Review of the Payment Services Regulation

Telecoms industry perspective: cooperating to fight impersonation fraud

PSR review: Telecoms industry views

The European telecommunications industry supports the European Commission's Payments Service Regulation proposal for **closer cooperation between the banking sector and telecommunications operators** in the fight against impersonation fraud. While there are numerous cooperation arrangements between the two sectors in several Member States, the industry is ready to further enhance and develop such cooperation to effectively fight against impersonation fraud.

We note with concern that the European Parliament deviated from the concept of enhanced cooperation and proposes a transfer of liability from the banking sector to the telecoms sector.

This is disproportionate and it raises serious reservations insofar as it conflicts with current technical and legal constrains that govern the provision of electronic communications services according to EU legislative provisions applicable to telecommunications operators (net neutrality, secrecy of communications, prohibition of generalized Internet traffic monitoring, technical controls workable on voice networks etc.).

To be effective in fighting impersonation fraud and safeguarding consumers, the upcoming Regulation needs to **strike the right balance** and duly consider the roles of the various players in the chain.

It must be stressed that telecommunications operators only have oversight of a very small part of the process when impersonation fraud leads to financial fraud. In fact, they are only carriers (mere conduits) of the information to the recipient and do not have visibility or control over the contents of communications.

Fighting fraud by impersonation: what telecom operators can and cannot do

In cases where impersonation fraud leads to financial fraud, telecoms operators only have **oversight of a small part of the process**. Their responsibility is confined to ensuring the delivery of an SMS or the initiation of a call, with no involvement in the payment process itself. Given their minimal role in the overall fraud process, telecom operators and the financial services sector must collaborate to gather the necessary data points to detect fraud and implement preventive solutions.

The European Parliament's proposal, which places the liability burden on telecom providers, overlooks the **legal and technical constrains** the industry faces. Imposing a liability regime without addressing these constraints would leave operators vulnerable, expecting them to combat increasingly sophisticated fraud without sufficient tools, legal clarity, or flexibility.

Telecom companies focus primarily on **providing connectivity.** They cannot be held liable for how their services are used. They are 'mere conduit service' and, much like a postman not being permitted to open a letter, operators are expected to maintain the integrity of communications.

Companies can **only process data on strict, limited grounds** under applicable laws. For instance, in principle, all traffic data must be erased or anonymized once it is no longer needed for communication transmission, with a few exceptions, such as billing purposes or direct marketing or value-added services (pending user consent). Furthermore, data processing and sharing is limited by different laws which may hinder data sharing for fraud prevention and collaboration with third parties, such as the banking sector.

These restrictions are essential to uphold the fundamental principle of communication confidentiality. However, at times, they also limit providers' ability to implement broader fraud prevention measures.

There is also some uncertainty around the ePrivacy directive which is outdated, with national implementing laws diverging from it, leading to reduced harmonization and increased legal ambiguity. As national implementations vary and market conditions evolve, creating an EU liability regime without adequate harmonization could lead to significant challenges.

Important to bear in mind that operators must ensure **access to and interoperability** with telephone numbers in the EU and by the International Telecommunication Union to maintain end-to-end connectivity. While telecom traffic should be routed where economically feasible, it can only be blocked individually for fraud or misuse as determined by national authorities/courts. This results in different regulations across Member States, causing legal uncertainty about when blocking is permissible. Consequently, this limits providers' ability to implement broad, scalable solutions to prevent caller ID spoofing fraud.

<table>
<tr><th>What telecom operators CAN do</th><th>What telecom operators CANNOT do</th></tr>
<tr><td>Enhanced cooperation with banks

• Telecom companies are willing and able to work with banks to fight impersonation fraud.

• Telecom companies do need an assessment by the bank to know if the communication is fraudulent. Therefore, cooperation between banks and telcos is essential.</td><td rowspan="2">General obligation to monitor content

• General monitoring of the content of electronic communications is prohibited (with very limited exceptions in some countries).[1]. This is essential to ensure confidentiality of communications and respect of private life. There cannot be a general obligation to monitor the information transmitted or stored, nor to actively seek facts or circumstances indicating illegal activity.

• The Digital Services Act[2] and the eCommerce Directive, define electronic communications services as mere conduit services (‘services used for communications purposes’). Mere conduit providers may only to act on the basis of an order of a judicial or administrative authority. It should be noted that notice and action mechanism only applies to providers of hosting services.

