Future of Payments

JOURNAL OF FINANCIAL SERVICES

PUBLISHED BY: **PROJECTIVE GROUP INSTITUTE**

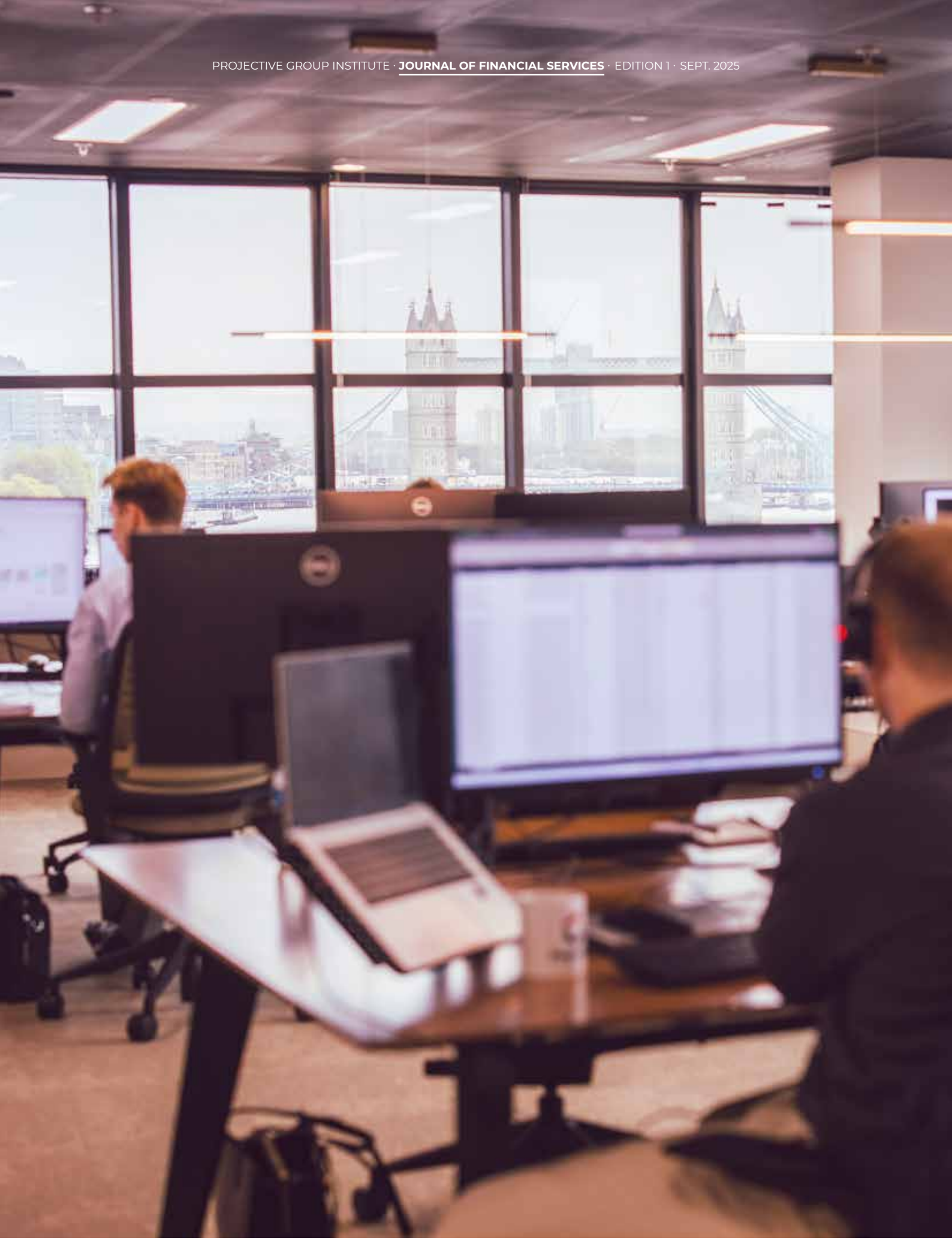
01
2025

Projective
INSTITUTE

JOURNAL OF FINANCIAL SERVICES

Future of Payments

Contents



Dear reader,

Welcome to this, the inaugural edition of the Projective Group Institute's new Journal of Financial Services!

We're very excited to be launching our Journal at a time of immense challenge and change for the financial services industry, and we've drawn upon the deep subject matter expertise of the many renowned contributors to this edition of the Journal to bring you what we hope you'll find to be a highly stimulating series of articles.

We'll be publishing editions of the Journal on a regular basis, and each time we will be focusing on those topics our Advisory Board members, who are leading academics and executives, are telling us are of key strategic importance to them. And it's for that reason that we've chosen to focus this edition on the world of Payments.

Payments has gone from being an often-overlooked, quite slow-changing, typically back-office, function to becoming one of the most transformed - and transformative – functions in the financial services industry. And all of that has happened within the space of only a few years. Digitization, cloud native technology, financial crime and fraud, artificial intelligence, and many other recent developments, combined with ever-greater regulatory scrutiny and ever-increasing client expectations, have created the perfect storm for legacy Payments providers and have opened this area up to newer and more agile competitors.

We focus on the drivers of that transformation, the implications of those drivers for the various players in the Payments value-chain, and the key decision points firms will therefore soon face if they intend to remain leaders in this field.

I'm conscious that in creating the articles in this Journal, many individuals have spent many hours researching and writing, and I'm very grateful for their time and expertise!

I look forward to getting your feedback on our new Journal of Financial Services, and to speaking with you again soon.

Stefan Dierckx, Founder & CEO, Projective Group

Future of Payments

A launchpad for Payments innovation: the renewed **RTGS service**

Victoria Cleland,
Chief Cashier and Executive Director for Payments, Bank of England[1]

ABSTRACT

The renewal of the U.K.'s Real-Time Gross Settlement (RTGS) service, recently delivered by the Bank of England in collaboration with the payments industry, marks a pivotal moment in the evolution of the U.K.'s payments infrastructure. In this article, I reflect on the significant benefits delivered by the renewed RTGS service (RT2) and its transformative potential. RT2 enables innovation in wholesale payments by acting as a platform for innovation, which will be delivered through close collaboration with industry.

1. The author is a member of the Payments Vision Delivery Committee, chair of the Retail Payments Infrastructure Board, and chair of the RTGS/CHAPS Board in the U.K. She is also a member of the Committee on Payments and Market Infrastructures hosted by the Bank for International Settlements.

1. Introduction: payments are a catalyst for economic growth

Payments are the lifeblood of the economy. They support economic activity and trade by enabling value to flow across sectors and across borders. During a time where the payments landscape is changing globally, it is essential to think creatively about how payments – both retail and wholesale – can deliver meaningful benefits to households and businesses. The driving force that makes this transformation possible is innovation. Innovation can help make payments better suited to the needs of an increasingly digital and interconnected world. It can unlock new products and services that are more secure, more efficient, and ultimately more beneficial to the wider economy.

Andrew Bailey, Governor of the Bank of England, recently announced an updated approach to delivering the next generation of U.K. retail payments infrastructure, embedding collaboration between the public and private sector. The strategy for U.K. retail payments infrastructure will be set by the authorities through the Payments Vision Delivery Committee, and the Bank of England will chair a new Retail Payments Infrastructure Board to work with industry to translate this strategy into design. Having set the design, this Board will oversee its delivery by a new industry-owned and led Delivery Company, responsible for procuring and delivering the next-generation retail infrastructure. Pay.UK will retain its crucial role operating existing interbank payment systems. This new structure is designed to deliver the UK authorities' ambitions for a world-leading payments ecosystem which drives innovation, supports competition, and ensures security.

In approaching innovation in retail payments, we can look to learn from the developments in the wholesale payments ecosystem where there is considerable innovation already. Wholesale payments are high value payments typically made by financial institutions, large businesses, and governments. They are used to settle obligations in financial markets and represent most of the value of payments. They are, therefore, vital to the financial system and central to the innovation agenda. This article highlights how the Bank of England, in particular through the renewed Real-Time Gross Settlement (RTGS) service, is enabling innovation in wholesale payments, and how this in turn enables innovation in the financial markets these payments underpin. It explains how we will continue to adapt and evolve our service to allow new business models and technologies to benefit from a reduction in risk through settlement in central bank money. This is part of a broader vision. We work closely with other authorities, at home – including H.M. Treasury and FCA – and abroad, so that our initiatives are aligned, mutually reinforcing, and create the conditions for positive change in payments. It is through this collaborative approach and through close cooperation with industry that we can deliver a payments ecosystem that is resilient, inclusive, and fit for the future.

This article outlines the importance of RTGS. It explains the innovation recently delivered through the RTGS Renewal Programme, the benefits the new service is already unlocking, and the opportunities it opens for the future.

Renewing RTGS has similarities to launching one of the first satellites into orbit. It is a major technical achievement, made possible by the dedication and collaboration of many with a shared vision. Safety has been central to every step in the process. Like early satellites, it is also a launchpad for future change: a platform that opens up new frontiers for innovation, enabling the private sector to develop the next generation of services to benefit people and businesses making payments across the U.K. and cross border. Ultimately, its benefits apply to everyone, however indirectly. Alongside changes to regulation and policy, the renewed RTGS infrastructure (RT2) facilitates a diverse and innovative ecosystem. One where banks, non-banks, and market infrastructures – including new entrants and Fintechs – have a safe platform on which to innovate, fostering economic growth and financial inclusion.

2. What is RTGS and what was RTGS Renewal?

RTGS is the infrastructure at the heart of the U.K.'s financial system, enabling the real-time transfer of payments between financial institutions, settled in central bank money – the ultimate risk-free settlement asset.

RTGS underpins the settlement of payments through CHAPS (the U.K.'s high value payment

system and key cross-border payment corridor), supports securities settlement in CREST, and plays a crucial role in the settlement of exposures in the U.K.'s retail payment systems. It averages settlement of almost £800bn per day (over a trillion U.S.$). Ultimately, it plays a role in the smooth functioning of every single electronic payment in the U.K. RTGS is essential for financial stability and for monetary stability, as it is a key component of the mechanism through which Bank Rate is transmitted through the economy.

In close collaboration with industry, we developed a vision for an RTGS service that was not just more resilient but would also promote competition and innovation. Four objectives guided the RTGS Renewal Programme: higher resilience, broader access, wider interoperability, and improved user functionality.

The first major deliverable was the introduction of ISO 20022 messaging for CHAPS payments in June 2023. This was a foundational step in modernizing the U.K.'s wholesale payments infrastructure and enhancing interoperability. The Programme reached its final milestone on April 28, 2025 when we successfully launched our renewed RTGS core ledger and settlement engine. This included a new user interface and delivered improved resilience and enhanced functionality, providing a strong platform for further change.

This major transformation Programme was delivered in a complex environment, during a time of change for payments globally. It would not have been possible without the dedication, professionalism, and collaboration of all involved. This was not only the teams at the Bank, our Technology Delivery Partner (Accenture), and key suppliers, but also nearly 250 industry participants involved in the Programme, shaping the vision and ensuring their own readiness. Engagement with industry was embedded from the outset and this inclusive approach meant that what we built not only met the highest standards of resilience, but also reflected the needs of the industry.

Building the system was only part of the challenge. We also needed every participant to be ready for go-live. Each one had to make the necessary changes to their own technical and operational processes. The fact that every participant was prepared and ready on time is a great achievement, and a testament to the strength of collaboration between the Bank and the wider payments community.

In the first three months of operation, RT2 settled over 13 million CHAPS payments and a total value exceeding £51 trillion across all settlement services. This amount would cover the cost of running the International Space Station for nearly 23,000 years! These numbers are a reflection of the importance of the infrastructure and the payments that make up the U.K. economy. Each payment is important to the household or business making it.

3. Benefits already unlocked

RT2 is already delivering tangible benefits in line with our four objectives. RT2 is not only more resilient, it is also an enabler of competition and innovation.

3.1 Higher resilience

As a critical part of the U.K.'s national infrastructure, RT2 needs to be well protected, monitored closely, and have excellent response and recovery capabilities. We have delivered improvements in all three areas. In terms of protection, we have enhanced security and segregation of the system's core components, leveraged new geographically diverse data centers, and introduced a new robust independent data source. We have upgraded our monitoring capabilities, both during and outside of business hours, and introduced continuous and cross system reconciliations to improve detection of issues. We have also undertaken extensive major incident testing to recover quickly and within our risk tolerance.

3.2 Improved user functionality

Our new user interface, affectionately known as BERTI (the Bank of England Real Time Interface), provides participants with a more modern experience, supporting smoother operations and better access to information, including 24/7 access to BERTI for account queries. We have also introduced APIs, enabling participants to interact with the system in a more dynamic and programmable way. In the first two months of operation, over 43,000 API calls were made as industry began to make use of this new enhanced functionality.

3.3 Broader access and inclusion

Over recent years, we have extended our access policies significantly. We gave a wider range of

financial institutions and new business models the ability to settle transactions directly in central bank money.

In 2017, we were the first major central bank to allow non-bank payment service providers to hold accounts in RTGS. This enabled them to join CHAPS and the retail payment schemes for the first time, and to compete with the traditional high-street banks.

We have also welcomed our first omnibus account holder into CHAPS: a wholesale digital settlement platform provider. Omnibus accounts allow recognized payment system operators to pool participant funds. This allows them, in effect, to tokenize central bank money, ensuring it retains its crucial role at the heart of digitalized, as well as traditional wholesale markets. This structure also mitigates credit and settlement risk, even outside RTGS operating hours, and marks a significant step forward in enabling new models of digital settlement.

RT2 supports our ongoing access ambitions by enabling a far larger number of participants in the system and by streamlining onboarding processes.

3.4 Wider interoperability

The migration to the global messaging standard ISO 20022 for CHAPS payments in 2023 was a significant step towards global harmonization and greater interoperability. It is a key contributor to reducing frictions and inefficiencies in cross-border payments [BIS (2023)]. This was highlighted by the G20 as something which, alongside other roadmap priorities, supports economic growth, international trade, global development, and financial inclusion [FSB (2024)].

Richer, more structured data within these messages enhances transparency and efficiency. It lays the ground for innovation both for domestic and cross-border payments. We have mandated the use of Legal Entity Identifiers (LEIs) and purpose codes in certain CHAPS payments, reflecting our belief that enhanced data benefits a wide range of stakeholders. Since the requirement took effect on May 1, 2025, we have seen population of this data skyrocket. Improved data in payments can help the industry detect fraud, manage risk, and provide insights into payment trends. For the Bank, this data enables us to identify early changes in behavior and risk to support our monetary and financial stability policy decisions.

3.5 Enabling future change

We have developed RT2 to be adaptable. Its modular architecture allows us to update or replace individual components as technology evolves. This makes maintenance easier and enables us to respond swiftly to future innovation and policy needs in the ever-evolving payments landscape.

4. Our strategy for RT2

Satellite technology laid the foundations for innovations such as GPS, mobile phones, and satellite television. RT2 is also designed to be a platform for the future, enabling private firms to innovate and develop new products and services that deliver real benefits. This innovation has the potential to change the way that end-users interact with payments through products that reduce risk and cost, offer new services and functionality, and are faster and smoother. This in turn can support U.K. economic growth through reducing liquidity needs, freeing up collateral, and making assets more monetizable while driving efficiencies.

Our Vision is that RTGS is a resilient and widely used platform for central bank money settlement, enabling growth and innovation. To achieve this, we are committed to excelling in providing a platform that is resilient and responsive. We are taking several steps to make this vision a reality.

We have created RT2 to act as an open platform for change and innovation, supporting the Bank's monetary and financial stability objectives. This will also drive improvements in wholesale settlement efficiency and competition. As the payments landscape evolves, we need to preserve the critical role of central bank money and confidence in the financial system, including trust in money. This will mean evolution to ensure that RT2, along with the regulatory system and wider ecosystem, can support new business models and technologies, from both new entrants and existing players.

We are committed to continuously improving our services to keep pace with this rapidly changing world and to enable ongoing innovation, but we know we cannot do this alone. Collaboration with other infrastructure providers in the U.K. and beyond is essential. In a similar vein to satellite networks relying on coordination across borders, we are actively sharing lessons learned and working on design of new functionalities with peers undertaking similar modernization programs. The G20

roadmap for cross border payments demonstrates the benefits of continuing to work together to deliver payment systems that are interoperable through consistent messaging standards, access policies, opening hours, and legal, regulatory, and supervisory frameworks [FSB (2020)]. Interoperability is important domestically too. It makes it more efficient for new technologies and overlay services, as well as existing organizations, to interact with both CHAPS and the U.K.'s retail payment systems.

Informed by responses to our consultations, our "Future Roadmap" is our strategic plan for how we continue to evolve the service to meet changing user demands and policy objectives [BoE (2024a)].

We are working with industry to explore enhancements across four key dimensions:

- **What** we offer.
- **Who** can use the service.
- **When** the service is available.
- **How** it is used.

4.1 What services we offer

4.1.1 Synchronization

Synchronization can enable conditional settlement across accounts in RT2 with movements on another asset ledger - such as digitized bonds - reducing settlement risk and enabling digitalization of these activities. Our proposed model would see the Bank delivering the functionality required for this within RTGS but would leave development and delivery of specific products utilizing this functionality to "synchronization operators" in the private sector, driving further competition and innovation. We have recently demonstrated the feasibility of such a model for foreign exchange transactions, through Project Meridian FX [BIS (2025)]. This was a collaboration with the BIS Innovation Hubs in London and Eurosystem centres, and other central banks. Building on this, the Bank will launch a synchronization lab in 2026 to enable potential synchronization operators to test real-world use cases with our planned synchronization functionality. Dependent on its success, our intention is to deliver this into production as soon as we can.

4.1.2 Wholesale experimentation

We are also planning a series of experiments around wholesale settlement. We will explore what we can do, beyond synchronization, to enable the next generation of innovative use cases to emerge. This model might involve a wholesale Central Bank Digital Currency, enabling a unified single ledger for tokenized assets and payments. Our first experiment will test synchronized settlement of a tokenized bond, with findings expected by the end of 2025. We published in June a DLT Innovation Challenge [BoE (2025a)], in collaboration with the BIS Innovation Hub London, seeking input from the private sector to understand how to incorporate distributed ledger technology into wholesale central bank settlement through an external programmable ledger managed by a third party [Cleland (2025)].

4.2 Who can use the service

While our existing access policies provide a strong basis for supporting innovation [BoE (2025b)], we have recently issued our response [BoE (2025c)] to a discussion paper [BoE (2024b)] setting out where we believe further enhancements can be made. We have made information about participating in RTGS more accessible and transparent, including clarifying the access requirements for non-bank payment service providers. Drawing on the successful model of mobilization for banks, we have introduced a new "stage gate" approach to facilitate new entrants. This new stage allows participants, particularly new financial market infrastructure, to grow their business in a controlled way subject to risk reducing controls. Looking further ahead, we are exploring the thresholds for CHAPS access, i.e., when an organization should be direct rather than indirect. We are also exploring whether we should allow non-bank payment service providers to safeguard client funds at the Bank, potentially reducing their reliance on the very organizations in the commercial sector who they compete with.

4.3 When the service is available

Building on the G20 roadmap, our analysis has shown that longer RTGS settlement hours in the U.K. could unlock further benefits, including alignment with international peers, reduced cross-border frictions, and lower settlement risk [BoE (2024c)]. We are assessing how best to implement this. We believe it is most appropriate to deliver this through a phased approach with earlier opening of CHAPS, aimed for 2027, with an ambition to move closer to near 24/7 settlement around the end of the decade. We are currently consulting on the earlier opening of CHAPS, and we strongly encourage both current and prospective users of RTGS and CHAPS to share their views and contribute to this

important consultation before it closes on October 21, 2025 [BoE (2025d)].

4.4 How the service is used

4.4.1 APIs

We continue to evolve our API offerings to meet the needs of a more dynamic and programmable financial ecosystem. This will be a process of gradual improvement. While most of our current APIs allow participants to access data, we are expanding the range of APIs and working towards a world where participants can instruct payments via API, subject to key risk controls.

4.4.2 ISO 20022

We continue to iterate the ISO 20022 messages used in CHAPS and RTGS to ensure that we maintain international interoperability and deliver ongoing improvements. We remain a champion of standardization and richer data. We are in active dialogue with industry about whether further requirements of specific data elements could unlock even greater benefits, particularly for end-users, through development of new products utilizing this data and richer analysis by linking these with other datasets.

4.4.3 Resilience enhancements

While RT2 itself is strong and robust, we are committed to continuous improvements to address evolving threats and new services. In particular, we are looking at how new ways of accessing RTGS would strengthen resilience and reduce reliance on third parties and single points of failure. We continually look for ways to further strengthen the overall resilience of the U.K. wholesale ecosystem, including review of our tertiary contingency solution for RT2: MIRS.

It would not be amiss to mention that while this article has focused on RT2, highlighting what it now does and further enhancements in train to further support innovation in the U.K. payments ecosystem, the other parts of the wholesale payments jigsaw that are being delivered by the U.K. authorities should not be overlooked. We continue to work with colleagues across the Bank on other wholesale initiatives. This includes the pilot program launched by the Bank and HMT exploring the use of DLT technology in the issuance and management of sovereign debt (DIGIT). It leverages the Digital Securities Sandbox (DSS) launched by the Bank to support innovation in post-trade settlement. The Bank is also leading the ongoing drive towards T+1 securities settlement in 2027. In the retail space, the Bank is exploring a digital pound. If introduced, it would be like a banknote for the digital era. This would be accessible through digital wallets provided by private sector intermediaries and could be spent in shops or online.

We are delivering these initiatives collaboratively, through both co-creation with the industry and working closely with authorities here and overseas.

5. Conclusion: call for action

We have provided the initial foundations for success in building the next generation market infrastructure for money, payments, and securities settlement. The industry should now use the new infrastructure to the full and to reap its benefits, securing the U.K. as a world leading digital wholesale market. The industry should also continue to engage. Industry insights, innovation, and partnerships are essential to ensuring that RT2, and the wider wholesale payments ecosystem, continues to evolve and support end users.

Just as satellite technology transformed the way we navigate the world, we believe RTGS can help transform the way value moves through the economy. In doing so, it will be a major contributor to growth and to the U.K. leading the way in payments innovation.

Acknowledgements

I would like to thank Rebecca Hall, Pierre Wang, Nina Turnbull, John Jackson, Richard Windram and Samantha Leighton for their help in preparing this article.

