2025, such messages will be automatically blocked. ComReg is working with bulk SMS providers to ensure readiness for these changes.
Another planned measure is a dynamic SMS scam filter, functioning like an email spam filter, capable of blocking malicious links and fraudulent content. According to Europe Economics, it could block up to 85% of scam texts, preventing around 40 million messages annually and delivering up to €500 million in benefits over seven years. However, its rollout is currently delayed due to the lack of legal authority, with ComReg actively pushing for enabling legislation - ideally using an opt-out or default-on model.
ComReg also faces structural and cultural barriers in enforcing user identification. Ireland lacks a national ID system, and anonymous prepaid SIMs remain available. Public resistance to mandatory identification complicates the adoption of SIM KYC (Know Your Customer) protocols. These gaps allow anonymity and hinder traceability, with evidence showing that prepaid SIMs are sometimes used in criminal operations. Telecom fraud is increasingly linked to organised crime, making this a matter of national and cross-border security.
ComReg advocates for a cross-sectoral approach to spoofing prevention, involving telecoms, banks, platforms, law enforcement, and policymakers. A multi-agency forum, led by the Banking and Payments Federation, has already been established to support quicker takedowns and coordinated public messaging. Regulators play a key role in enabling the legal and financial frameworks necessary for technical defences.
Mrs. Brennan concluded by stressing the importance of public education. Even with advanced AI filters, scammers continue to evolve. Educating consumers to spot scam patterns and act cautiously remains central to ComReg’s anti-fraud strategy.

Johannes Myhre Vallesverd – Norwegian regulator (NKOM)

During his intervention, Mr. Johannes Myhre Vallesverd presented a pragmatic and strategic perspective on tackling digital fraud, emphasising that collaboration is essential: not only among regulators and industry stakeholders, but also with law enforcement and international partners.
He outlined three key principles for an effective anti-fraud approach: a clear and deliberate decision to act, the allocation of adequate resources, and strong political and institutional support. In his view, fraud prevention is not merely a technical issue but a strategic one that demands leadership and prioritisation at the highest levels.
In Norway, Nkom has adopted a proactive approach, establishing a national task force on digital fraud involving the financial police, major banks, digital service agencies, and relevant ministries. This group meets regularly and operates with a shared mandate to detect, prevent, and respond to fraud in a coordinated way.
Among the main measures, Mr. Vallesverd described the launch of the “Digital Shield” initiative—a nationwide mechanism to filter and block fraudulent calls and SMS. Operators are required to block traffic from number ranges that are improperly allocated or unverified. A key component of this initiative is the roaming proxy introduced on 19 November 2024, which made Norway the second country after Finland to implement such a system. It assesses users' network status in real time to detect and block scam calls. Since its deployment, it has

intercepted over 60 million fraudulent calls, though fraudulent traffic still exceeds legitimate volumes—evidence of the threat's persistence and the need for continued vigilance. He stressed that the proxy's effectiveness relies on aggregating roaming checks across networks; otherwise, fraudsters may exploit gaps.
To prevent SMS impersonation, Norway has also introduced a Sender ID registry that ensures only authorised entities may use certain alphanumeric IDs. Over the past year, this system has contributed to the blocking of millions of scam messages and calls.
Strict Know Your Customer (KYC) requirements have been enforced for entities capable of generating large volumes of traffic, ensuring that the true originator of messages and calls can be identified. Without this, fraud mitigation measures risk being ineffective.
Looking forward, Norway is exploring the "polluter pays" principle, where those responsible for originating fraudulent traffic could face financial or operational consequences for the harm caused.
Internationally, Mr. Vallesverd highlighted the cross-border nature of fraud. Criminals exploit regulatory gaps between countries, making it essential to strengthen global cooperation. He encouraged wider participation in organisations or initiatives such as ECC WG NaN2, GIRAF, ETSI, BEREC, and The One Consortium – all focused on aligning responses and improving information exchange.
In Norway, Nkom has established a centralised fraud data archive to track patterns, assess the impact of interventions, and adjust responses. For instance, fraud tends to decrease during holidays and weekends, suggesting that many attacks remain human-driven rather than fully automated.
In closing, Mr. Vallesverd urged stakeholders not to wait for ideal solutions. The tools already exist—technical, regulatory, and organisational. What's needed now is decisive implementation, shared responsibility, and continuous cooperation. Even voluntary common standards could offer significant improvements and better protect users across Europe.

Session 4 – Panel discussion

The last session of the workshop on practical issues preventing number misuse and possible fraudulent activities, which was moderated by one of the BEREC's End Users working group co-chairs, gathered various stakeholders as well as representatives from EU institutions and bodies. Speakers exchanged views on the content of previous sessions and delved into specific topics relating to number misuse and fraudulent activities.

Alvaro Azofra Martinez – Europol

Responding to a question on how law enforcement agencies could improve cooperation and data sharing, given that fraud was considered a cross-border activity, Mr. Alvaro Azofra Martinez recalled that Europol's investigations always follow the same procedure and mentioned that every actor has a responsibility, also from the perspective of end-user protection, and that all the information needed is not in the hands of a single stakeholder. He underlined that, in this regard, there is a need for holistic legislation which clearly states the role and responsibility of each party. He also observed that since some European legislation

needs to be transposed to the national level, the result is sometimes a fragmented regulatory landscape, which leaves gaps for fraudsters to abuse. Mr. Azofra Martinez also stressed the importance of Know-Your-Customer measures.

In more details, Mr. Azofra Martinez said that concerning regulatory measures Europol believes that technological solutions are an important part of the response to criminal misuse of telecommunications services; however, they are not sufficient on their own. Without clear, effective regulation and policy, there is no certainty that technical measures will be implemented consistently or successfully. Existing regulations should be reviewed to identify and remove or amend provisions that hinder effective action, while new requirements should be introduced where necessary to strengthen the regulatory framework. Proactive engagement with regulators and legislators is essential to prevent new legislation or court rulings from creating legal gaps that could be exploited by criminals. Fragmentation of the regulatory framework across the EU is already being exploited by offenders, and stricter controls should be applied at critical points, such as Know Your Customer (KYC) procedures and other mechanisms addressing anonymity in services prone to abuse. The issuance and use of SIM cards require stronger regulation; in particular, the anonymous acquisition of prepaid SIM cards, commonly used by criminal groups, should be addressed. Automated detection systems implemented by industry, capable of flagging unusual call patterns, suspicious location behaviour, or bulk SIM registrations, can significantly reduce fraud. Direct, secure channels for urgent case coordination and real-time threat intelligence sharing are highly valuable in combating cyber threats.

As the Europol is an EU hub for criminal data, collected from and shared with Member States, they analyse, enrich, and coordinate actions leading to cross-border takedowns and arrests. Structured cross-sector operational partnerships have proven effective in tackling criminal activity, and closer cooperation with the telecommunications sector should be explored to identify additional solutions. To address the cross-border nature of fraud and improve efficiency, minimum harmonised rules at the EU level should be established, particularly regarding data formats, to reduce delays in processing telecom data and metadata. Established technical standards (e.g., ETSI) should be adopted for sharing (meta)data for cybersecurity and cybercrime prevention purposes.

Mr. Azofra Martinez also emphasised that security and privacy should not be opposed, quite the contrary: they go hand in hand, as security aims to protect citizens' privacy.

Alessandra Chiarini – European Banking Federation

Relating to the banking industry’s best practices for preventing fraud, Ms. Alessandra Chiarini highlighted the banking sector’s long-standing expertise in this area. She noted that the Payment Services Directive (PSD) represented a step forward, particularly through the introduction of mandatory reimbursement. However, Ms. Chiarini emphasised that this approach alone is insufficient to protect end-users effectively, as it does not address the root cause and that is consumer manipulation.