• Therefore, telecom operators are not/cannot be liable for content they transmit or store at the request of users.</td></tr>
<tr><td>Sharing key (anonymized) data with banks

• Telecom operators can share some relevant data with banks on suspicious activities – within the limits of the ePrivacy Directive and national laws.</td></tr>
<tr><td>Blocking with strict limits

• Technically, electronic communication service providers may block SMS or access to (originating) numbers to combat fraud but this is often restricted by law.</td><td>Blocking numbers or services

• According to the European Electronic Communications Code: a legal mandate is required for blocking, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse. Only on the basis of an order of national regulatory or other competent</td></tr>
</table>

[1] Digital Services Act, Article 8
[2] Digital Services Act, Article 4(1)

• In some countries a specific regulation is in place to combat CLI spoofing resulting in impersonation fraud. Reference can be made to the ECC recommendation "Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers" as approved on 28 November 2023 recommending blocking calls or suppressing the CLI under specific conditions.	authorities can ECN and ECS block access to (originating) numbers to combat fraud.
Fraud Detection Technologies • Utilizing advanced analytics and machine learning, telecoms can identify patterns indicative of fraud attempts, such as repeated attempts to change account details or frequent international call routing (this may require investing in high-end technology).	**Intercept /block / reclaim communications** • **EU Open Internet Regulation**, prohibits providers of internet access services, or providers of Internet to block, slow down, alter, restrict, interfere with, degrade or discriminate specific content, applications or services and only allows blocking (e.g. of websites containing unlawful content) if specifically instructed to do so by a national authority / Court based on national law[3]. • Telecom operators providing Internet access services are unable to 'remove the fraudulent and illegal content'. Operators cannot remove or delete content from the Internet, they can only block access to it. • Notice and action mechanisms ('take down') only apply to providers of hosting services – such as a website.
Monitor SIM swap activity • Telecom operators can track and flag unusual or frequent SIM card changes, a common tactic used in impersonation fraud.	**Verify call origination / legitimacy** • Verifying the legitimacy of calls and blocking numbers is very difficult for telecoms operators because international incoming calls can originate in any jurisdiction (subject to different obligation on the integrity or identity of the person making the call).
Promote strong security measures • Operators can promote security measures.	**Access customer bank accounts/ intercept bank transfers** • Telecoms operators are only responsible for an SMS being sent or delivered, or an audio call being originated or terminated, there is no involvement in the payment process itself. • They do not and should not have the authority or capability to access or monitor customer bank accounts directly.

[3] Open Internet Regulation, Article 3(3)

Review of the Payment Services Regulation

Telecoms industry perspective: cooperating to fight impersonation fraud

Educate Customers	Prevent all phishing attacks/ block numbers
• Operators - together with public authorities and banking sector - can run awareness campaigns to educate customers about impersonation fraud, how to recognize it, and steps to protect their personal information.	• While operators can warn customers and block known malicious numbers, telecoms cannot entirely prevent phishing attacks since these often involve sophisticated social engineering tactics that fall outside their purview. Blocking numbers requires legal mandate.

Cooperating with banks

The European telecommunications industry recognises the importance of adequate payment service rules to improve consumer protection in electronic payments. We are committed to **cooperate cross-sector** to fight impersonation fraud.

We note with concern that the European Parliament deviates from the concept of enhanced cooperation and proposes a transfer of liability from the banking sector to the telecoms sector. This disregards all the efforts done to date by the industry as well as successful national initiatives.

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 and consider collecting data points that indicate fraud and to implement the solutions that can help to prevent impersonation fraud.

Where telecom operators take relevant, proportionate, preventive, and curative measures against fraud, these should in principle benefit all sectors, not only the financial sector. The implementation of these solutions should not be interpreted as creating a liability towards the financial sector or any other sector.

In order for this cooperation to be successful, it is essential that it remains flexible in nature. **Fraud is constantly evolving**, and the responses to it must be able to change quickly and creatively. This is also why there is no one technical solution to combat spoofing fraud; it is important to ensure that the right technical models are developed according to the legal context faced, and the fraud landscape presented. It is therefore very important to have strong cooperation between the actors involved, as set out in the original European Commission proposal, and we believe that this is the most successful way forward to tackle impersonation fraud.

There are several examples of bank/telco cooperation resulting in efficient and effective anti-spoofing measures. In addition to voluntary bilateral cooperation, some Member States have facilitated this exchange (e.g. with some regulators organising workshops or providing guidance on cooperation and facilitating exchange of views).

Examples of best practices in various EU countries

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 **dynamic nature of impersonation fraud tactics** means that continuous adaptation and cooperation with other sectors, including banks and regulatory bodies, is necessary to enhance overall security.

Banks and telecom service providers have different mechanisms to leverage their in the combat against fraud. Banks can provide deep insights into financial transaction patterns and sophisticated fraud detection algorithms, while telecoms can offer critical data on mobile phone usage and SIM card activities.

Working together, these sectors can enhance the detection and prevention of impersonation fraud, protecting consumers more effectively. While best practices should be shared and encouraged by policy-makers, liability should be proportional to the role different actors play in the chain of events.