References

BIS, 2023, "Report to the G20: harmonised ISO 20022 data requirements for enhancing cross-border payments," Bank for International Settlements, October, https://tinyurl.com/rn3n94df

BIS, 2025, "Project Meridian FX: exploring synchronised settlement in FX," Bank for International Settlements, April 24, https://tinyurl.com/39ecrhsh

BoE, 2024, "Future roadmap for RTGS," Bank of England, February 8, https://tinyurl.com/mf268uyr

BoE, 2024b, "Reviewing access to RTGS accounts for settlement," Bank of England, February 8, https://tinyurl.com/2j97wa3x

BoE, 2024c, "Response to the discussion paper exploring extended RTGS hours," Bank of England, October 3, https://tinyurl.com/2ptb3k8a

BoE, 2025a, "DLT Innovation Challenge," Bank of England, July, https://tinyurl.com/2sure6cs

BoE, 2025b, "Access policy for RTGS settlement accounts and services," Bank of England, April, https://tinyurl.com/mr3v2n29

BoE, 2025c, "Response to the discussion paper on reviewing access to RTGS accounts for settlement," Bank of England, February 8, https://tinyurl.com/2j97wa3x

BoE, 2025d, "Proposal to extend RT2 and CHAPS settlement hours (phase 1)," Bank of England, July 29, https://tinyurl.com/4ky24pvr

Cleland, V., 2025, "Synchronisation and beyond: enabling the next wave of financial innovation," Speech delivered at the 15th annual edition of City Week, July 1, https://tinyurl.com/39ce42wb

FSB, 2020, "Enhancing cross-border payments: stage 3 roadmap," Financial Stability Board, October 13, https://tinyurl.com/4j2ev2vy

FSB, 2024, "G20 roadmap for enhancing cross-border payments: consolidated progress report for 2024," Financial Stability Board, October 21, https://tinyurl.com/44dwuv4v

Future of Payments

Payments are in change: **where is the journey heading?**

Carlos Nasher,
Managing Partner, Thede Consulting
(part of Projective Group)

Robert-Jan Wekking,
Group Practice Lead Payments,
Projective Group

ABSTRACT

The payments industry is undergoing significant transformation as cash loses relevance and innovations such as the digital euro, embedded finance, and European initiatives like Wero gain momentum. Alongside these shifts, regulatory changes including PSD3/PSR, DORA, and the potential FIDA framework, as well as the rollout of the E.U. Digital Identity Wallet (EUDIW), will reshape market operations. While compliance poses challenges, greater data availability combined with Artificial Intelligence offers vast opportunities for personalized services. This article provides an overview of these trends and examines five possible future scenarios, offering strategic recommendations for payment stakeholders.

1. Introduction

We live in a complex world shaped by ambiguity and uncertainty. To boil down this multitude of challenges into a concise formula, business thought leaders have coined the term VUCA: "volatility, uncertainty, complexity, ambiguity". This four-part concept was meant to describe the chaotic nature of the modern era, but it also perfectly applies to the reality in many business sectors.

Due to rapid technological progress, the world is volatile. Swift developments are difficult to predict - hence, uncertain. The global interconnection of countries, companies, and other actors adds increased complexity. All of this is overlaid by an ambiguity about whether a decision or trend is good or bad. This is often difficult to judge at first glance - especially given the global information overload and the uncertainty about which of these sources are trustworthy.

Anyone professionally involved in payments will recognize their own working reality in this description. Technological disruption is currently "the name of the game", even though no one really knows where it is all heading. Complexity is inherent to the industry, as anyone who has ever seen an infographic illustrating the path of a simple credit card transaction through the payments jungle can confirm. The drivers - digitalization, regulation, and cybersecurity - further increase the complexity of the payments landscape and amplify the uncertainty surrounding its near future.

This article is intended to provide more clarity on the direction in which payments will develop, and how companies can best prepare for events and developments.

Which trends will prevail? Is there even a single driver that will ultimately gain the upper hand? We will answer this question at the end with a series of conceivable scenarios for the payments world of tomorrow and beyond.

If you want to master the VUCA world, you have to understand it. This is exactly what this article intends to help with.

2. What influences the payments industry?

An incredible 1,411.3 billion transactions were conducted worldwide in the area of cashless payments in 2023 alone.[1] And the trend is upwards. Equally impressive is the number of debit cards issued in Germany alone, which stood at around 155 million in the first half of 2024. [2]

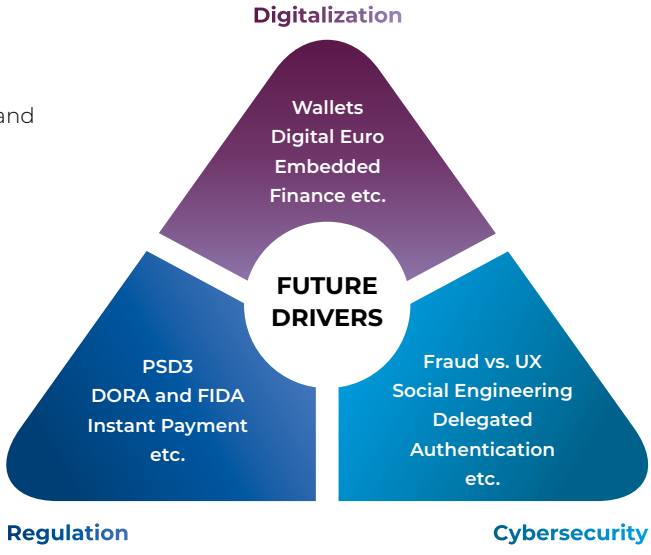
Payments are the backbone of commerce and thus a key economic factor - an industry that has under-

Figure 1: Dynamic drivers of the payments industry

Regulation
New laws and guidelines are intended to help ensure the security, innovation, transparency, and fairness of the industry

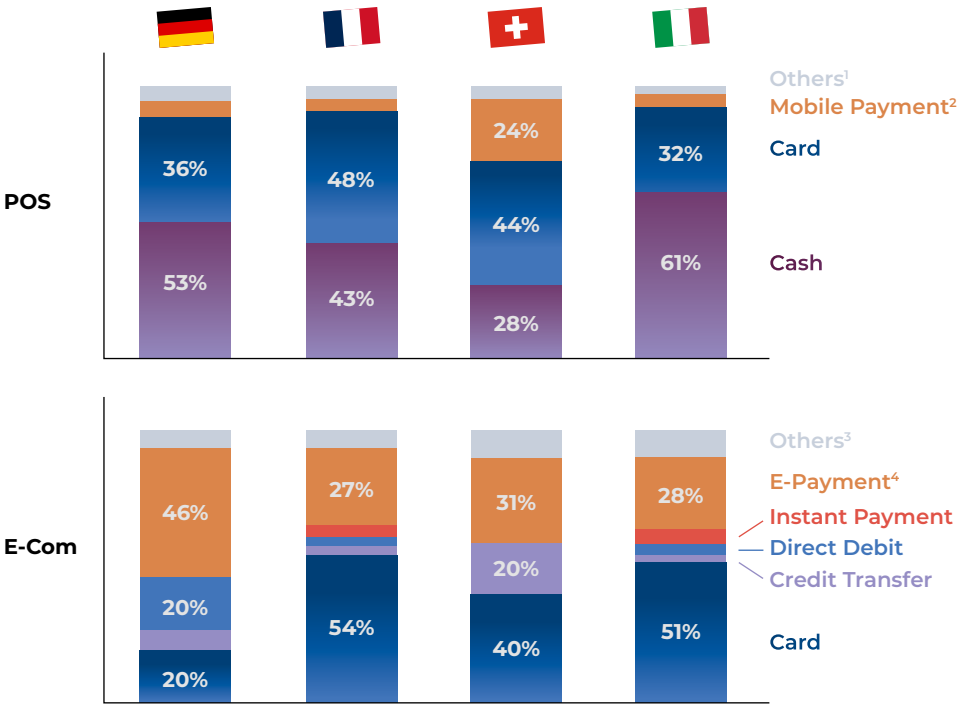
Digitalization
Technological progress increases customer demands and enables efficiency gains

Cybersecurity
Attacks increasingly target complex vulnerabilities such as API gaps, malware, and man-in-the-middle attacks, as well as human weaknesses through phishing and social engineering



1. https://tinyurl.com/4jyw275s
2. Deutsche Bundesbank

Figure 2: Comparison of payment behavior in Europe



Source: ECB 2024, Swiss Payment Monitor
1. Payment via loyalty programs, vouchers, crypto, and other
2. Contactless payment with cell phone via wallet, mobile payment app
3. Payment by cheque, loyalty programs, vouchers, and more
4. Payment via PayPal, Klarna, iDeal, and other

gone massive change over the past two decades. The following are currently the most relevant developments.

2.1 The digitalization continues

Ongoing digitalization continues to shape our lives and society. It is profoundly influencing the world of banking and is changing customer expectations. In a recent study, nearly a quarter of respondents stated that they prefer to use online or mobile banking instead of visiting a physical branch.[3]

This naturally also affects the way we pay. The scale of this development becomes clear when comparing the different payment methods at the point of sale and in e-commerce. The use of cash - bills and coins - is steadily declining. According to a study by the Bundesbank,[4] the share of cash payments in all transactions fell to just 51 percent. While that is still a high proportion in a European comparison, it was 58 percent in 2021. Looking at total turnover, debit cards have already overtaken cash.

Digitalization not only makes payments more convenient, faster, and more comfortable, it also opens up opportunities to offer more customer-centric payments solutions through the use of AI. Thanks to digitalization and AI, banks benefit from increased efficiency as well as new options for engaging with customers. AI can analyze transaction data in real time, detect suspicious patterns, and prevent fraud.

3. https://tinyurl.com/3sjv3s2u
4. Deutsche Bundesbank, 2023, "Zahlungsverhalten in Deutschland 2023".

AI can also relieve payment service providers from reporting obligations by automating them. Finally, the clever use of algorithms can enhance customer experience, for example, by analyzing customer preferences and suggesting the preferred payment method during checkout.

Digitalization does not only change customer behavior and accelerate processes, it also paves the way for new business models and payment innovations, many of which would have been unthinkable just a decade ago. Only through ongoing digitalization, the creation of APIs, the development of cloud computing, and the success of mobile devices in everyday life have the necessary foundations been established.

The EPI initiative, for example, aims to establish a new payment method for everyday use and strengthen Europe's sovereignty in the payments space. Another example of a development driven by digitalization is "embedded finance". The impact of this business model is still only faintly visible. However, innovative service providers could use it to shake up the payments market and wrestle market share from established players through smartly structured partnerships.

2.2 The digital euro becomes reality

In 2019, Meta - the parent company of Facebook - announced its intention to launch its own digital currency under the name "Libra". Due to the sheer size of the network, this announcement caused a major stir. The reactions from central banks in the U.S. and Europe were harsh. From their perspective, "Libra" (which was later renamed "Diem") posed a threat to the stability of the monetary system.

The central banks' response came in two parts:

1. The definition of a regulatory framework.
2. Plans and projects to create CBDCs (Central Bank Digital Currencies).

The success of the cryptocurrency Bitcoin further fueled the discussion around CBDCs. Monetary authorities also saw their influence waning with the rise of crypto assets.

In 2023, the European Central Bank (ECB) began preparing the introduction of the digital euro. A two-year investigation phase has now been completed, and work is beginning on the infrastructure and platforms needed. In the current phase, the ECB wants to test whether the digital euro is actually feasible and useful. The Governing Council of the central banks will decide on the issue of the digital euro once the legislative framework has been adopted.

The ECB positions the digital euro as legal tender. It is not intended to replace cash, but rather to complement it. In principle, all citizens of Europe should be able to use the digital euro.

However, as legal tender, merchants will be required to accept the digital euro. This is a key distinction from other payment methods such as credit cards. For payment service providers, the designation as legal tender will likewise result in an obligation to offer the digital euro.

However, as is typically the case with new payment methods, they must offer users a clear benefit in order to be adopted - acceptance alone is not enough. The key to success will, therefore, lie in the user experience that the ECB and its partners will develop. The fact is, however, that there is potential for considerable conflict among those involved.

Payments with the digital euro require more stakeholders than the traditional four-party credit card model. The digital euro is more of a six-party model - or even up to eight parties, depending on how they are counted. New players will enter the scene, such as wallet providers (e.g., PayPal, Apple, Google), who will manage the customer interface. Issuer banks, meanwhile, will take on a new role: providing customers with the digital currency - essentially acting as digital ATMs. The ECB will step in as the central system provider (scheme).

This fundamentally alters the business models of banks and acquirers. Unlike Visa and Mastercard, the ECB does not plan to charge scheme fees to either banks or acquirers. For providing acceptance infrastructure, acquirers will receive a so-called Merchant Service Charge per transaction from merchants. The biggest difference to Visa and Mastercard: the Merchant Service Charge will be capped by regulation.

Similar to the interchange fees, banks will receive a so-called Inter-PSP Fee per transaction as compensation for providing services related to the digital euro - this fee, too, will be regulated by the ECB and paid by the acquirer. The ECB has already published initial approaches for determining the level of both fees, though no specific figures have been disclosed yet.

There is still much to clarify before the digital euro can be introduced. According to a study by the

Bundesbank, however, customers already appear ready to accept the digital euro today.

In contrast, German banks are more skeptical about the digital euro. They question its usefulness and level of acceptance, likely because they see a well-established business model potentially slipping away.

2.3 Wero/EPI – a private sector initiative

Wero is another project that is causing waves both within and beyond the industry - similar to digital euro. Behind it stands the European Payments Initiative (EPI), which includes 14 banks and 2 payment service providers from across Europe. In Germany, participants include the savings banks (Sparkassen), cooperative banks (Volks- und Raiffeisenbanken), Deutsche Bank, and Postbank.

Figure 3: Implementation of digital euro could begin as early as 2025/2026 – banks must act now!

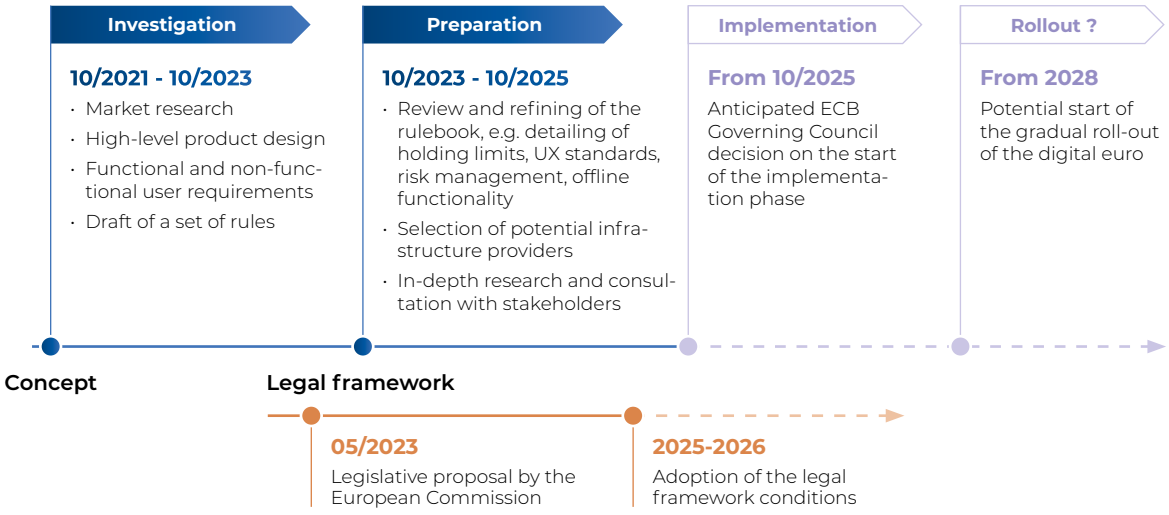
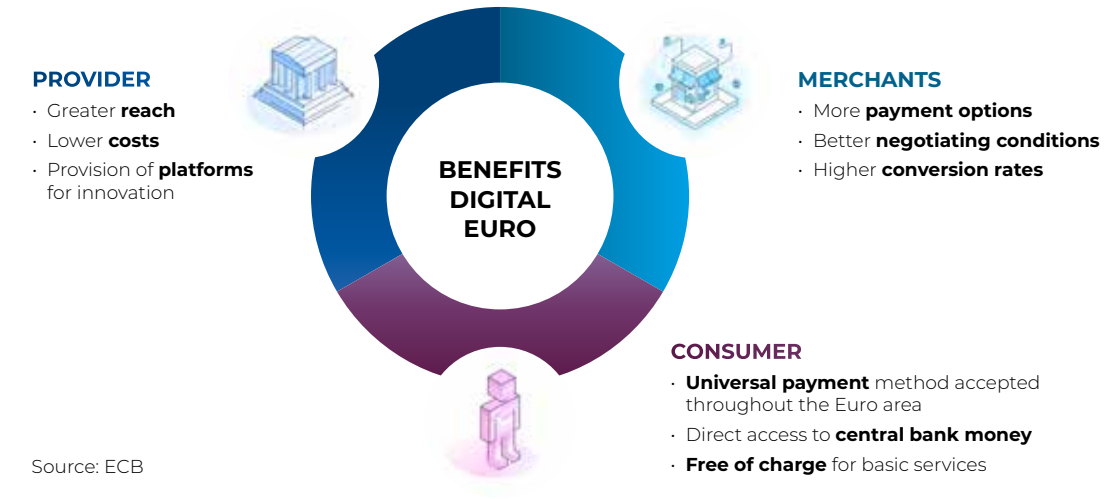


Figure 4: Advantages of the digital euro over existing payment methods from the ECB's perspective



Source: ECB

The press were quick to label Wero as merely a European alternative to PayPal. In other European countries, similar projects have already proven successful. The prime example is Swish in Sweden, which is used by three-quarters of the population and accepted in most stores. Other successful examples include Twint in Switzerland and MobilePay in Denmark.

However, when the first usable version of the Wero app was presented in 2024, it faced considerable criticism due to its limited functionality.[5] As with the digital euro, convenience will be critical to success. Only if the user experience is seamless will people use Wero at scale. Broad acceptance in the retail sector will also be essential.

But that will not be easy. A key difference with the digital euro is that Wero is a purely private sector initiative. The ECB is not involved and, therefore, cannot enforce Wero as legal tender. Thus, it will be entirely up to merchants whether they want to accept it or not.

Customers, too, are not as yet convinced on a broad scale. In an October 2024 survey by Verivox, 88% of participants stated they had never heard of Wero, and 61% did not believe Wero or any similar system could compete with established U.S. providers like PayPal.

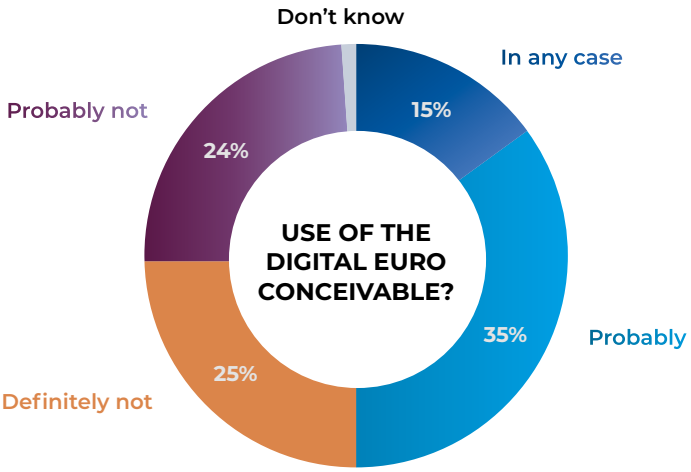
Because Wero is being developed by actors other than public institutions, it lacks the direct protection and regulatory endorsement of the ECB. Wero is not legal tender, so merchants are under no obligation to accept it. However, it does have one major advantage over the digital euro: it already exists and is available to consumers today.

Wero shares one key ambition with the digital euro: the idea of strengthening Europe's independence from U.S. giants. A payment/acceptance function for retailers is planned for 2025.

2.4 Embedded finance is gaining traction across sectors

Embedded Finance is a development that has been unfolding for some time now. The core idea: payments, banking, and insurance become "invisible". The corresponding functions are seamlessly integrated into the products and platforms of non-financial service providers.

Figure 5:
The digital euro is meeting with growing acceptance among the population as a payment option



According to the Bundesbank, half of respondents in Germany can imagine using the digital euro as an additional payment option.

Source: Bundesbank survey (2024): https://tinyurl.com/2jtad53b

5. https://tinyurl.com/4nbaz6uj

This means customers no longer need to leave those platforms to complete a transaction.

Real-world examples that are already working include:

- A loan for furniture offered directly by the retailer.
- Car insurance purchased at the car dealership.
- Instalment payments or credit cards offered by technology and retail companies.
- Merchant financing offered via online marketplaces.

These offerings are often backed by Fintechs that partner with the platform providers. The appearance of an invisible financial service is made possible by fully digitized application and process workflows. The PSD2 Directive played a key role in enabling access to customer accounts at traditional banks. And regulation is entering the next stage - with the PSD3 Directive expected to follow no later than 2027.

Also in discussion is the Financial Data Access (FIDA) Regulation, which would require financial services providers to make customer data available via standardized APIs. For embedded finance providers, such data sets could be a goldmine. Of course, any bank could also position itself as an embedded finance provider - if it were to allow access to its services and offerings via APIs.

FIDA is currently on the E.U. Commission's agenda, though only with conditional status. Whether and when the regulation will actually be implemented remains unclear for now.

3. Cybersecurity caught between protection and user experience

On the dark side of digitalization lie the risks of cybercrime and money laundering - for banks, payment service providers, and customers alike.

The European Union is paying increased attention to cybersecurity. Its focus is on building a resilient structure for the financial system. The current drafts of the Payment Services Directive 3 (PSD3) aim to hold banks and payment service providers more accountable in the event of cyberattacks. (More on this in the next section on regulation.)

In the future, merchants, banks, and payment providers must not only ensure the security of their own infrastructures but also protect their customers from all forms of fraud risk.

Customers remain the biggest vulnerability in the system. Techniques like social engineering and spoofing are used to manipulate users into revealing sensitive credit card or account information. This problem is further exacerbated by the growing use of Artificial Intelligence (AI). With AI, cyberattacks can be industrialized and scaled. Constant AI advancements lead to increasingly convincing phishing attempts - for example, through fake emails or text messages.

Beyond the standard cybersecurity and fraud prevention measures - such as security awareness training for staff, regular updates, and penetration testing of all hardware and software components - banks and payment providers should implement a holistic approach to cybersecurity and fraud defense, consisting of four phases:

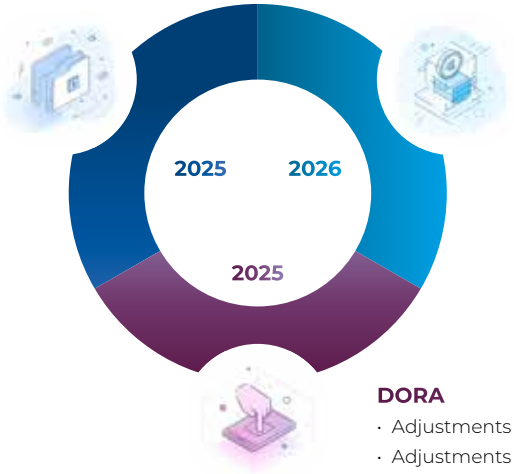
1. **Prevention**: use of advanced security infrastructure such as firewalls, encryption protocols, and intrusion detection systems, to minimize technical failures.
2. **Identification**: detecting potential vulnerabilities and areas where fraud may occur. This includes regular audits, anomaly detection, and flagging risky transactions or users.
3. **Detection**: rapid identification of fraud when it occurs or is in progress, using monitoring tools, behavioral analytics, fraud detection systems, or real-time alerts.
4. **Resolution**: once a fraud attempt is identified, immediate action must be taken to reverse it and contain any damage.

Implementing cybersecurity and fraud prevention in payments is complex and requires addressing both technical and regulatory aspects. Detailed gap analyses for technical and compliance requirements are essential steps toward an effective cybersecurity strategy.

Innovative solutions such as risk-based authentication and fraud scoring engines are vital to minimizing fraud risk and managing it effectively. Choosing the right partners and product solutions is an important step in this process. Banks and payment providers must assess their current cybersecurity posture and determine how they want to position themselves, both strategically and operationally, to remain competitive in the future.

