EUROPEAN CENTRAL BANK

EUROSYSTEM

30 April 2026

Sixth Meeting of the European Fintech Payments Dialogue

The 6th meeting of the European Fintech Payments Dialogue took place on 24 March 2026. Representatives of eight European fintechs and payment experts from the European System of Central Banks (ESCB) held a discussion on the theme of '*Fraud prevention'.* Ahead of the meeting, a set of questions was distributed to help structure the dialogue (Annex 1).

Current developments

Fintech participants highlighted synthetic identities[1] as one of the fastest-growing threats in payment fraud, exacerbated by the increasing availability of generative AI tools to create convincing fake profiles supported by real or manipulated documents. Fintech representatives emphasised the challenge of protecting customers against rapidly evolving fraud tactics while preserving a seamless user experience and avoiding undue friction.

One approach discussed was the use of "silent" fraud prevention methods, where detection systems operate invisibly to avoid exposing controls to fraudsters. This may involve analysing phone numbers and email addresses to detect fraud signals without directly interfering with the user experience. Fintech participants also noted that the authorised push payment (APP) fraud[2], including tactics such as "camping" (using legitimate residential addresses to register fraudulent companies), remains a widespread issue and varies significantly across European jurisdictions due to differences in company registry systems.

Privacy-enhancing technologies[3] (PETs) and zero-knowledge proofs were identified as promising tools for enhancing the deployment of digital wallets, information sharing and other tasks while minimising data exposure. However, fintech participants noted that regulatory and legal barriers in some EU countries restrict the use of these technologies, contrasting with other more permissive geographical areas. Criminals often exploit such regulatory asymmetries. One fintech noted that identity takeover of technically secure eIDs (typically via social engineering) may also warrant future attention as a potential new fraud vector.

Decentralised finance[4] (DeFi) was highlighted as another growing risk area, with complex financial products being used to obscure fraudulent activities. Fintech participants noted that DeFi's market capitalisation has grown significantly, increasing its potential impact. Finally, fintech participants stressed the importance of being always informed and updated by following legal and regulatory developments, conducting policy research and maintaining ties with the relevant law enforcement agencies.

---

1 Synthetic identities are created by putting together pieces of data from real people like the bank account from person A, driver's license number from person B and the social security number from person C. This information is then used to make a completely fake identity, which looks real.

2 APP fraud occurs when scammers trick victims into willingly authorizing bank transfers to them, often posing as trusted organizations or people. Unlike traditional fraud, victims initiate the payment, making it harder to detect and reverse.

3 PETs are hardware and software solutions that protect personal data, ensuring privacy, confidentiality, and compliance with regulations like GDPR.

4 DeFi is an open-source and permissionless financial ecosystem built on blockchain technology.

Fraud detection and transaction monitoring

Fintech participants underscored the need to move beyond reactive transaction-level controls to pre-emptive and more holistic, account-focused approaches. One fintech described a system that integrates omnichannel data sources (e.g., card usage, ATM withdrawals, branch visits) to classify accounts as suitable or unsuitable for payment activities. This system targets both traditional unauthorised fraud and newer APP fraud, with a focus on identifying malicious accounts such as money mules. Additionally, the use of decoy mule accounts to identify and disrupt fraudster activity was mentioned.

AI-based tools were identified as key enablers for fraud detection, but fintech participants agreed that a human-in-the-loop approach is necessary to mitigate risks such as "hallucinations" or unintended actions by AI systems. Explainability and accountability were stressed as vital principles, particularly for decisions that may need to stand up in court. Fintech participants also highlighted the importance of network-level analysis to understand the roles and connections within fraud rings. This is related to the fact that organized fraud groups do not work in isolation but operate complex structures employing a large number of witting or unwitting money mules.

Another important aspect raised was the increased fraud activity targeting vulnerable segments of the population and mainly the elderly. These scams usually involve an element of social engineering. To protect potential victims and build real effective fraud prevention tools, access to phone data is warranted. So far, experience has shown that telecommunication operators have no incentive or lack the legal basis to share such data with financial institutions.

