Retail payment innovation

1. Overcoming fragmentation to achieve strategic autonomy in payments

1.1 'Supervisory fragmentation prevents scaling': fostering cross border payments under Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR)

An official explained that the French Ministry of Economy, Finance and Digital and Industrial Sovereignty has long prioritised strategic autonomy, but the current European retail payments landscape remains inconsistent with this goal. Nationally fragmented markets and regulatory divergences hinder the development of EU wide players. For instance, only nine of the 27 EU member states have national card schemes. One of the key barriers is supervisory fragmentation. This is very important in the payments space because companies seeking to be genuinely pan European still have to deal with many different supervisors. This issue will have to be addressed as part of the work on PSD3 and PSR.

1.2 European Payments Initiative (EPI) and EuroPA interoperability: a promising signal for EU level initiatives

An official remarked that the recently announced interoperability between the EPI and EuroPA consortia is a promising development. While Europe is not yet where it needs to be, this trend towards interoperability points in the right direction.

1.3 Strategic autonomy cannot be legislated into existence; regulation should create the conditions for the EU payments ecosystem to thrive

An official noted that strategic autonomy cannot be legislated into existence. Instead, regulators should focus on creating the conditions which will enable the EU payments ecosystem to thrive. While PSD2 has not fulfilled its potential, it has opened up several new opportunities. However, these opportunities have not been capitalised on. The ongoing discussions between the Commission, Parliament and Council are focused on what else can be done to make PSD2 a success. The next step is to build trust, notably through transparency on fees. Introducing robust transparency clauses into PSD3 and PSR will be very important in fostering trust. Furthermore, the regulators need to broaden their understanding of the payments ecosystem. They need to look beyond traditional payment services providers (PSPs) and consider the roles played by telecommunications firms, digital wallet providers and technical acceptance provider, among others.

2. Ensuring resilience and continuity in a digital payment environment

2.1 'Fallback mechanisms must be ready': building systemic resilience to outages

A Central Bank official cited the example of a recent payment system outage in Denmark, which occurred on a Saturday evening. This incident provided a real world stress test of the Danish payments system. Although some firms had offline solutions, some of their staff members lacked the training to activate them properly. On a positive note, some shops and retailers were able to shift to account to account (A2A) systems, which are integrated into the Danish payments system, as an alternative to card based payment rails.

An industry representative commented that the growing reliance on digital payments underscores the importance of resilience. If electricity or connectivity fail, as recently happened in Spain, fallback mechanisms such as offline payments must be ready to be deployed. Industry and government need to develop and test these back up systems jointly. Testing will be very important to ensure that these systems can act as a necessary to ensure the resilience of payments system during a crisis.

2.2 Offline payments in mobile centric systems: the Danish deferred authorisation model

A Central Bank official remarked that Denmark's national card scheme already includes an offline capability, but consumer habits have shifted, and younger consumers are increasingly paying with their smartphones. Around 25% of in store transactions are conducted via mobile wallets such as Apple Pay or Google Pay. In recognition of these changes in the behaviour of Danish consumers, Denmark is seeking to implementing a deferred authorisation model, which works in a similar way to inflight transactions, in which payments are recorded and processed once the system reconnects to the network. This initiative aims to integrate an offline capability into modern mobile centric payment infrastructure. The largest grocery chain in Denmark has agreed to join this project and hopefully the remaining major Danish grocery chains will have joined by early 2026.

2.3 Resilience is a shared responsibility

A Central Bank official emphasised that the experiences in Denmark and Spain underline the need for broader contingency planning and system wide preparedness.

An industry representative agreed that resilience must be a shared responsibility across different actors. Governments and industry players should engage in

joint testing and scenario planning rather than acting in isolation. Visa recently r published a European resiliency report which contains recommendations on how to drive resilience in the EU payments ecosystem. No payment system is stronger than the weakest link in the chain. Everybody in the payments industry, including electricity companies and telecommunications firms, needs to work together to secure the payments system.

3. Securing the payments system and maintaining trust

3.1 'Fraud is the biggest threat to trust'

An industry representative observed that trust is the key ingredient in all payment methods, and fraud is the greatest threat to trust. Visa deflects up to 10,000 attacks per minute every day and it has invested €11 billion in fraud prevention over the last five years. It is not a coincidence that Visa's systems are secure. The fight against fraud is incredibly resource intensive and essential to the security of the payments ecosystem.

An official commented that fraud today is not about stealing a bank card; it is about social engineering. The victim uses their credentials to authorise fraudulent payments. Regulation must try to provide an answer to this challenge. Indeed, payments is a network business. All the stakeholders in the industry must be involved in fighting these issues.

3.2 Telecommunications firms are key enablers in fraud prevention

An official explained that telecommunications firms need to be involved in the fight against fraud, as digitalisation and communication channels are being increasingly used as vectors of fraud. This is a challenge for telecommunications firms, which have a duty to enable communication. In many cases, they are not legally allowed to block communications. In countries such as Spain, Belgium and the Netherlands, national legislation allows telcos to block calls and SMS messages that do not comply with domestic numbers authorisation regulations. In Spain, millions of phone calls and SMS messages have been blocked since this piece of legislation was implemented in February. The fraudsters will always find another way to defraud, but the cooperation of telecommunications firms is essential in fighting back.

3.3 Strong customer authentication (SCA) and IBAN checks, effective but not sufficient

An industry speaker observed that the introduction of measures such as requirements for IBAN checks or mandatory strong customer authentication (SCA) are highly effective fraud prevention tools. This is one way in which regulators can play an important role in the payments space.