Figure 6: Overview of regulatory regulations

FIDA?
- Secure data exchange
- Standardized interfaces
- Simplified integration
- Promotion of innovation



PSD3/PSR
- Increased bank liability in cases of fraud
- Obligation to offer direct debit, standing and collective orders
- Expansion of strong customer authentication
- Ban on fees & obligation to verify IBAN names

DORA
- Adjustments to ICT risk management
- Adjustments to reporting
- New test cases
- Exchange of information in the industry

4. Regulation remains a long-term construction site

Consumers rarely come into contact with dynamic regulations. Changes to legal provisions only become apparent when familiar payment processes change (keyword "strong authentication"). Banks, Fintechs, and payment service providers will have to implement a number of regulatory requirements in the coming years, which will inevitably have an impact on the entire industry and its processes.

4.1 PSD3 and PSR

With the current discussions surrounding the Payment Services Directive 3 (PSD3) and the Payment Services Regulation (PSR), the European Commission is presenting a concrete vision for harmonized and secure payment transactions, as well as fair competition within the European Economic Area.

The upcoming PSD3 builds on its predecessor, PSD2. The focus is on strong customer authentication and the transparent organization of payment transactions. The PSR complements PSD3 and will become directly applicable law in all E.U. member states.

Initial drafts for PSD3 and PSR were published in 2023. Since then, the proposals have been undergoing revisions. The Directives and regulations are expected to come into effect in the second half of 2025 or in 2026. Industry stakeholders, such as the German banking association Deutsche Kreditwirtschaft, have criticized this ambitious timeline, calling for a more realistic plan and suggesting 24 to 36 months would be needed for implementation.[6] The division of PSD2 into two parts has also drawn criticism from observers who fear regulatory duplication.

Key topics include:

- **Strong Customer Authentication (SCA)**: requirements will become stricter. Banks and payment service providers must invest in the development and implementation of stronger and more innovative security mechanisms.
- **Expanded liability for payment institutions**: in the future, banks and payment providers will have to prove that a fraudulent transaction was clearly caused by customer error. The burden of proof will shift - bringing new urgency to fraud prevention.
- **Transaction monitoring and fraud data sharing**: a better exchange of fraud-related data between banks and payment providers is intended to support more effective fraud detection and prevention.

6. https://tinyurl.com/3mdx5drk

- **Ban on surcharges for certain payment services**: PSD2 already introduced a surcharge ban for specific payment methods. PSR expands this ban to include transfers, direct debits, and e-money payments.
- **Verification of Payee (VoP / IBAN-name check)**: the IBAN and the name of the account holder must be verified in order to reduce fraud and increase transaction security.

The integration of new technologies and collaboration with Fintechs opens up new opportunities for banks to offer innovative services. Additionally, improved security measures and innovative offerings can help build customer trust and loyalty.

PSD3 and PSR promote competition and facilitate market entry for new payment service providers. These providers gain the opportunity to develop new technologies and services while strengthening their relationships with partners and customers.

For e-money institutions, PSD3 and PSR mean they will need a license under the Payment Services Supervision Act (ZAG) and will be subject to stricter regulatory requirements.

At the same time, the burden of fraud-related losses will increasingly shift from customers to banks, posing a serious challenge for fraud management systems.

For end users, PSD3 and PSR offer:

- Enhanced security through improved authentication processes.
- Increased transparency around fees and costs.
- Better decision-making when choosing banks and payment providers.

PSD2 already banned surcharges for specific payment methods. PSR extends this ban to further services such as transfers, direct debits, and e-money payments.

4.2 DORA: Digital Operational Resilience Act

With the Digital Operational Resilience Act (DORA), the E.U. has created a regulation for the financial services sector addressing cybersecurity, ICT risks, and digital operational resilience. DORA has been in use since January 17, 2025.

The regulation's goal is to strengthen IT security in the areas of crisis management, business continuity, and ICT protection. The consequences for payment service providers include:

- Establishing an appropriate governance framework to ensure compliance.
- Setting up an early warning system to trigger timely action in the event of IT attacks.
- Critical review of contracts related to IT outsourcing.
- Optimization of communication and control processes with service providers - especially in situations requiring rapid response.

It also entails investments - such as adjustments to regulatory reporting, the implementation of new systems, and the establishment of required penetration testing processes. Changes in risk management may also affect capital requirements. Furthermore, ICT third-party providers will need to be monitored more closely and comprehensively in the future.

Despite its challenges, DORA also offers advantages, especially for financial service providers operating across borders. National regulatory inconsistencies will be eliminated, and the described cybersecurity standards will apply E.U.-wide.

4.3 FIDA: Financial Data Access Regulation

The Financial Data Access (FIDA) Regulation aims to create a unified Open Finance framework across Europe. However, whether this initiative will be implemented in the near future remains uncertain. In February, rumors circulated that the European Commission might drop the regulation. In the end, FIDA was added to the agenda - though only as "pending", meaning its future remains in question.

This regulation intends to give consumers transparent oversight and control over their financial data. By granting authorized third parties access to this data, FIDA aims to increase the supply of innovative and tailored financial products and services while promoting competition.

FIDA presents significant opportunities for banks, payment service providers, and insurers to strengthen customer relationships by developing personalized services and products. Increased transparency can also help improve fraud management and claims processing.

FIDA may also encourage cooperation between traditional financial institutions and Fintechs, enabling strategic partnerships to reach new customer segments.

End users would benefit from:

- Greater transparency.
- Simplified financial management.
- Personalized financial products, including embedded finance solutions.

However, implementing FIDA will be an immense challenge - especially for banks, payment service providers, and insurers. Although the regulation builds on PSD2, it broadens the scope significantly: no longer just delivering access to current accounts, but also to investment portfolios, savings accounts, and other financial data.

Preparations for FIDA include:

- Developing scalable and robust APIs for data transmission.
- Creating a dashboard for consent management, which must be provided to users free of charge.
- Upgrading legacy IT systems to meet these requirements.
- Participating in the design of so-called Financial Data Sharing Schemes, through which data exchange will take place.

A key component of these schemes will be the definition of compensation payments, in case third-party providers want to access data.

Despite the complexity, FIDA also presents opportunities: for example, banks could use the insights from the shared data themselves. With the user's consent, they would gain access to data held by other financial institutions, Fintechs, or insurers. With these broader datasets, companies could provide even more individualized products.

It would also give a major boost to embedded and open finance models, since companies could integrate payment solutions into their platforms without needing to build the infrastructure themselves.

FIDA could also enhance fraud prevention. If data is available across companies, suspicious transactions could be identified more effectively - especially if paired with the right AI-powered algorithms.

4.4 EUDIW: E.U. Digital Identity Wallet

The European Digital Identity Regulation (EU 2024/1183) came into effect in May 2024. By 2026, each E.U. Member State will offer at least one version of the E.U. Digital Identity Wallet (EUDIW). These wallets will provide a safe, reliable, and private means of digital identification for everyone in Europe. Each Member State will ensure that at least one wallet is available to all its citizens, residents, and businesses, allowing them to prove their identity and securely store, share, and sign important digital documents. Furthermore, the E.U. plans to amend the regulation on a dedicated E.U. Business Wallet, planned for the fourth quarter of 2025.

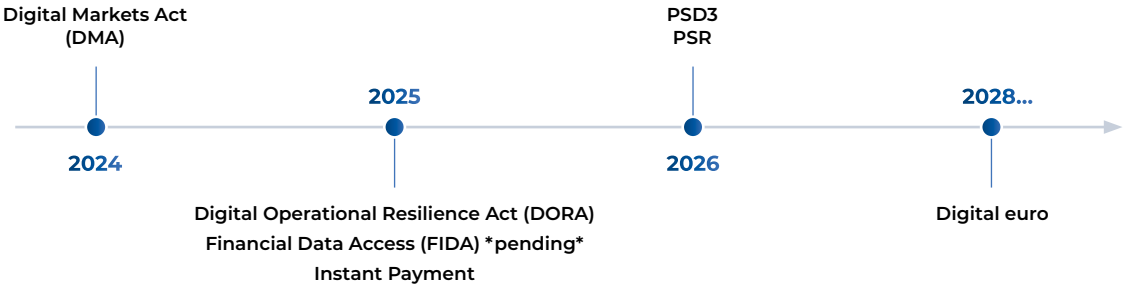
There are three key milestones:

1. The European Commission defines uniform technical specifications and procedures through implementing acts (IAs). These acts contribute to the interoperability and acceptance of EUDI-wallets throughout Europe. The first set of IAs was published on December 4, 2024, and came into force on **December 24, 2024**.
2. Each Member State is required to provide at least one national EUDIW within 24 months after the first set of IAs comes into force. Consequently, Member States must offer an EUDIW to citizens and businesses by **December 24, 2026**.
3. Relying parties - natural or legal persons that depend on electronic identification - who are required by law or contractual obligation to perform strong user authentication for online identification, must accept EUDIWs within 36 months after the first set of IAs comes into force, i.e., by **December 24, 2027**. Relying parties include banks, payment institutions, and electronic money institutions. (source: Dutch Payment Association)

Payment Service Providers (PSPs) will be required to accept the EUDIW for opening accounts and approving payments. This will force banks to adapt their current authentication processes, affecting not only technology but also the carefully designed user experience flows in their portals. Since PSPs have invested heavily in optimizing customer journeys and strengthening brand visibility, they will need to rethink how to minimize the wallet's impact on both user experience and branding.

An even greater challenge will be adhering to the PSD2 regulation. The EUDIW is intended to function as a two factor authentication (2FA) tool for online payments requiring Strong Customer Authentication (SCA) under Article 97(1) of PSD2. It seems highly problematic for PSPs to comply with both the intended acceptance of the EUDIW mandated by eIDAS 2.0 as a 2FA tool and the SCA

Figure 7: Regulations require timely planning and preparation for implementation



requirements laid down in PSD2 and the dedicated Regulatory Technical Standard (RTS) on SCA ((EU) 2018/389). To address this, the Dutch Payments Association has set up a task force to seek clarification and guidance from the legislator.

Although it is not the first time that regulations have partially conflicted, experience shows that timelines do not always shift to allow for further amendments. PSPs are, therefore, advised to allocate budgets in 2026 to start their own projects.

5. Convergence of developments

The E.U.'s regulatory initiatives, as well as the efforts around the digital euro and EPI, are being developed and will need to be implemented in parallel.

DORA has already come into force. PSD3 and PSR are expected to become legally binding around 2026. The digital euro could (conservatively estimated) appear at scale starting around 2028/2029.

If the E.U. continues pursuing the matter, FIDA could also be launched sometime in the coming years. All of this will require careful planning and early project initiation, especially by banks and payment service providers, who often have limited resources.

It will also be interesting to see whether supervisory authorities themselves can actually meet the tight regulatory deadlines - particularly for audits and reporting under DORA.

5.1. Who needs to act now?

Due to regulatory changes, banks and financial service providers are facing a wide range of areas where action is needed:

1. **Forming partnerships with Fintechs**: establish partnerships to expand the range of services offered.
2. **Creating alternative revenue streams**: introduce new services and payment solutions; diversify business models by exploring new markets or forming alliances.
3. **Third-party risk management**: review and update outsourcing policies and contracts; conduct regular due diligence.
4. **Advanced authentication**: implement secure, user-friendly login technologies that meet customer expectations.
5. **Fraud detection**: integrate fraud detection and risk management systems; train staff to identify suspicious transactions.
6. **ICT governance**: analyze and adapt internal policies and processes for continuous risk assessment and management.
7. **Technology investments**: modernize IT infrastructure and develop secure real-time data exchange APIs.
8. **Scalable IT infrastructure**: invest in cloud-based solutions and advanced systems to handle large transaction volumes, e.g., for instant payments.
9. **Digital resilience testing**: conduct annual baseline tests and threat-led penetration tests (TLPTs).
10. **Incident management**: develop internal reporting systems for ICT incidents and synchronize all systems with a reliable reference time.

Banks and payment service providers must act now to respond in time and remain competitive. This includes analyzing current business processes, identifying gaps related to regulatory requirements and evolving customer expectations, and developing new business models - because simply continuing as before will not be enough.

5.2 The state of the payments industry in Germany

In the previous sections, we outlined the driving factors that we believe are transforming the payments market.

But what is the current state of play in Germany? Various studies and our own surveys reveal clear trends.

At the point of sale, **cash** still holds significant value, but it has come under increasing pressure in recent years. This trend is expected to continue. However, an end to cash is not yet in sight.

Card payments are on the rise. This includes debit and credit cards from international card schemes (ICS), as well as the girocard. The girocard, in particular, has shown strong growth in recent years.

In contrast to the media attention they receive, mobile and other digital payment methods still account for a single-digit percentage of payment volume. These include merchant apps and loyalty programs.

In online commerce, e-payment methods dominate the German market. Notably, PayPal holds a leading position, with 32 million users in Germany.

Other major players in e-commerce revenue include card payments, which, together with e-payment, account for over 70% of total online sales. Bank transfers also remain strong.

These developments are also influenced by the behavior of issuers in the market. Large institutions and banking groups are increasingly relying on debit cards from international schemes. Issuers currently pursue heterogeneous and distinct product strategies in the payments space.

6. Scenarios for the payments world of the future

On the previous pages, we have outlined what we consider to be the key influencing factors for a change in the payments landscape in Germany. This almost inevitably raises the question regarding what the outcome of this change might be. In our opinion, the following scenarios are conceivable:

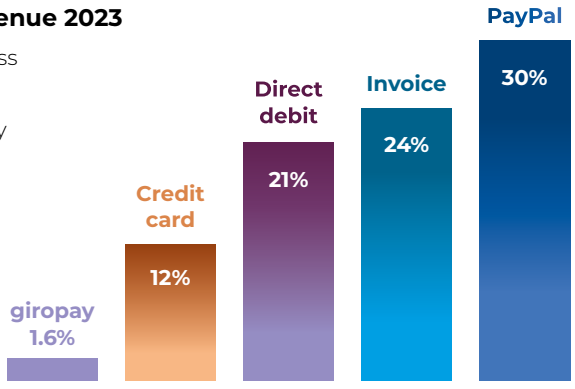
6.1 Scenario 1: A2A payments replace card schemes

For any party receiving money, a system like EPI/Wero could seem highly attractive. Just seconds after a transaction is initiated, the amount is securely available. Especially in retail, there may be considerable interest in such a solution. However, discussions and publications about A2A (account-

Figure 8: Current German payment market: E/M-Commerce payment methods in Germany

Payment methods and share of revenue 2023

- Payment offerings in e-commerce address the same target customers
- Bank-owned payment methods currently play a minor role
- Cannibalization of national products helps competitors to further expand their market share



Source: EHI Study 2024

to-account) payments often leave one key question unanswered: what will convince payers to switch?

As the section on the current payments market in Germany has shown, people in stationary retail (at the PoS) are used to paying either by card or cash. A2A payments, as of today, require the use of an app. To encourage a shift in consumer behavior, there would likely need to be a clear added value and convenience benefit. Only when operators can articulate such benefits will the real competition begin.

Payment service providers (PSPs) would still be needed in this scenario. Technical implementation and orchestration of the payment processes would remain essential. The banking sector would likely welcome this development, as the bank account would remain the central hub of payments; potentially becoming even more important than it is today. Even the girocard could benefit from such a shift.

However, regulation remains a significant question mark. If a politically imposed ban on monetizing such transactions were to be introduced, it would create major challenges. Building the infrastructure for A2A payments requires substantial investment; without a way to recoup those costs, it would be difficult to sustain.

Today's dominant players would likely respond quickly to any shift toward A2A by adjusting their pricing models and launching additional services.

6.2 Scenario 2: the digital euro prevails – who needs other payment methods?

As previously discussed in the context of the digital euro, German consumers are open-minded when it comes to a central bank digital currency (CBDC). It is, therefore, conceivable that a future payments landscape could revolve around CBDCs.

Whether this scenario is realistic or likely depends on two key factors:

6.2.1 Technical feasibility

A reliable infrastructure in line with DORA must be developed for the digital euro. In practice, this means that banks will likely need to establish new treasury management systems. Since the digital euro must be compatible with other (digital) currencies, standardized APIs will be necessary.

The ECB, and potentially the banks, will accumulate vast amounts of sensitive data, which will also need to be protected. Ultimately, these new systems must be able to process high volumes of transactions in real time and potentially guarantee offline capability for the digital euro. It is a massive undertaking; both time- and resource-intensive.

6.2.2 Customer adoption

The bigger challenge may be convincing users to actually adopt the digital euro. Although surveys show people are open to the idea, turning that openness into real usage will require much more effort.

Institutions backing the digital euro must clearly communicate its added value. This includes real-time transactions combined with the anonymity consumers expect from cash. Another important aspect is financial inclusion; digital currencies can enable participation in digital payments even for those without a bank account or smartphone.

Widespread acceptance will also be critical to success. In this regard, the digital euro is already at an advantage: it is intended to become legal tender, which means acceptance by merchants will be mandatory.

Still, while merchants can be required to accept the digital euro, consumers cannot be forced to use it. To break habits and move people away from familiar payment methods, the digital euro must offer a tangible benefit. It also needs to be as seamless as possible; otherwise, people will simply not switch.

This scenario would pose a challenge to international card schemes and PSPs. Their role in processing and managing digital euro transactions remains unclear. What tasks will the ECB take on? What will remain for PSPs? How are they expected to recoup IT investments?

After all, consumers will likely not pay fees for using basic digital euro services. Banks will receive a regulated inter-PSP fee from acquirers, as compensation for offering digital euro services, but like interchange fees today, the amount will be capped.

And while merchants will be obliged to accept the digital euro, it is unlikely that lawmakers will impose additional burdens beyond implementation.

6.3 Scenario 3: International card schemes push out local initiatives

One possible outcome is that neither of the new initiatives - whether the digital euro or EPI - achieves significant traction or broad acceptance, and instead the international card schemes (ICS) continue expanding their dominance and push local solutions out of the market.

This would mean that the E.U.'s efforts to establish a meaningful European payment alternative had failed.

For merchants and payment service providers, this scenario would result in a less complex technological environment.

The overall market would be shaped by the innovation power and speed of a few global players. That said, it is unlikely that the ICS would remain the only survivors in such a future. Policymakers, regulators, and merchants all have a vested interest in maintaining diversity in the Payment's ecosystem.

6.4 Scenario 4: Breakthrough of a transnational super app

Whenever the term "super app" appears in media coverage or panel discussions, such as recently, when Elon Musk announced plans to enable payments via X in cooperation with Visa, attention often turns immediately to Asia.

The success of WeChat, which combines messaging, payments, shopping, and even public services in one platform, would not have been possible without strong political backing.

In Europe, several apps have already achieved notable market penetration. Examples include Twint in Switzerland, Swish in Sweden, and Vipps in Norway. Each story is unique, but they all share one key factor: exceptional timing at market launch.

In Twint's case, there were already plans to replicate this success abroad, but so far, these plans have not materialized.[7]

Meanwhile, Alipay reportedly paid €200 million to sponsor the European Football Championship (Euro 2024).[8]

So, the real question is not whether such super apps will enter the German market, but when.

A conceivable future for the German payments landscape could see a transnational European app gain traction and come to dominate the market.

However, this path would be a long one. Twint's core features, for example, are already covered by existing e-payment solutions like PayPal.

Achieving broad merchant acceptance would also require enormous investment.

Moreover, any new app would face massive competition right from the start; namely the wallets from Google and Apple, PayPal, Klarna, and others. This market fragmentation would be a major hurdle for any would-be super app.

Such a breakthrough would only be possible through partnerships with established providers or, at the very least, interoperability with existing services. Only then could a super app achieve the critical mass of users needed to become an all-in-one platform on par with WeChat.

All in all, this scenario - the breakthrough of a still-unknown transnational app - appears relatively unlikely.

6.5 Scenario 5: Business as usual – parallel systems persist

What if nothing really changes? What if the payments landscape remains just as diverse as it is today?

The only difference: new players (such as the digital euro, EPI, and app-based payment methods) enter the market, but only manage to secure niche positions?

This "business as usual" scenario is actually not so far-fetched - especially when we look at the history of payments. On average, new payment systems have only lasted about ten years before disappearing again. The reasons for their failure are often complex: too expensive, too little acceptance from one or more market participants, and/or a lack of marketing resources. And frequently, users do not understand what added value a new system offers compared to existing ones.

7. https://tinyurl.com/ynvkadpe
8. https://tinyurl.com/ujfuf5s7

Many attempts have also failed because providers have begun back-to-front - focusing on the product before ensuring widespread acceptance. But if a product is not accepted, users will simply not adopt it.

Acceptance often fails at a technical level; for example, because retailers and service providers cannot easily integrate the new solution into their existing IT infrastructure. Or they can, but only poorly.

Finally, regulatory hurdles - from GDPR to PSD1 through PSD3 - make it hard for new players to succeed. And there seems to be little political will to change that.

7. Conclusion

The linear presentation of the forces driving change in the world of payments should not lead to the false assumption that market players can simply follow a step-by-step playbook. The future, especially in the payments space, remains unpredictable. All the scenarios we have outlined are entirely plausible. That is precisely the challenge facing all actors, because they will all be affected.

The key for every player, whether bank, payment service provider, or retailer, will be to strategically position themselves so that they can respond adequately to any of the possible developments.

Banks should critically examine the potential impact of each scenario on their business model. Where are the levers to future-proof their current offerings, or even to develop entirely new ones?

If the diversity of the payments landscape remains intact, these changes will result in numerous projects and developments that must be observed and managed in parallel. Open Finance-capable interfaces will need to be built. Institutions must address the role of AI and continue investing in IT and data security.

Payment service providers, in turn, will need to adapt their business models so they continue to generate revenue, regardless of whether the digital euro prevails, EPI/Wero gain traction, or things remain as they are. As simple as it sounds, PSPs earn money from transactions but only if they are involved in those transactions and do not offer a fully interchangeable service.

Creating real added value to build customer loyalty will require creativity. Political lobbying will also play a role, especially since frameworks for the digital euro are being defined now. Those who want to ensure that PSPs maintain a relevant role in the future must act now.

Merchants, too, must take a close look at their payments strategy. It must be flexible enough to accommodate EPI/Wero and the digital euro. Those who prepare wisely will gain a competitive advantage. The challenge lies in participating in the value creation of payments. Regulatory changes may provide opportunities to develop proprietary services and business models.

Future of Payments

Smarter payment algorithms for liquidity-saving in RTGS: a practitioner's guide

Jean-Paul Lam, Associate Professor of Economics, University of Waterloo, and Chief AI of Research, Goodlabs Studio

Thomas Lo, CEO and Co-Founder, GoodLabs Studio

Donald McGillivray, Lead Applied AI Developer, GoodLabs Studio

Chris McMahon, Director, AI & Emerging Technologies Research, GoodLabs Studio

Alex Ostrovsky, AI Advisor, GoodLabs Studio

ABSTRACT

Real-time gross settlement (RTGS) systems are the foundation of modern financial infrastructure, yet many still rely on outdated and liquidity-intensive algorithms. This paper offers a practical guide to improving liquidity efficiency through more innovative payment algorithms, with a focus on liquidity-saving mechanisms (LSMs). We survey recent innovations in queue management, graph-based methods, and AI-driven techniques, including both classical and quantum-inspired optimization. Drawing on our own research and simulations, we demonstrate how non-invasive, real-time reordering of payments can reduce peak liquidity needs without compromising system safety or speed. These insights are relevant not only for central banks and financial institutions, but also to a wide range of sectors, including logistics, operations, and resource-constrained environments.