Consumer trust and fraud awareness

The conversation focused on advancements in biometric authentication and identity verification as trust-building measures. Fintech participants described multi-layer security approaches, including identity verification via NFC-enabled biometrics, palm recognition, and dynamic PIN challenges in case of presumed suspicious transactions. It was also mentioned that according to market research palm-based biometrics are perceived by users as more convenient and secure than facial recognition or fingerprint methods. This is corroborated by the fact that this method involves an elaborate three-factor authentication procedure.

Fintech participants noted that traditional fraud awareness campaigns often fail to engage customers, who are inundated with generic messages. The vast array of alerts, notifications, and advertisements dilutes the impact of awareness efforts, leaving consumers less informed and less prepared to navigate fraud risks. Interactive, event-driven communication—such as explaining the reason for PIN authentications during suspicious transactions—was suggested as a more effective way to raise awareness and build trust.

Information / data sharing and industry collaboration

This session explored the challenges of interbank cooperation, legal and privacy constraints, and the need for standardised approaches to detect and prevent fraud more effectively. Intelligence-sharing frameworks across institutions were discussed as critical for improving fraud detection.

Fintech participants described various privacy-preserving data sharing mechanisms, such as multi-party computation[5] (MPC) and fully homomorphic encryption, which enable institutions to collaborate without exposing personal data. Such approaches ensure that no single organisation has access to the complete dataset, only the final aggregated results. However, mutual trust and clear agreements between banks on data sharing remain essential. MPC requires banks to agree on a "rulebook" that defines key criteria for identifying suspicious behaviour. The use of zero-knowledge proofs in this process adds an additional layer of security, allowing banks to demonstrate adherence to these rules without exposing transaction details like timestamps or destinations.

[5] Multi-Party Computation (MPC) is a cryptographic technology that enables multiple parties to jointly analyse, compute, or share data without revealing their individual raw, private inputs to one another. It allows banks to split sensitive information like suspicious account numbers into encrypted pieces and use them to jointly detect fraud.

One fintech introduced the concept of distributed aggregation protocol[6] (DAP), which enables organisations to share aggregated risk data without revealing sensitive personal information. These risk aggregates may include geographical risks, social and professional category-based risks, as well as behavioural indicators. While sharing such aggregated data within a single organisation is relatively straightforward, the process becomes significantly more complex when multiple institutions are involved. Despite these challenges, fintech participants emphasised that data sharing should focus on non-personal information to minimise privacy concerns while still enabling effective fraud detection.

Fintech participants acknowledged that during the last decade, the concept of fraud detection has evolved from being a competitive advantage for individual organisations to a shared priority. Financial institutions have now realised that achieving a satisfying level of fraud prevention is only possible through collaboration. Nevertheless, agreeing on common standards and methods remains an ongoing challenge. One fintech pointed out that the financial industry should copy areas such as cybersecurity that developed efficient collaborative approaches (including structures and taxonomies on what to share on a need-to-know basis) a long time ago. The need for interoperability was also emphasised as a critical step in expanding and strengthening collaborative fraud prevention efforts.

The discussion highlighted the importance of full lifecycle data management, emphasising that data quality and structure are essential for effective interbank cooperation, which currently remains fragmented. One fintech commented that technical committees dedicated on financial services standards can serve as vehicles for developing common frameworks. Fintech participants stressed that fraud is a global issue requiring international agreements and rulebooks.

Regulation

The argument was made that technology alone cannot address the legal challenges surrounding data sharing. Regulatory frameworks, such as anti-money laundering (AML) legislation[7], grant the legal permission to share. In this context, fintech participants advocated for a speedy and timely implementation of any new regulation contributing to combatting fraud.

Information security standards must also ensure that only authorised personnel have access to sensitive data, safeguarding against potential misuse. Among the topics discussed were the possibility of replicating existing successful regulatory efforts, the increased need for harmonisation and the creation of collaborative best practices.

Finally, the discussion touched on the challenges posed by legal restrictions on information sharing among financial institutions putting them into disadvantage compared with criminal networks. Criminals have the advantage of freely exchanging information and coordinating their activities across borders, whereas banks often face regulatory restrictions or lack of legal clarity that limit their ability to collaborate. This imbalance creates vulnerabilities in fraud prevention systems, as the financial sector appears unable to match the speed and efficiency of criminal networks.