Referring to Authorised Push Payment (APP) scams, Ms. Chiarini explained that the novelty introduced by the Payment Services Regulation (PSR) proposal, covering bank employee impersonation fraud, would not necessarily enhance consumer protection or reduce fraud. She outlined three key reasons for that:

- Lack of source intervention**:** Victims are manipulated into authorising payments before the transaction reaches the banking system, meaning the problem arises well before the bank's involvement.
- Shared responsibility across sectors**:** Fraud typically involves a chain of events, and platforms such as social media providers and telecommunications operators should share responsibility. While some initiatives are in place, more coordinated action is needed.
- Risk of reduced vigilance: Mandatory reimbursement may unintentionally encourage users to be less cautious online, fostering a belief that any losses will be covered regardless of their actions.

In addition to awareness-raising initiatives for both customers and employees, banks also implement preventive mechanisms such as payment limits—set either by customers or by the bank itself—and "cooling-off" periods before executing transactions. Ms. Chiarini concluded by stressing that effective fraud prevention ultimately depends on the ability to detect suspicious activity early, through a deep understanding of criminal modus operandi.

Ms. Chiarini also argued that enforcement of existing regulation, such as the Digital Services Act, should be given a chance, claiming, for instance, that fraud is by definition illegal content. Ms. Chiarini also mentioned that transaction monitoring should involve all the ecosystem's actors and not be limited to payment service providers only and explained that some countries like Australia have already implemented this approach.

Angela Coriz – Connect Europe

When asked about the role of electronic communications service providers in preventing fraud, Ms. Angela Coriz emphasised the importance of clearly understanding the responsibilities of each party, particularly at every stage of the process. From the perspective of telecommunications operators, Ms. Coriz stressed that their primary function is to act as carriers of information, operating upstream in the process and therefore having only a limited view of the fraud itself. To illustrate this, Ms. Coriz used the metaphor of the mailman: delivering the message but not opening or examining it, for privacy reasons. Ms. Coriz also pointed out that certain legislative provisions, especially when fragmented, as in the case of the ePrivacy Directive, can create obstacles to effective action.

Ms. Coriz underlined that cooperation among all actors involved must be the cornerstone of any strategy to combat fraud. As no single party has a complete overview of this type of criminal activity, effective communication and collaboration are essential. Existing successful

cooperation mechanisms at the national level can serve as valuable examples for developing productive approaches.

Ms. Coriz further stressed that any solution should be grounded in legal certainty, harmonisation, and flexibility. Given that fraudsters continuously develop new techniques, countermeasures must be equally adaptable and capable of rapid adjustment; otherwise, they quickly become outdated. A harmonised understanding of what telecommunications operators are permitted and not permitted to do, while still complying with applicable regulations, is therefore crucial to ensuring an effective and coordinated response.

At the end, Ms. Coriz emphasised that cooperation across sectors is key and therefore stressed the need for enhanced cooperation. In this regard, Ms. Coriz mentioned some good current examples that one could learn from, such as in The Netherlands, with voluntary coordination between banks, operators and additional task forces which has proved to be very successful.

Katja Kmet Vrčko – BEREC, Cybersecurity and Resilience working group

Ms. Katja Kmet Vrčko underlined that NRAs have a specific role for the market, as well as BEREC at EU level, as regulators are concerned about safeguarding end-users. Ms. Vrčko also mentioned that the whole ecosystem should tackle fraudulent activities, as operators are also victims of fraud, while stressing that coordination and synchronisation are essential. In addition, Ms. Vrčko noted that fraudulent activities are not limited to electronic communications alone, taking the example of scams on social networks. Ms. Vrčko also stated that ongoing dialogue with ecosystem players should be strengthened, and she acknowledged that enforcement was not sufficient at present and that some national dispositions could be reopened, without undermining privacy, in order to move forward quickly in this regard.

Mariana Figueiras Alves Dos Santo – DG FISMA, European Commission

When asked about the measures the European Commission is taking to protect consumers from fraudulent activities, Ms. Mariana Figueiras Alves Dos Santo highlighted the Revised Payment Services Directive (PSD2) and its imposition on regulated entities to implement two-factor authentication systems as an effective tool, at least at the time, for preventing fraud. While emphasising that consumers should feel safe within a diverse payment ecosystem, Ms. Dos Santo acknowledged that manipulation fraud now accounts for more than half of all payment fraud.

Ms. Dos Santo stressed the inherent complexity of the situation, noting that there is no single “silver bullet” solution. She emphasised the importance of maintaining a robust anti-fraud toolkit, a principle which the European Commission has considered when reviewing PSD2. According to Ms. Dos Santo, this toolkit rests on three main pillars which are enhanced

information for payment service users, consumer awareness campaigns, including updates on current fraud trends, and transaction monitoring.

Finally, Ms. Dos Santo underlined the necessity for payment service providers to have the appropriate tools at their disposal and stressed that all feasible measures to combat fraudulent activities should be implemented as quickly as possible.

Ms. Dos Santo stressed the need for cross-sectoral cooperation. In this respect, the European Commission's proposal for a regulation on payment services provides for an obligation of cooperation between electronic communication service providers and payment service providers.

Claudio Texeira – BEUC

Mr. Claudio Texeira emphasised that there is often a tendency to attribute responsibility to others rather than oneself. He noted that, given the current level of number misuse, as a result of new technologies, it is essential to ensure thorough implementation of existing legislation.

Highlighting that end-users can only be defrauded if scammers gain access to their personal data, Mr. Texeira called for more effective enforcement of the General Data Protection Regulation (GDPR), stressing that this legislation should not be reopened. The same principle applies to cybersecurity rules. Overall, he argued that regulatory provisions must first be properly enforced before questioning their adequacy.

With the rise of new technologies making fraud increasingly sophisticated, sometimes to the point where it is unclear to users when they are being scammed, Mr. Texeira advocated for a proactive approach. This includes acting directly at the source of scams and implementing a series of preventive filters. Using the metaphor of the mailman, he explained that while a messenger's role is to deliver information, suspicious or unknown correspondence must be checked or withheld.

Finally, Mr. Texeira stressed that existing rules are sufficiently clear, and that enforcement must be taken seriously. Regulatory authorities, including NRAs and EU bodies responsible for ensuring compliance, must be provided with adequate resources to carry out their mandates effectively.

Next steps and recommendations for further work

The different perspectives presented during the Workshop tended to converge on a few common points. First, speakers underlined the need for continued collaboration between various actors. The collective expertise and diversity of the interventions show how essential collaboration is to achieve meaningful solutions. Also, technical solutions implemented should

support a systemic approach, and legal requirements should not prevent efficient anti-scam feasibility.

All speakers agree that proper technical solutions, efficient enforcement of the requirements established, together with education of the experts and end-users should be key in the developing environment.

After careful consideration of the expert content and discussions during the Workshop, it is important that BEREC is also kept well informed about relevant issues related to end-user trust in digital services and digital ecosystem. In doing so, BEREC will be equipped with relevant information about the changing world and the outcome of newly adopted legislation in order to actively contribute to fostering collaboration among all relevant actors involved in the prevention of fraudulent activities.

All the slides (non-confidential versions of them) are published on the BEREC website.