1. Introduction

Real-time gross settlement (RTGS) systems are designed to settle high-value transactions instantly, with finality and security. However, this comes with a cost as transactions are settled one by one in real time, which often requires participants to hold large amounts of intraday liquidity. The challenge is balancing these objectives: fast, risk-free settlement on the one hand, and efficient liquidity usage on the other. Most existing RTGS designs prioritize security and immediacy, but this comes at the cost of heavy liquidity consumption.

RTGS around the world settle trillions of dollars every day. The European Central Bank's (ECB) T2 system processes over €1.8 trillion daily across more than 420,000 transactions [ECB (2024)]. In the U.K., the Bank of England's CHAPS system settles an average of £344 billion each day, with about 208,000 payments [BoE (2024a)]. In Canada, the LYNX system processed CAD 386 billion per day on average in 2024, across nearly 55,000 transactions [Payments Canada (2024)]. Despite their central role, most RTGS systems still rely on first-in, first-out (FIFO) settlement logic, which prioritizes processing speed over liquidity efficiency. Although simple, the FIFO method can waste liquidity and trigger delays that spread across the financial system. These frictions are especially costly as payment volumes continue to grow and regulatory capital pressures intensify.

The consequences of inefficient liquidity allocation go beyond balance sheets. Banks maintain billions in intraday liquidity buffers, and with prevailing interest rates, the annual opportunity costs can exceed hundreds of millions of dollars per institution. Even more concerning, delays caused by rigid settlement logic, rather than system capacity or risk, can ripple through the system. Delays by large institutions propagate through the network, leading smaller participants to face increased uncertainty. At the same time, the broader system becomes more vulnerable to liquidity shocks and gridlocks [Bech and Garratt (2003)]. These dynamics are especially dangerous under stress, when modest frictions can lead to broader instability and increase the risk of payment failures and systemic default.

The regulatory environment has only intensified these pressures. Basel III's Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR) rules have made liquidity more expensive to hold and more closely monitored. Simultaneously, central banks are demanding both faster settlement and greater system resilience. The apparent trade-off between speed and safety has renewed interest in advanced liquidity-saving mechanisms (LSMs) that reorder payments to reduce liquidity needs while ensuring timely settlement [Byck and Heijmans (2020), Davey and Gray (2014)].

LSMs help institutions manage liquidity more effectively, and thus reduce capital needs, and operational risk. Moreover, they improve the predictability of payment flows, reduce last-minute funding pressures, and allow institutions to offer more reliable services to corporate clients. Banks that modernize in this area are more resilient in times of market stress. Those that do not may face higher costs and fall behind on regulatory and client expectations.

Central banks and payment system operators worldwide are actively implementing enhanced settlement algorithms to improve liquidity efficiency. For example, the Bank of England has argued that smarter algorithms can more efficiently match incoming and outgoing payments, helping to lower the amount of intraday liquidity needed to settle payment obligations [BoE (2024b)]. Similarly, modern payment systems, such as Singapore's FAST system, have shown that rapid settlement capabilities can coexist with sophisticated payment processing, challenging the notion that speed, and efficiency are trade-offs.

Despite growing interests, implementing advanced payment algorithms is challenging, especially in a regulated and risk-averse banking environment. Algorithms must be transparent and easy to understand, not just practical. Their goals must align with both business needs and regulatory rules. They also need to fit smoothly into systems that process trillions in payments each day, without causing any disruption. Most importantly, their decisions must be explainable, auditable, and subject to human oversight to ensure accountability.

A major obstacle in adopting more advanced payment algorithms is complexity. Liquidity efficiency depends not only on the amount of liquidity available, but also on when payments are sent and in what order they are processed. The space of possible payment ordering in a high-volume RTGS system is vast, and identifying the optimal sequence is a computationally intractable problem. As shown by McMahon et al. (2024), the payment reordering problem is an NP-hard problem, similar in complexity to the well-known Travelling Salesman

problem [Lawler (1985)], meaning that as the number of payments increases, the time required to find the optimal sequence grows exponentially. In this case, no known algorithm can guarantee an exact solution within a reasonable time frame. This is why payment systems typically rely on heuristics and rule-based methods that produce good and quick results to meet real-time processing requirements. However, these rule-based mechanisms and simple heuristics, while practical, are not necessarily optimal solutions and often leave substantial efficiency gains untapped [Galbiati and Soramäki (2010), Rivadeneyra and Zhang (2022)].

That said, technological advances have created unprecedented opportunities to modernize RTGS operations. Contemporary systems can perform real-time optimization calculations, assess systemic impacts, and implement complex netting logic that would have been computationally prohibitive just a decade ago. Machine learning models can predict payment behavior with increasing accuracy, while graph-based algorithms can identify settlement sequences that minimize peak liquidity requirements. Recent research, including our work on quantum-inspired optimization, has further expanded the frontier by demonstrating how novel computing approaches can solve complex payment scheduling problems more efficiently than traditional methods.

In our recent Management Science publication [McMahon et al. (2024)], we demonstrated how quantum-inspired optimization techniques can be applied to improve liquidity efficiency in RTGS systems. We formulated the payment settlement problem as a mathematical model (Quadratic Unconstrained Binary Optimization), which represents decisions as binary variables and seeks the optimal combination to minimize liquidity usage. We evaluated our solution using both quantum annealing hardware and quantum-inspired classical solvers using Canadian payment data. Our results showed that, while current quantum hardware remains limited in scale and noise, quantum-inspired solvers outperformed traditional FIFO and heuristic approaches across a range of scenarios and simulations using historical payment data.

In scenarios where batches of 70 payments arrived simultaneously, the quantum-inspired solvers achieved an average liquidity savings of 1.36% per day compared to FIFO processing. This translated to an average daily reduction of 240 million Canadian dollars in liquidity usage, with a median savings of 128.8 million CAD. Despite the complexity, the optimization process remained fast enough to operate within the real-time constraints of RTGS systems, showing that these approaches can be practically deployed in a live environment.

Building on these methods, we have since extended our work and developed a broader set of classical algorithms for liquidity optimization, including greedy heuristics, virtual liquidity models, and network-aware prioritization. Using both synthetic and anonymized historical data, we benchmarked these methods against traditional FIFO rules. We designed our simulations to mirror real-world RTGS conditions and showed that these algorithms can significantly reduce the liquidity usage and cost of financial institutions without affecting settlement speed. The results highlight the practical benefits of our quantum-inspired approaches in improving the efficiency of high-value payment systems.

This paper provides financial professionals with a practical guide to understanding and applying advanced LSMs in RTGS systems. We focus on approaches driven by advanced computational techniques, including both classical optimization techniques and quantum-inspired methods. As RTGS platforms continue to evolve, institutions that adopt smarter liquidity management strategies will not only improve their own performance but also contribute to the resilience of the broader stability of the financial system.

2. Evolving payment algorithms: a review of modern approaches

This section outlines key developments in modern payment algorithms, focusing on the main directions the literature has taken in recent years. Rather than offering a comprehensive survey, the goal is to highlight the most influential approaches shaping current thinking. These algorithms reflect different priorities, such as speed, liquidity efficiency, and risk control. A good understanding of these methods can help financial institutions choose the tools that best suit their operations and risk profile.

2.1 Queue management and prioritization algorithms

Modern queue management has moved beyond

simple FIFO rules. Many now use some form of real-time and dynamic prioritization, adjusting the order of payments as conditions change [Chen et al. (2025), BoE (2022)]. Dynamic priority scheduling algorithms adjust the payment processing order in real time based on multiple factors such as payment urgency, participants' liquidity positions, and the potential for creating settlement opportunities. Many high-value payment systems allow payments to be assigned priority categories (e.g., urgent versus normal) and even re-ordered in the central queue to improve efficiency [Bank of Canada (2022)]. One common approach is to assign a score to each payment based on how long it has been waiting, whether the sender is tight on liquidity, or if it plays a key role in the flow of funds. A high-value, time-sensitive payment might be prioritized over smaller ones, but only if it does not risk causing gridlock elsewhere in the system. One of the main challenges is to calculate these scores efficiently to maintain the stability of the system, while guaranteeing that the payment flow remains transparent and easy to audit.

An important improvement in modern payment systems is early gridlock detection [BoE (2024b), Garrat et al. (2023), Bech and Soramäki (2001)]. In the past, systems would wait until gridlock had already occurred, when payments could not move, before taking action. That often meant delays and wasted liquidity. Newer algorithms utilize graph theory to catch problems before they happen. In these systems, the payment network works as a directed graph, where banks are represented as nodes and payment instructions are represented as edges. The system scans the graph for circular dependencies, that is, loops where payments are stuck waiting on each other. When it spots one, it can reshuffle priorities or proactively activate liquidity-saving tools to prevent gridlock formation.

Some systems are beginning to utilize forecasting tools to help in determining which payments to process first. Instead of reacting only to what's in the queue at that moment, these algorithms consider expected payment flows and liquidity inflows when determining optimal processing sequences. That means a payment might be held briefly if the system expects another one to come in, which would make settlement more efficient. Machine learning can help with these predictions by analyzing historical patterns in payment timing and behavior [Vishnevsky and Gorbunova (2022)]. Using these methods in a live setting, however, is not straightforward, as it requires careful testing to avoid errors that could disrupt the system or unfairly delay some payments.

2.2 Optimization-based approaches

Researchers have employed various mathematical optimization techniques to improve liquidity efficiency in payment systems [McMahon et al. (2024)]. One approach, called Mixed-Integer Programming (MIP), treats the settlement process as a mathematical problem. The goal is to settle as many payments as possible using the least amount of liquidity, while still respecting rules around payment priorities, participant limits, and regulatory requirements [Cambe and Xing (2023)].

The problem is that optimization algorithms face a fundamental trade-off: finding the mathematically best solution takes time, but payment systems often cannot wait. MIP solvers can find optimal solutions, but solving large batches of payments may take several minutes, far too long when payments must clear immediately. Most practical systems, therefore, sacrifice mathematical perfection for speed, using faster heuristic methods that deliver solid results within the tight timing constraints that payment processing demands. Fortunately, recent advances in solver technology and hardware (like GPUs) are making real-time optimization more practical for larger problems.

Not all payment algorithms aim to minimize liquidity usage. Some are designed simply to ensure that all payments are settled on time and in line with system rules. These so-called constraint satisfaction algorithms are designed to ensure that every payment clears correctly and on time while meeting all the necessary conditions, such as timing rules, participant-specific limits, or regulatory requirements. This approach is especially useful when the focus is on reliability and compliance rather than efficiency.

In many real-world systems, though, there is more than one goal. Payment platforms often need to balance multiple priorities at once: using less liquidity, speeding up settlements, maintaining fairness across participants, and keeping decision-making transparent. That is where multi-objective optimization comes in. These methods do not try to find a single best solution. Instead, they produce a set of trade-offs called Pareto-optimal solutions, where no one objective can be improved without making another worse. This gives system operators a menu of viable options, letting them

choose the right balance for the moment based on business goals or market conditions.

2.3 Graph-based approaches

Because payment systems can be represented as networks where banks are nodes and payment obligations are links, graph-theoretic tools are a natural fit for analyzing and improving settlement efficiency. One class of methods utilizes maximum flow algorithms to maximize the number of payments that can be processed through the system, given the available liquidity at each participant [Fleischman and Dini (2021)]. Well-known algorithms, such as Ford-Fulkerson and Push-Relabel, help find the most efficient way to move payments through a network given a fixed set of constraints. But in real-time payment systems, conditions are rarely constant. Payments arrive throughout the day, and liquidity positions are constantly changing. This implies that these flow solutions cannot be static and must be updated continuously. Incremental flow algorithms, which can adjust existing solutions as new information becomes available, are crucial for maintaining performance in live environments.

Another important area is cycle detection. If the system identifies a closed loop of payment obligations where Bank A owes Bank B, Bank B owes Bank C, and Bank C owes Bank A, it can often settle that loop with very little liquidity. The challenge lies in identifying these cycles quickly, without creating gridlocks or unfair outcomes for specific participants. More advanced systems use techniques such as strongly connected component analysis to focus their search on parts of the network where netting opportunities are more likely.

Graph analysis is also useful to understand how the whole payment system works. For example, network metrics, such as centrality, can show which banks play an important role in the flow of payments. Moreover, algorithms that detect communities within the network can identify groups of participants that might benefit from shared liquidity or netting arrangements. These tools are helpful not only for improving day-to-day efficiency but also for managing risk.

2.4 Machine-learning and AI approaches

Artificial intelligence (AI) is opening new possibilities for how payment systems manage liquidity and scheduling [Beckstrom (2021), Rossi and Duigenan (2021)]. AI is also used to detect anomalous transactions, which, if left undetected, can lead to operational outages and systemic risk [Desai et al. (2024)]. One key application is pattern recognition. By analyzing past settlement data, machine learning models can spot recurring behaviors such as how specific participants tend to time their payments, or how payment flows shift around major market events. These are patterns that traditional rule-based systems often miss.

More advanced deep learning models can pick up subtle relationships in high-dimensional data [Rubio et al., (2020)]. For example, recurrent neural networks (RNNs) are well-suited to capturing how payment patterns evolve, while convolutional neural networks (CNNs) can be used to detect structural features in the payment network itself. Still, these models come with trade-offs as they are complex, often hard to interpret, and must be implemented carefully to meet transparency and regulatory standards.

Another promising area is reinforcement learning (RL), which allows an algorithm to learn by trial and error [Castro et al. (2021)]. In this setup, the system receives feedback “rewards” based on outcomes such as settlement speed or liquidity use and gradually learns strategies that improve over time. But RL brings its own risks. It can be difficult to define reward functions that encourage the right behavior, and unstable policies or unexpected responses to new conditions are unacceptable in critical financial infrastructure. For this reason, RL models must be tested extensively before being used in practice.

As a forward-looking tool, predictive analytics helps payment systems anticipate the sequence of future payments. Models that can forecast incoming payment flows, liquidity shortages, or periods of network stress allow operators to adjust their processing strategies in advance before problems arise. The most advanced systems also include external information, such as interest rates, macroeconomic indicators, or market sentiment data. However, as with any predictive system, these models require ongoing monitoring to ensure they continue to function effectively as conditions change.

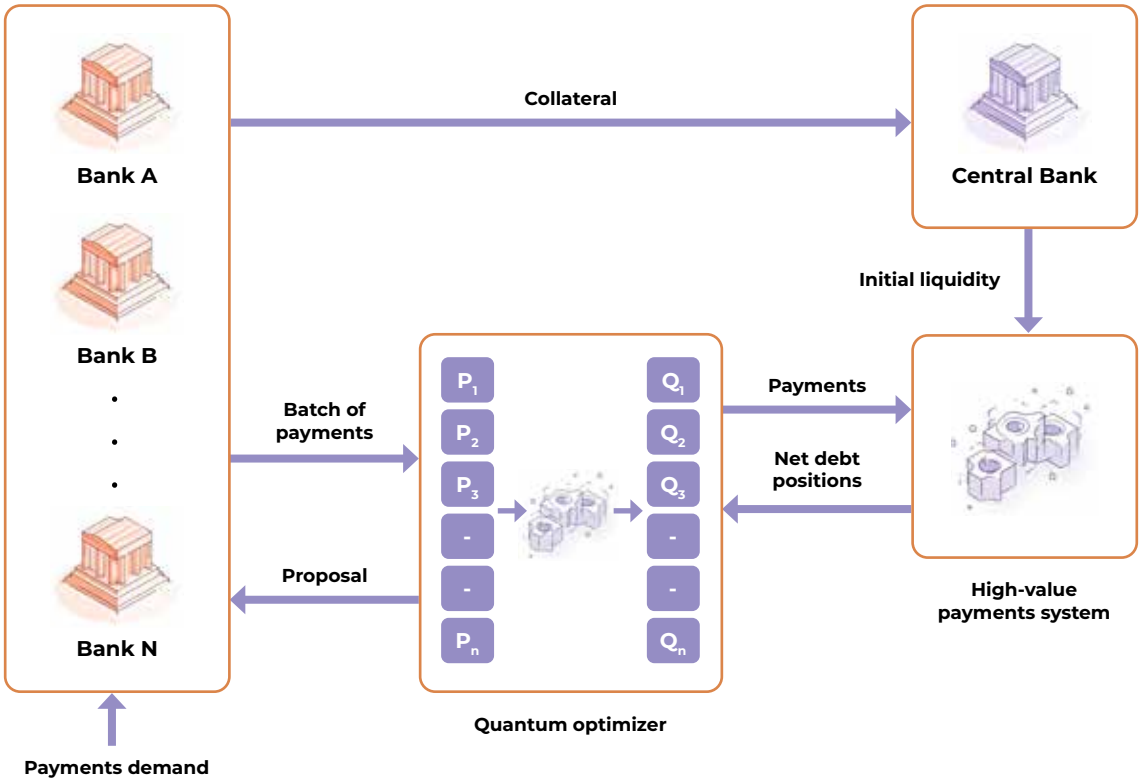
3. New approaches to payment reordering: classical preprocessing and quantum

While the literature offers a variety of queue management and optimization strategies for real-time gross settlement (RTGS) systems, our research has focused on bridging the gap between theoretical improvements and implementable tools that work within the technical and regulatory constraints of live systems. Our team at GoodLabs Studio has taken two different approaches to improving liquidity efficiency, both designed to work within existing system frameworks, without the need for major infrastructure changes.

The first project explored whether quantum-inspired optimization could reduce liquidity usage in Canada's high-value payment system [McMahon et al. (2024)]. We formulated the payment scheduling problem as a Quadratic Unconstrained Binary Optimization (QUBO) model, a framework well-suited for expressing combinatorial problems with large, discrete solution spaces such as payments data. Our objective was to minimize peak liquidity usage over a given batch of payments, subject to settlement constraints that mimic the operational realities of an RTGS system. To solve this problem, we used a quantum-inspired approach built on D-Wave's platform, which combines classical preprocessing and postprocessing techniques with quantum annealing executed on D-Wave's quantum hardware.

Our approach was intentionally designed to be non-intrusive and easy to integrate into LYNX's workflow. Rather than modifying the core infrastructure of the RTGS system, we decided to frame the optimization as a standalone preprocessing layer (see Figure 1). To reflect real-time operational constraints, the preprocessor was designed to handle batches of up to 70 payments at a time. For each batch, it calculated an execution order

Figure 1: Schematic of the quantum optimizer as a preprocessor to the payment system



Source: Reproduced from McMahon et al (2024)

that minimized liquidity usage before the payments were submitted to the system to be settled. This reordered payment list can then be voluntarily adopted by participants, without disrupting settlement protocols, affecting transaction finality, or introducing new security risks. Our approach is attractive for institutions seeking to reduce intraday liquidity needs without altering system-level infrastructure.

We compared the performance of this hybrid solver against baseline methods, including standard FIFO ordering and a more flexible FIFO-bypass strategy. The tests were conducted on historical payment data from LYNX, Canada's real-time gross settlement system, using anonymized data. Across these simulations, the quantum-enhanced scheduling algorithm consistently outperformed several benchmark algorithms, such as FIFO and others we tested. With the quantum-inspired algorithm, we achieved average liquidity savings of 1.36% per day, equivalent to 240 million Canadian dollars in liquidity on high-volume days. The median daily savings stood at 128.8 million CAD. These gains were particularly significant during periods of heavy congestion or simulated market stress, precisely when efficient liquidity management is most critical.

In our experiments, we also tested larger batch sizes of up to 140 payments. While these larger batches yielded slightly greater liquidity savings compared to smaller batches (70 payments), the marginal gains diminished as batch size increased. More importantly, the runtime grew disproportionately, making it harder to meet real-time operational requirements. For instance, solving a batch of 140 payments could take several seconds, which is acceptable in some contexts, but too slow for continuous settlement flows. As a result, we focused on 70-payment batches as a practical compromise: they offered a meaningful improvement in liquidity efficiency (up to 1.36%) while remaining fast enough to support near-real-time processing.

We also compared our quantum-inspired method against a classical optimization approach using the Solving Constraint Integer Programs (SCIP) solver for mixed-integer nonlinear programming. While SCIP can, in principle, solve the problem optimally, it proved impractical in real-world settings. For batches of 70 payments, the average runtime exceeded two hours and occasionally failed to converge after 24 hours, far beyond the limits of real-time settlement. In contrast, D-Wave's hybrid solver handled 70-payment batches in under two minutes on average, with the core optimization step taking only about five seconds.

However, we observed that as batch sizes increased beyond 140 payments, two limitations emerged. First, the total time to compile and solve the optimization problem increased sharply, approaching the limit of real-time feasibility. Second, the quality of the solutions began to degrade as the solver returned fewer feasible solutions. In some cases, the resulting liquidity usage exceeded that of the FIFO benchmark. These effects highlight the current scalability limits of quantum-inspired methods. Nevertheless, within practical batch sizes, the approach delivers meaningful efficiency gains that are currently out of reach for classical solvers.

Our more recent work takes a different approach, using conventional computing resources and classical optimization methods to achieve similar goals. In recent work, we developed a preprocessing algorithm that reorders payments using a combination of virtual liquidity levels (VLLs) and greedy optimization within sliding or tumbling time windows. The main idea is to simulate artificial liquidity constraints at the start of the day and progressively relax them, encouraging the algorithm to delay non-urgent payments just long enough to unlock better settlement sequences. Each queue of payments is then optimized by local swaps that reduce peak liquidity demand, while respecting constraints on maximum delay, both absolute and value weighted.

Even with partial information and real-time constraints, this method showed important improvements. In simulation environments that replicate typical RTGS conditions, our approach consistently reduced aggregate liquidity needs while introducing only modest delays, though in some cases the delays extended beyond what would be acceptable in an RTGS environment. Liquidity savings compared to the benchmark case were often more than 10%, typically 30% when historical payments data were used. To address the longer payment delays, we found that tuning the VLL parameter yields a clear liquidity-delay trade-off frontier, with an identifiable "sweet spot" where liquidity savings are significant, and average delay costs remain tolerable. The algorithm operates purely at the submission layer and makes no assumptions about internal settlement logic, making it deployable as an external tool. Importantly, improvements were observed across the board, not just for the largest institutions supporting broader fairness and adoption.

These two contributions share a common approach: rather than reinventing the architecture of RTGS systems, we focus on improving what participants submit and when. By making smarter use of existing flexibility in payment timing and sequencing, and by providing real-time tools to guide that decision-making, it is possible to achieve liquidity savings without disrupting the safety, fairness, or legal finality of existing settlement systems.

4. Broader applications of liquidity optimization and scheduling

While our work has focused on improving liquidity efficiency in real-time gross settlement systems, the methods and principles we have developed are also applicable across the financial sector and have numerous use-cases. Many institutions face similar challenges: how to manage constrained resources (liquidity, capital, computing) while dealing with time-sensitive and high volumes of transactions. Smarter strategies for reordering, prioritizing, or netting these transactions can yield significant gains in efficiency, risk reduction, and operational resilience.

A natural extension of our work is collateral optimization in capital markets. Large institutions often manage multiple margin calls across clearinghouses and counterparties. Firms can minimize the fragmentation of collateral and reduce overposting by sequencing obligations more strategically using the optimization techniques we have applied to real-time payments. Similarly, in securities settlement, especially in systems with multiple counterparties and delayed matching, algorithms that identify optimal settlement cycles or minimize failed trades can enhance both liquidity usage and operational throughput, particularly under settlement compression regimes or in T+1 transition contexts. In corporate treasury operations, daily cash sweeps and payment scheduling could benefit from predictive and reinforcement learning tools similar to those we applied to RTGS queues. Firms could dynamically prioritize payables and receivables to reduce daylight overdrafts or borrowing costs, especially when liquidity is tight, or markets are volatile.

