Denis Beau: Strengthening the security of European payments

Keynote speech by Mr Denis Beau, First Deputy Governor of the Bank of France, at the conference "Digital fraud: detect, respond and prevent", hosted by the Banco de Portugal, Lisbon, 26 May 2026.

* * *

Introduction

I would like to thank Governor Santos Pereira for his invitation to this conference, and to speak on digital fraud. Like Banco de Portugal, we pay at the Banque de France significant attention to payments security. We were invited to do so some time ago by the French Parliament which decided in 2001 to formally task us with the mission to ensure that payment instruments are safe. To help us delivering on this, the legislator adopted a law to establish a platform called the Observatory for the Security of Payments Means (OSMP).

Led by the Banque de France, this Observatory was conceived as a forum to promote dialogue and coordination among all relevant stakeholders to prevent fraud. To that end, the Observatory has three specific tasks:

- **First, to collect, compile, and publish fraud statistics** reported by payment service providers and card payment schemes, ensuring consistency through the use of harmonised calculation criteria across payment means;
- **Second, to steer**, coordinate and monitor actions taken by stakeholders in the fight against fraud;
- **Third**, to monitor technological developments in the field of cashless payments, that can have an impact on fraud.

I am happy to see that in Portugal a sister platform is being established.

In that context I will focus my remarks today on **the lessons I learned from now 25 years of recourse to our OSMP** to help prevent payment fraud as I have been significantly and directly involved in its functioning, first as secretary of that body when it was created, and today as its President.

I. The first lesson is that an effective contribution to fraud prevention requires an ongoing mobilisation of relevant expertise and users' attention.

The fundamental reason for the need for this on-going mobilisation is the evolving nature of fraud techniques. As we are increasingly turning to digital payments, **targets of fraudsters evolve, shifting from technological vulnerabilities towards human weaknesses.**

Indeed, over the last ten years, there has been a significant shift towards the use of cashless payment means, as illustrated in our regular monitoring statistics. In

France, a rise of 70% in the use of cashless payments means was observed over the past ten years. Card payments are now the preferred payment method for point-of-sale transactions since 2024. This digitalisation trend is also common to the Euro area: the latest SPACE report illustrates the slowing down of cash in POS transactions over the years, down from 79% in 2016 to 52% in 2024, and the steady rise of online payments in day-to-day payments, accounting for a fifth of total payments.

Against this background, in France, we gradually sharpened our approach in the fight against fraud. To enhance the security of cashless payment instruments, the PSD2 offered an important lever in the mid-2010's, by requiring the Strong Customer Authentication (or SCA) for online payments and internet security protocols, a journey the OSMP actually started as early as 2008 in France. The statistics collected by the Banque de France show that SCA implementation had a very significant and positive impact: the fraud on online card payments was reduced by 50% between 2018 and 2025 and hit an all-time low in France in 2025.

However, fraud has been evolving, through schemes aiming at circumventing our SCA technical defences. A surge in manipulation frauds – sometimes called authorised push payments –, using social engineering and user persuasion, has been observed in France since 2021. Fraudsters operate often within international criminal networks that can industrialise their attacks while tailoring their approach to victims. The victim is reassured, put under pressure, and guided to carry out actions that ultimately precipitate the fraudulent transaction. There is broad consensus that all profiles can be targeted, regardless of age, gender or socio-professional background.

In addition, the appropriation of artificial intelligence tools by fraudsters, create today the risk for new, more sophisticated attacks and fraud schemes. This development could potentially allow for the emergence of industrialised attacks, on a massive scale, which could be more difficult to detect. This could also facilitate new forms of scams, for example through the production of deepfakes, or by the issuance of fake documents, that could bypass users' normal vigilance.

Our reaction in that context has been to mobilise regularly the expertise of the stakeholders represented in the OSMP to develop a better understanding of these new fraud schemes to help address them with adapted strategies and good practices. This has proved quite helpful. The output has taken the form of technology watch studies, published in our annual report, and which we publicise through conferences and public communication campaigns.

