

Payments Tomorrow Conference

Paris, 16 October 2026

# Francois-Louis Michaud keynote speech: Enhancing trust in Europe's payment ecosystem

Check Against Delivery  
Seul le texte prononcé fait foi  
Es gilt das gesprochene Wort

Ladies and Gentlemen,

I am very happy to join you here in Paris again for this new edition of the Payments Tomorrow Conference.

Today, I would like to focus my remarks on two topics. I would like to start by touching on payment fraud and how we can enhance trust in Europe's payment ecosystem. Then I will give an update on the EBA's work in the context of the new payment services directive and regulation ("PSD3 and PSR").

## **How can we further enhance trust in Europe's payment ecosystem?**

Let's first take stock of what has been happening in the market over the past decade. As you will probably agree, Europe's payments market has undergone a profound transformation. Competition has increased, digital payment solutions have expanded, and instant payments are becoming a mainstream means of transferring money. Consumers now expect payments to be fast, seamless and available around the clock, and this is generally happening.

At the same time, payment fraud, in general, is growing in both scale and sophistication. The last EBA-ECB payment fraud report showed that the total value of payment fraud rose from €3.5 billion in 2023 to €4.2 billion in 2024. The next edition of the EBA's report on payment fraud, which will be published by year-end, is expected to show even higher fraud levels in 2025.

As many of you will probably concur, fraudsters are increasingly relying on social engineering techniques to persuade customers to authorise fraudulent transactions or disclose sensitive credentials. Many scams now also originate outside the payment sector, through social media platforms, search engines, online marketplaces or messaging applications. For instant payments, for example, fraud volumes increased by 175% over three years, outpacing the 98% growth in transaction volumes for this service.

Artificial Intelligence is accelerating this trend. Fraudsters can generate highly convincing phishing messages, create deepfake audio and video content, and automate large-scale scams with unprecedented efficiency. And artificial intelligence (AI tools) of course further increases the magnitude and credibility of these deception tactics. Against that background, the EBA, jointly with ESMA and EIOPA, has recently issued a consumer factsheet describing how AI can trick consumers and what they can do to detect and react. The factsheet has been translated into all EU languages and is being rolled out across all national authorities in the EU, to maximise reach to consumers. We encourage everybody to contribute to disseminating it.

Beyond what can be done to increase customer awareness, fraud prevention must continue to evolve to adapt to these developments. Strong customer authentication (SCA) under PSD2 played a pivotal role in successfully reducing unauthorised payment fraud. But it was not designed to address authorised payment fraud, where customers are manipulated into initiating payments. Protecting users requires a different but complementary approach, one that moves towards prevention, detection and intervention across the payments ecosystem.

We see that the industry is already adapting. Many payment service providers are strengthening real-time transaction monitoring and deploying AI-based tools to intervene before losses occur. Additional safeguards, such as tailored spending limits and targeted consumer awareness initiatives by firms, are becoming more common. In parallel, several Member States introduced measures to combat telephone number spoofing and other forms of impersonation.

EU Regulation is evolving in the same direction. A key milestone was the introduction at the end of 2025 of Verification of Payee (VoP) for Euro credit transfers under the Instant Payments Regulation. By enabling users to verify that a beneficiary's name matches the account identifier before a transfer is executed, VoP addresses a vulnerability frequently exploited by social engineering scams. Thanks to the efforts of the European Payments Council and its members, the roll-out has largely been a success and remaining teething problems are being sorted out.

The forthcoming PSD3 and PSR go even further. They strengthen transaction monitoring requirements, extend Verification of Payee to credit transfers in all EU currencies, facilitate targeted information sharing between payment service providers and introduce anti-fraud obligations for actors beyond the payment sector. This reflects an important reality: fraud is rarely

confined to the payment transaction itself. It often exploits vulnerabilities elsewhere in the digital ecosystem.

PSD3 and PSR also foresee that the EBA continues to strengthen fraud prevention in areas which include payment security, transaction monitoring and fraud reporting. In doing so, we will of course have to recognise that individual actors often see only part of the fraud picture. Strengthening payment security and transaction monitoring will, therefore, require drawing on fraud intelligence from a wide array of sources. Proper arrangements will be needed to facilitate information-sharing, remaining proportionate, avoid undue friction for users, and most importantly protect civil liberties.

Technology will of course be front and centre in the solutions that the EBA will be considering. AI can help institutions analyse large volumes of data in real time and detect emerging threats that escape traditional monitoring tools. Equally important will be mechanisms enabling institutions to exchange fraud intelligence rapidly and securely, allowing coordinated responses. As the use of AI increases, payment service providers remain accountable for its outcomes, maintaining oversight and ensuring they can explain decisions affecting customers.

Diversity and innovation are key strengths for our payments ecosystem. But fraudsters are quick to exploit gaps between payment service providers, sectors and jurisdictions. The challenge ahead is therefore to ensure that protection is as smart as the threats, to maintain effective fraud prevention without undermining the speed, convenience and innovation that users expect. This requires real-time monitoring, effective information sharing and closer cooperation across the digital ecosystem, combined with continued vigilance from all stakeholders, including consumers, PSPs, online platforms, telecommunications providers and public authorities.

### **The EBA's work in the context of PSD3/PSR**

Let me now turn to the EBA's work in the context of PSD3 and PSR, including the Technical Standards on strong customer authentication.

As you will be aware, the publication by the co-legislators of the PSD3 and PSR in the Official Journal of the EU has been delayed several times this year. At present, publication is estimated to take place in December 2026 or January 2027. Before the publication of these texts, the EBA cannot really discuss the content of the mandates it will receive from the legislators. Only their publication in the Journal provides the legal confirmation that the EBA is indeed mandated to develop them. It is only at that point that the precise content of the Articles will be known, as well as their underlying reasoning as expressed in the recitals.

However, we of course have a good understanding of what will be asked of us.

The main topics include: the safeguarding of client funds; prudential requirements such as own funds calculation; authorisations, passporting, limited network exclusions, and payment security, among which strong customer authentication. We are also likely to be asked to work on dedicated interfaces for open banking, on performance metrics for those interfaces, and, probably very

important for you, on the notifications to be submitted by bank to their competent authorities when they refuse or closure an account of a payment institution.

We have been approaching this task in the spirit of our current focus on resilience and efficiency, which means that we are systematically reviewing the expected value of a legislative mandate to the EBA in the light of the burden it may create for authorities or firms, and when we believe the balance is not right, we engage with the Commission, the Council and the Parliament. Thanks to such constructive discussions with the co-legislators, we now expect that the final texts will contain around 18 mandates only to the EBA, compared with a total of 29 initially (this means that more than a third will have been removed).

Once the texts have been published, we plan to communicate on our website the sequence in which we will deliver the mandates, including the quarters when we will publish the consultation papers and when we will deliver the final requirements.

I can only advise that you have a good look at this roadmap, identify the mandates that you think impact you, and then submit a response to the draft requirements that are proposed in our consultation paper – and do so as an individual PSP and/or as a trade association. These consultation papers are certainly not a compliance (“tick-box”) exercise for the EBA. They constitute an integral part of the EBA’s policy development process. We will assess every single response received. We will publish a ‘feedback table’ alongside the final requirements, in which we will explain and assess the comments received, and whether and how we took them into account.

We look forward to developing these mandates and count on your input into that effort to make it a full success to the benefit of a striving European payment industry and more importantly to the benefit of European citizen.

Thank you for your attention.