Buy-side institutions, particularly asset managers and hedge funds, may find value in using our scheduling and queueing frameworks to improve order execution timing, especially for block trades or large-volume redemptions. Models that account for counterparty behavior, settlement friction, and operational latency can help reduce slippage and settlement risk. Finally, in retail and instant payment systems, where transaction volumes are high, but margins are tight, our methods could support smart routing, liquidity pooling, or delay-based netting at microsecond timescales. Even small improvements in efficiency can lead to significant savings when applied across millions of transactions.

5. Conclusion

As real-time payment volumes pressure grows, improving liquidity efficiency has become a crucial operational and strategic priority for financial and other institutions. This paper has outlined how payment reordering, whether using classical algorithms or quantum-inspired techniques, can lead to significant gains without requiring disruptive changes to the existing system. Our results demonstrate that substantial improvements in liquidity usage are possible with practical tools and minimal implementation risk. As computational methods and quantum technologies, in particular, continue to improve, we believe these innovations will become essential not only to modern payment infrastructure but also to optimization challenges across a range of industries.

References

Bardoscia, M., P. Barucca, S. Battiston, F. Caccioli, G. Cimini, D. Garlaschelli, F. Saracco, T. Squartini, and G. Caldarelli, 2021, "The physics of financial networks," Nature Reviews Physics 3, 490-507

Bech, M. L., and K. Soramäki, 2001, "Gridlock resolution in interbank payment systems," Bank of Finland Research Discussion Paper No. 9/2001

Beckstrom, J. R., 2021, "Auditing machine learning algorithms," International Journal of Government Auditing 48:1, 40-41

BoE, 2022, "Roadmap for real-time gross settlement service beyond 2024," Bank of England Consultation Paper, Bank of England, https://tinyurl.com/yu6ymac7

BoE, 2024a, "Payment and settlement statistics," Bank of England, https://tinyurl.com/mr36hzvd

BoE, 2024b, "Artificial intelligence in UK financial services," Bank of England, https://tinyurl.com/2nrwn7px

Byck, S., and R. Heijmans, 2020, "How much liquidity would a liquidity-saving mechanism save if a liquidity-saving mechanism could save liquidity? A simulation approach for Canada's large-value payment system," Payment Canada Discussion Paper

Cambe, J., and Z. Xing, 2024, "Just solve it: a simple method to improve the design and performance of liquidity-saving mechanisms," Journal of Financial Market Infrastructures 24:2, 13-37

Castro, P. S., A. Desai, H. Du, R. J. Garratt, and F. Rivadeneyra, 2021, "Estimating policy functions in payment systems using RL," Bank of Canada Staff Working Paper 2021-7

Chen, S., O. Baron, and N. Chen, 2024, "Optimal dynamic clearing for interbank payments," Management Science 71:4, 2953-2974

de Avillez, R., D. Millard, N. Bulusu, M. McNeely, L. Sabetti, K. Wai, and N. Zhang, 2022, "An overview of Lynx, Canada's High-Value Payment System," Bank of Canada Working Paper 2022-05, https://tinyurl.com/5y23t5jy

Davey, N., and D. Gray, 2014, "How has the liquidity saving mechanism reduced banks' intraday liquidity costs in CHAPS?" Bank of England Quarterly Bulletin Q2, Bank of England

Desai A., A. Kosse, and J. Sharples, 2024, "Machine learning framework for anomaly detection in HVPS," BIS Working Paper 1188, https://tinyurl.com/mr34aj48

ECB, 2024, "Target services annual report," European Central Bank, https://tinyurl.com/yf64vef4

Fleischman, T., and P. Dini, 2021, "Mathematical foundations for balancing the payment system in the trade credit market," Journal of Risk and Financial Management 14:9, 452

Gaffeo, E., L. Gobbi, and M. Molinari, 2019, "The economics of netting in financial networks," Journal of Economic Interaction and Coordination 14, 595-622

Garratt, R. J., Z. Lu, and P. Tian, 2023, "How banks create gridlock to save liquidity in Canada's large value payment system," Bank of Canada Staff Working Paper 2023-26

Lawler, E. L., J. K. Lenstra, A. H. G. Rinnooy Kan, and D. B. Shmoys, 1986, "The traveling salesman problem: a guided tour of combinatorial optimization," Journal of the Operational Research Society 37, 535–536

McMahon, C., D. McGillivray, A. Desai, F. Rivadeneyra, J-P. Lam, T. Lo, D. Marsden, and V. Skavysh, 2024, "Improving the efficiency of payments systems using quantum computing," Management Science 70:10, 7325-7341

Payments Canada, 2024, "Lynx Canada's High-Value Payment System," https://tinyurl.com/wubhd93z

Rossi, F., and J. Duigenan, 2021, "The future of finance is trustworthy AI," Payments Journal, https://tinyurl.com/5b39hc2z

Rubio, J., P. Barucca, G. Gage, J. Arroyo, R. Morales-Resendiz, 2020, "Classifying payment patterns with artificial neural networks: an autoencoder approach," Latin American Journal of Central Banking 1:1-4

Rivadeneyra, F. and N. Zhang, 2020, "Liquidity usage and payment delay estimates of the new Canadian High-Value Payments System," Bank of Canada Technical Report no. 9

Vishnevsky, V., and A. Gorbunova, 2022, "Application of machine learning methods to solving problems of queuing theory," in Dudin, A., A. Nazarov, and A. Moiseev, (eds.), Information technologies and mathematical modelling. Queueing theory and applications, ITMM 2021, Communications in Computer and Information Science, vol. 1605. Springer

Future of Payments

Stablecoins: a new technology, or older than the Knights of Templar?

Paul H. Kupiec, Senior Fellow and Arthur F. Burns Chair in Financial Policy, American Enterprise Institute[1]

ABSTRACT

Stablecoins are the traveler's check of the internet era. Once tendered and confirmed genuine by some public cryptologic process, a stablecoin's monetary value is trustworthy and readily convertible into legal currency. Stablecoins have seen only limited use in commercial transactions, but this seems certain to change. Compared to stablecoins, traditional bank deposits offer more favorable capital/reserve requirements, federal deposit insurance, and the ability to pay interest. New legislation poised to pass the U.S. Congress will enable banks to offer stablecoin financial services. This legislation will likely catalyze the development of hybrid deposit accounts, where bank depositors earn interest on balances that can seamlessly be transformed into bank-issued stablecoins, which can then be traded and subsequently transformed back into traditional deposits.

1. The author was formerly the Chairman of the Research Task Force at the Basel Committee on Bank Supervision, and Director of the Center for Financial Research at the Federal Deposit Insurance Corporation (FDIC).

1. Introduction

Private stablecoins are a form of digital money that can be purchased and traded over the internet. A significant share of private stablecoin transactions can be attributed to their use in facilitating the purchase and sale of other digital assets. Thus far, private stablecoins have achieved only a limited degree of public acceptance as a means of payment in commercial transactions, but with new legislation on the horizon, this may soon change.

Private stablecoins serve a function similar to travelers' checks, which have been in use since at least the Crusades, perhaps longer. The only difference being that private stablecoins can be spent over the internet. Stablecoins' use of cryptology to prevent fraud and double spending may be just the newest incarnation of an ancient practice.

1.1 A new solution to an ancient problem

After Jerusalem fell to Christian Crusaders in June 1099, Christian pilgrims from across Western Europe visited the Holy Land. Many were robbed and killed as they travelled through Muslim-controlled territories. Around 1120, a French knight, named Hugues de Payens, founded a military order called the Poor Knights of the Temple of King Solomon (later known as the Knights Templar).[2] The Knights of Templar were warrior monks, bankers, pirates, and part of a religious order that reported directly to the pope. They had headquarters on Jerusalem's sacred Temple Mount and pledged to protect Christian visitors to the city.

To facilitate pilgrimages to the Holy Land, the Knights of Templars accepted specie and coins and in return issued paper bills that could be exchanged for money at Knights of Templar outposts called preceptories in England, throughout Christian Europe, and in the Holy Land. To prevent fraud, the Knights reportedly developed a system of codes for the secure passing of information, and pilgrims' deposits and withdrawals from preceptories were recorded on paper bills using coded ciphers. In essence, the Knights invented the travelers' check.

Others historical accounts argue that these pious monks actually stole the idea from their Muslims adversaries. Proponents of this theory claim that a similar system existed in the 5th Abbadis Caliphs, which would imply traveler's checks were in use from about the year 790 AD. My guess is that the Muslims could have learned the practice from the Greeks or Romans who traveled extensively in earlier times, but I have not seen any documentation that confirms this conjecture.

2. Stablecoins: the traveler's check of the internet era

Traveler's checks and money orders are of course still in use today. They are not issued by monks or even banks necessarily. Many are issued by state-licensed money transfer agents and even the post office. Some banks do issue traveler's checks (or have done so in the past), but all banks issue similar instruments in the form of letters of credit, bank cashier's checks, prepaid or stored-value cards, and even revolving credit cards - all of which are a means to solve the underlying problem of paying someone, perhaps some distance away, who has no reason to know or trust you. Unlike private stablecoins, all of these products settle using private access payments systems controlled and operated by banks. In contrast, stablecoin transactions are processed using a public distributed ledger system where agents called "miners" compete to earn rewards for processing stablecoin transactions. Different stablecoins transact using different public ledgers that are not interoperable.

Modern stablecoins are digital assets designed to maintain a stable values relative to a reference currency like the U.S. dollar. Many U.S. dollar denominated stablecoins attempt to maintain their value by investing the dollar proceeds from a newly-issued stablecoins in high-quality, short-term, liquid, dollar-denominated assets of equivalent value held by the stablecoin sponsor as a reserve that can be used to stabilize the coin's market value. There are other versions that are an entirely separate breed of stablecoin. These coins hold crypto assets as reserves or use algorithmic arbitrage trading to maintain parity with the dollar. It is unclear to me why these types of stablecoins should be recognized as a legitimate means of payment rather than as a risky security.

2. https://tinyurl.com/5ankvdt5

3. Stablecoins and commercial transactions

Thus far, private stablecoins are not commonly used in the U.S. retail banking environment. JPMorgan-Chase issued its own private stablecoin, JPM Coin, that was designed to facilitate transactions internally between its institutional clients. The coin has not been made available to the retail public and the blockchain it trades on is private.

More recently, two niche banks, Custodia Bank and Vantage Bank, reportedly designed a system wherein Custodia Bank's public stablecoin, Avit, is used to process commercial transactions.[3] The system transfers bank deposit balances between two banks without using the Federal Reserve or Automated Clearinghouse payments systems. Instead, the banks transform deposits into the stablecoin Avit, transact over the Ethereum blockchain, and redeem the stablecoin for a deposit at a participating counterparty bank. The end result is that insured bank deposits are digitized into a stablecoin, traded and settled over a public blockchain, and transformed back into a bank deposit.

In the near future, as banks develop ways to use stablecoin technology to safely and efficiently digitize bank deposits, it is likely that private stablecoins will become better integrated into the U.S. retail banking system. Bank deposits are already a form of digital currency, and in many ways dominate private stablecoins: they can pay interest, are federally insured up to U.S.$250K, and they clear and settle over highly secure systems. The downside for many is that the settlement systems are centrally controlled by banks and the Federal Reserve and, as it currently stands, these systems will not support the use of the smart contracts being developed in the private stablecoin space.

4. Modernizing stablecoin regulation

New stablecoin legislation has not been finalized, but two largely compatible bills enjoy wide support within the U.S. Congress. Should one of these bills pass, it will likely accelerate the integration of private stablecoins into the retail banking environment.[4]

New stablecoin legislation would define and regulate private stablecoins as a digital asset that:

- Has a reasonable expectation of maintaining a stable monetary value.
- Is redeemable for currency.
- Is designed to be used as a means of payment.
- Is not a national currency.
- Is not a security.
- Is not a deposit as defined in the Federal Deposit Insurance Act or the Federal Credit Union Act.

Private stablecoins will not be permitted to pay interest, and, unlike bank deposits, will not benefit from federal deposit insurance. However, they will be required to maintain dollar-for-dollar reserves in short-term high-quality liquid assets, including Treasury Bills, bank deposits, reserve deposits at a Federal Reserve district bank, Treasury securities with remaining maturities of 3 months or less, and money market fund shares backed by Treasury securities. Stablecoin reserves held by bank subsidiary stablecoin issuers would not be subject to bank capital requirements and would not be included as liabilities at the consolidated bank holding company level.

Stablecoin issuers will be required to file reports on a monthly basis that provide the public with information that certifies that the stablecoin issuer is complying with legal reserve requirements. Public reports must be periodically certified, perhaps as frequently as bi-monthly, by an accredited public accounting firm. In the case of a stablecoin issuer bankruptcy, stablecoin owners would have priority after administrative expenses in a bankruptcy proceeding.

3. https://tinyurl.com/mdfe9u83

4. In July 2025, the U.S. Congress passed the GENIUS Act, which provides a new legal and regulatory framework for licensing payment stablecoins. The final legislation (available at: https://tinyurl.com/mrya7t6y) closely mirrors the provisions of earlier versions of proposed bills that are described below.

Proposed legislation would allow private stablecoins to be issued by a subsidiary of an insured depository institution using federal or state approved regulatory frameworks. Nonbank entities could also issue stablecoins under a federal national license if approved by the Office of the Comptroller of the Currency (OCC) or under a state license if approved by a state regulatory agency. Bank issued stable coins would be subject to regulations promulgated by their parent bank's primary federal regulator while stablecoins issued by a subsidiary of a credit union would be regulated by the National Credit Union Administration.

Most private stablecoins issuers to date are entities licensed as state-regulated money transfer agents, or licensed as limited-purpose trust companies. Should the legislation pass, the law will likely specify that state regulatory authorities would have to certify annually that their state stablecoin regulatory regimes impose standards that meet or exceed the standards required under federal stablecoin regulations. It is possible that the legislation may require stablecoins larger than a specified market cap to be licensed by a federal stablecoin regulator. Should conflicts arise, federal stablecoin regulations will likely preempt those issued by states. Stablecoin issuers will be required to comply with anti-money laundering laws, but the exact rules and oversight arrangements that will apply have yet to be determined.

5. Stablecoins and traditional retail banking

It seems likely that new stablecoin legislation will foster the creation of hybrid bank accounts that will allow customers to transact using traditional banking clearing and settlement systems, as well as transact using private stablecoins and a permissioned, if perhaps not fully public, blockchain. Banks' subsidiaries and nonbank firms licensed to issue private stablecoins will likely form a consortium - a jointly owned payments system processor - that develops and runs a ledger-based payments platform that can be used by private stablecoin issuers and banks alike. Such an arrangement would mirror the way credit, debit, ATM, and ACH processing systems were developed in the past. Under such a scenario, the common stablecoin blockchain would likely be permissioned with only limited retail public access through a stablecoin issuer portal. Indeed, recent press reports suggest that the largest U.S. banks are considering developing a joint stablecoin to compete in the retail crypto transactions space.[5]

It remains to be determined whether the Federal Reserve would have oversight powers over private stablecoin blockchains. If the Fed were given regulatory authority, it could require that proof-of-stake processors satisfy certain minimum regulatory requirements, including gaining "fit and proper" approval similar to ownership suitability requirements in banking, as well as compliance with anti-money laundering laws.

6. Conclusion

In order to safeguard their deposit bases against competition from private stablecoin issuers, it seems likely that banks will develop and offer deposit accounts that include transactions services that either use, or approximate the use of, private stablecoins as a transacting option. These hybrid bank deposits will be a new type of checking account. Bank capital, liquidity, and other regulations are already in place to manage the associated bank safety and soundness risks and new stablecoin legislation will provide for a unified federal regulatory framework that allows bank subsidiaries to issue and transact in private stablecoins. These new hybridized deposit accounts would modernize retail banking and could potentially accelerate clearing times and reduce transactions processing costs, especially in cross border transactions. Regardless, retail consumers seem destined to benefit from healthy competition between legacy transaction clearing and settlement systems and systems based on the internet and blockchain technology.

5. https://tinyurl.com/5ankvdt5

Future of Payments

Impact of new technologies on the **cash management** competitive landscape

Koen Vierendeels,
Head of Transaction Banking, Belfius

Robert-Jan Wekking,
Group Practice Lead Payments,
Projective Group

ABSTRACT

Corporate treasurers already had enough on their plates before the recent geopolitical challenges made their jobs significantly more complicated and challenging. From trying to remain compliant with the numerous regulatory environments, to preventing fraud, keeping up with the latest technologies, and trying to find the best way to manage the funds of the enterprise, corporate treasurers already had quite a bit to deal with. However, the recent trade wars have made that task somewhat more complicated, with expectations that taxes could become even more complex to manage for globally diverse organizations. These challenges come at a time when, like most other functions, corporate treasuries were working on their digital transformation strategies, made somewhat more complicated, and exciting, by the AI revolution. Interestingly, these same new technologies can, and will, have a profound impact on how organizations manage their cash, and with whom they will partner going forward. In this article, we posit that these new technologies will make the corporate cash management market much more competitive, and allow regional and local banks to compete head-on with global players.

1. Introduction

Most people still view corporate treasury as the division that works hard at finding ways to keep the company's funds away from the taxman. Using offshore locations, and complex tax structures, they spend all day moving money around to minimize the company's tax obligations. Even those who study the subject at major universities are primarily taught about whether centralized or decentralized treasury structures are better at managing a multinational organization's taxes. And while it is true that corporate treasuries do work hard to help multinational companies minimize their global tax obligations, the job of a corporate treasurer is much more complicated than that.

At its core, treasury management is still about managing an organization's liquidity, using a myriad of instruments and relationships to help improve how that is done. Constantly monitoring cash inflows and outflows, identifying and hedging risks that emanate from currency and interest rate fluctuations, ensuring working capital is maintained and allocated efficiently, and managing investments and debt, to name a few, ensure that a company's liquidity position is optimized. But to ensure that optimization, corporate treasurers need to be constantly aware of regulatory changes within the markets in which they operate, specifically with regards to transfer pricing and taxation, how currencies might move, their implications for a company's liquidity across its regions, forecasting how both currency and liquidity needs might fluctuate, and obviously make informed decisions about how and where funds are allocated.

To put things in context, a typical corporate treasury of a multinational corporation needs to be cognizant of a large number of major global regulations when undertaking its liquidity management tasks, including the Sarbanes-Oxley Act (SOX), which requires companies that operate and publish accounts in the U.S. to ensure that their disclosures are accurate and free from fraud, resulting in significantly more work in documenting and testing; the Office of Foreign Assets Control (OFAC) sanctions list, which requires cross-border payments processed by the U.S. treasury to be screened against OFAC's Specially Designated Nationals (SDN) list, slowing the process down; and Basel III, which impacts how treasuries can allocate their cost of capital and how they invest their cash, including lending. This is by no means an exhaustive list, and does not include local regulations and restrictions, but does highlight some of the key regulatory challenges corporate treasurers face to remain compliant.

To manage some of these challenges, corporate treasurers are increasingly relying on advanced treasury management systems to help them improve efficiency, have access to better and more reliable data, and, consequently, make better financial decisions. They often also establish strong relationships with major legal and tax advisory firms, and major global banking organizations, who can help them navigate some of their liquidity challenges and provide cash management and advisory services. It is with the help of advanced internal, and third-party, cash management capabilities that corporate treasurers can track where liquidity is based, forecast where it needs to be, and take the necessary actions to make it happen in the most efficient manner possible. Maintaining control over where money is coming from and going to continues to be the main challenge facing the corporate treasury function.

Given the global nature of the operations of most major global corporations, this has typically meant establishing close relationships with a number of global banking organizations such as JPMorgan, Bank of America, Citi, HSBC, or Deutsche Bank. The result has been a highly concentrated corporate cash management market, where a handful of large global banking organizations have dominated.

In our view that is going to change. We firmly believe that with the advent of new technologies, in specific instant payments, which is more of a new capability than a technology but is increasingly becoming more prevalent, and Application Programming Interfaces (APIs), which allow services to be provided to third-party companies, regional players will be able to compete head-on with the more global players and make the market for cash pooling and management significantly more competitive.

2. Evolving nature of cash management

An important subset of treasury management is cash management, which is tasked with tracking, managing, and investing cash across the entire enterprise.

Cash management is responsible for both long-term issues such as how much and where excess cash should be invested, and short-term ones, such as ensuring there is enough cash to cover payroll and supplier invoices and making sure cash is collected on invoices that are outstanding. And all the while trying to minimize so-called idle cash and maximize the returns obtained.

How corporations managed their cash management, or their treasury, functions, was up for debate up to around a decade ago when, according PwC's Global Corporate Treasury Benchmarking Survey of 2017[1], 83% of the more than 200 corporates surveyed stated that they had established a dedicated central treasury department for the management of cash, foreign currencies, and other key financial matters.

This finding was interesting, since the trend in many multinationals corporations has been to decentralize their strategic and operational management so as to be more responsive to rapidly changing consumer needs.

Nevertheless, that trend has continued and most major global corporations have established a centralized treasury that acts almost as an in-house bank, with some such as BP even having their own market trading functions to improve their "Buying Power" (playing on the BP initials!) in financial markets. There are also corporate treasuries that provide retail and corporate financing, with some such as GE Capital having spun off those operations (in their case to create Synchrony Financial).

While the pros and cons of centralized and decentralized cash management, and treasury, functions is beyond the scope of this article, there a number of benefits of the former that we believe are valid and pertinent for the arguments made here. They include:

- **Centralized dashboard of cash positions**: centralized cash management operations allow corporations to have a clear view of their global cash positions, and anticipated inflows and outflows; helping them to make reliable forecasts about needs and, consequently, better manage their liquidity. By consolidating cash in a central location, organizations will also have better control over how liquidity is managed.
- **Increased efficiency**: pooling of liquidity can help reduce transaction fees and improve interest rates paid and received, and of course consolidating functions typically improves efficiency. Corporations are also able to benefit from having a small number of experts managing the treasury function centrally rather than a large number of less experienced individuals scattered across the group.[2]
- **Better investment management**: having a holistic view of the company's global cash positions allows firms to increase balances invested for the long-term, obtaining better investment returns, reducing borrowings or obtaining better rates, and minimizing idle cash across the entire enterprise. Idle cash management also benefits from diversification, meaning a smaller total is needed to maintain the minimum balances required across the group.
- **Improved risk and regulatory management**: being able to improve coordination across a group to manage financial and regulatory risk will help organizations to mitigate and better manage them. Hedging strategies also benefit from centralization, since not only is the treasury able to obtain better rates, it gains from diversification effects across the group.
- **Applying the latest technologies**: the complexities of today's treasury function demands that it applies the latest technologies, some of which are expensive and complicated. Having a centralized treasury function allows for the hiring of the most capable people, needed to implement, manage, and apply these new technologies, and to standardize the systems across the group. The treasury function requires access to real-time reporting and analytics to be able to effectuate its strategies, and that demands the most advanced technologies, capabilities, and personnel - things that are hard to decentralize.

To achieve its goal of improving control over the organization's cash positions and automate as much of their internal and external processes as

1. https://tinyurl.com/y245u5z6
2. Within centralized treasury functions, corporations often separate international treasury centers (ITCs), that deal with management of the corporation's finances, as discussed in section 2, from shared service centers (SSCs), which constitute the grouping of resources for standardized operational functions to improve efficiencies in HR, Finance, IT, etc.

possible, the cash management function also needs to apply the latest technologies. This is no mean feat, and forces most corporations to consider centralizing their cash/treasury management technological capabilities in order to achieve their objectives.

