GSMA ETNO position on impersonation fraud in Payment Services Regulation

March 2024

The GSMA and ETNO strongly encourage policymakers to reconsider their approach to increasing liability for electronic communications services (ECS) providers in cases of impersonation fraud. Imposing liability on ECS providers will move responsibility of repayment to the victims of fraud, rather than helping to combat fraud from happening. The financial services sector has the direct consumer contact, designs the financial products, and they should and can setup sufficient safeguards when they do so. Telecoms operators provide access to the free and open internet. Our products, including text messages and numbering are widely known and are not designed to cater to the need of the financial sector specifically. If the telecoms sector is to be made financially liable, then it will have to change the way internet access and communication services are provided and setup strict safeguards for the use of text messages to the severe detriment of both the consumers and the financial sector.

Telecoms operators have seen the most effective solutions come from bilateral cooperation with the financial services sector and would encourage policymakers to combat fraud by working with industry to facilitate and encourage this cooperation. The Payment Services Regulation should focus on the cooperation as a solution to combat fraud.

Telecoms operators value consumer trust and are invested in combatting 'spoofing' fraud. Members of the GSMA and ETNO are already implementing anti-spoofing and wider anti-fraud solutions on a voluntary basis, which have already proven their effectiveness. However, there are obstructions, both technical and legal, to implementing EU-wide measures - obstructions which can vary in different member states where different legislation applies. These would prevent telecoms operators from complying with proposed measures in the Payment Services Regulation, so removing regulatory obstructions must be a first step in a challenging process.

Cooperation between the finance sector and telecoms operators

In cases where impersonation fraud leads to financial fraud, telecoms operators only have oversight of a very small part of the process. Telecoms operators are only responsible for an SMS being sent or delivered, or an audio call being originated or terminated, there is no oversight or involvement in the payment process itself. A number of national and EU-level legislations including the ePrivacy Directive, the General Data Protection Regulation (GDPR) and the Open Internet Regulation (OIR), prevent telecom operators from having oversight of the content of messages or calls. RCS is end-to-end encrypted for the purpose of protecting the privacy of the end-user.

Given telecoms operators play only a minimal part in the chain of events that leads to fraud, telecoms operators and the financial services sector must work together in order to collect the data points that indicate fraud and to implement the solutions that can help to prevent financial fraud in cases of impersonation fraud. There are several examples of bank/telco cooperation resulting in efficient and effective anti-spoofing measures:

- In Denmark, the Danish telecoms industry has established a close cooperation with the finance sector (Finans Danmark) and with Danish police. Measures include protection for selected fixed numbers (those 'owned' by banks or financial institutions) which prevents them being spoofed. Additional forms of cooperation are being put in place, including SMS

Sender ID protection for numbers associated with financial institutions to be implemented in Q1 2024 subject to a discussion in relation to their compliance with the ePrivacy provisions.

- In Norway, Sender ID protection for SMS from the largest mobile operators is in use by several banks and financial institutions for the protection of end users and companies.
- In France, a working group has been organised by the national bank, Banque de France, in order to design technical solutions with the input of both ECS providers and financial institution, such solutions could include blocking lists and 'do not originate'[1] (DNO) lists.
- In Spain, telecoms operators proactively engage with banks to monitor fraud and prevent SMS spoofing, this has included procedures to prevent spoofing of A2P (application to person, e.g. automated two factor authentication) SMS platforms.
- The global financial service Revolut has launched an advanced scam detection feature which uses AI to detect whether a customer is being scammed and will decline any payment being made, issue an alert to the customer in-app which instructs them to "Hang up the phone", and require more information before allowing an authorised payment to be completed.[2]
- In Mozambique, government authorities, mobile network operators, internet service providers and financial institutions have developed standardized procedures for subscriber registration, including establishing a central database for subscriber identification, and a risk centre to detect fraudulent activities[3].

The GSMA and ETNO encourage policymakers to focus on facilitating cooperation and collaboration between sectors, with the participation of competent national regulators, which will allow for the reduction of incidents of impersonation fraud rather than shifting the liability for repayment of fraud after the fact, thus putting at risk existing voluntary measures. The EU, alongside national governments can further help the fight against spoofing fraud by ensuring legal obstructions are minimised and telecoms operators and financial services are supported to put preventative measures in place, with some consistency. Technical obstruction can be mitigated with support and investment, as demonstrated by the Belgian government and its promotion and financing of a new software[4] to allow operators to stop fraudulent text messages, with the pilot offering promising results.