We also strive to involve directly the final link in the chain: the user. We believe that they must be also involved in the fight against fraud, keeping in mind that a proper balance must be kept between their adequate protection and their accountability in the use of payment means. To that end, we conducted at Banque de France several communication campaigns over the last years, in coordination with our ministry of Finance and the banking sector, to raise users' awareness on the rise in manipulation techniques. These campaigns were carried out through traditional media – such as radio and newspapers – but were also disseminated via social networks and displayed in transport networks and shopping centres. I therefore welcome that the future PSR will invite member states to conduct such awareness campaigns, while also defining a clear liability regime for the new type of "spoofing" frauds.

As we speak, new fraud schemes are emerging, leveraging the crypto-assets ecosystem. Where tokenisation is gaining momentum in financial services, some providers claim to develop alternative payment solutions, notably with stablecoins. However, the security standards of the crypto sphere do not compare with those of retail payments, due to lack of users' awareness of the associated risks and regulatory discrepancy, where crypto wallet providers are not regulated as strictly as payment service providers. This development of crypto assets in retail payments was therefore the topic of our latest technological watch study[1], which was published last month, with the aim to inform our ecosystem about those risks and issue recommendations.

II. The second lesson is that an effective contribution to fraud prevention requires agility

As fraud techniques evolve regularly, this agility starts with adequate data collection to build a common understanding of the trends in the fight against fraud. To guide our discussions and decisions on means to address fraud, the use of fraud statistics and their regular monitoring has proved essential for the OSMP. This required significant efforts, including through on-site inspections to ensure reliability of this data, but its output for the French community outweighs the investment. In this regard, I am pleased to note that the European community benefit since 2021 from a common statistical framework on fraud[2]. It is now crucial that each national central bank continues to invest in data quality to ensure comparability of data across countries.

This data-driven agility to direct fraud prevention plans can be usefully complemented with a forward-looking approach. In the OSMP functioning, this is notably the role played by the technology watch studies I mentioned earlier. They were developed with the objective of anticipating new fraud risks. Over the recent years, we have performed deep-dives on quantum computing, AI or digital identity, which helped us reach a collective understanding of these new technologies and the risks they can create for the security of payment means. These studies are conducted by experts but are always drafted with the aim of being accessible to the widest possible audience. This is a prerequisite for ensuring that our recommendations are taken on-board by all stakeholders and by their decision¬-makers.

It has proved important for the effectiveness of the OSMP that this agility also extends to the parties involved in its activities. Representation from the supply side is of course essential with payment service providers, payment systems and schemes. But representation from the demand side is not less important, with representatives from the **consumers, businesses and merchants** as they are also key actors in the payment chain, and **bear also some responsibility in fraud prevention through the way they use payment means and the attention they pay to security issues and procedures**. The rollout of the SCA has been a success in France, because the merchants were taken on board our steering committee. Three years ago, in 2023, the OSMP also issued recommendations on the prevention and reimbursement of manipulation frauds, which provides common guidelines on how the European regulatory provisions on liability should be implemented. Here again, the direct contribution of consumer associations was essential in preparing and supporting those recommendations. Last but not least, the OSMP also benefits from the contribution of

other public stakeholders, such as law enforcement authorities, the Ministry of Justice, and the data protection and cybersecurity agencies.

Over the years, we gradually reviewed and enlarged the participants to the works of the OSMP. We have notably pursued this approach with the telecommunication sector to involve them in the fight against spoofing and smishing techniques. This led to two major achievements: first, the rollout since end 2024 of a mechanism to authenticate calling phone numbers preventing spoofing attacks and, second, the securing of SMS messages with a clearer identification of professional senders. As fraudsters also leverage on social networks and instant messaging applications to recruit and manipulate their victims, **we are currently launching a similar approach towards major tech firms such as Google**, Meta or Tik-Tok. These tech players have undertaken many initiatives to fight against scams and are ready to cooperate with the financial industry under the umbrella of the OSMP.

Conclusion

As you can easily infer from my remarks, we consider at the Banque de France that our Observatory has proved to be a useful institutional body to help combat fraud and support us in the fulfilment of our mission regarding the security of payment means. I very much wish that you will come to the same conclusion with your own platform. **My conviction however is that their impact could be strengthened if they were part of a European framework. In that perspective**, the adoption of the Payment Services Regulation (PSR) triggers the creation of a European platform aimed at steering the fight against fraud at European level – definitely a most welcome and promising development. Thank you for your attention.

---

[1] OSMP_2025_chapitre_3.pdf

[2] See the joint EBA-ECB report on payment fraud