Automation of the treasury function will help reduce the costs of erroneous data being manually entered into the system, ensure compliance with the ever-growing list of regulations, and control fraud. It will also help in identifying errors and allowing for remedial action to be taken earlier in the process.

The AI revolution is expected to accelerate the process of automation, and have a transformational impact on the treasury function as well. In the specific case of cash management, AI's predictive capabilities will help organizations to speed up error detections and reconciliations, as well as use seasonal cash flow patterns and payment behaviors to drastically improve how much idle cash they need to keep across the group, making sure it goes to where it is needed most.

APIs, which allow different software applications to communicate and exchange data using a set of protocols, is another technological capability that is expected to have a profound impact on cash management.

APIs are expected to help organizations obtain real-time information across the different accounts and currencies they hold, no longer waiting for overnight processing cycles to end, automate data flow across different systems, streamline routine transactions to speed up processing, minimize manual errors, and have access up to date information from across the group.

By integrating APIs with the treasury's own banking application, rather than third-party solutions, organizations will be able to streamline their reconciliation processes and manage cash pools directly from their own enterprise resource planning (ERP) systems, eliminating the need to navigate multiple banking platforms.

2.1 Automation, instant payments, and pooling

Within the corporate treasury ecosystem, it is not just the treasury function that aims to automate as much of its processes as possible: the banks and payment providers companies deal with have also been working hard to automate their processes, one important manifestation of which is instant payments.

2.1.1 Instant payments

Instant payments, which are processed and settled in real time, avoid the need to wait days for them to clear. The funds move within seconds, 24 hours a day, 365 days a year. The immediacy of payments, while having many attractive features such as certainty of payment, rapid confirmations for sender and recipient, and enabling just-in-time working capital management, also means that once an instant payment is sent, the transaction is irrevocable and the recipient has immediate access to the funds. This means that the payment processing systems need to be designed to be as foolproof as possible, since mistakes are much harder to correct. Obviously, managing fraud is also an important issue that the treasury function needs to manage effectively.

Integrating real-time payments within legacy systems in the treasury function is also a challenge for many organizations, with most being forced to upgrade or modernize their systems. The cost-benefit analysis will, over time, tend to favor undertaking such a system modernization.

The fact of the matter is that a major challenge for treasurers is that they will now have to manage their funds and cash positions 24/7, as there is no end of day closing anymore. This is difficult, given different time zones and is something that is contrary to the notion of a centralized treasury function.

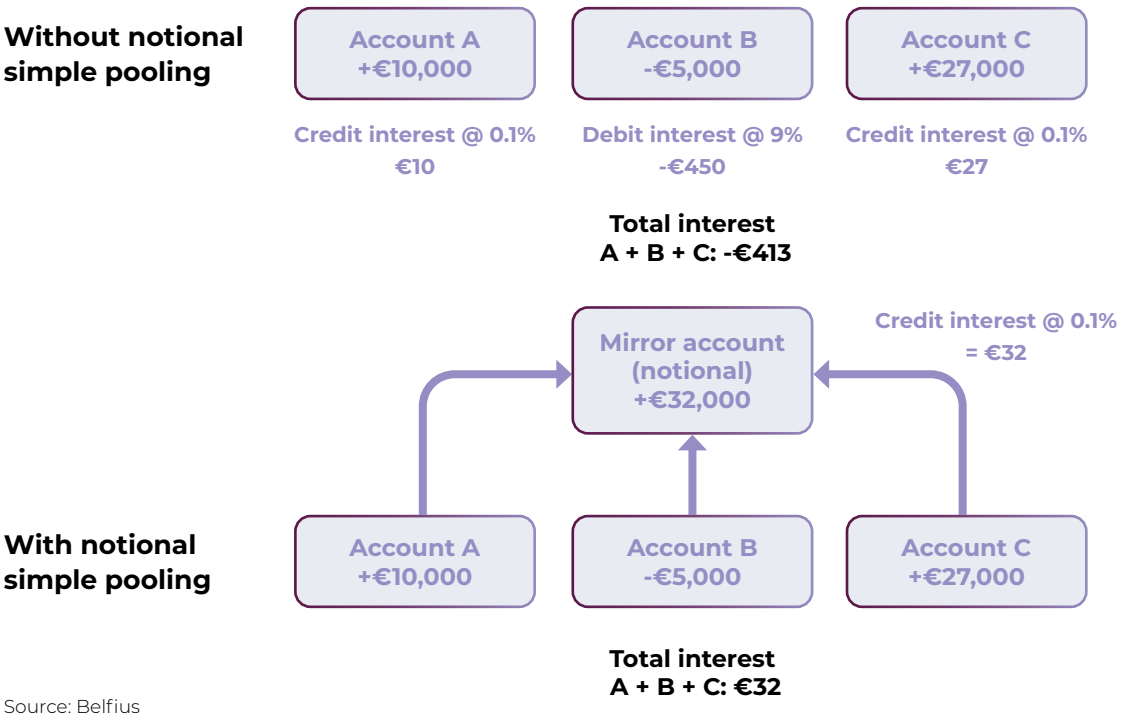
2.1.2 Cash pooling

Cash pooling, which optimizes liquidity by centralizing account balances, allows organizations to aggregate the cash sitting in various accounts into a single pool, making it possible to offset short-falls in one account with surpluses in another.

Cash pooling can either be physical (zero-balance account[3], where the funds are physically transferred at the end of each day so that sub-accounts are brought to zero and all excess cash is concentrated in a master account (Figure 1)), or notional (where balances are virtually consolidated without phys-

3. Alternative types of physical pooling exist, such as target balance accounts, where the subsidiaries maintain a target or fixed balance.

Figure 1: Simple pooling (merger of accounts)



Source: Belfius

ical transfer). In the case of the latter, the company's bank will calculate interest on the net aggregated balance of all accounts and treats them as one for interest and reporting purposes, even though each subsidiary's account remains separate.

Cash pooling adjustments (sweeps), which used to take place at the end of each day and where funds would move once daily to concentrate balances, have also been impacted by instant payments, making cash pooling timelier and more dynamic, and allowing treasuries to maintain near-zero latency in liquidity management.

Instant payments have also made it possible for the treasury function to undertake intraday pooling, since real-time transfers allow them to sweep balances a number of times a day, if not continuously throughout the day, permitting optimization of net positions immediately, including outside of normal working hours. Real-time pooling allows for monitoring of the consolidated cash position, helping to improve forecasting of short-term needs and reducing idle funds.

In response to these capabilities, a number of banks are offering to their clients API-driven real-time cash pooling services that allow intraday sweeps. Some are even offering these services for virtual account structures, which make it possible for treasury to have immediate centralization of cash with full visibility, without needing to make physical transfers for every single transaction.

3. The changing competitive landscape

Despite the aforementioned benefits that instant payments afford cash pooling strategies, treasuries will struggle to achieve real-time pooling across the entire enterprise should they have relationships with a number of banks, as is typically the case. They will, therefore, be forced to limit their banking relationships to only those banks that either support instant payments or are able to use overlay solutions that enable real-time transfers.

Ironically, the same capabilities that are forcing corporates to choose the more global of banking part-

ners are also changing the market dynamics in the cash management ecosystem, creating opportunities for both local and regional banks to compete with the very biggest.

For example, while cash pooling (especially physical pooling or notional pooling) has traditionally meant that corporations were forced to hold accounts with a single global bank, with instant payment as the new normal, and a modern connectivity architecture such as APIs and ISO20022, this model is evolving.

Corporations are now able to establish in-house structures where subsidiaries transact via internal accounts, external payments and collections are routed through regional banks, and liquidity is managed via real-time or intraday transfers to the central pool.

Having the option to also partner with local and/or regional banks for their cash management needs means that corporations will now be free to choose the partners that best meet their specific requirements, rather than being forced to choose only the largest global players.

As with everything in life, there are pros and cons to choosing to partner with local and/or regional banks, as opposed to the large global banking giants, but new technologies have certainly made it possible for corporations to benefit from the ability to build a modern treasury model with them that is both agile and efficient.

By partnering with those local and/or regional banks, corporations will be able to benefit from greater local expertise and market access. They typically offer stronger local market knowledge and faster tailored support. They are also more knowledgeable about the local regulatory environment, which is very valuable in areas with complex financial regulations and growth potential.

Furthermore, by decentralizing banking relationships across multiple providers, corporations will be able to avoid having to pay the premium prices charged by global banks and negotiate better fees and FX spreads. They will certainly be in a stronger negotiating position because of the advent of local and regional banks in the provision of cash management services.

Finally, corporations will be able to mitigate the risk of being dependent on a single bank's infrastructure and/or credit risk – an issue that becomes more pertinent in times of crisis, when banks face liquidity or technological issues.

For corporations that are considering partnering with more local and/or regional banks for their cash management services, there is, however, a note of caution. And that is that while the aforementioned benefits are certainly real in markets that have developed technologically, there are still countries where instant payments are not as yet guaranteed. Where cross-border flows are required in countries that do not provide instant payments, it may be advisable to allocate this part of the cash flows to a single cash pooling bank.

Hence, treasurers and cash managers are typically managing a hybrid model by using a global player as the cash pool bank for all non-instant payment flows while using local/regional banks for the instant flows.

A potential benefit of such a model is that since global banks are well-versed in international regulations, and local/regional banks have a good understanding of local compliance requirements, corporations can take advantage of this dual expertise to navigate complex regulatory environments more effectively.

4. Conclusion

New technologies are changing every facet of our lives, and treasury and cash management is no exception. New technologies are creating a very different landscape in this industry than most corporations are used to.

Companies that manage cash across borders are now able to choose who manages that cash and how, be they global banks as was the case in the past or local/regional players as new technologies have made possible (or a hybrid of the two for markets that are still instituting these technologies). But change is the only constant in this environment.

New technologies such as APIs have even made it possible for treasurers to manage their cash pools directly from their ERP systems, eliminating the need to navigate multiple banking platforms. APIs can also automate routine tasks such as fund transfer, reconciliation and reporting, reducing the need for manual intervention and minimizing the risk of error. Furthermore, the new technologies come with enhanced security, ensuring that finan-

cial data is transmitted securely between systems. Their capabilities will further accentuate the ability of local and/or regional banks to even more aggressively compete in this market, since they will be able to leverage those capabilities to innovate and differentiate their offerings to rival with those of the global banks.

As those who are familiar with this market will be fully aware, modern treasury is about more than just pooling cash. It is about optimizing liquidity in real time by maintaining visibility across accounts (made possible by real-time reporting via APIs) and building a resilient banking model to optimize working capital across regions through real-time information and forecasts.

Regional banks such as Belfius can now offer specific added value by linking local banks to global pooling. The newcomers to the global marketplace realize that they will need to provide more than mere cash management services, and become true partners to their clients. Today's clients demand more, and thanks to the new technologies and the new competitive environment they have created, they might finally get what they demand and deserve.

Future of Payments

The evolution of **customer interaction** and future expectations

Jorissa Neutelings,
Chief Digital Officer,
ABN AMRO Bank N.V.

ABSTRACT

In an era where customer expectations are fluid and technology defines experience, banks must evolve from rigid structures to adaptive, customer-centric ecosystems. In this article, I explore the imperative for financial institutions to become “liquid companies” - organizations that seamlessly integrate data, technology, and trust to meet clients in their own digital spaces. I outline the strategic shifts required to deliver hyper-personalized, secure, and intuitive interactions, and argue that trust, once a passive asset, must now be actively engineered into every customer touchpoint. Through insights on digital convergence, intelligent friction, and organizational redesign, the article offers a roadmap for banks to lead the future of customer interaction.

1. Introduction

In the near future, customers will no longer visit your digital estate – you will be invited into theirs. A space that is fluid, ever-shifting, and shaped by context. Clients will move seamlessly across channels, devices, and moments. So how are we at ABN Amro - a solid, structured, and well-established organization - preparing for that future? What does it take to meet customers where they are, without losing who you are? This article explores how to embrace that shift, and why becoming a liquid company is no longer optional, but essential.

2. Customer expectations are no longer static - they flow

The modern customer journey is no longer linear. Clients move fluidly across channels, devices, and contexts. In banking, this means that the traditional segmentation of services - retail, private, and business - must give way to a more integrated, responsive model. The rise of mobile-first interactions, real-time service expectations, and hyper-personalization demands a rethink of how we define and deliver value.

Tomorrows' customers expect seamless experiences that transcend traditional boundaries. They want to start a transaction on their mobile device, or rather by just posing a question via a conversational interface, continue it on their preferred messaging app, and complete it in a sometimes needed Teams call with a financial advisor without any friction. This fluidity requires banks to break down internal silos and create a unified view of the customer. By leveraging data analytics and AI, banks can anticipate customer needs and deliver personalized experiences that drive loyalty and satisfaction.

2.1 Technology is not a channel - it is the experience

Digital is no longer a support function; it is the primary interface between bank and client. Whether through apps, web platforms, or embedded services, technology defines the customer experience. Our internal Digital Interaction Strategy shows that clients prefer mobile for simple tasks and desktop for complex ones. This insight must guide how we design journeys, not just where we place buttons.

The integration of technology into every aspect of the customer journey is essential. From AI-powered chatbots that provide instant support to blockchain technology that ensures secure transactions, the tools we use shape the customer experience. Banks must invest in cutting-edge technologies and continuously innovate to stay ahead of the competition. By doing so, they can create a seamless, intuitive experience that meets the evolving needs of their customers.

2.2 The future of client interaction is liquid

The "liquid company" is not a metaphor - it is a mandate. As I outlined in my speech at the 2025 "Identity week", a liquid company adapts in real time, wrapping itself around the customer's needs, not the other way around. This means dissolving silos, enabling data fluidity, and designing systems that anticipate rather than react. In banking, this translates to seamless transitions between personal and business views, proactive financial advice, and zero-friction onboarding.

A liquid company is agile, responsive, and customer-centric. It leverages real-time data to make informed decisions and quickly adapts to changing customer needs. This requires a cultural shift within the organization, where employees are empowered to take ownership of the customer experience and collaborate across departments. By embracing the principles of the liquid company, banks can create a dynamic, customer-focused environment that drives growth and innovation.

- **If you need to start**: start with identifying how many different views of a singular customer there are in your organization. Begin by mapping out the various touchpoints your organization has and wants with customers. Understand the data sources and systems that hold customer information.
- **If you need to accelerate**: create a unified customer experience. Leverage data analytics and AI to anticipate customer needs and preferences. Ensure that transitions between different channels and touchpoints are smooth.
- **If you want to reach the pinnacle**: implement interactive always on, data-fed platforms that are decoupled and can play well with systems of other vendors.

2.3 Trust is the new currency - and it must be engineered

With the rise of generative AI, cyberattacks, war threat, and deepfakes, trust is under siege. According to Edelmans' Trust Monitor '25, European consumers are increasingly skeptical of digital interactions. Banks must respond by embedding trust into every layer of the experience - through zero-knowledge identification, secure-by-design architecture, and transparent data use.

Trust is the foundation of any successful customer relationship. In the digital age, banks must go above and beyond to protect customer data and ensure the security of their transactions. This includes implementing robust cybersecurity measures, providing clear and transparent communication, and fostering a culture of trust within the organization. By prioritizing trust, banks can build lasting relationships with their customers and differentiate themselves in a competitive market.

2.4 Trust means customer friction - how to leverage that

In a digital world where convenience is king, friction is often seen as the enemy. But in banking, friction can be a feature - not a flaw - when it signals trust. Customers do not just want speed; they want safety. They want to know that their data is protected, their identity is verified, and their financial future is secure. In a recent study, we found that customers view keeping their money safe as their number one priority. In second place, they want the bank to keep their identity and data safe. In our long existing role as "keepers of the vault" we must balance seamlessness with security.

This is where intelligent friction comes in. By designing authentication and verification processes that are intuitive yet robust - like app-based sign-ins, biometric ID, and conversational AI that confirms intent - we transform friction into reassurance. Our strategy is not to eliminate every step, but to make every step meaningful. In doing so, we turn trust into a competitive advantage. Customers who feel safe are more likely to engage, share data, and deepen their relationship with the bank. In the liquid company, trust is not a compliance checkbox, it is a design principle.

3. Digital trends are converging - and they demand convergence in strategy

From hyperpersonalization to ambient banking, the trends shaping the next decade are not isolated, they are interlinked. Our "Ecosystem Strategy" outlines how device-specific behaviors and modular architecture can support differentiated, yet unified experiences. The challenge is not just to adopt these trends, but to orchestrate them into a coherent, scalable strategy.

The convergence of digital trends presents both opportunities and challenges for banks. On one hand, it allows for the creation of highly personalized, context-aware experiences that delight customers. On the other hand, it requires a holistic approach to strategy that considers the interplay between different technologies and customer touchpoints. By adopting a unified strategy that leverages the strengths of each trend, banks can create a seamless, integrated experience that meets the needs of their customers.

3.1 Organizations must be designed for flow, not control

To deliver on these expectations, banks must evolve structurally. The liquid company requires fluid teams, modular platforms, and decision-making at the edge. This means rethinking governance, KPIs, and even leadership roles. It also means embracing ecosystems - partnering with Fintechs, platforms, and even competitors to deliver value where the customer is.

The traditional hierarchical structure of banks is no longer sufficient to meet the demands of the modern customer. Instead, banks must adopt a more flexible, agile approach that allows for rapid innovation and adaptation. This includes creating cross-functional teams that can quickly respond to customer needs, implementing modular platforms that enable seamless integration with third-party services, and empowering employees to make decisions at the edge. By doing so, banks can create a dynamic, customer-centric organization that is well-positioned for the future.

4. Banking must lead the way - because we are the custodians of trust

As financial institutions, we are uniquely positioned to lead this transformation. We hold the trust, the data, and the responsibility. But we must act with urgency. The future of client interaction is not a trend; it is a tectonic shift. And those who fail to adapt will find themselves irrelevant.

Banks have a unique opportunity to lead the way in the digital transformation of customer interaction. By leveraging their trusted position, vast amounts of data, and deep understanding of customer needs, banks can create innovative, customer-centric experiences that set them apart from the competition. However, this requires a commitment to continuous innovation, a willingness to embrace change, and a focus on building lasting relationships with customers. By doing so, banks can not only survive but thrive in the digital age.

5. Conclusion

The future of customer interaction is not a distant possibility; it is an immediate necessity. As custodians of trust and data, banks like ABN AMRO must lead the charge in redefining how value is delivered in a digital-first world. By embracing fluidity in structure, strategy, and technology, and by embedding trust as a design principle, banks can create seamless, secure, and meaningful experiences that resonate with tomorrow's customers. My message to companies that want to develop for a prosperous future: becoming a liquid company is no longer optional, it is essential for survival and relevance.

Future of Payments

Issuing and investing in **tokenized financial assets**: what to look out for and why

Phoebus L. Athanassiou,
Senior Lead Legal Counsel, European Central Bank, and Associate Professor, Goethe Universität, Frankfurt am Main[1]

ABSTRACT

The asset tokenization phenomenon – broadly defined as the conversion into digital and marketable tokens of certain rights, and their holding and trading through distributed (shared) ledgers – is taking capital markets by storm, promising to leave a lasting imprint on the issuance and trading of financial assets. This paper seeks to (i) explain, in lay terms, what asset tokenization is about and where its true novelty resides, (ii) provide a high-level account of how asset tokenization and its outcomes are regulated in the E.U., the U.S., and the U.K., and (iii) draw attention to the importance of the private law treatment of tokenized assets in circumscribing the rights that prospective investors can expect to acquire in them, if they should decide to add them to their portfolio, and the obligations that their issuers can expect to incur vis-à-vis their holders, if they should decide to issue those assets. As will be explained in this article, depending on whether certain tokenized assets (also) qualify as regulated financial instruments under the law of the jurisdiction of their issuance, asset tokenization may leave unaffected their fundamental legal nature as objects of regulation, and the obligations of their issuers. For tokenized assets that do not qualify as regulated financial instruments, the nature of the aforementioned rights and obligations is difficult to determine, absent dedicated legislation, inevitably impacting on the decision to issue or to invest in them, as the case may be.

1. The views expressed here are purely personal. This paper builds on some of the author's observations in "Asset tokenisation, asset tokens and their E.U. regulation, present and future," (forthcoming in Journal of International Banking Law and Regulation).

1. Introduction

The financial press is, as of late, rife with discussions on asset tokenization, the last in a chain of innovations to have swept through capital markets in recent years. The asset tokenization phenomenon encompasses, on the one hand, the transformation into "tokens"[2] (i.e., digital representations) of pre-existing assets, and their hosting on distributed ledger technology (DLT)[3] platforms, where tokenized assets are held and traded, and, on the other hand, the creation (i.e., the issuance), *directly* on innovative technology platforms, of (financial)[4] assets in digital form, followed by their trading through those platforms. It follows that, unlike asset tokenization, which merely adds a technological spin to a traditional (financial) asset, by putting its record of ownership on a distributed ledger, the creation of so-called "endogenous" (i.e., native) tokens that double as (financial) assets will bring into existence *entirely new objects* of law.[5] What one needs to appreciate from the outset is that the transformation of real-world assets, including valuable commodities, into digital and marketable tokens is nothing new, and that the true novelty of tokenized assets, in either of the above two forms, is in their issuers' use of DLTs and DLT platforms, either to *create* them or to also *host* them, for trading purposes. As digital tokens come in many different shapes and forms, serving different legal and economic purposes,[6] and as the author is a financial lawyer, the emphasis of this work is on tokens that qualify as digital financial assets (i.e., are intangible financial assets) and that have the economic characteristics of "securities", i.e., equities, bonds, and other types of marketable securities that derive their value either from an ownership right or, failing that, from a mere contractual claim. Settlement assets (defined as those that are intended as means of payment) are beyond the scope of this paper.

2. What are the promises and risks of asset tokenization?

Asset tokens (and the process of their creation) hold considerable potential, largely sourced in their underlying DLTs and their various attributes. In particular, asset tokens promise issuers and investors alike greater cost-efficiency (not because DLT network costs are negligible but because of the lower intermediation costs associated with the issuance, management, and trading of assets through distributed ledgers),[7] lower barriers to investor access (thanks to the global scope of shared ledgers, and their investment opportunities-related "democratizing" effects), programmability (defined as "the ability to encode specific rules and automated actions directly into the digital tokens themselves"),[8] and round-the-clock trading, also outside the business hours of conventional regulated markets and trading venues. Other tokenization-specific benefits for prospective investors include infinite divisibility, fractional ownership,[9] portfolio diversification, and the easier use of tokenized financial assets as collateral.