Annex I – Workshop Agenda

BEREC Workshop on practical issues preventing number misuse and possible fraudulent activities

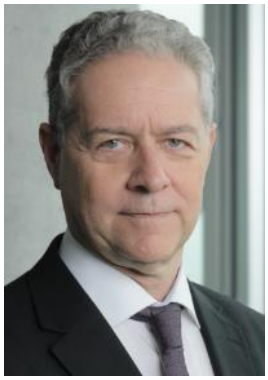
21 May 2025, Brussels (Belgium)

Location	**IRG Secretariat** Rue de la Science 14, 3rd floor B-1040 Brussels
Date & Time	**21 May 2025 10:00 – 16:00**

9:30-10:00	**Welcoming coffee/tea**
10:00-10:05	**Opening speech** • Tonko Obuljen, BEREC Vice-Chair 2025
10:05-10:35	**Session 1: Overview of the problem** • Rens Grim – GASA • Els Bruggeman – Euroconsumers • Marnix Dekker, – ENISA
10:35-12:10	**Session 2 – Stakeholders perspective** • Rita de Castro – GSMA • Katia Gonzalez Gutierrez – BICS • Tomas Grinevičius – Telia Lietuva, AB • Filip Filković – Infobip • Tomas Jakimavičius – Microsoft Q&A/Discussion
12:10-13:00	**Lunch Break**
13:00-14:15	**Session 3 – NRAs activities and regulatory measures** • Laurence Nivot – Cullen International • Alīna Stafecka – Latvian regulator (SPRK) • Darius Kuliešius – Lithuanian regulator (RRT) • Sharon Brennan – Irish regulator (ComReg)

	• Johannes Myhre Vallesverd – Norwegian regulator (NKOM) Q&A/Discussion
14:15-14:30	**Coffee Break**
14:30-15:55	**Session 4 – Panel discussion** • Mariana Figueiras Alves Dos Santos – European Commission • Katja Kmet Vrčko – BEREC • Claudio Texeira – BEUC • Alvaro Azofra Martinez – Europol • Angela Coriz – Connect Europe • Alessandra Chiarini – European Banking Federation Q&A/Discussion
15:55-16:00	**Closing Remarks** BEREC End User Working Group co-chairs

Annex II – Speakers Bios



Tonko Obuljen, the BEREC Vice Chair 2025

President of the Council of Croatian Regulatory Authority for Network Industries (HAKOM) in 2018 and is currently serving his second five-year mandate. Prior to the presidency, he served as Director of HAKOM from 2006 to 2009 and as a Member of HAKOM's Council from 2009 to 2013. During the accession of the Republic of Croatia to the European Union (2005-2013) he was a member of the Information Society working group and also served as a member of the drafting teams for the harmonization of Electronic Communications Act and bylaws with EU legislation. From 1993 to 2006, he worked in the Croatian electronic communications industry, mainly in microwave and satellite communications. He participated in developing the Croatian state aid programs for backhaul and access networks and in setting up current end-user protection ecosystem in Croatia. In 2020, Tonko Obuljen also served as a Vice-Chair of the Body of European Regulators for Electronic Communications - BEREC.

Indrė Jurgelionienė, Co-chair of the BEREC EU WG

Indrė Jurgelionienė is a Chief Advisor at the Communications Regulatory Authority of the Republic of Lithuania (RRT). She joined RRT in 2013. Indrė has been, among other things, resolving out-of-court disputes between end-users and communication service providers, responsible for forecasts and data analysis of trends and developments in the regulated sectors, and international communications. She has also been engaged in various regulatory aspects, including access and ex-ante regulation, universal service provision, numbering and number portability, complaint handling, and consumer protection in electronic communications and postal sectors. Indrė has experience in team management as well as public policymaking and implementation, including the transposition of European Union legislation into national law and involvement in various national multi-stakeholder projects on both national and international levels. Indrė holds a Bachelor's degree in Law and a Master's degree in Civil law – from Mykolas Romeris University (Lithuania).

Marina Ljubić Karanović, Co-chair of the BEREC EU WG

Marina Ljubić Karanović is a Senior Legal Expert, Deputy Head of the Legal Affairs Department at the Croatian Regulatory Authority for Network Industries (HAKOM). At HAKOM, Marina provides legal support for all of HAKOM's activities, especially regarding consumer regulation and consumer protection strategies. Marina is involved in resolving disputes between consumers and operators, representing them in court in consumer disputes, drafting regulations under the Electronic Communications Act, and overseeing and ensuring compliance of terms of use and price lists with Telecoms Regulations. In addition, she actively participated as a Croatian expert participant in the adoption of the European Electronic Communication Code in the Council of the European Union. Furthermore, she has extensive media experience, participating in media, radio and Television programmes on consumer protection together with press statements.

Rens Grim, Global Signal Exchange Advocate GASA

Rens Grim is a dedicated team member at the Global Anti-Scam Alliance (GASA), where he works to engage stakeholders across both public and private sectors in support of the Global Signal Exchange (GSE). The GSE is a groundbreaking initiative aimed at creating a global clearinghouse for indicators of criminal behavior. His mission is to build strong partnerships that contribute to a unified global overview of malicious actors, raising the bar in the fight against fraud and online scams.

Els Bruggeman, Head of Policy and Enforcement, Euroconsumers

Els Bruggeman is Head of Policy and Enforcement at Euroconsumers, a leading global consumer group that gathers five national consumer organisations: Testachats (Belgium), Altroconsumo (Italy), OCU (Spain), Deco Proteste (Portugal) and Proteste (Brazil). Together, they represent almost one and a half million consumers. Els is responsible for all policy-related issues, with a specific focus on digital and sustainability, and has also coordinated joint enforcement cases, such as the class actions against Volkswagen (Dieselgate) and Apple (premature obsolescence) that were launched in Belgium, Italy, Spain and Portugal. Els joined the consumer movement in 2014 when she started working as an EU Public Affairs advisor for the Belgian consumer organisation Testachats/Testaankoop. Before, she was active for more than 10 years in the political world, both as a policy advisor and spokesperson, i.e., for the Belgian minister of consumer protection. Els Bruggeman has Master Degrees in both History and Law, and an Advanced Master's in International Politics and Conflict & Development Studies. She is a member of the Executive Board of BEUC (European umbrella organisation for consumers).

Marnix Dekker, Marnix is the Deputy Head of Unit for Resilience of Critical Sectors at ENISA, the European Union Agency for Cybersecurity. He leads a team of experts supporting the EU Member States with the implementation of the NIS Directive and with increasing the cybersecurity and resilience of the EU's critical sectors. His team works on the implementation of policies such as NIS2 and DORA, on the Union-wide risk evaluations supporting the EU 5G toolbox and Nevers process, on the NIS2 implementation in critical sectors such as Telecoms, Energy, Finance, Transport and Health.

In the past, he was the deputy CISO of the European Commission, and before joining the EU institutions, he worked as an IT architect for the Dutch national digital identity systems.

Marnix has a Ph.D. degree in Computer Security and a Master's degree in Quantum Physics.

Rita de Castro has 15 years of experience in European public and regulatory affairs, with a strong focus on the digital and telecommunications sectors, and a mix of international private sector and public sector experience.

Rita worked in the European Commission Directorate General for Communications Networks, Content and Technology (DG CONNECT). She was EU Affairs Manager for Hutchison Europe (Three Group). Having also worked for a consultancy specialising in European public and regulatory affairs, advising FTSE 100 clients, Rita has extensive experience in the sector.

Rita holds a Master's in European Political & Administrative Studies from the College of Europe. She graduated from Lisbon Nova University. As a Portuguese native, she is also fluent in English, French and Spanish.

