VATM e. V. • Rue de Trèves 49/51 • B-1040 Brüssel

Polish Presidency of the European Union

Permanent Representation of the Republic of Poland to the European Union

Rue Stevin 139, 1000 Brussels, Belgium

Contact Person	E-Mail	Telefon	Datum
Lilyana Borisova	lb@vatm.de	+32 489378065	28.05.2025

VATM Comments on Draft Art. 59a(3) PSR of the Council: Technical Limitations for ECS Providers

In the context of the Council's discussions on the proposed Article 59a(3) of the Draft Payment Services Regulation (PSR), VATM would like to offer preliminary remarks highlighting the technical and operational challenges that Electronic Communications Services (ECS) providers face in meeting the obligations currently foreseen in the draft provision.

Our members remain firmly committed to supporting cross-sectoral efforts to fight fraud, including through active collaboration with payment service providers (PSPs), public authorities, and law enforcement.

However, **the newly proposed paragraph 3 under Article 59a appears to depart from essential regulatory principles such as technological neutrality, proportionality, and the need for future-proof legislation**. Instead, **the provision risks introducing prescriptive, static obligations that may prove not only ineffective in tackling fraud but also technically unfeasible for ECS providers to implement.**

The provision currently under discussion by the Council has been formulated, as follows:

Article 59a(3)

Electronic communications services providers as defined under Article 2, point 4 of the Directive 2018/1972/EU shall ensure that all necessary technical measures, including specifically the security of the communication between payment service providers and payment service users are in place to prevent fraud within their sphere of competence. In the case of providers of electronic communications services, such technical measures shall at a minimum include:

(a) Confirming the authenticity of all calls and messages routed through telecommunication networks and preventing the use of a particular telephone number that is contrary to the conditions of attribution, authorization or allocation of that telephone number;
(b) Preventing the use of electronic mailing for fraudulent purposes;
(c) Storing proof of all IT and identity verification measures, in particular in the event of SIM SWAP, to justify their due diligence in line with national legislations.

We would like to highlight several specific concerns:

1. Technical Impossibility to Guarantee Fraud Prevention

A. The current wording obliges ECS providers to "*ensure that all necessary technical measures, including specifically the security of communication between payment service providers and payment service users are in place to prevent fraud within their sphere of competence*." This expectation **goes beyond what is technically achievable**. Telecommunications networks are based on international, open, and interoperable standards. These allow the originating party – in another network, including non-EU jurisdictions – to set caller ID and SMS identifiers accordingly. As a result, **spoofing** remains a structural vulnerability.

   ECS providers do **not have the ability to verify the sender ID or telephone number of an incoming call or SMS** nor the respective allocation information when it originates from another network. Consequently, **they cannot prevent fraud with certainty** and should not be made liable for it.

   For further practical examples of the hurdles the ECS provider would face should the wording of the draft Art 59a(3) be implemented, and the practical measures taken by the regulatory authorities in different Member States, we would like to refer to the common position of ecta, GSMA and Connect Europe.

B. **From a German perspective, we would like to underline that in the German Telecommunications Act there are already sufficient safeguards addressing fraudulent behaviour related to the subscriber number and we would like to preserve those** (§120 TKG).

2. Limitations of Current Infrastructure

Even when ECS providers deploy technical tools – such as call-blocking systems or anomaly-based filtering in cooperation with PSPs or public authorities – these measures are **mitigation techniques**, not full-proof safeguards. The effectiveness of such tools is constrained by:

- Network design limitations – the fraudulent behaviour cannot be technically verified by the ECS provider;
- Data protection and privacy laws that restrict any inspection of content.

3. Email-Related Fraud

Email providers – in contrast to ECS providers – operate on closed or semi-closed platforms and manage domain-based authentication mechanisms (e.g., SPF, DKIM, DMARC). However, even in this context, **the prevention of fraud or impersonation (e.g., in phishing) is not technically guaranteed**, particularly given the **diverse and decentralised nature** of email services and the **sheer volume of potential spoofing targets**.

Internet access providers, meanwhile, act as **mere conduits**, as legally defined under the Digital Services Act (DSA). They are not in a position to monitor or alter the sender fields of emails or their contents – such monitoring would be counter to EU data protection legislation.

4. Role of Balanced and Flexible Regulation

Fraud patterns evolve rapidly. Regulatory tools must leave **sufficient flexibility for market actors** to adapt and respond in real time. Hardcoded technical obligations that prescribe specific measures are unlikely to remain relevant over time and risk becoming counterproductive. A future-proof framework should focus instead on **incentivising collaboration**, **supporting industry best practices**, and enabling ECS providers to contribute within the boundaries of what is technically and legally feasible.

Conclusion

We urge the Council to reconsider the current formulation of Article 59a(3). While we share the goal of enhancing fraud prevention, **the proposed wording imposes unrealistic and technically unattainable obligations** on ECS providers. A more balanced approach – one that promotes **collaborative frameworks**, recognises **technological constraints**, and builds on **voluntary and risk-based mechanisms** – would better serve the regulation's objective and ensure practical enforceability.

Therefore, **VATM respectfully asks the Council to delete the proposed Art. 59a(3), as it does not provide for legal certainty or clarity but rather puts a technical and legal challenge to the companies falling under its scope and jeopardises the technical flexibility of innovative tools and measures supporting the fraud preventing efforts of the telecommunication industry.**

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Rue de Trèves 49/51 • B-1040 Brüssel • Tel.: +32-2-446 00 77 • E-Mail: vatm@vatm.de