It remains the case that, at the time of writing, DLTs had yet to be tested in a mainstream financial markets context, with various questions outstanding regarding their operational risk management, governance, and scalability: given the intimate link between tokenized assets and their underlying DLTs, to invest in the former is, inevitably, to take certain risks on the latter, the extent of which is difficult to assess but will, in any event, depend on their design and core characteristics (e.g., whether these are permissioned or *permissionless*).[10] Headline risks include operational and security vulnerabilities (e.g., in the face of hacking, software defects,

2. In as much as it conjures up the idea of a bearer instrument, the term "token" is something of a misnomer, as "tokens" are invariably digital and account-held, not corporeal assets, amenable to physical control.
3. Distributed ledger technologies are technical arrangements that facilitate the storage, across a network of computers (nodes), of a digital record of transactions and balances, making up a shared, immutable database that can serve as a single, shared "source of truth" regarding those transactions and balances. They encompass, amongst others, blockchain technology, which denotes a data validation structure where batches of validated transactions (or updates) are arranged in blocks, linked sequentially to one another, through cryptographic tools, to preserve the full history of transactions over the data or assets recorded in a shared ledger.
4. Asset tokenization can also be of non-financial nature (as in the case of off-plan real estate or digital products/tools for gamers).
5. References, in this paper, to "tokenized assets" are to both of these types of financial assets.
6. There are security tokens (representing fractional ownership in assets, much like transferable securities), utility tokens (serving multiple functions but not normally considered as securities), payment tokens (such as e-money tokens and stablecoins, serving as means of exchange), and hybrid tokens (possessed of the features of more than one category of assets).
7. Asset tokenization enables direct, peer-to-peer trading of tokens as representations of assets whose trading currently requires middlemen.
8. See World Economic Forum, 2024, "Code as law: tokenization of assets and the paradox of programmability," October 28, https://tinyurl.com/2zthm9zu.
9. The reference is to the re-packaging into smaller, digital parcels of higher value assets, such as shares in venture capital funds or artworks, previously inaccessible to anyone other than institutional or private investors.
10. Permissionless blockchains are decentralized networks where no restrictions apply on participation in the consensus process used for the validation of transactions and data, whilst permissioned blockchains are closed networks, where only previously designated parties may participate in the consensus and data validation process.

and weaknesses in user interfaces), legal and compliance risks (such as those arising from money laundering and terrorist financing), and, last but not least, settlement finality risks.[11]

Setting aside the operational parameters of asset tokenization, and the risks that this may come with, I explore, in the remainder of this paper, the questions of (i) the fundamental legal nature of securities-like tokenized financial assets, and (ii) their regulation, in select jurisdictions.

3. Tokenized assets: legal nature and regulation

One of the difficulties that prospective investors in, or issuers of, tokenized assets may face in deciding whether to invest in, or to issue them, respectively, is the lack, in most jurisdictions, of dedicated regulation governing asset tokenization, and the difficulty of applying to them, and to their underlying technologies, extant financial services regulation, which was not designed with DLTs and tokenized assets in mind. This is despite the fact that, over the last few years, several legislative attempts have been made to regulate certain aspects of the issuance and marketing of tokenized and native digital assets.

At the level of the European Union (E.U.), the entry into force, in December 2024, of the Markets in Crypto-assets Regulation (MiCAR)[12] signaled the E.U. legislator's ambition to experiment with the establishment of a pioneering regime for "crypto-assets" (although the MiCAR does not govern the tokenization process per se, nor does it cover all types of tokenized assets – see infra). Earlier, individual Member States, including Germany,[13] France,[14] Italy,[15] and Luxembourg,[16] had adopted limited national frameworks, recognizing to tokenized assets and to native digital assets a legal status similar to the one enjoyed by traditional financial instruments, including securities and bonds issued and traded on regulated markets, or regulating the use of DLTs in a financial services context.

In the U.S., the year 2024 signaled a watershed in domestic digital asset regulation, with the passage of the Lummis-Gillibrand Act – which establishes a framework for token classification, subject to the oversight of the Commodity Futures Trading Commission (CFTC) (save for those digital assets that are deemed to be securities, which fall within the purview of the Securities and Exchange Commission (SEC), and clarifies the SEC's role in regulating security tokens with clear investment contracts – and the Digital Commodity Exchange Act, which, building upon existing legislation (including the Commodity Exchange Act of 1936),[17] empowers the CFTC to regulate digital asset exchanges as "designated contract markets" and "swap execution facilities". U.S. Legislation adopted in 2022 (in the form of the Responsible Financial Innovation Act), had already introduced rules to govern digital assets, seeking to integrate them into the extant banking and tax legal frameworks.

In the U.K., the Government published, in April 2025 – only a few months following the entry into force of the MiCAR – draft legislation aiming to establish a dedicated regulatory framework for crypto-assets,[18] while the U.K.'s Financial Conduct Authority (FCA) published discussion and consultation papers

11. The reference is to the risk of a transfer or funds or securities being unwound on account of the insolvency of one of the participants to it or of the system responsible for the processing of that transfer.
12. Regulation (E.U.) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L 150/40.
13. In Germany, issuers may issue dematerialized bearer securities that are entered into a central electronic securities register maintained by a crypto securities registrar, solely on a DLT platform.
14. In France, issuers may issue security tokens in registered (not bearer) form, provided those tokens are not exchange-listed or traded. France has also created a sui-generis type of optional regime for the supervision of token-related activities by financial intermediaries, and their licensing, under the auspices of the French securities supervisor. French law distinguishes between tokens that are securities (hence, subject to the full force of national securities legislation), and other digital tokens, to which the above-mentioned optional regime applies. Finally, the French legislator has introduced a specific regime to govern the transfer of ownership and the pledging of crypto-assets.
15. In Italy, national law regulates the legal effects of electronic timestamps and the electronic storage of title documents on DLT platforms.
16. In Luxembourg, the issuance, conversion, or transfer of unlisted "dematerialized bonds" is possible where those bonds are registered on accounts held on a DLT platform. Moreover, custodians may use secure electronic registration devices, including distributed electronic registers or databases, in which case the transfers operated through them are equivalent to wire-transfers between securities accounts.
17. This is the Act that established the CFTC's basic regulatory framework for derivatives markets.
18. The reference is to the (draft) Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) Order 2025, which aims to bring within the regulatory fold issuers of crypto-assets, crypto-exchanges, and relevant stakeholders, including dealers and agents, by creating new types of "specified investments" in, amongst others, qualifying crypto-assets, such as token on a blockchain representing an interest or a right in an equity, a bond, or a derivative contract), and "specified activities", such as issuance and custody of crypto-assets, the operation of trading platforms, and agency trading and arranging, which can only be engaged in where the relevant party holds an authorization form the U.K.'s Prudential Regulation Authority and/or the FCA, under Section 19 of Financial Services and Markets Act 2000.

setting out its proposed regulatory approach to tokenized assets,[19] identifying their three main types (namely, security tokens, utility tokens, and e-money tokens), each with different use cases and legal characteristics.[20]

As also explained below, none of the aforementioned legislative initiatives encompasses rules specifically covering the tokenization phenomenon and its outcomes. And yet, although securities-like tokenized assets (including asset tokens) were not, at the time of writing, subject to a customized, comprehensive legal regime in any of the jurisdictions explored in this paper, this is not to say that tokenized assets in those jurisdictions were unregulated: as explained below, those that qualify either as securities or as other types of regulated financial instruments are to be treated as such, irrespective of their tokenization. Otherwise put, the tokenization of security-like financial assets does not automatically result in their distinct legal treatment as objects of law, any more than it can carve them out from the fold of general financial law.

Starting with the E.U., the MiCAR includes *no* definition of tokenization (nor of tokenized assets, as such), despite regulating the various types of "tokens" that, for the purposes of E.U. law, qualify as "crypto-assets". The DLT Pilot Regime Regulation,[21] which establishes a harmonized "regulatory sandbox" for the trading and settlement of financial instruments using DLTs, was the closest that the E.U. legislator came, at the time of writing, to regulating certain aspects of the asset tokenization phenomenon (including the issuance of tokenized assets/asset tokens but, significantly, not their private law attributes): the only reference to asset tokenization in the harmonized E.U. legal framework was in one recital to that Regulation.[22] The better view is that tokenized assets that qualify, legally, as "financial instruments" and, more specifically, as transferable securities, will remain subject to MiFID II[23] – the backbone of the E.U.'s financial markets regulatory framework – regardless of their tokenized form. Such tokenized assets, their issuers, and any entity engaging in activities relating to them would also remain subject to the "full set of E.U. financial rules".[24] To determine whether a tokenized asset can be a MiFID II transferable security,[25] regard should be had to the test in Article 4(1)(44) of MiFID II, according to which certain cumulative conditions need to be fulfilled: first, the financial asset in question (whether or not it is tokenized) should be *negotiable* on the capital market; second, it should *not* be an instrument of payment; and third it should be security, i.e., a share in a company, a bond, or another form of securitized debt, or any other security granting to its holder the right to acquire or sell any of the above or giving rise to a cash settlement determined by reference to transferable securities. It follows that the tokenized form of a particular asset will, in principle, change nothing to its legal treatment, as a matter of E.U. financial law, if the underlying asset (in the case of a tokenized asset proper) or the asset token itself can be classified as a MiFID II "financial instrument".[26] It also follows that, security-like tokenized assets that fall within the MiCAR's definition of "crypto-assets", will remain subject to MiFID II (as will their issuers),

19. See discussion paper DP25/1 of May 2, 2025 (on the regulation of crypto-asset activities), as well as consultation papers CP25/14 & 15 of May 28, 2025 (on stablecoin issuance and crypto-asset custody and on a proposed prudential regime for crypto-asset firms, respectively).
20. In a nutshell, security tokens represent ownership or investment rights in underlying assets, and are akin to traditional securities, such as stocks or bonds; utility tokens do not, generally, represent ownership or investment rights, whilst e-money tokens are settlement media, and are akin to electronic money.
21. Regulation (E.U.) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (E.U.) No 600/2014 and (E.U.) No 909/2014 and Directive 2014/65/E.U., OJ L 151, 2.6.2022, p. 1–33.
22. See DLT Pilot Regime Regulation, Recital 3, which defines the "tokenization of financial instruments" as "the digital representation of financial instruments on distributed ledgers or the issuance of traditional asset classes in tokenized form to enable them to be issued, stored and transferred on a distributed ledger."
23. Directive 2014/65/E.U. on markets in financial instruments, amending Directives 2002/92/E.C. and 2011/61/E.U. The MiFID II defines "financial instruments" by reference to the list of examples in Article 4(1)(15) thereof. That list includes "transferable securities", "money-market instruments", units in UCITS, and various types of derivative contracts (see MiFID II, Annex I section C. Article 4 of MiFID II sets out distinct definitions of, amongst others, transferable securities, money market instruments, structured deposits and exchange-traded funds).
24. See Commission Staff Working Document, Impact Assessment Accompanying the MiCAR Proposal, Brussels, September 24, 2020 SWD(2020) 380 final, p. 6. The reference is to the Prospectus Regulation, the Transparency Directive, the Market Abuse Regulation, the Short Selling Regulation, the Central Securities Depositories Regulation, and the Settlement Finality Directive.
25. The E.U. law concept of "transferable security" is fairly broad (and it has been approached liberally, also by the Court of Justice – see, by way of example, the Opinion of Advocate General Richard De La Tour of September 5, 2024 in Case C 627/23, Commune de Schaerbeek and Commune de Linkebeek v Holding Communal SA, ECLI:EU:C:2024:692, §§60, 66 and 70), without regard to whether a security is represented by a physical certificate or merely registered electronically (in the case of intermediated securities) or, indeed, created on a distributed ledger: the better view is that, as long as an instrument is negotiable on the capital market, even if not freely negotiable (a term only used in Article 51 of MiFID II, but not in the actual definition of transferable security), and not a payment instrument, it will qualify as a transferable security.
26. A different conclusion would raise the obvious risk of a circumvention of mandatory E.U. legal rules, through the medium of asset tokenization, by all accords an undesirable outcome.

as long as they are, also, MiFID II "financial instruments".

In the U.S., no tokenized securities-specific rules applied at the time of writing. However, although DLT-based tokenization may be a novelty, the issuance of instruments representing a security is not. The extent to which asset tokenization will be subject to regulation will depend on the nature of the tokens involved: where those tokens qualify as securities, within the meaning of the *Howey* Test,[27] tokenization will trigger the application of federal securities laws (notably, the Securities Act of 1933 and the Securities Exchange Act of 1934) as well as of registration requirements, with the involvement of the SEC and, possibly, also the CFTC and FinCEN. Otherwise put, a tokenized U.S. law security will remain a security, with all the legal implications derived therefrom (in the sense that the SEC will require tokenized securities to comply with existing securities laws, and that exchanges/brokers dealing in such securities will be expected to register with the SEC), irrespective of whether a given instrument is on- or off-chain.[28] Even if a token is *not* a security, it is always possible that it can qualify as a "security receipt", distinct from the underlying security held by the token distributor; alternatively, if it does not provide its holder with legal and beneficial ownership of the underlying security, a token can be a "security-based swap", within the remit of the CFTC. At the time of writing, the SEC was considering a conditional exemptive order, to allow firms to use DLTs to issue, trade, and settle tokenized securities.[29]

In the U.K., asset tokenization is only subject to the applicable financial services regulation if it concerns financial assets and/or activities falling under the purview of the FCA, the leading crypto markets' regulator in the U.K. Financial assets that meet the above requirement include transferable securities and money market instruments. Certain other types of assets (such as exchange tokens and other types of tokenized assets) fall outside the regulatory perimeter, as there is, as of writing, no dedicated, domestic regime in place to cover them. Apart from the draft legislation referred to earlier in this section, which aims to address some of the specificities of tokenized assets, a Property (Digital Assets etc.) Bill had been tabled before Parliament, to clarify the property law status of certain digital assets, including crypto-tokens.

4. The case of unregulated tokenized assets and the importance of private law

For those tokenized assets that cannot be subsumed under the family of regulated financial instruments (in particular, those to which the "securities" label cannot be attributed), the questions of determining their legal nature and the rights and obligations that these come with can be difficult ones to answer. Can these be the objects of property rights or do they merely represent contractual claims against their issuer? What formalities would a valid transfer of title over them require? Can those tokens be used to transfer property rights (or, alternatively, claims) in the real-world assets that those tokens represent? How does the insolvency of their issuer or depository affect the rights of their holders? Can they be used as collateral and how is that collateral to be created and enforced? And what limited rights, if any, can the holders of unregulated tokenized assets create in them? Some of the above private law questions may also pose themselves in the case of tokenized assets that *do* qualify as regulated financial instruments (and, more specifically, as securities), since traditional concepts of property and contract law need not be easy to apply to all types of tokenized assets; but it is especially in the context of unregulated tokenized assets that answering those questions poses the greatest of challenges, absent, in their case, of any concrete reference points for the application, by analogy, to them of those concepts.

27. The reference is to a venerable jurisprudential test, established in the U.S. Supreme Court case of SEC v. W.J. Howey Co. (1946), to determine whether an investment qualifies as a "security", for the purposes of U.S. law. This test is based on the fulfilment of four cumulative criteria: (i) there needs to be an investment of money, (ii) that investment need to be "in a common enterprise", c) there should be "an expectation of profits", and d) those profits should be derived from the efforts of others.

28. See https://tinyurl.com/4ehseckw

29. See Peirce, H., 2025, "A creative and cooperative balancing act," Speech at the 31st International Institute for Securities Market Growth and Development, Washington D. C., May 8.

As a general proposition, one of the obvious perquisites for investments in novel asset classes is a basic understanding of the rights or claims accruing to their holder. In the case of tokenized assets (especially, those that do not readily fit into any of the existing types of financial assets), the property law effects of an entry in a registry operated by a market intermediary, such as a CSD, and the legal preconditions for the contractual creation and enforcement of a security interest over them are matters that will need to be explored and clarified before these assets can be issued, in significant amounts, and relied upon by investors, either domestically or, a fortiori, across borders in their dealings. For new categories of financial assets, such as tokenized assets, legal uncertainty on the above fronts is likely to obstruct their take up, condemning them to only unfold a fraction of their true potential on account of the legal ambiguity surrounding the status of their ownership and the modalities of their deployment, e.g., as collateral. The regulatory status quo seems, to this author, unsatisfactory, and could, considering the promises of tokenized assets, warrant action in the direction of the more comprehensive regulation of the substantive private law applicable to them. Less ambitious regulatory solutions or reliance on legal interpretation and the *mutatis mutandis* application to them of conventional financial and private law regulatory concepts are unlikely to represent viable long-term solutions, apt to meet the challenges that tokenized assets pose, and do not look set to greatly help their issuers and investors reap the full benefits that these may come with, as per the account earlier in this paper.

5. Concluding remarks

As explained in this paper, the tokenization of financial assets with security-like characteristics in the jurisdictions explored in it does not automatically mean a change in their legal treatment, merely because it would entail their representation on a distributed ledger, as tokenized assets, or their issuance, storage, or trading in tokenized form, as asset tokens, any more than it can exempt them from the application of regular financial services law. Reassuring as that may sound, it is not clear that the status quo is ideal, as it creates scope for some tokenized assets to remain in the shadows of financial regulation. Although the tokenization of security-like financial assets need not affect their regulatory treatment, whether by exempting them (and their issuers) from compliance with securities laws or by making them exclusively subject to such dedicated legal frameworks as may exist in certain jurisdictions (to the extent, that is, that those exist in the first place), question marks subsist regarding their private law treatment, as objects of the law of property and contract, in particular. These will only be definitively set aside once dedicated legislation is adopted to regulate their private law status. Until then, both prospective issuers and investors may have difficulty to decide whether to create or invest in them, respectively, not on account of their lack of interest in them but due to the legal uncertainty that accompanies them, as a new and ill-defined legal phenomenon.

The likelihood of the introduction, in the short to medium term, of such dedicated legislation will largely depend on the success (or otherwise) of pilot projects around the world, and on how broad the range of use cases will become, overtime. What will strengthen the case for dedicated legislation is a scenario where asset tokenization gradually finds its way in mainstream finance, in particular through the issuance of tokenized securities (both equities and bonds) but, also, commodities. The launch, in 2021, by the Swiss Stock Exchange, of the SDX platform for digital assets was an early indication of the potential of the tokenization phenomenon to, eventually, spread to the world of equities and bonds, hence, beyond the universe of initial coin offerings and payment tokens. The recent legislative initiatives in some of the jurisdictions covered in this paper suggest that the likelihood of regulatory intervention to facilitate the issuance of tokenized assets is far from negligible, although it is premature to make any predictions regarding their efficiency in promoting the asset tokenization phenomenon. In those jurisdictions where the legal and regulatory frameworks currently in place impose upon market intermediaries (such as the CSD operators of securities settlement systems) the responsibility for issuing certain types of securities, legislative action will be indispensable to cater for the use of DLTs as the necessary foundation of any asset tokenization process.

Legislative action aside, what will, ultimately, shape the fortunes of the asset tokenization phenomenon is the extent to which tokenized asset platforms will be allowed access to the central bank-operated payment infrastructures (including the large value payment system), by being granted the right to hold settlement accounts with the relevant central bank: the DvP settlement in central bank money of tokenized assets held on a DLT platform would

greatly boost the efficiency of those platforms and decrease the costs and risks of their holders, reinforcing, in the process, their fortunes and the popularity of tokenized assets amongst investors and issuers alike. The alternative is settlement in some form of commercial bank money, including through recourse to privately-issued stable-coins, the latest (and the most potent) in a series of challengers to the supremacy of central bank money as the settlement asset of choice for wholesale financial transactions. Asset tokenization could, therefore, contribute to shaping not only capital markets but, also, the world of money, one of the most hotly disputed battlefields of our times.

Future of Payments

Cross-border Payments beyond 2027: how to **crack speedy progress**

Magali Van Bulck,
Head of Public Policy (EMEA), Wise

ABSTRACT

International payments remain incredibly slow, expensive, and hard to do. This inefficiency stems from financial systems built for domestic needs and the creation of complex correspondent banking chains. The G20 Roadmap for Enhancing Cross-Border Payments was launched in 2020 to tackle this issue. It aims to make international payments faster, cheaper, more accessible, and transparent by 2027 for retail/wholesale payments and by 2030 for remittances. The Roadmap is built on four pillars: cost, speed, access and transparency. This article argues that urgent action is needed in two foundational areas: access, and transparency, or more specifically, direct access for non-bank payment service providers (non-banks) and price transparency. These are prerequisites for achieving broader reductions in price and increases in speed.

1. Introduction

International money flows are the lifeblood of the global economy, facilitating global trade, enabling remittances that support 800 million families and friends, and fostering economic growth and financial inclusion worldwide. In 2025, consumers are expected to send U.S.$4.1 trillion in cross-border payments. Business will add another U.S.$18.7 trillion to that. By 2029, those numbers are projected to rise to U.S.$6.9 trillion and U.S.$23 trillion respectively[1] – a huge opportunity by all accounts.

This is one of the key reasons that it is our conviction that sending money should be as easy as sending an email. While moving text around the world is now virtually free and instant, moving money remains often incredibly slow, hard, and expensive. Historically, financial systems were primarily built with domestic needs in mind. Sending money from one country to another still involves a circuitous chain of banks across a number of borders – a system we are largely reliant on even today. The problem with this setup is that more middlemen in the money movement process means additional costs and delays, and ultimately, it is the end customer who loses out and ends up having to wait longer for their money to arrive.

The good news is that cross-border payments are having a moment. Deprioritized while countries were busy mending - or in some cases building - their own payment systems, 2020 saw these international money flows gain mainstream attention. Launched in November that year, the G20's Roadmap for Enhancing Cross-Border Payments recognized the profound challenges payments face when they are no longer domestic: they remain inefficient, costly, and opaque. That is why the 20 biggest economies in the world came together to set ambitious targets to make payments faster, cheaper, more accessible, and transparent by 2027 for retail and wholesale payments and 2030 for remittances.

Making these payments flows more efficient, faster, cheaper, and more transparent is crucial. At Wise, a global technology company focused on moving and managing money internationally, we are fundamentally aligned with this vision and believe urgent action is needed, particularly in the critical areas of price transparency and direct access for non-bank payment service providers (non-banks). Why these two areas? Because the G20 Roadmap for Enhancing Cross-Border Payments is built on four interconnected pillars: access, transparency, price, and speed. Progress in the first two - access and transparency - is a prerequisite for achieving meaningful reductions in both price and speed.

2. Foundational framework for global payments

The Roadmap, overseen by the G20, the Financial Stability Board (FSB), and the Committee on Payments and Market Infrastructures (CPMI), sets out targets for expanded and democratized access to payment systems, as well as for a reduction in the cost of remittances to <3% by 2030 and retail payments to <1% by 2027. According to the FSB, no single retail use case meets the target of <1%[2] and the World Bank estimates that the average remittance cost from G20 countries was 6.6%[3] in 2024 - more than double the target of <3%.

Genuine improvements in cost and speed cannot be achieved without addressing fundamental structural issues in how payments are processed and how their costs are disclosed. If payment systems continue to be a restricted playground for some players - mostly banks - rather than accessible to all, that select group will continue to set the pace of innovation and dictate the cost. If all players were allowed to participate, true competition could create incentives for the whole industry to be more efficient, lower costs, and improve speeds in a bid to keep their end users happy. In an ideal world, all payment providers would also disclose the real costs of cross-border payments to their customers, giving them the information and tools to find better deals if it turns out that the (usually hidden) cost is deemed too high, or if the payment speed is too slow.

In 2024, Wise published its first annual G20 Report to highlight progress, or lack thereof, against the

1. Economic study by Edgar Dunn & Company, September - November 2024.
2. FSB, 2024, "G20 Roadmap for Enhancing Cross-border Payments - Consolidated progress report for 2024," Financial Stability Board, October, https://tinyurl.com/9zhyu3wb.
3. World Bank, 2024, "Remittance Prices Worldwide - Quarterly Report December 2024," December, https://tinyurl.com/2s3k5pd9.

