Retail payment innovation

1. Innovation and resilience are not alternatives — it is both

The moderator framed the discussion around one question: how Europe can support innovation in retail payments while preserving trust, inclusion, resilience and sovereignty. The moderator concluded that innovation will succeed only if it strengthens, rather than weakens, trust.

1.1 New payment instruments need to earn consumers' trust in order to be durable

A central bank representative observed that consumers have proved willing, and indeed eager, to embrace innovation in payments whenever options such as mobile wallets were offered. The central bank representative stressed, however, that in one recent large-scale consumer survey, speed and convenience were not the top concerns, whereas security, fraud safeguards, trust and reliability ranked highest. The central bank representative therefore concluded that innovation and resilience are not alternatives — it is both.

1.2 Safety and security are not brakes on innovation — they enable it

An industry representative argued that innovation is not only about speed, reducing friction, or making things easier on the surface, but equally about ensuring that every user has confidence the system will continue to work under stress. The industry representative added that security allows innovation to scale with the trust it requires. The moderator concurred: innovation is not only about new technology, but also about trust, scale and governance.

1.3 Cash will remain a critical part of the payments' ecosystem

A central bank representative pointed to an apparent paradox: in one Member State, consumers have reduced their use of cash faster than the European average yet remain above that average in wanting the option to pay with it. The central bank representative described cash as critical for financial inclusion, but also, frankly, for resilience, being the ultimate payment method in the event of system-wide disruption, as we saw in the Iberian peninsula — hence the lesson is not innovative or traditional, but both. A central bank representative extended this resilience logic to the digital euro, which in their view should not be limited to online payment options, but should also support offline use.

2. A single, interoperable European payments system

The moderator described instant payments as the new normal and the new standard and saw the digital euro, Wero and EuroPA as underlining the need for pan-European solutions that are efficient, sovereign and scalable. A central bank representative called the transformation not single-dimensional but multifaceted: Europe is moving towards an integrated retail payments market, which calls for a holistic approach, for instance through national payments strategies building on European foundations.

2.1 The question this raises, is not only one of sovereignty but of resilience

A central bank representative noted that thirteen European countries depend entirely on non-European card payment schemes. The central bank representative compared this to a country's electricity depending on a neighbour through a single cable, raising the question of a backup. The central bank representative presented the digital euro as that backup: a European scheme backed by central bank money, which is not meant to replace existing card or payment schemes but to add one further option. The central bank representative welcomed Wero and EuroPA but judged them not yet fully pan-European today. The central bank representative summarised the objective as a single, interoperable system delivered through a combination of publicly run infrastructure and privately run initiatives.

2.2 The ability of all these different solutions to interoperate efficiently, at scale and in a resilient way

An industry representative rejected the idea that the future will be shaped by a single new technology, method or network. The industry representative argued that Wero, EuroPA, the digital euro and open banking will all be judged on the same test: creating economic value through a superior user experience, while ensuring resilience. The industry representative welcomed innovation, investment and increased competition as a source of consumer choice and productivity. The industry representative asked public authorities for a framework ensuring predictability and proportionality, a level playing field and greater investment in cybersecurity, anti-fraud solutions and interoperability.

2.3 Payments are not just about facilitating transactions

A central bank representative highlighted the macroeconomic stakes: payments can lead to new products and services, improve businesses' liquidity management and deliver the productivity gains Europe needs. The central bank representative turned the fragmentation of the European market into a real opportunity, citing studies showing that integrating payment systems increases trade with an effect broadly comparable to around half that of a new trade agreement — a foundation for strengthening the Single Market. The moderator likewise observed that payments are evolving from a largely technical service into a central interface between consumers, merchants, banks, payment providers and digital platforms.

3. Faster payments mean faster fraud

The moderator warned that faster, more frictionless payments can also mean faster fraud, and that AI-enabled scams and social engineering are challenging traditional fraud-prevention tools.

3.1 Criminals continue to find, and exploit, the gaps between institutions

An industry representative set out the scale of the threat: according to one industry estimate, US$4.4 trillion in illicit funds moves across the global ecosystem each year, including US$579 billion linked to fraud, and these funds ultimately come from ordinary people. The industry representative identified speed as the central concern, citing authorised push-payment fraud in the UK, now above 19% year on year, a pace at which our economies simply do not grow. An industry representative agreed that if payments are instant, fraud becomes instant too, calling for prevention, detection, authentication and clear liability design. The industry representative also noted a qualitative shift, from credential theft towards more sophisticated social engineering and manipulation, to be countered with systems based on behavioural signals and dedicated analysis. The industry representative explained how AI amplifies this: an individual fraudster can now operate at the scale of a large criminal consortium.

