Retail payment innovation

1. Strengthening Europe's strategic autonomy in payments: from geopolitical vulnerability to sovereign infrastructure

1.1 Payment sovereignty has become a matter of economic security

A Central Banker framed the central question as whether Europe can build a retail payments ecosystem that is coherent, innovative and inclusive, combining convenience and speed with security, choice, resilience and inclusion. EU rules on instant payments are making real-time euro credit transfers a standard capability across the single market, PSD3 and the PSR are strengthening consumer protection and harmonising open banking, and the digital euro is moving into a new phase, while private initiatives such as Wero and EuroPA advance in parallel. AI-enabled agentic payments are beginning to emerge, adding further urgency to the strategic debate.

Another Central Banker argued that payment sovereignty has become a matter of economic security and, in the Baltic context, national security. Latvia and its neighbours have long been exposed to financial and cyber pressure from Russia, and their highly digitalised economies are particularly sensitive to disruptions and sanctions-related spillovers. The strategic question is whether Europe wants the resilience of commerce, banking and consumer payments to depend on infrastructures governed outside the EU, or whether it should build and govern more of that infrastructure itself. Stablecoins compound the challenge: most are USD-denominated, and Europe still lacks a globally scaled euro-denominated stablecoin ecosystem. The response must combine stronger European payment rails, technical innovation, public-private cooperation and reinforced cybersecurity.

1.2 A public alternative that can connect merchants as well as banks

A Central Banker made the most explicit case for a public payment infrastructure. Europe must complement the existing instant payment rail with a public alternative that can connect merchants as well as banks. The digital euro could provide exactly that: a public rail, free of processing and scheme fees, that would widen merchant acceptance, help European providers compete with global players, and provide a stronger base for innovation. Use by end users would remain voluntary, but the legislative process must move quickly so that the infrastructure — including offline functionality — can be built. Another Central Banker reinforced this view, pointing to tokenised finance as an additional avenue and calling for public-private cooperation to support the project. A Regulator noted that the EBA fully supports the digital euro and sees no immediate consumer protection concerns, while flagging that public awareness remains low and that financial education will matter considerably.

1.3 Backup arrangements only work if people use them in normal times

A Central Banker illustrated the cost of inadequate resilience with the recent Iberian outage, in which some consumers were unable to pay or withdraw cash. Backup arrangements only work if people use them in normal times, not only in crises; otherwise they fail precisely when most needed. Cash must therefore remain available as a fallback.

Another Central Banker placed this within the broader financial stability framework. Secure, efficient and resilient payment infrastructure is a backbone of financial stability. Because banks are the link between the payment ecosystem and the wider economy, preserving trust in both is essential. Any disruption can cascade rapidly through households, businesses, public confidence and the wider financial system. Denmark's high degree of digitalisation brings major efficiency gains but also new operational and cyber vulnerabilities. Central banks must therefore prioritise robust systems, strong cybersecurity and close public-private cooperation, while ensuring that the full diversity of payment methods — cash, cards, account-to-account solutions and potentially a digital euro — is actively used in everyday life, so that each can genuinely strengthen resilience when a crisis occurs.

2. Aligning public policy with private innovation: the right conditions for a coherent and scalable ecosystem

2.1 Complementary, not competing tracks

An official argued that the digital euro and private initiatives should be complementary, not competing tracks. Private solutions are already more advanced in some use cases, while the digital euro is still under development. In the point-of-sale space, success will depend on whether every participant in the value chain has the right incentives to support innovative account-to-account solutions. Two conditions are particularly critical: the remuneration model for financial institutions, and robust protections for merchants, especially smaller merchants. Unless these issues are resolved for both private solutions and the digital euro, neither will achieve the scale needed to make a lasting difference.

An Industry representative welcomed the digital euro as part of the European ecosystem while stressing that its long-term success will depend on whether it meets genuine customer and merchant needs and can be implemented sustainably. His main concern was mandatory participation: broad access does not require

mandating every provider, especially where some actors would face significant costs without an obvious use case. If participation were mandated, the incentives would need to be right and non-bank PSPs would need to compete on fair terms. He also stressed the importance of a multi-wallet model and smooth access to funding accounts.

2.2 Foster innovation and competition while creating a more level playing field

Another industry representative argued that Europe has succeeded in enabling payments innovation largely because regulation has built trust. Europe can be proud of having led on instant payments and on direct access for non-bank PSPs, both of which strengthen competition. Yet other regions are moving quickly: deregulatory trends and new licensing approaches in the United States could accelerate payments and stablecoin adoption. Europe risks becoming too prescriptive and not bold enough, especially on AML harmonisation.