Katia González, Head of Public Policy, Proximus Global

I3Forum Board member, chair of i3Forum Fight Fraud workstream and Leadership Council for One Consortium

After spending almost 15 years heading the anti-Fraud and Security operational and product management activities at BICS, and a strong believer in the value of cooperation, Katia González is ever more motivated and committed to and actively working in enabling collaboration in the International communications industry to Restore Trust in communications.

Katia has been an active member of the i3Forum Board for the past 4 years and has been chairing the i3Forum Fight Fraud workgroup for more than 10 years. Additionally, Katia has actively participated in the creation of One Consortium in March 2024 and GIRAF in June 2024, each representing the Industry at large and the National Regulatory Authorities, respectively, to restore trust in international communications and is part of its Leadership Council.

With more than 20 years of experience in the Mobile and Wholesale Telecom industry, Katia has held different positions in the National and International Telecoms Carrier Business providing a complete understanding of the various aspects of the business, its challenges and more specifically of the fraud and security risks for the different industry verticals (M(V)NO, OTT, IoT, Enterprise, Cloud Communications, wholesale, etc.) and the cross-sectoral impact of telecommunications-enabled fraud and scams.

Tomas Grinevičius, Leading Service Architect | Network, Telia Lietuva, Lithuania

Biography

Tomas Grinevičius was born in 1980 in Lithuania. He obtained a Master's Degree in Telecommunication and Electronics from Kaunas University of Technology.

Tomas started his career as an engineer in a solution integration company and was promoted to technical project leader after a few years. He gained experience in different fields: VoIP, LMDS, synchronisation, network security, billing, mediation and integration into solutions for customer needs.

Since 2006, Tomas has been working at Telia as a telephony network and services development expert and architect. He had various responsibilities related to voice and messaging network and service transformation, evolution, strategy development, and its execution. His main fields are smooth IMS environment development and ensuring ecosystem quality, safety and performance.

Filip Filković is a seasoned telecommunications executive with over 12 years of international experience in strategic leadership, consultancy, and partnership development across the global telecom ecosystem. As Telecom Business Director at Infobip, Filip leads initiatives empowering mobile operators with innovative fraud prevention, revenue assurance, and messaging security solutions. He specialises in helping operators address emerging threats such as A2P SMS fraud, grey routes, and the impact of OTT messaging platforms, drawing on a deep understanding of both regulatory frameworks and advanced security technologies. Filip has worked closely with mobile network operators, regulators, and industry bodies throughout Europe, Africa, and beyond, providing expert guidance on telecom security, monetisation, and compliance. Filip is recognised for his thought leadership in the areas of network security, fraud prevention, and digital transformation, and is committed to fostering collaboration between industry stakeholders to build a safer and more resilient communications landscape.

Tomas Jakimavicius, Director of Government Affairs, Microsoft

Tomas is a European Government Affairs Director at Microsoft, focusing on Digital Infrastructure, Connectivity, and Cloud policies. Tomas has a wide range of senior-level experience in both private and public sectors, specialising in digital and tech policy. Before Microsoft, Tomas led the European Government & Regulatory Affairs department at the global mobile operators' trade association. Earlier in his career, he worked in the public sector and served as a diplomat at the Council of the European Union. Tomas also steered the planning and preparation of the first Lithuanian Presidency of the EU Council in the field of digital & tech policy, where he also chaired relevant EU Council Working Groups comprised of the EU Member States' representatives that negotiate EU laws before national ministers approve them. He holds a master's degree in Leadership with International Relations concentration, a master's degree in Enterprise Information Systems, and has further specialised in diplomacy studies focused on the legal and institutional system of the EU and international negotiations.

Laurence Nivot, Manager, Cullen International

Laurence leads Cullen International's research on consumer protection, publishing country-by-country comparisons on key regulatory topics. She also monitors telecoms regulatory developments in Belgium and Lithuania. Before joining Cullen International in 2012, she worked for the European Commission's news website. Laurence holds a master's degree in European Law from the Aix-Marseille University (France).

Darius Kuliesius brings extensive leadership experience in the fields of national security, transport, and communications.

In addition to contributing to the broader objectives of the EU Digital Decade, his recent focus has been on enhancing the resilience and security of the electronic communications sector, protecting consumers in the digital environment, and driving innovation through the implementation of change-oriented projects. He holds a Master's degree in Law and Management from Mykolas Romeris University (Lithuania).

Alina Stafecka is the Chief Networks Infrastructure Expert at the Public Utilities Commission of Latvia (SPRK), with a decade of experience in the field. Her expertise primarily encompasses interconnections, numbering, and fraud prevention related to numbering. Alina has also been involved in various regulatory topics, including access networks and frequency spectrum allocation. She holds a PhD in Telecommunication Engineering from Riga Technical University, where she continues to contribute to scientific research and shares her knowledge as a docent and researcher. Alina is actively engaged in the activities of the CEPT Working Group on Numbering and Networks (WG NaN), where she serves as the Vice-Chair of WG NaN2 – the working group addressing regulatory issues related to number portability, switching, trust in numbering, and network technology.

Sharon Brennan is the Manager of Network Trust in ComReg, the Irish Communications Regulator, a new team set up to develop and implement a national strategy that will position Ireland as a leader in nuisance communications mitigation.

The objective is to constantly evolve interventions to maximise consumer protection and minimise the adverse impact of scams on society and the economy.

Previous to this, she worked in Ericsson for 25 years, having many different roles.

Johannes Myhre Vallesverd is a senior legal advisor and team leader of the antifraud team in the Norwegian Communications Authority. He is chairing the Norwegian expert group against digital fraud and the Global Informal Regulatory Antifraud Forum.

Mariana Santos is a Policy Officer in the Retail Financial Services unit at the Directorate-General for Financial Stability, Financial Services and Capital Markets Union of the European Commission. Over the last two and a half years, she has worked on the review of the second Directive on Payment Services in the internal market (PSD2), with a particular focus on fraud prevention. Mariana holds a PhD in Financial Geography from Durham University, UK, and before joining the European Commission, worked as an academic researcher at the Vrije Universiteit Brussel.

Katja Kmet Vrčko is a lawyer with more than 20 years of experience in electronic communications. Prior to her current role as Advisor to the Director for International Affairs, she was heading the Inspection and Security Department at Slovenian regulators AKOS for 9 years. She is an active member of different European expert working groups in the cybersecurity field. Since 2019, she has served as a Co-Chair of the BEREC Cybersecurity and Resilience Working Group, which cooperates with the European Commission, NIS 5G Cooperation Group and ENISA. For the second mandate, she was appointed as a BEREC representative to the ENISA Advisory Group.

Alvaro Azofra Martinez is the Head of Expertise and Stakeholder Management Unit of the European Cybercrime Centre (EC3) at Europol. After receiving his Bachelor of Science in Computer Science, he started his professional career in the private sector as a Software Engineer. Later on, he joined the Spanish National Police working on Counter Terrorism and National Critical Infrastructure Protection Cyber domains. He joined Europol in 2017, and in different roles he supported international Law Enforcement investigations, managed pan-European Law Enforcement projects and developed partnerships with public and private stakeholders. His Unit is responsible for the management and steering of the Industry and Academic Advisory Groups of EC3, the coordination of Cyber (Offender) Prevention and Awareness campaigns, e-Governance and Lawful Access to Data initiatives, the draft of strategic reports like the Europol's flagship report on cybercrime known as Internet Organised Crime Assessment (IOCTA), research and development of new technologies like AI and Quantum and capacity building projects among other commitments.