3.2 Should we then impose significant friction on the other 99,997 customers as well?

A central bank representative argued for proportionality: in one national market, around 2.5 payments in every 100,000 are linked to fraud, and imposing heavy friction on everyone else is probably not the answer. The central bank representative suggested distinguishing the speed of technology from the speed of transactions: should a credit disbursement reach an account within five seconds? Should a utility bill be paid that quickly? An industry representative added that younger customers expect payments to be instant and final — I want it here, I want it now, and that is the end of the story. An industry representative saw behavioural biometrics as a way to combine security and smoothness: inherence can be confirmed through the way someone holds their phone, or the speed at which they type, or through transaction patterns. The industry representative emphasised that this confirms authentication without disrupting the purchase journey, which is particularly valuable for people with disabilities, less digitally confident or older customers. The request of the industry representative was very concrete: that the EBA clearly recognise behavioural biometrics as a valid means of confirming inherence in the context of SCA, the technology having already been introduced at level 1 in PSD3 and the PSR.

3.3 Unless we operate as a network among ourselves we will inevitably lose ground

An industry representative identified an asymmetry: Criminals, unlike us, operate as a network, and they are not bound by regulation. The industry representative therefore called for regulation supporting information-sharing within a safe-harbour environment, near real-time action and a move from detection to a genuinely preventive approach, using AI in defence — fighting fire with fire — within a secure framework and sound governance. The industry representative stressed that consortium approaches, such as scoring counterparty risk across institutions, are not, strictly speaking, about sharing personal information, but about sharing risk insights, and called for collaboration rather than mere coordination, extending to law enforcement, telecoms and technology companies. A central bank representative illustrated the cross-sector dimension: in one small Member State, telecom companies block tens of millions of fraudulent calls and messages each year, and draft national legislation would ease information exchange between telecoms, banks and the police, since fraudulent funds cross borders almost instantly, whereas police authorities cannot. The central bank representative also urged more attention to beneficiary banks, and how they can prevent fraudsters from opening accounts and moving money further in the first place.

4. The history of payments has been one of partnership between the public and private sectors

A central bank representative recalled that throughout history payments have been built through public–private partnership. The moderator noted that AI can improve fraud detection and efficiency but introduces new risks around scams, automation, accountability and user control.

4.1 It is still early days, but it is happening

An industry representative described agentic commerce as one of the biggest shifts we have seen in e-commerce since its emergence in the early 2000s, with US use cases to reorder household essentials, pay bills, or compare prices and forecasts that it could represent between 10% and 25% of e-commerce by 2030. The industry representative listed the questions it raises: whether the agent is properly authenticated, whether the purchase matches the customer's actual intent, and who is accountable when something goes wrong. The industry representative explained that their international payment institution provides developers with tools to authenticate agents and verify intent, that the human is not taken entirely out of the loop, and that it remains accountable in case of fraud. The industry representative added that, as a human may be present at the start and the end, but not necessarily in the middle, authenticating both the agent and the underlying person will remain essential.

4.2 It is important that legislators do not move too quickly

An industry representative argued that agentic commerce is not a European question alone but a global one, and that rushing into disproportionate regulation risks creating a competitive disadvantage for

European players in a market that [...] recognises no real borders. The industry representative favoured observing initial use cases, considered that reopening the AI Act would not be the right approach, and suggested that the EBA address the issue through technical standards.

4.3 No single participant can, on its own, transform the overall payments system

A central bank representative cited fraud as a first example, where a national payments strategy can establish a coordination mechanism bringing together technology, financial services, telecoms and regulators, and where a central bank can obtain trusted-flagger status. The central bank representative then turned to system-level resilience, since individual resilience is a necessary condition, but not a sufficient one. The central bank representative finally cited public infrastructure: the Eurosystem's work on the digital euro and DLT-based wholesale settlement provides foundations that allow the private sector to do what it does best: interface with customers, innovate, compete for business and, ultimately, meet the evolving payments needs of households and businesses.

5. If you could change one thing in Europe's retail payments ecosystem by 2030

5.1 A genuine payments single market

An industry representative wanted consumers and merchants to move seamlessly from one country to another within a genuine payments single market, provided everyone is held to comparable standards of consumer and security protection. A central bank representative called for greater integration and greater diversity of payment rails, because choice matters, also for resilience, and a central bank representative fully supported this goal. The industry representative also committed their global payment scheme to completing, by 2030, its move to processing European transactions in Europe, on European soil.

5.2 Fraudsters are certainly not going to wait until 2030 to act

An industry representative wanted cross-border collaboration tomorrow, sharing at the very least shared insights, so that institutions work as a network, rather than as individual actors. A central bank representative endorsed this and added that society must find its own balance between convenience, speed and security, noting a study suggesting that when the internet freezes, the heart responds in much the same way as it does when hanging off a cliff edge.

5.3 I would ask legislators to continue to collaborate with industry

An industry representative recalled that their international payment institution had not waited for PSD1, 2 or 3 to focus on fraud management and has consistently maintained low fraud levels. The industry representative also insisted that the digital euro's business model makes commercial sense, as real innovation has come from those who listened closely to the market.