A Regulator set out the regulatory programme. PSD3 and the PSR pursue three objectives: fostering innovation and competition by improving access for non-bank PSPs; strengthening security through payee verification, stronger monitoring and clearer liability rules; and deepening EU harmonisation for a more level playing field. The EBA is preparing around 32 regulatory products, alongside the EU cross-sector anti-fraud platform whose core phase will come in 2027.

An industry representative further identified AML and onboarding as a strategic bottleneck: if non-bank PSPs continue to face de-risking and Europe does not apply a risk-based AML approach, innovation will be constrained before it reaches consumers. He called for greater legal certainty, smoother remote onboarding and better access to central bank settlement infrastructure. A Central Banker added that banks should see payments as a core service: digital payments lower costs and increase self-service, making continued investment in secure, modern payment services central to competitiveness.

2.3 Inherence is often interpreted too narrowly

Another industry representative argued that innovation in payments must start with concrete consumer needs and work within market realities and regulatory expectations. Contactless payments exemplify a once-novel innovation that has become effortless for users, even though it depends on complex layers of security, speed and reliability behind the scenes. Tokenisation is a typical behind-the-scenes innovation — barely noticed by consumers but essential to security and resilience, including in a world where AI is reshaping risks. Innovation is not only about growth but also about adaptation and endurance in unstable conditions — war, outages, environmental shocks. Visa is therefore working on resilience as well as convenience, including on how Strong Customer Authentication should operate in offline environments with deferred authorisation.

An industry representative identified the treatment of inherence under SCA as the most impactful area for improvement. Inherence is often interpreted too narrowly as physical biometrics such as fingerprints or facial recognition. Broadening the definition to include behavioural biometrics would allow PSPs to use richer passive and continuous authentication signals, reducing fraud without adding friction. Supervisors and regulators should allow sufficient flexibility for behavioural biometrics within SCA.

3. Turning fraud prevention into a European competitive advantage in an AI-driven environment

3.1 AI is both part of the problem and part of the solution

An Industry representative described AI as simultaneously the most serious threat vector and the most powerful defence tool. Sophisticated impersonation and deepfakes mean consumers exposed to AI-generated scam advertisements are far more likely to fall victim to fraud. The industry must move from reactive to proactive AI use, identifying scams before the consumer is even contacted. Frictionless payment journeys should not come at the expense of consumer awareness: users need clearer signals about what a legitimate payment journey looks like. E-ID is a useful building block for reducing anonymity and strengthening trusted interactions.

A Central Banker noted that AI is unavoidable and that the AI Act provides the risk-based framework for its use in Europe. In payments, AI can support fraud detection and decision-making, becoming a tool for resilience as well as innovation. The key issue is explainability: PSPs will remain responsible for being able to explain how AI contributes to decisions. Central Banker added that PSPs and card schemes must look beyond payment behaviour and focus on how customers log in and navigate, since that behavioural layer is much harder for fraudsters to imitate. Digital fingerprinting is a promising tool; mismatches should trigger blocking, supported by a strong legal basis.

3.2 Fraud often starts outside the financial sector before ending inside it

An industry representative argued that fraud prevention must focus on prevention, not only on compensating victims. That requires better information-sharing within financial services and cooperation across the whole fraud chain — including social media platforms, marketplaces and telecom operators — because fraud often starts outside the financial sector before ending inside it. Europe must monitor whether new cooperation mechanisms deliver results and act quickly if they do not.

An official identified three main risk areas: fraudsters posing as authorised providers; impersonation of banks and public authorities; and social engineering more broadly. Better cybersecurity is needed in financial and large non-financial companies alike, as stolen data enables highly targeted attacks. Cooperation must go beyond information-sharing and lead to action — such as blocking the SMS messages or phone calls through which scams reach consumers. Victims need effective relief, but without removing the duty of care from users and companies.

3.3 Europe needs both strong protection and a high-quality service experience

A Central Banker described the current situation as a fraud pandemic. Even mature e-identity systems can be misused when fraudsters manipulate users into authorising transactions. EiDAS and future identity wallets may make it harder to determine whether an authentication was genuinely performed by the user. A growing share of fraud is formally strongly authenticated because the victim has been manipulated into approving the transaction: information must be shared faster, fraudulent actors expelled more quickly from the system, and liability cannot automatically be shifted onto the customer. Anti-fraud measures should not simply degrade the service for legitimate users — Europe needs both strong protection and a high-quality service experience.

An industry representative reinforced the point: if fraudsters are using AI, the payments industry needs to use AI better. A Central Banker oncluded by identifying four central imperatives: aligning public policy with private innovation; treating strategic autonomy as a practical necessity rather than an abstract ambition; strengthening consumer protection and fraud prevention in an always-on environment; and reconciling convenience with inclusion, resilience and trust as AI becomes ever more prominent.