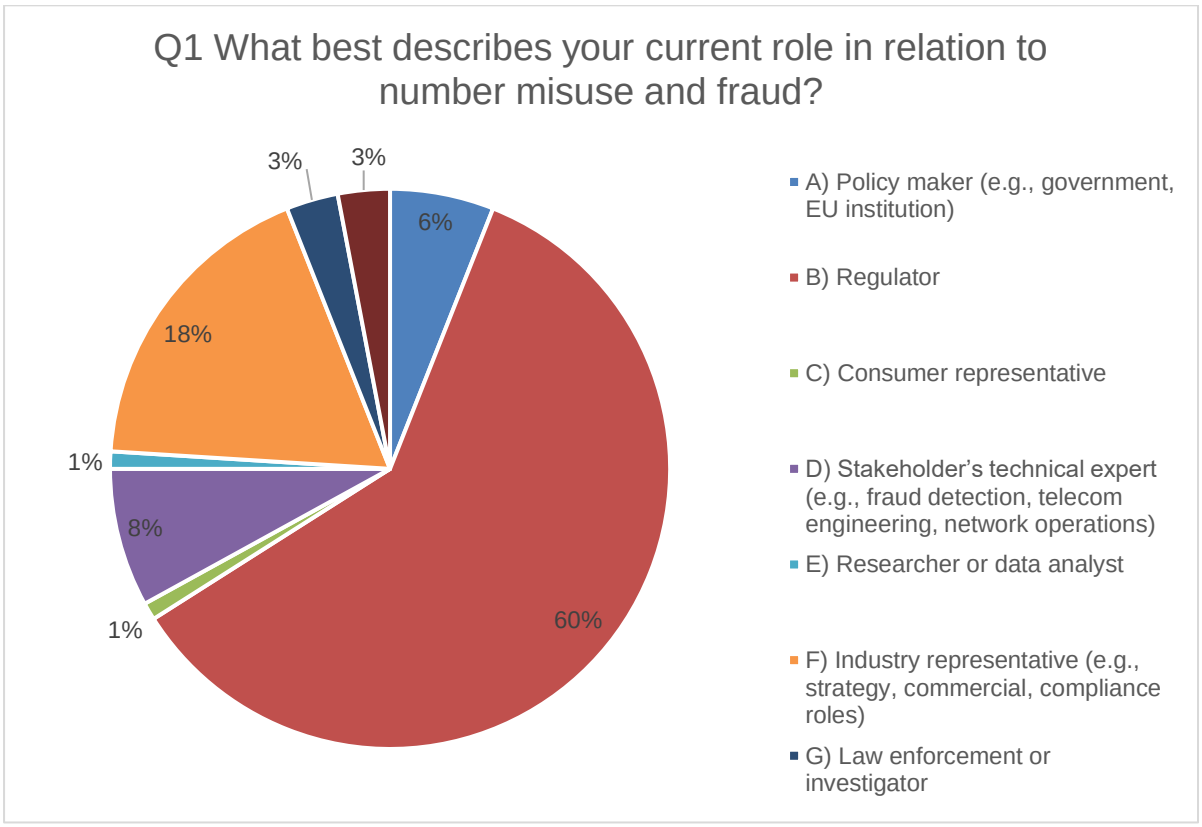
Cláudio Teixeira, Legal Officer, Digital and Consumer Rights, BEUC

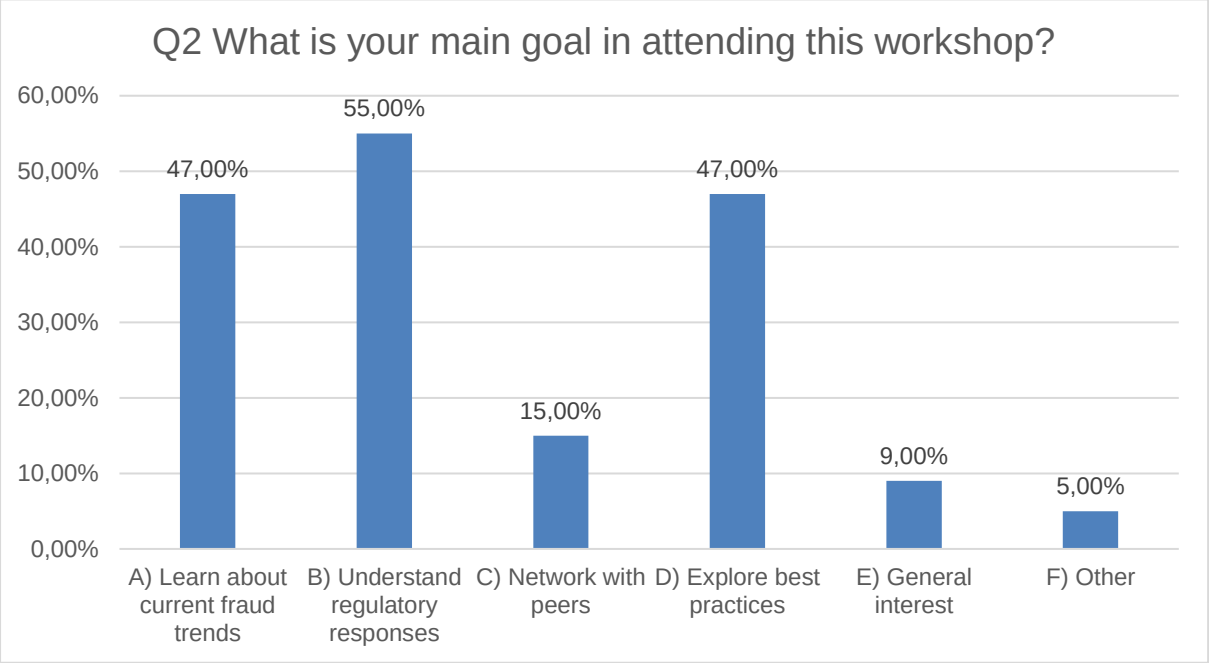
Cláudio Teixeira is a Senior Legal Officer for Digital Rights in BEUC, the European Consumer Organisation, working on telecommunications, digital services and cybersecurity. As a law graduate, holds a Bachelor and Master of Laws in International and European Union Law from the University of Coimbra in Portugal, and a LL.M. in European Law from College of Europe in Bruges, Belgium. Prior to joining BEUC, Cláudio served as a Junior Legal Attaché in the Permanent Representation of Portugal to the European Union in Brussels during the Portuguese Presidency of the Council of the EU in 2021, working on the institutional negotiations of the Digital Markets Act and the Public CbCR Directive.

Angela Coriz joined Connect Europe in January 2024 as a policy officer. She is part of the regulatory and public policy team, and focuses primarily on artificial intelligence, taxation, international affairs, and naming, addressing and numbering. Prior to this, she was working as an assistant to the Regulatory Affairs Department of WSBI-ESBG, an association representing European Savings and Retail Banks. She holds a European Master's in Global Studies from Universiteit Gent and Universität Leipzig, and holds a double Bachelor's degree in Global Affairs and French from George Mason University in the US.

