BEREC
Body of European Regulators for Electronic Communications

Responses to Survey of NRAs and MSPs

BEREC External Workshop on Combating Fraud

Sharon Brennan

Manager Network Trust ComReg

21 May 2026

#empowering EUconnectivity

NRA Survey Q&As

- Does your country have any legal or regulatory instruments that allow the fight against spoofing and other types of frauds carried out through electronic communications, where the end-user receives fraudulent communications?
  - Yes 23/28 No 5/28
- Do you consider that those legal or regulatory instruments are sufficient to combat all types of spoofing and other types of frauds carried out through electronic communications?
  - Yes 3/23 No 20/23
- 22/23 Block calls that are assessed as scams
- 9/23 SMS SenderID Registry in place
- Do the current legal and regulatory instruments allow to check the content of SMS? For example, check if there is any potential fraudulent link.
  - Yes 5/28 No/Other 18/28

NRA comments

- Regulations must be constantly updated to meet the ever-changing fraud landscape
- Currently there is a limited applicability to OTT services which tend to fall outside telecom regulation.
- Certain fraud types remain difficult to be fully addressed, particularly SMS spoofing through content analysis and OTT-based scams.
- ComReg are unable to mandate content scanning for SMS as we do not have an appropriate legal basis.

MSP Survey Responses

- Interventions implemented currently
  - Vast difference in interventions implemented between various countries
  - Blocking calls is the primary intervention implemented (45/83)
  - Scanning/Analysing SMS content/structure is lowest (8/83)
- Both of the above are the main interventions that MSPs would like to see underwritten in national legal and regulatory instruments
- Do you believe that the regulator sufficiently understands the practical challenges of implementing measures to combat spoofing and other types of frauds carried out through electronic communications?
  - Yes 52/83

MSP Comments

- Does the fact that national legal and regulatory instruments do not allow you to implement measures, have an impact on your business and on the relationship with your end-users?
  - Yes. Legal and regulatory limitations negatively affect both business operations and the relationship with end-users, by restricting the deployment of effective fraud-prevention measures and impacting customer trust, satisfaction and operational efficiency.
  - Yes, both our subscribers, media, banks and politicians' express expectations that we should protect users from online fraud.
  - "Yes. The current national legal and regulatory framework has a tangible impact on our business and on our ability to effectively protect end users against fraud.
  - National rules are heavily dependent on the interpretation of the ePrivacy Directive, whose outdated and imprecise wording is increasingly ill suited to addressing modern fraud schemes…. This creates a high degree of legal uncertainty, making it difficult for operators to invest in and develop robust fraud prevention tools.
  - Key legal measures that hinder the implementation of anti-fraud measures include the secrecy of telecommunications (Fernmeldegeheimnis), the Telecommunications Digital Services Data Protection Act (TDDDG) and the General Data Protection Regulation (GDPR). Together, these frameworks restrict the analysis and processing of communications content and traffic data, thereby limiting the scope for proactive and data-driven fraud detection by operators of legal uncertainty, making it difficult for operators to invest in and develop robust fraud prevention tools.

Conclusions

- Fraudulent activities are becoming increasingly sophisticated, particularly through the use of artificial intelligence.
- When a new measure to combat fraud is implemented, fraudsters quickly evolve and adapt, discovering new methods and channels to continue their activities or discovering countries that do not have such measures implemented.
- Regulation must quicky adapt to successfully combat an ever-evolving scam ecosystem.
- The legislation should not limit the possibility to combat all types fraud since it will ultimately protect the end-users, without prejudice to the right to privacy of communications.
- Privacy Regulations are preventing data sharing between MSPs and also to the wider ecosystem (Financial institutions etc).
- Number independent interpersonal communication service (OTT services) are also used by fraudster to commit frauds, therefore they need to be more firmly regulated as scams moving there once protection put in legacy systems.