Belgium	• Belgian operators introduced a full operational blacklist - including the public bank telephone numbers. This blacklist stopped CLI spoofing fraud for bank telephone numbers awaiting a generic solution against CLI spoofing for all Belgian numbers. • The regulator organizes regular meetings (at least 2 times per year) between the telecom and bank sector to monitor the evolution of the fraud and to analyze new fraud scenarios. • The legislator is working to offer more legal certainty to telecommunications operators in order to efficiently combat and prevent fraud. Some examples of implemented measures: ○ legal obligation for operators to adopt appropriate, proportionate, preventive and curative measures to detect fraud and malicious use on their network and services (without accessing the content of the communication). ○ processing of certain categories of traffic data is a legal obligation for fraud prevention purposes. There is also a legal authorization to process all other categories of traffic data where necessary to prevent fraud. • Legal exception to confidentiality of communications allowing operators to process content of SMS/MMS communications to prevent fraud (Smishing) under strict conditions. Mainly, the processing must be limited to mechanical examination of messages to detect fraud; human intervention is permitted solely to verify the proper functioning of computer algorithms
Denmark	• In Denmark, the Danish telecoms industry has established a close cooperation with the finance sector (through Finans Danmark) and with Danish police. • Measures include protection for selected fixed numbers (those 'owned' by banks, shipping companies, public entities, or financial institutions) which prevents them being spoofed as well as SMS Sender ID protection for numbers associated with similar institutions which was implemented in Q1 2024. Additional forms of cooperation are ready to be launched pending legal clearance in relation to their compliance with the ePrivacy provisions and the rights to correspondence secrecy.
Finland	• In Finland, the National Regulatory Authority (Traficom) set up a task force to address the problem. It's recommendation: mobile telephone CLI validation for an international incoming roaming call. • Finnish authorities, telecommunications operators and the financial sector are working closely together to prevent fraud. This cooperation has e.g. led to implementation of a technical solution to stop scam calls. Mobile telephone CLI (calling line identity) validation checks if traffic originates from abroad using Finnish numbers or if a Finnish mobile subscription is currently abroad. This makes it possible to block other traffic originating from abroad using Finnish numbers. Similar preventive measures have also

	been implemented for text messages and national authority Traficom has also issued new regulatory requirements concerning filtering text and multimedia message traffic. In addition to this, during spring 2024 Traficom has started the registration of protected SMS Sender IDs, which e.g. banks and financial institutions can register. This allows parties sending out text messages to Finnish citizens to make sure that no one else can use the same SMS Sender ID.
France	• 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 electronic communication providers and financial institution, such solutions could include blocking lists and 'do not originate' (DNO) lists. • In France, law mandates telecom operators to verify that a call originates from a number associated with them and that the caller is assigned to that number or has permission to use it. If verification fails, the call must be interrupted. However, there are technical challenges with real-time authentication. The system cannot be applied to certain lines and many mobile interconnections, limiting its impact on spoofing fraud.
Ireland	• In Ireland, via the ITSFF (Irish Telecoms Security & Fraud Forum), operators have built a relationship with the BPFI (Banking & Payments Federation Ireland) over the last number of years. This has allowed them to create and nurture networking and relationships, which in turn has enabled them to work on initiatives to help reduce the impact of fraud in Ireland.
Italy	• In Italy, the national regulatory authority (AGCom) asked for a new article in the Italian communication code which entered into force from 28 April 2024. AGCom can now require Italian operators to block communications coming from abroad that illegitimately use national numbering or are not compliant with the ITU-T Recommendation. The regulator can also ask for domain names to be blocked in the case of aggressive commercial practices, fraud or abuse. It plans to summon the operators to discuss the issue in the coming months.
The Netherlands	• In the Netherlands two effective and voluntary operational measures have been implemented. There is a successful cooperation between banks and the telecom sector by means of best practice. In order for these measures to combat fraud be effective, no content monitoring is required. • There are 2 pilots running specifically to cooperate with the banking sector: (1) A pilot to mitigate spoofing of phone numbers used by NL banks; (2) A pilot to mitigate smishing with alphanumeric SMS Sender IDs of NL banks. Both pilots are very effective and present a good example of collaboration between telecom and banking on voluntary basis, whereby relatively simple measures can effectively counter spoofing. These relatively simple solutions target the cases whereby it may be most easy to mislead customers (with the use of actual phone numbers and IDs from the bank).
Norway	• 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. Moreover, measures include protection for almost all fixed and to a large degree mobile numbers, which protects them from being spoofed from abroad. Anti-fraud mechanisms have been implemented to identify and block fraudulent SMS (e.g. based on fraudulent URL in content)
Spain	• 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.
Sweden	• The Ministry of Finance has launched a dialogue with financial institutions and mobile operators/ISPs to explore solutions and responsibilities. The Swedish regulator Post- och telestyrelsen has introduced regulations on spoofing and is evaluating further measures to combat payment fraud. • Mobile Operators are compliant to the spoofing regulations blocking suspicious calls and have other voluntary measures in place, such as SMS Sender-ID control and blocking of fraudulent SMS as a service. The Swedish implementation of the ePrivacy Directive is strict and leaves little room for operators to analyze the content of communications.