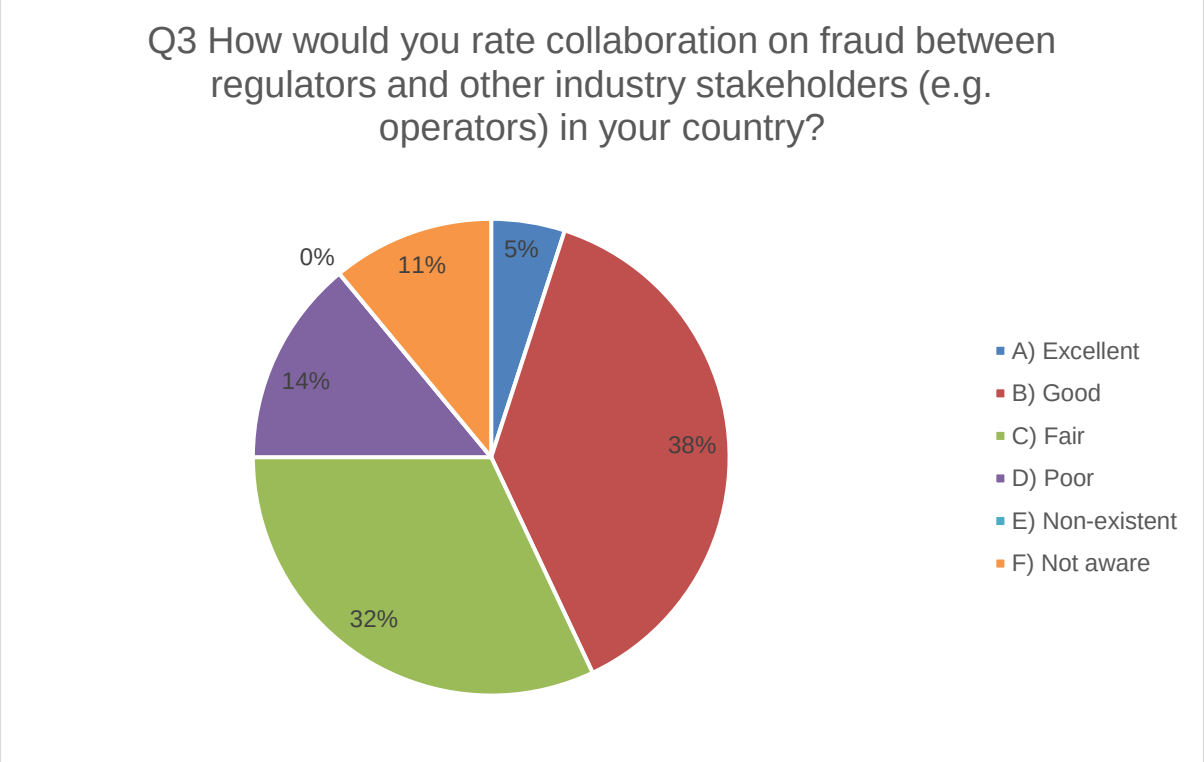
Alessandra Chiarini is a Policy Adviser in Payments and Innovation at the European Banking Federation (EBF). As part of the Innovation and Cybersecurity teams, she contributes to key initiatives across multiple digital finance policy files with a focus on fraud in payments. Before joining the EBF, Alessandra gained experience in data protection, data economy, and digital rights through various roles and internships. She holds a Master's degree in Law with a specialisation in Economics, blending legal expertise with an understanding of digital policies to navigate complex regulatory environments.

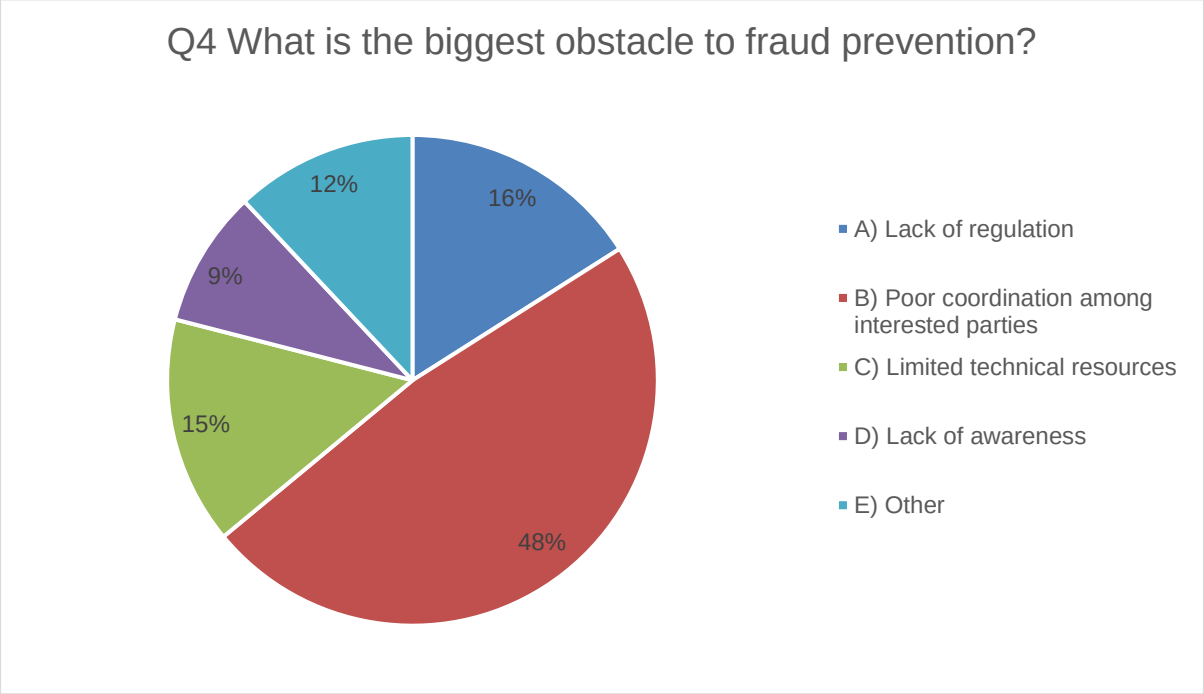
Annex III – Results of the live poll during the workshop