Concluding, fintech participants agreed that fraud prevention requires a co-operative and multi-faceted approach, including the strong involvement of relevant authorities and central banks.

---

6 The Distributed Aggregation Protocol (DAP) is a privacy-preserving technology developed to collect aggregate statistics without accessing individual, sensitive user data.

7 Mainly article 85 of the proposed EU Payment Services Regulation (PSR) and article 75 of the EU Anti-Money Laundering Regulation (AMLR) 2024/1624.

Annex 1 – Discussion questions

Participants were invited to answer and discuss the following questions:

- What emerging trends and developments in payment fraud do you consider most significant (e.g. social engineering scams, push payment frauds, DeFi etc.)? What challenges do you foresee in the coming years and how are you preparing for them?
- How do you successfully adapt to the rapidly evolving fraud dynamics? How do you balance rapid innovation with robust fraud prevention measures?
- How could industry efforts to monitor payment fraud patterns, block fraudulent transactions and recover stolen funds be improved?
- If you use AI for payment fraud detection, do you find a human-in-the-loop approach or a fully autonomous system to be more effective for combatting fraud?
- What approaches are you using to build consumer trust, particularly in addressing spoofing cases or improving authentication processes?
- What initiatives are you currently implementing to increase customer awareness of payment fraud and prevention strategies?
- To what extent are you involved in information sharing and cross-sectoral or cross border collaboration related to payment fraud? What specific challenges do you face in this area?
- How do you balance the need to share data for fraud prevention purposes with privacy and data protection requirements (anonymity vs security)?
- What role do you see for industry-wide anti-fraud platforms, and what incentives would encourage you to actively participate in such initiatives?
- To what extent do regulatory developments related to payment fraud influence your service provisions?
- How can regulation promote meaningful fraud prevention without increasing customer friction to an unacceptable level?

Annex 2 – List of participants

Chair

Mr. Dirk Schrade	Deutsche Bundesbank

Fintech Participants

Mr. Patrick Töniges	spotixx
Mr. Taavi Tamkivi	Salv
Mr. Patrick Curry	Sedicii
Mr. Alán Alcoverro	Acoru
Mr. François Saulnier	Bleckwen
Mr. Marko Maras	Trustfull
Mr. Oskars Lakšēvics	Handwave
Mr. Bernhard Haslhofer	Iknaio

National Central Banks Participants

Ms. Geneviève Janssens	Nationale Bank van België/Banque Nationale de Belgique
Mr. Mihail Dimov	Българска народна банка (Bulgarian National Bank)
Ms. Jana Fajstlová	Česká národní banka
Ms. Ditte Johanne Jensen	Danmarks Nationalbank
Ms. Inga Schultze	Deutsche Bundesbank
Ms. Linda Lelumees	Eesti Pank
Mr. Noel O'Connor	Central Bank of Ireland
Ms. Aikaterini Vinga	Bank of Greece
Ms. Rosa María Brave Castellón	Banco de España
Mr. Pierre Bienvenu	Banque de France
Mr. Tomislav Mišić	Hrvatska narodna banka
Mr. Guerino Ardizzi	Banca d'Italia
Ms. Stella Ioannidou	Central Bank of Cyprus
Ms. Edīte Grīnvalde	Latvijas Banka
Ms. Jūratė Butkutė	Lietuvos bankas
Ms. Li-Chun Yuan	Banque centrale du Luxembourg
Mr. Stefano Savo	Central Bank of Malta

Mr. Wouter Vinken	De Nederlandsche Bank
Mr. Simone Mingione	Oesterreichische Nationalbank
Mr. Robert Klepacz	Narodowy Bank Polski
Mr. Rui Pimentel	Banco de Portugal
Ms. Rebeka Reven	Banka Slovenije
Ms. Iveta Behunova	Narodna banka Slovenska
Ms. Maria Huhtaniska-Montiel	Suomen Pankki
Mr. Anders Mölgaard Pedersen	Sveriges Riksbank
Ms. Karine Themejian	European Central Bank
Mr. Stylianos Chrysomallis	European Central Bank
Mr. Henri Tuorila	European Central Bank
Ms. Kerstin Junius	European Central Bank