Joint conference of the Banque de France and the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI)

Strengthening retail payment security: tackling fraud to safeguard trust

Thursday 13 November 2025

Banque de France, Paris

Our compass for preventing retail payments fraud: adapt technical defenses and extend the scope and the reach of cooperation

Opening keynote speech
by Denis Beau, First Deputy Governor, Banque de France

- Good morning to everyone, at the Banque de France premises and those participating remotely. It is a great pleasure for me to open this first-of-its-kind conference on retail payment security, jointly organised with the Committee on Payments and Market Infrastructures of the Bank for International Settlements.
- As central bankers and public authorities, we are all familiar with the fact that the security of payment means is an essential pillar of the public's trust in the currency. In recent years, retail payment fraud has increased in line with rising cross-sectoral and cross-border activity, alongside the rise of digital, faster payments.
- It is my conviction, based on our experience at the Banque de France that this evolution of the payment and associated fraud landscape requires strengthening and enhancing coordination among the key stakeholders of the payments ecosystems in order to continue to ensure a high level of retail payment security globally. Indeed, the Banque de France benefits from a rich experience in fraud prevention policies and their implementation, since it was granted a legal mandate in 2001 to ensure the safety of retail payments and to chair the French Observatory for the Security of Payment Means (OSMP) to help meet this objective. For this reason, I am delighted to host today's conference at the Banque de France and I am greatly looking forward to sharing the lessons we have learned from our involvement in fraud prevention and from the experiences of other CPMI members and fellow organisations.
- Before handing over to the first panel, let me share with you quickly, as a possible input to the forthcoming panel discussions, one observation and one conviction, drawn from my involvement in payment security at the Banque de France and the OSMP.

The observation is that there has been a significant shift in the profile of payment fraud, in response to the efforts made to technically secure the development of digital payments.

Indeed, as the supply and demand of payment services in France has progressively shifted towards the dominance of digital solutions over the last two decades or so, fraud prevention policies and practices have evolved towards a significant strengthening of technical defences.

- As shown in the CPMI Brief of March 2025, this digitaliszation of payments is widely shared across CPMI jurisdictions. It is embedded in the diffusion of innovative solutions, such as instant payments, wallets or mobile payments, while the overall use of paper-based instruments, including cash and cheques, has strongly decreased. In France, the use of cashless payments has risen by more than 70% in the past ten years, and card payments have become the preferred payment method for point-of-sale transactions in 2024. New instant payment solutions have surfaced, such as Wero, a wallet launched by European banks, that enables instant and cross-border European payments using a phone number as a proxy.
- **For this reason, we have gradually enhanced the technical security of these cashless payment instruments, by incorporating more security features in their design**. A strong catalyst in that respect was the adoption of the 2nd European Directive on Payment Services (PSD2), which established Strong Customer Authentication as a key pillar of electronic payments and the upgrading of internet security protocols (e.g. 3-D Secure). The statistics collected by the OSMP show that the deployment of strong customer authentication in France reduced the fraud rate for online card payments by 40% between 2018 and 2024. Instant payments should benefit from a similar policy and outcome with the recent introduction in the European legislation requiring the mandatory Verification-of-Payee mechanisms for all credit transfers.
- As a result, building through the Observatory on a shared vision within our payment ecosystem of the importance of security for payment means and of a shared involvement in the deployment and appropriate use of technical fraud prevention tools, **we have successfully managed in France to maintain payment fraud at a stable level since 2022**, despite the rapid digitalisation occurring in our payments.

However, this success has led fraudsters to adapt and develop additional fraud techniques that do not try to break technical defences but to circumnavigate them.

- Indeed, In France, a significant rise in **authorised push payments,**[1] using social engineering and user persuasion, has been observed since 2021. The impact on fraud has now stabilised, thanks to coordinated actions we took to raise users' awareness via communication campaigns, but remains too high.
- **In addition, more sophisticated and massive attacks have become possible with the appropriation of AI by fraudsters.** It allows them to industrialise their attacks on a massive scale. This could facilitate new forms of scams for users, for example by issuing fake documents or using deepfakes to bypass users' vigilance.
- **This explains why we have, over the past few years, conducted technology watch studies on Artificial Intelligence (AI) and quantum computing** to explore their implications, positive and negative, for payments through the lenses of security and to issue recommendations.
- **We are currently focusing our monitoring and analysis on cryptos.** With tokenisation gaining traction in financial services, some crypto-asset providers have claimed to represent alternative payment solutions, especially with stablecoins. However, **crypto payments do not provide security features equivalent to our current payment means**. Recent large-scale hacking incidents, which have led to substantial losses for consumers, have brought to the fore the vulnerability of the sector and highlighted the failings of some providers when it comes to upholding security standards. This is also due to a regulatory discrepancy, where crypto wallet providers are not regulated as strictly as payment service providers. **This development of crypto assets in retail payments is therefore on the radar of our technology watch, especially since they are used for cross-border retail payments**. This leads me to the conviction that I would like to share with you now.

The conviction is that these trends call for increased cooperation in the area of payment security in order to extend it across sectors, beyond borders and between regulators.

Our experience at the Banque de France indeed shows the **usefulness of extending the scope of the actors involved in payment security and of creating new forms of cooperation**.

- Within the French Observatory, **this is what we have done with the telecommunication sector** to help us to be more effective against spoofing and smishing techniques. This cooperation, involving French telecommunication operators

and their regulator, has led to two major achievements: the first was the technical implementation of an authentication mechanism of phone numbers during calls, to put an end to the spoofing of bank numbers; the second was on the protection against fraudulent SMS messages, by securing professional sender identifiers and facilitating the reporting of fraudulent messages by users and their collective exploitation by anti-fraud professionals.

- **We are currently launching a similar initiative with digital platforms and tech players**, such as social networks and messaging services operators, where fraudsters tend to flourish. Our aim is to ensure that they actively contribute to the fight against fraud in all its dimensions. This implies that they get involved in information campaigns, aimed at consumers, on fraudulent techniques and the appropriate behaviours to limit their impact. But we also expect them to upgrade their own anti-fraud tools, for instance in detecting and removing fraudulent ads from their networks, or in sharing the information collected on fraudulent messages with the other stakeholders.
- In addition, enhancing **information sharing and dialogue between stakeholders, starting with regulators and central banks, with a view to facilitating convergence in the** promotion and adoption of good practices to ensure payment security, could help address a **payment fraud of significant international magnitude. In Europe we have started heading in this direction with** a “European platform on combating fraud”, which features prominently in the provisions of the upcoming updated regulation on payment services in Europe

To conclude, let me say that

- **I trust that the CPMI is particularly well placed to catalyse such information sharing and dialogue at international level** and I very much hope that this conference will help create a positive momentum in this respect, as we have the privilege to welcome twenty or so outstanding panellists from public and private institutions around the world.
- After describing the state of play in retail payment fraud, which will help us understand trends, new risks, and persistent challenges, we will tackle, in the second panel, the relationship between technology and the fight against fraud. We will be joined remotely, this afternoon, by Mr. Fabio Panetta, who will deliver a keynote address as Chair of the CPMI. The afternoon sessions will then cover the regulatory responses to payment fraud and public-private partnerships and cooperation models in payments security.
- I will now hand over to our colleague and co-organiser Mr. Thomas Lammer, Deputy head of the CPMI secretariat, who will moderate the first discussion panel. I wish you all an insightful conference and fruitful exchanges between peers.