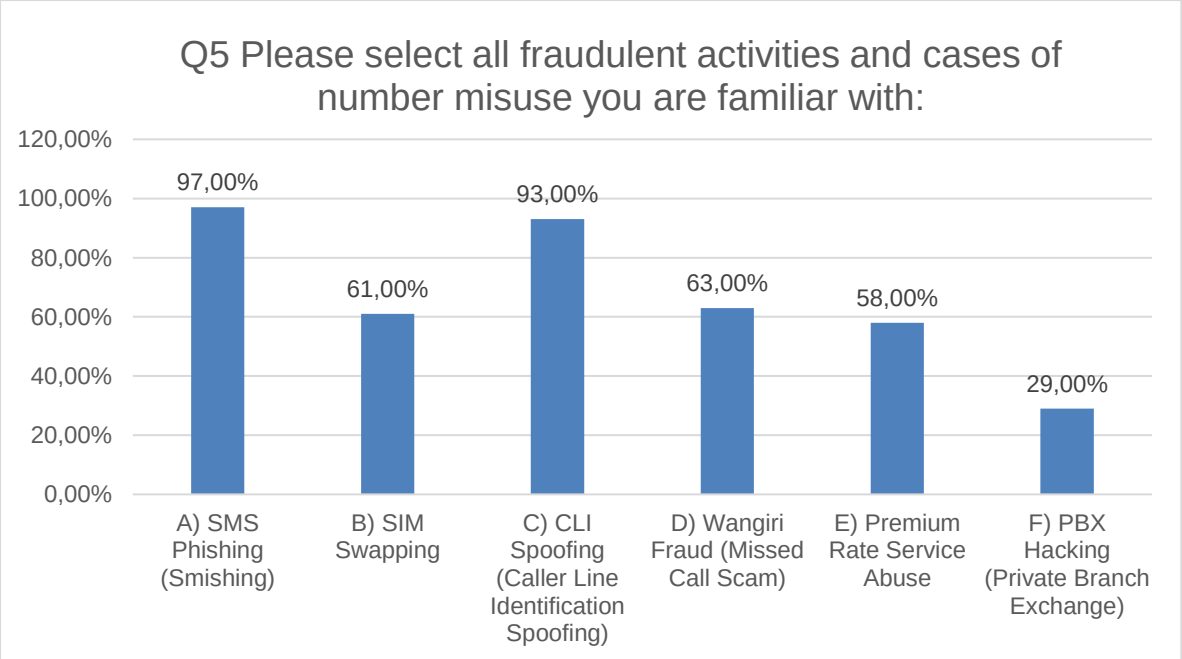




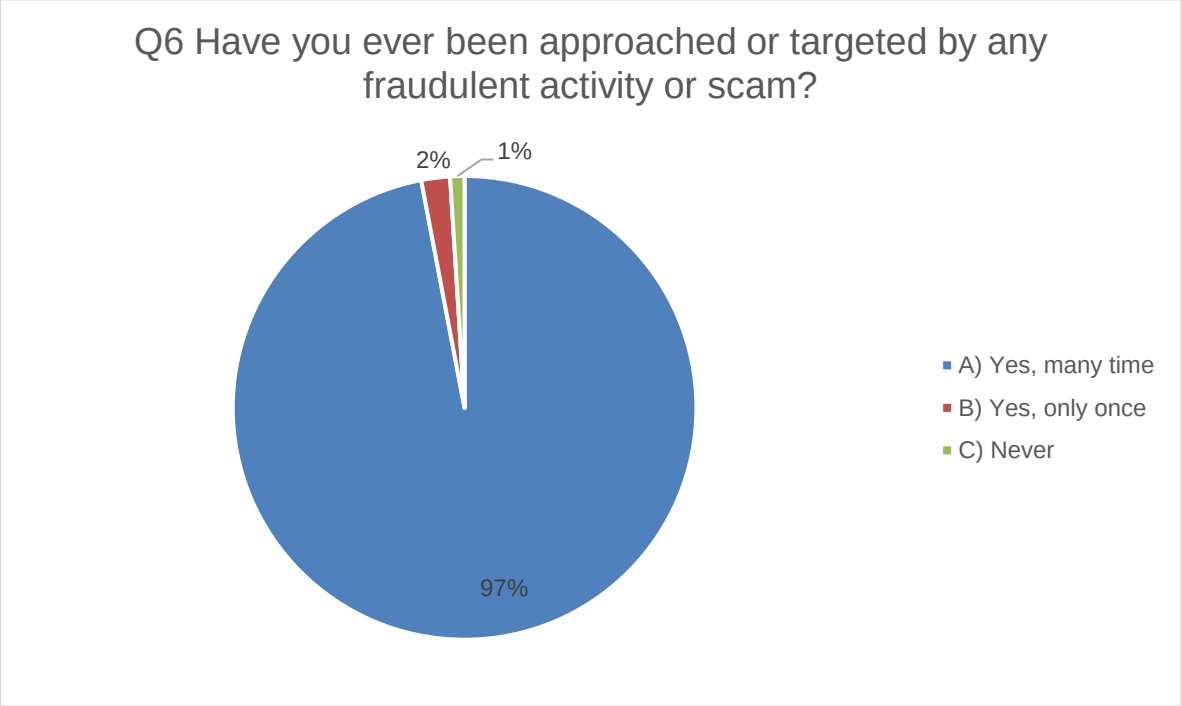
Multiple answers were possible for this question