An official noted that the PSD2 and PSR reforms are focused on fraud prevention, liability and the involvement of telecommunications companies. On prevention, the Council's compromise text seeks to enable the monitoring of suspicious activity through data sharing that adheres to the EU's data protection rules. On liability, the Council has endorsed a balanced approach that provides legal certainty and ensures that the victims of bank impersonation fraud will be reimbursed by the relevant financial entity.

4. Inclusivity and consumer centric innovation

4.1 Avoiding single points of failure

An industry representative emphasised that consumers need to be able to access a diversity of different payment methods that are secure and can be trusted, especially during crisis scenarios. There should not be a single point of failure. It must be as safe to pay with using A2A or instant payments as it is to pay by card or cash.

4.2 Avoiding digital exclusion

An official explained that the digitalisation of financial services risks excluding many different vulnerable populations, including the elderly, the disabled, low income groups and people who live in rural areas. This digital divide became more evident during the pandemic.

In 2021, several Spanish associations of elderly people called for greater accessibility of financial services, including payment services. The Spanish Finance Ministry has constantly promoted a self regulatory approach to improve financial inclusion, and the answer from the industry was fantastic. In July 2021, the Spanish Banking Association (AEB), the Spanish Confederation of Savings Banks (CECA) and the National Union of Credit Cooperatives (UNACC) signed a protocol on financial inclusion, which has since been updated twice. The first protocol included specific measure to improve in person and telephone attendance by extending opening hours, adapting devices and ATMs, adding visual features, simplifying language used and ensuring that the interaction is as easy as possible. The second update to the protocol focused on access to financial services in rural areas and sought to guarantee access to cash in every municipality in Spain. Many other jurisdictions are facing this issue. The solution cannot be to put a branch in every single local area. The use of mobile points of access or the use of postal infrastructure are two potential solutions. The Spanish government operates a national observatory to monitor the implementation of these measures. The website is updated every six months, detailing how access to cash is guaranteed and the types of measures that are available to help the elderly and disabled people.

Today, 98% of Spain's population live within five kilometres or 10 minutes of a point of access to financial services. These results demonstrate that public–private self regulation can be more effective than formal legislative mandates.

4.3 Innovation must be useful and fun, and it cannot be imposed by regulation

An industry speaker emphasised that regulatory attempts to foster innovation, such as PSD2, have

largely failed. In France, open banking is not a success. Fewer than 10% of clients have used account aggregation and only 1% have initiated payments via third party providers. At Société Générale, over 99% of retail consumer transfers are initiated within the bank. For business customers, the proportion of payments initiated outside the bank is around 0.1% or 0.2%. The proposed Financial Data Access (FiDA) regulation risks becoming an even more costly misstep. The EU should learn the lessons from Australia's failure to implement a similar legislative approach. In contrast, innovations such as contactless, mobile wallets, instant payments and peer to peer (P2P) transfers have thrived because they bring something fun or useful to consumers. People only use new features when they are fun or useful. Ultimately, the consumer will decide whether an innovation is successful or not. Mandating innovation by law is useless. Innovation is a process of trial and error, and regulation cannot be done by trial and error.

An official commented that FiDA will be able to build strategic autonomy in payments on its own. If FiDA proves necessary, it will need to be implemented using a market based solution.

An industry representative stated that payment innovations must be secure, easy to use and aligned with evolving consumer expectations. If consumers are worried about whether a payment will be successful or whether they will be defrauded, they will not use a new and innovative payment method. Trust is a key requirement for all new payment methods or products, including the digital euro.

5. Incentives and business models for the digital euro

5.1. The incentives need to be properly aligned to ensure the digital euro is a success

An industry speaker remarked that the current digital euro proposals do not offer a viable business model to distributors, such as banks. Distribution should not come with an additional cost burden. There must be a fair business model which covers distribution costs, running costs and fraud costs. The cost of fraud is often overlooked. Financial firms have to spend very significant amounts of time and money to prevent fraud and deal with its consequences.

5.2. Legal tender status is not enough: the digital euro must offer user experience, trust and privacy

An industry speaker explained that the legal tender status of the digital euro will ensure merchant acceptance, but consumer adoption will hinge on user experience, trust and privacy. The ECB's efforts on privacy are promising, but citizens must be convinced it is private. In this regard, the marketing of the digital euro will be crucial. Even if it is a technical and strategic achievement, it will not work if consumers do not trust it. While there are legitimate reasons to launch the digital euro, such as the need to maintain strategic autonomy, the current proposals do not offer anything new or attractive for consumers. There is no compelling reason why a consumer would choose to use the digital euro.

5.3. Interoperability and coexistence

An industry speaker stated that Private solutions face a competitive disadvantage because they do not benefit from legal tender. To ensure a level playing field, regulation could mandate the distribution or acceptance of at least one pan European private solution and enforce interoperability between these private solutions. Ultimately, the industry will need time to develop its own private solutions. When the digital euro project is launched, banks will struggle to invest simultaneously in their own private solutions and the mandatory public solution. Therefore, the launch of the digital euro project should not happen too soon and it should follow a staggered approach.

Even if the digital euro is launched, the EU will also need private solutions for resilience reasons. The EU payments industry will build a pan European payment solution based on its assets. This is the private sector's answer to strategic autonomy and banks will deliver it. All use cases will be rolled out: P2P payments, point of sale transactions and online payments. It will be vital to develop and adopt common acceptance standards to make these systems interoperable. There are ongoing discussions between consortia such as Wero and EuroPA to build interoperable A2A solutions in Europe. Wero has already enrolled 44 million users and 25 banks, and it plans to expand beyond the eurozone. The digital euro will not be able to compete with private global solutions if its use is limited to the eurozone.