Legal obstructions

The telecoms industry is able to implement additional safeguards against impersonations fraud, however existing regulation at the EU and national level prevents it from doing so. Should telecoms operators be required to prevent fraud in this manner, work must be done to remove the existing regulatory barriers.

Directive 2002/58/EC or the ePrivacy Directive does block telecoms operators from implementing anti- 'spoofing' solutions in most EU member states, by banning the scanning of content of phone calls or SMS messages. In some countries, for example Finland, special provisions have been made by implementing the ePrivacy Directive at national level with allowances for telecoms operators to "undertake necessary measures […] in order to prevent preparation of means of payment fraud"[5], including scanning of calls and messages for this purpose. Any obligations laid out in the Payment

[1] The Do Not Originate (DNO) list - Ofcom

[2] Revolut launches AI feature to protect customers from card scams and break the scammers "spell" | Revolut United Kingdom

[3] Collaborative Efforts: How Governments, Telecom Operators, and Financial Institutions Can Join Forces Against Telecom Fraud - 1Route (1routegroup.com)

[4] Belgium to introduce better protection against scam text messages (brusselstimes.com)

[5] en20140917_20201207.pdf (finlex.fi)

Services Regulation for telecoms operators, would require that this interpretation of the ePrivacy Directive was applied in every member state.

In the UK a scam signal solution has successfully been implemented, however in EU member states, for example the Netherlands, the same measure is not possible to put in place. The scam signal solution uses cooperation between banks and telecoms operators to collect enough data points to flag a transaction as fraudulent and block it. This process will take under a minute and is extremely effective at identifying potential fraud. In the Netherlands however, it is impossible to implement this solution, because under the national Telecoms law[6], operators are unable one of the key data points needed.

Technical obstructions

Both verifying the legitimacy of calls and blocking any number that has not or cannot be authorised are very difficult for telecoms operators because international incoming calls can originate in any jurisdiction, and there is no obligation on the telecoms operators in other parts of the world to provide any information on the integrity or identity of the person making the call.

A recent report from Ofcom[7] found that whilst Calling Line Identity (CLI) authentication, confirming the identity of the person using a certain phone number, has potential to be an effective tool in preventing some harmful calls from spoofed numbers, telecoms operators should not proceed with CLI authentication at this time. This is because:

- Calls arriving from overseas displaying international numbers are unlikely to be fully verified. This is because overseas operators are not obliged to follow the same rules on verification, which would mean this approach is unlikely to sufficiently hinder scam calls that originate outside the EU, a large proportion of all scam calls.
- CLI authentication on its own would not adequately address the risk of calls from abroad spoofing EU member state mobile numbers. This means there would be a need for a complementary process, running alongside, to ensure that calls from abroad displaying EU mobile numbers are from genuine EU roamers. Without this process, authentication alone would not adequately address the problem of inbound calls spoofing EU mobile numbers.

In France, 'Loi Naegelen (2020-901)' requires telecom operators to ensure that a call is made by a phone number that is listed as associated to that operator, that the person making the call is in fact assigned to that number, or the assignee has given permission for the number to be used.
If this check is not complete or is failed, the operator must interrupt the call. Whilst in theory this may solve the issue of 'spoofed' calls and messages being made and received by customers of French telecoms operators, due to technical restrictions it has yet to be implemented. So far it has been impossible to verify the authentication of the number without error, and in real time. Similar use cases from North America, primarily with the objective of ending robocalling have been experimented with for several years without perfect application. In addition, this standard cannot be implemented on certain lines and on a large part of mobile interconnections at this stage so consequently, this system will only have a small effect on spoofing fraud.

Whilst the above example would require blocking calls before they reach the terminating end-user, the same is not possible for SMS messages, and so spoofing fraud via SMS would not be affected. It is possible to set up a firewall for SMS messages, dependent on content, however as mentioned above, due to GDPR and ePrivacy Directive it is not possible to scan the content of an SMS message

[6] wetten.nl - Regeling - Telecommunicatiewet - BWBR0009950 (overheid.nl)
[7] https://www.ofcom.org.uk/__data/assets/pdf_file/0036/276687/01-24-cli-authentication-update.pdf

for this or any other purpose without the express consent of both the sender and recipient. In cases of fraud the sender would of course not give consent for this purpose.