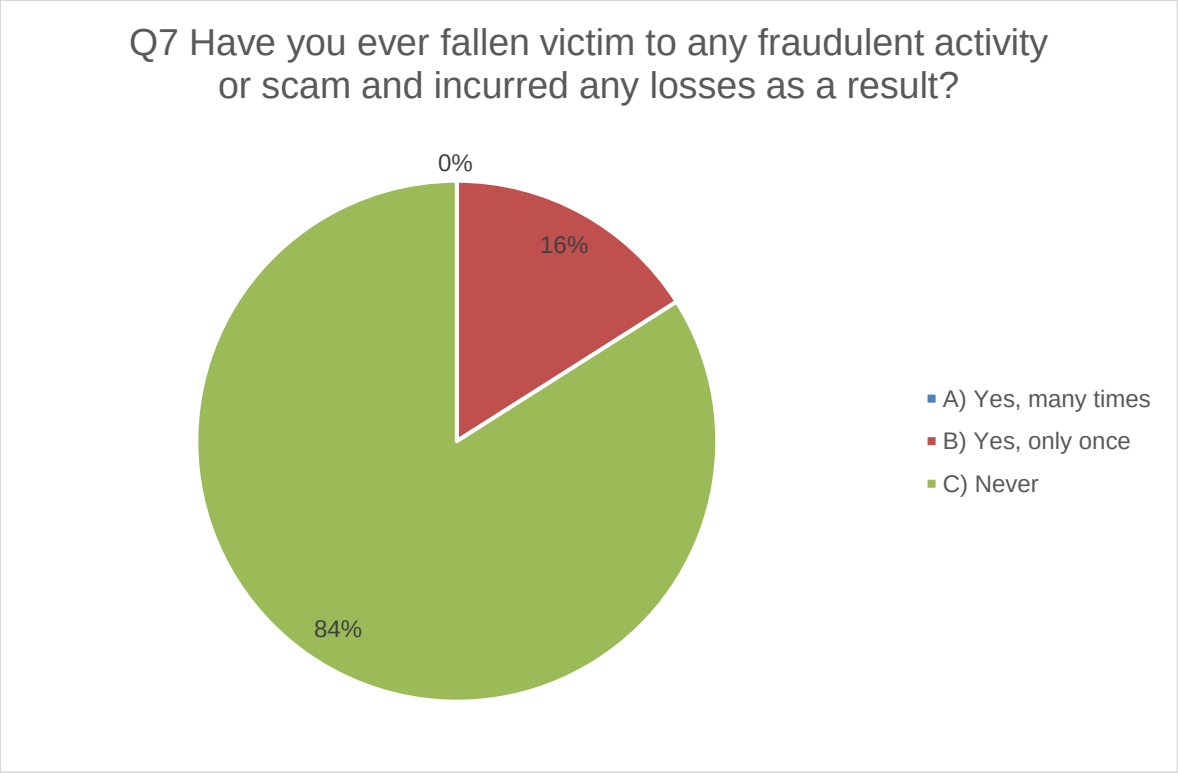


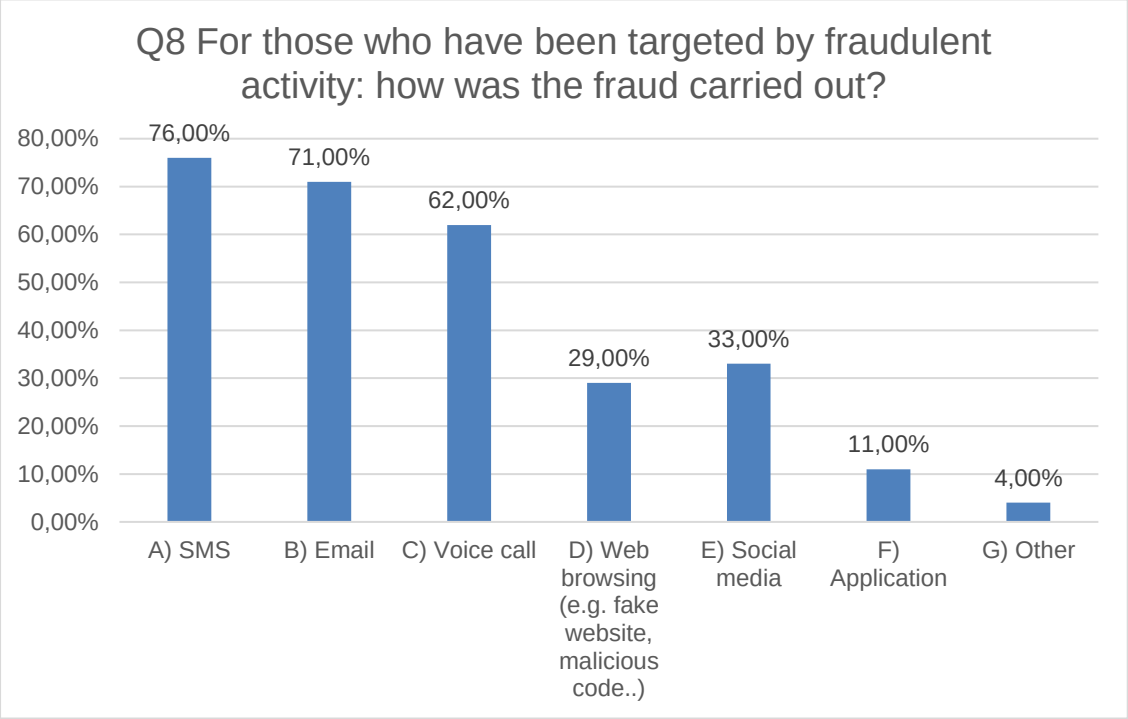




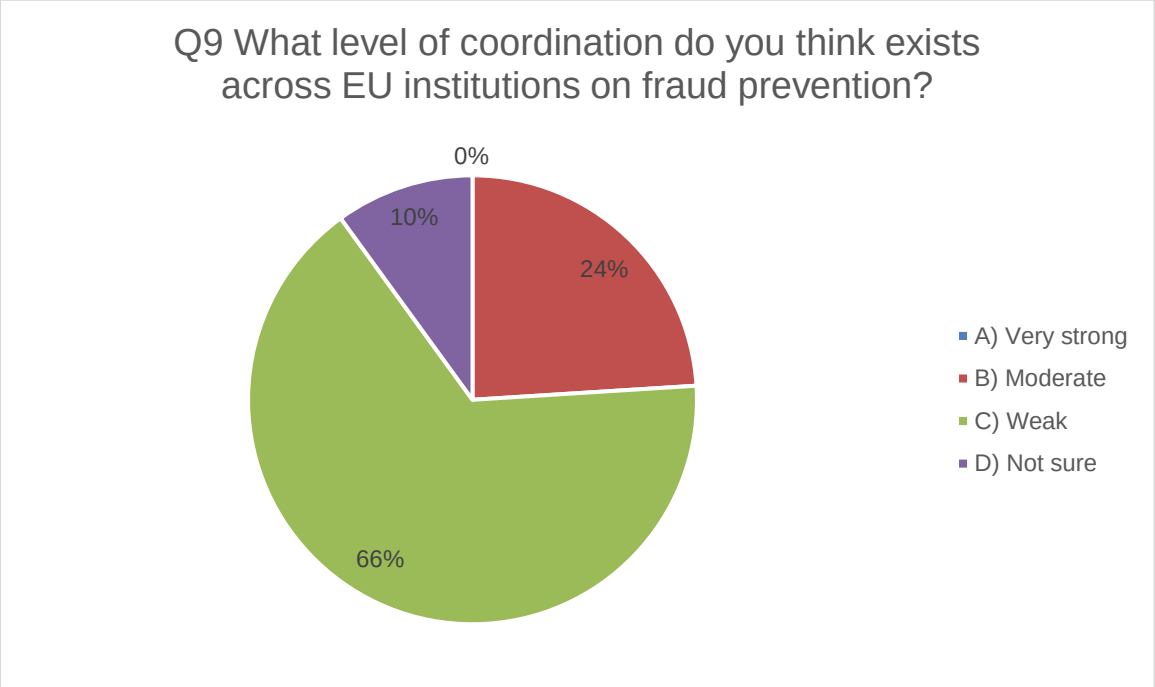
Multiple answers were possible for this question

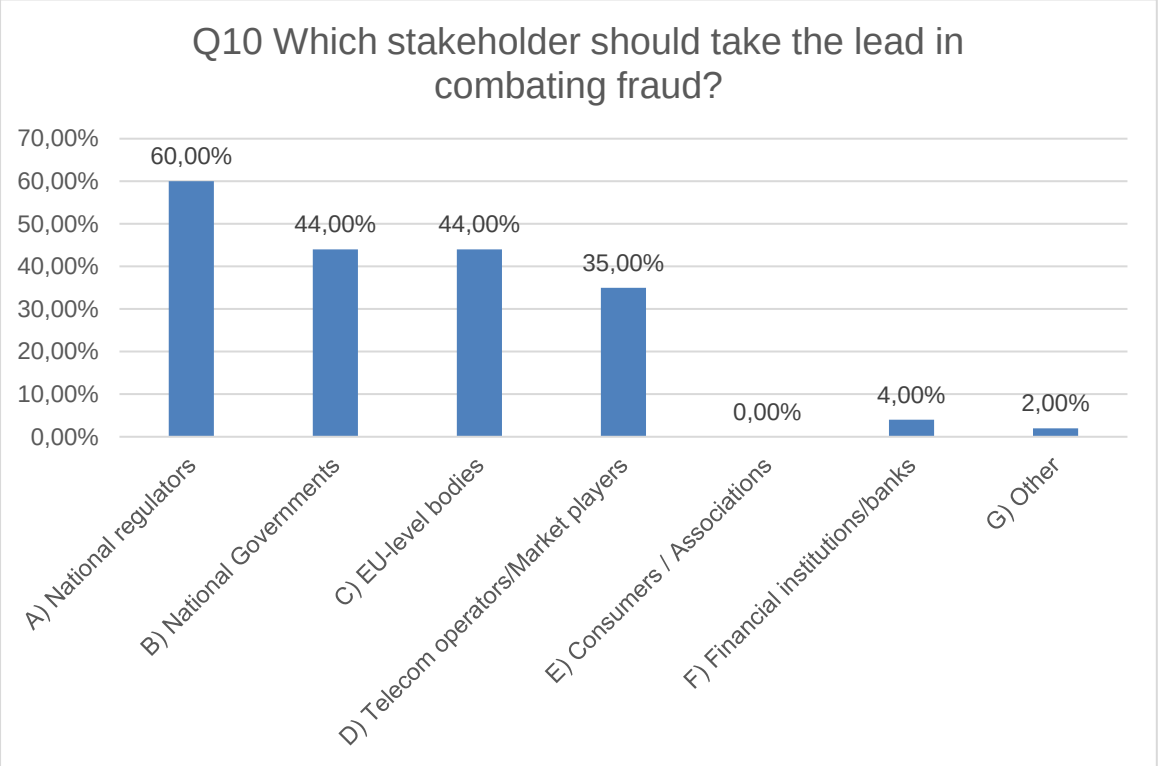

Q6 Have you ever been approached or targeted by any fraudulent activity or scam?
2%
1%
97%
A) Yes, many time
B) Yes, only once
C) Never


Q7 Have you ever fallen victim to any fraudulent activity or scam and incurred any losses as a result?
0%
16%
84%
A) Yes, many times
B) Yes, only once
C) Never



Multiple answers were possible for this question





Multiple answers were possible for this question