Roadmap KPIs set out for (price) transparency and for expanding access to payment systems to non-banks.[4] While the Roadmap's KPIs are generally clear, Wise's analysis indicates that price transparency remains a significant blind spot in most countries. This is partly because the transparency pillar combines both speed and price and the FSB assesses progress towards the KPIs without looking at speed and price individually. Most frustratingly, progress is measured inadequately, by focusing on a subset of providers already deemed "transparent" about costs, skewing results. This would be similar to reporting on a country's unemployment rate by only including those who consider themselves to be in active employment – pointless. The transparency KPI should be split up, so both speed and price transparency get the scrutiny they deserve, exposing progress and gaps more accurately.

3. Direct access for non-banks: competition, speed, and savings

Generally, payments work well domestically - within one country, within one currency. But as soon as money starts crossing borders, it becomes slow, expensive, and hard to do because of the hoops money has to jump through in the correspondent banking chain. Even though the industry as a whole may not have cracked cross-border payments just yet, the progress for domestic payment systems has been significant. They have generally evolved to be instant and low cost, and many consumers and businesses now have baseline expectations that all payments should meet those criteria. The good news is that those domestic payment systems can be the facilitators for cross-border payments.

One of the most impactful ways to reduce costs and increase the speed of cross-border payments is by enabling direct access to those well-functioning, instant domestic payment systems for non-banks. This sets all institutions - whether they have a banking license or not - up to become the connecting tissue between all domestic payment systems around the world, in addition to the domestic benefits a direct connection can bring.

Historically, access to national payment infrastructures has been largely restricted to licensed banks. This has created a system where non-banks must rely on traditional banking partners for settlement, adding additional layers of cost, complexity, and delay. With increased regulatory scrutiny, many banks re-evaluate and even terminate partnerships with non-banks, leading to even fewer ways non-banks can facilitate payments for their customers. By limiting access, however, the forces of competition disappear, innovation is stifled, and it leaves end users worse off.

But times are changing. In 2018, Wise became the first non-bank to get access to the U.K.'s Faster Payment System (FPS) and obtain a settlement account with the Bank of England. Getting that direct access led to an immediate price drop of 20% for all Wise customers transacting in GBP and a 98% increase in payment speed. The Bank of England was a pioneer, setting the bar high for other countries in terms of democratized access. It has been a huge success story. There used to be just 11 banks with direct access to FPS, compared to roughly 40 today. Since then, progress has snowballed elsewhere, too.

The U.K. is no longer a lone open door. Wise's G20 Report assessed the degree of direct access granted to non-banks across G20 members, examining eligibility criteria, regulatory support, and operational integration. It shows an optimistic picture. Brazil, China, the European Union, Indonesia, Mexico, South Korea, and Türkiye are now leading the way in expanding direct access. Brazil's Pix system, for instance, even mandates participation from authorized payment institutions with a significant customer base and allows direct access for many others, fostering an inclusive financial ecosystem.

However, progress is not yet universal. India, South Africa, Argentina, Saudi Arabia, and particularly the United States, have not displayed a noticeable step change. India's United Payments Interface (UPI) - while a hugely innovative success story - currently excludes remittance-focused firms from direct access, requiring partnerships with banks. The U.S. maintains its status as the only G7 economy not to be advancing direct access. Despite the Federal Reserve's revised approval system for Master Accounts in 2022, the monopoly of banks as the gatekeepers to the payment system has remained in place.

4. https://tinyurl.com/3vnkj957

4. The transparency blind spot: lifting the lid on hidden fees

While direct access is crucial for the well-functioning of the payments infrastructure, price transparency is arguably the single biggest factor keeping the cost of remittances and cross-border payments artificially high. Despite claims in the FSB's October 2023 Progress report that "98% of remittance services in the dataset are transparent about total fees and FX margin for senders" – a claim repeated in the 2024 edition, where the FSB deemed 99% of providers "transparent" – Wise contests this figure. We believe it bears no resemblance to what actually goes on in the market and significantly misrepresents what is common practice in industry. In reality, the majority of cross-border payments are not transparent when it comes to the total cost of that payment, with the FX margin completely obfuscated.

The issue stems from the prevalent practice of undisclosed padding of FX rates, where financial institutions embed hidden fees within the exchange rate they offer to customers, often advertising "0% fee" or "best rate". This practice makes it extremely difficult for consumers or businesses to understand the true cost of their transactions and effectively compare providers. Independent research by Edgar Dunn & Company in 2024 indicated that consumers and small businesses paid over U.S.$250 billion in hidden exchange rate markups globally. That number is projected to rise to U.S.$318 billion by 2027, the deadline for the implementation of the G20 Roadmap. Action could not be more urgent.

Additionally, the FSB's Progress Reports do not adequately consider whether FX fees are obscured or whether domestic price transparency regulations are effectively enforced. But one of the FSB's G20 Roadmap taskforces, the Legal, Regulatory and Supervisory (LRS) Taskforce, has started to address this blind spot. In collaboration with the OECD, a stock take of the market has been commissioned, as well as a request for comments on transparency. Armed with the results of these two materials, the LRS Taskforce will convene again in December 2025 to decide on next steps.

Fortunately, we are also starting to see national glimmers of hope. The E.U.'s Payment Services Regulation (PSR) proposals include detailed requirements for disclosing FX markups, expressed as a percentage and monetary amount over a foreign exchange benchmark rate, to be displayed no later than the moment the payer authorizes the transaction. This new E.U. law is poised to become a gold standard for disclosure requirements, driving prices down.

The E.U. opted for more prescriptive rules, having learned from its experience in enabling the market to clean up its act on its own - it does not work. These prescriptive rules are intended to address a market failure. However, other markets, like the U.K., are opting for market-led approaches with set consumer outcomes. The U.K. regulator, the Financial Conduct Authority, mandates firms' adherence to the Consumer Duty, to deliver fair value to consumers and facilitate consumer understanding. In 2025, the FCA's Consumer Duty focus areas saw it dedicate a market study to firms' behavior when it comes to price transparency in cross-border payments. The outcome of that study resulted in the issuing of good and poor practice guidance. Unsurprisingly, half of all poor practice examples included the use of undisclosed FX markups, clearly showcasing the FCA's expectation that this market practice should cease to exist.

Other approaches, such as the one adopted by Brazil, are also sending encouraging signals: they require firms to display a "Total Effective Value", inclusive of all charges applicable to a cross-border payment. While the concept has not reached its full potential, the intention is there: enabling people and businesses to effectively compare providers and understand the total cost. Even countries outside of the G20, like the Philippines, a large remittance recipient, have introduced similar concepts - all aimed at greater transparency - which in turn reduce costs.

Conclusion: thinking beyond 2027

As much as we would like to highlight more progress, it is illusory to think that we will achieve all the goals set out in the G20 Roadmap by 2027. However, both access and transparency are low-hanging fruit, ripe for progress towards making money movement as easy as sending an email.

It is indeed encouraging to hear Klaas Knot, the former Chair of the FSB, state that, "we are intensifying our engagement at the regional level." How-

ever, while the path to a more efficient, transparent, and inclusive global financial system is clear, progress remains uneven. It is right to focus on regional initiatives to tackle inequalities in the financial plumbing and to help speed up the progress of countries that are lagging behind. Solidarity, best practice sharing, and increased impetus under a new presidency, and a new Chair, will breathe extended life in the Roadmap, well beyond 2027. It may provide the blueprint for better, more email-like cross-border payments, but its success hinges on the collective will and decisive action of its Members to drive real change.

Much like building a global highway system, it is not enough to simply pave new roads (innovation) or declare that traffic flows smoothly (misleading transparency metrics). We must also ensure that all vehicles, regardless of their make or model (bank or non-bank), have fair access to the highway, and that all tolls and charges are clearly displayed at every turn, rather than being hidden in the fuel price. Only then can we guarantee a truly efficient, equitable, and stable journey for global payments.

Future of Payments

The future operating model for Payments

Stephen Peters, Head of Enterprise Payment Solutions, FIS

Alan Verschoyle-King, U.K. Payments Practice Lead, Projective Group

ABSTRACT

Artificial Intelligence (AI) is reshaping financial services operations in ways most banks had not anticipated. This new technology will allow smaller, nimbler competitors to take on the more established players and provide faster, cheaper and more efficient payments services. Major banking institutions are responding to this challenge by investing significant sums in this new technology. However, the focus, at least at this stage, seems to be predominantly on how the technologies can be used to improve certain aspects of the value chain, such as increasing personalization and speed and reducing human intervention and errors, rather than on the overall infrastructure upon which the entire business model is built. This article aims to change the dialogue and focus the attention of the leaders of banking institutions to establish the kind of payments operating model that will not only allow AI, and its derivative technologies, to be utilized, but will place it as part of the foundation upon which the operating model is based.

1. Introduction

Artificial Intelligence (AI) and Generative AI (GenAI) are transforming our lives in ways that concern even their creators. Those changes are so significant that even those who are their advocates have suggested that regulators must somehow find ways to provide guardrails around them to prevent them from destroying humanity [Hern (2023)]. The founders of such technologies are not alone in being concerned about their potential implications for humanity: regulators and policymakers the world over are looking at the ways in which these new technologies might impact the future, and their own citizens specifically, and at how they should react, with the European Union being among the first movers [E.U. (2023)].

The implications are severe, with some anticipating massive job losses in many sectors, which would have implications far beyond mere economics [GS (2023)]. Recent assessments have become more measured, with some questioning whether the new technologies are as devastating – or alternatively as useful - as some had thought [Marcus (2025)]. Even skeptics acknowledge that AI will be transformational, if not actually developing as quickly as many had thought or be as concerning as many had feared.

Whether AI delivers on all its promises or not, it is already changing how businesses operate and meeting growing client needs without it will become impossible. Like mobile banking, AI and GenAI are becoming need-to-have rather than good-to-have. All businesses that wish to remain in the competition will need to find ways to successfully integrate them within their business strategies. And financial services is no exception, with investments of in excess of U.S.$125 billion expected from this sector by 2028 [Statista (2025a)].

AI is transforming finance across multiple areas, with some expecting it to take over from how a client is serviced all the way through to how investments are selected and managed. That transformation is already underway, with numerous Wealth Management companies already applying AI in different parts of their value chains [Weaver (2025)]. While certain aspects of the value chain currently demand human intervention, these will increasingly be automated as AI develops.

One of the areas in financial services that has been most impacted by this new technology is payments, with the old order being completely upended by newcomers. The new FinTech players have used the power of online and mobile technologies to force banks to change how they operate and what they charge.

AI will be even more transformative in payments operations. While most attention focuses on how AI will change client service and the payments business, few have examined how the operations that support these services must be modified to keep pace.

The banks we work with are struggling to incorporate AI's power into their businesses, but without spending the time necessary to think about just how transformative this could be. This explains why AI implementations are falling short of expectations. The focus of this article is on how AI will help shape the future operating model of tomorrow's payments leaders. It is the operations behind the services that will ensure clients experience a seamless process, and that is where the real competitive advantage lies.

This article examines how AI will impact payment operations, and focuses on the operational excellence necessary to make the industry's transformation a reality.

2. How AI will impact payments

AI is transforming payment operations across many areas, but the three drawing the most executive attention are fraud detection, new payment methods, and improving the payment process itself. While not exhaustive, these three represent the most common AI applications that executives are considering.

2.1 Fraud detection and prevention

Fraud detection models, which have typically been reliant on historical patterns and have, therefore, missed changes in the status of counterparties, have not been as effective as needed, predominantly because the technology evolved for both attacker and defender, and the costs and impacts tended to be asymmetric. AI models have improved the process somewhat by allowing banks to detect suspicious activities in real time, but even this has not been totally effective, with online payment fraud surpassing U.S.$44.3 bln in 2024 [Statista (2025b)].

The challenges caused by autonomous AI agents

Autonomous AI agents are tools that are permitted by individuals or organizations to make purchasing, payment, and investing decisions on their behalf. The challenge these agents cause is that determination of their authenticity by the tools available today is not easy, since authentication and payments infrastructures as a whole are built with the human counterpart in mind. Payment providers must ask themselves: "how will they develop their tools to deal with AI agents representing individuals who are now hidden behind them?"

GenAI promises to improve current AI models by allowing fraud data to be queried in natural language and assist with pattern creation and recognition, which should help mitigate false declines as well as fraud itself.

How GenAI will perform in practice remains to be seen, but its credentials certainly seem more promising than its AI predecessors.

2.2 New payment methods

While AI-powered personalization is not new and has been applied effectively across industries, payments is only now becoming a beneficiary. Beyond enabling banks to develop new products and services based on reliable client data, AI is advancing major new technologies such as biometric payments, face-pay, and voice-activated payments. As an increasing number of airline passengers have become accustomed to using so-called "smart gates" to avoid long airport queues, they are beginning to ask why such technologies are not available to them when paying for goods and services.

Technology companies are providing these payment capabilities, with Apple and the Ant Group, the parent company of Alipay, being among the most well-known. Such payment methods are already prevalent and well-developed in countries like China.

Regulations such as Europe's GDPR make biometric technology applications more complex, but this challenge is being overcome. The future looks promising when established banking giants like JPMorgan are helping clients "pay by smile"! [J.P. Morgan (2024)].

2.2.1 Emerging payment instruments

Digital payment rails are fundamentally different from the rails that banks operate today. Stablecoins backed by regulated reserves, wholesale and retail central-bank digital currencies (CBDCs), tokenized deposit coins, and on-chain repo networks deliver sub-second finality and 24 × 7 liquidity. Cross-border projects like BIS Nexus, mBridge, and the Regulated Liability Network bypass correspondent banking chains entirely. These instruments introduce two design variables that legacy workflows cannot handle: programmability where logic executes with the payment and atomic settlement across jurisdictions.

AI makes these new payment instruments practical at enterprise scale. Machine-learning models predict liquidity demand across tokenized and fiat pools, routing flows to the cheapest rail in real time. Natural-language agents convert heterogeneous smart-contract terms into human-readable controls for Operations and Audit. Anomaly-detection engines identify behavioral outliers in CBDC ledgers hours before rule-based monitors would react. AI-driven orchestration abstracts Treasurers and Product Managers from rail selection completely: the system decides when to use a stablecoin bridge, when to stay on RTGS, or when to trigger an FX-dematerialized swap under unified governance.

In short, while digital currencies provide new opportunities, operationalization of them into client products presents a series of challenges. Establishing a technology stack brings costs, risks, and other complexities. AI provides the operational intelligence to bring the opportunities to market safely and profitably.

2.3 Payment process improvements

The most expensive, yet at the same time most valuable, asset of any financial institution is the time of its expert staff. AI becomes valuable when it helps staff avoid wasting their time on non-revenue generating and repetitive tasks and is expected to deliver exactly that benefit.

In payments, AI helps bank employees spend less time reviewing and approving payments and more time providing better, value-generating services for clients and the banks themselves. Consider the cur-

rent processes that a simple international money transfer must navigate to reach its destination – AI and other new technologies can streamline every step.

Banks' payments teams can already share payment behaviors with client-facing advisors to help them sell other products that are better suited to their clients' needs, including loans, investments, and cards. GenAI makes those recommendations even more personalized.

These capabilities are moving up the value chain to include AI identifying the most efficient transfer/payments channel and make the approval process become less human-intensive and more frictionless. Clients can be confident in the knowledge that the fastest, safest, cheapest, and most efficient, route will be chosen for their payment, irrespective of the communication method used.

Access to these technologies also reduces error rates, including ensuring that transactions adhere to the latest regulations. Clients rarely praise a bank when all is running smoothly; it is only when a simple error causes issues that they make their opinions known. AI mitigates that risk.

Just as the internet helped FinTech/InsurTech companies compete in areas previously dominated by major global financial services organizations, AI will fuel a competition boom between established players and newcomers. Many of these newcomers could become white label service providers for established banking institutions that do not want to make the investments in their infrastructure necessary to compete actively. Regardless of how the future industry landscape develops, AI will have transformed it.

The history of online and mobile banking shows that global banking institutions will continue to make their own investments in AI, attempting to maintain their competitive advantage against their peers, but many of these efforts will prove insufficient.

The question is not whether AI will transform payments services delivery by major banking institutions and their nimbler smaller competitors - it is whether enough thought has gone into planning and executing this transformation and what the anticipated future payments operating model will look like.

3. Operationalization of AI in payments

These benefits will significantly impact client service, and clients will feel the impact of the application of the new technologies on their payments journeys. But the established players often overlook a critical issue and risk replicating the same mistake they made during the FinTech boom by applying new technology where possible without rebuilding their operations to benefit fully from it.

The FinTech revolution offers a cautionary tale about what is coming, not only in payments but across banking more broadly.

When online and mobile banking became possible, more established players tried to apply these new technologies to their legacy systems. They invested vast sums of money on transformation programs, which typically meant adding a middle-ware layer on top of their legacy systems. This new layer allowed banks to integrate online and mobile technologies with their core back-end banking systems, but it left those legacy systems intact.

Anyone who has worked in banks or helped with their transformation initiatives knows just how rigid, siloed, and expensive legacy systems are.

The operational challenges these legacy systems created in payments include what most of us still experience: high exception rates, limited straight-through processing (STP) via domestic and cross-border rails, and poor end-to-end visibility and root cause traceability.

The alternative was to replicate what the FinTechs did: rebuilding entire operations from scratch with the new technologies in mind. This approach allowed FinTechs to be significantly more flexible as the technologies improved and to generate client-centric cultures based on the new technologies. But, most of the major established payments providers did not pursue this option during the FinTech revolution, as is evident today.

Few would deny that FinTechs created niches that established players found difficult or impossible to penetrate, regardless of one's view of FinTech valuations.

The challenge is that these nimbler players' success stems as much from their mind-sets as the core technologies they use. Numerous established players have created their own FinTechs, only to

close them down. These include examples in payments, with HSBC deciding to close its payments app Zing within its first year of operation: Zing's failure had little to do with the underlying technology and instead reflected a misunderstanding about networked business.

What is needed is not a separate entity applying new technologies, but a complete overhaul of legacy systems and a change in the mindset of the people working in these banks.

Generating the benefits highlighted in Section 2 is worthwhile. But the possibilities that AI and its derivatives could create will be significantly greater than those coming from merely applying these technologies ad-hoc.

AI must be applied in the "hard" areas of banking and payments - payment processing, reconciliation, compliance operations, STP, exception handling, and liquidity forecasting - for established players to derive full benefits.

Redesigning entire payments operations with AI at their core will not be easy or cheap, but banks will realize it is necessary. Established players cannot keep trimming the edges and expecting different outcomes. New players will eventually take away not only loss-making clients, but profitable ones too - and it might be too late for established players to respond.

Many banking giants are in the same place they occupied in the 2010s when challenger institutions emerged. Those nimbler tech-savvy competitors established themselves with new technologies at their core and significantly impacted the industry. We believe the AI revolution will cause several established banks to disappear.

Banks face the same choice again. Invest in large transformational projects that will apply new technologies only to "soft" parts of their businesses, or put AI at the core of their operations. The decision depends on their investment appetite, capability maturity to execute on their vision, and risk tolerance.

The next few years will be fascinating as established players compete with a new group of digital, AI-enabled competitors.

Should banks make the necessary investments, AI could serve as a real-time orchestration engine, predictive decision layer, and execution support framework, across the entire payments value chain.

3.1 Core areas where AI could be embedded structurally

As banks modernize their payments systems, static rules and batch processes are no longer sufficient. AI does not just add horsepower, it changes how decisions get made, how exceptions are resolved, and how systems respond in real time to pressure, competition, and regulation. This section outlines key structural domains where AI enables sustainable competitive advantage, not just automation.

3.1.1 Payment operations

Payment flows are too complex for rigid workflows. Multi-rail networks, shifting formats like ISO 20022, and rising expectations for instant resolution, are stretching traditional systems. AI can intervene upstream, validating, repairing and routing, without requiring armies of analysts. More importantly, it shifts processing from best efforts to context-aware optimization, where systems understand what is happening and act accordingly. AI's ability to learn from historical patterns to detect anomalies, using those patterns to dynamically make corrections and continuously optimize routes, will transform payment provider operations (Table 1a).

3.1.2 Risk, compliance, and regulatory oversight

Rules-based controls struggle when the rules change faster than the systems. Static lists cannot catch dynamic risks. AI closes that gap by learning behavioral patterns, flagging anomalies early, and reducing false positives. This is critical with cross-border exposure and richer data formats under ISO 20022. Gartner (2023) highlights AI's utility in AML and fraud detection, where model-based approaches outperform static thresholds.

AI's ability to use behavioral models to identify evolving risk beyond encoded logic, reduce false positives and improve accuracy using contextual scoring, and undertake real-time conformity checks and breach predictions, will make AI an essential tool for any payments provider serious about risk and compliance (Table 1b).

3.1.3 Treasury and liquidity management

Real-time payments and market volatility break legacy liquidity models, especially when cash is fragmented across systems and legal entities. AI forecasts based on live flows, not lagging reports. It also automates margin, funding and exposure

Table 1: Comparison of traditional and AI-enhanced approaches

a: Payment operations		
Function	**Traditional approach**	**AI-enhanced approach**
Error detection and enrichment	Basic field validation and static lookups (e.g., IBAN-to-BIC)	AI learns from historical patterns to detect anomalies and enrich contextually in real time
Smart repair of rejected transactions	Pre-defined correction rules	AI predicts likely causes and dynamically corrects based on prior outcomes
Adaptive routing (fee, FX, failure likelihood)	Static logic trees or fixed rules	AI continuously optimizes routes based on live fee, risk, and SLA data
b: Risk and compliance		
Anomaly detection	Rules-based thresholds and alerts	Behavioral models surface evolving risks beyond encoded logic
Sanctions screening and risk scoring	Static list and geography filters	Contextual scoring reduces false positives and improves precision
SLA tracking and ISO 20022 monitoring	Manual reconciliation post-fact	Real-time conformity checks and breach prediction
c: Treasury and liquidity management		
Intraday liquidity forecasting	EOD balances or regression models	AI learns from real-time flow to update intra-day predictions
Parsing statements and agreements	Regex or RPA over structured docs	NLP parses unstructured inputs with context
Margin/collateral alerts	Static thresholds and daily checks	Event-based alerts triggered by live shifts in exposure
d: Servicing and workflow automation		
Triage of ops issues	Severity codes and static queues	Dynamic prioritization by root cause and urgency
Support summaries	Rule-based templates	Natural language summaries improve speed and clarity
Workflow optimization	Periodic reviews	Continuous analysis recommends changes based on throughput and error
e: Data intelligence and decision support		
KPI and trend analysis	Manual BI dashboards	AI identifies cross-signal trends, suggests actions
Decision support	Static spreadsheets	AI assistants answer ad hoc queries and simulate scenarios
Signal synthesis	Siloed tooling	Multimodal models merge ops, customer, and finance data

checks across messy, partial, data sets. McKinsey (2022) suggests that machine learning could improve liquidity predictions by double-digit margins in high-volume environments.

AI's ability to learn from real-time flows to update intra-day predictions, use Natural Language Processing (NLP) to parse unstructured inputs with context, and trigger event-based alerts based on live shifts in exposure, will profoundly impact on how payments providers manage liquidity (Table 1c).

3.1.4 Servicing and workflow automation

The biggest drag on payments processing is not systems but the human-to-human handoffs that slow everything down. Exceptions, escalations, and follow-ups can inundate Support teams. AI reduces that load by triaging issues, generating summaries, and surfacing true root causes. The goal is not to remove people, but to reduce the noise they waste their time on. BCG (2023) shows real-world deployments at tier-1 banks delivering up to 30% reduction in support tickets after deploying AI triage systems.

AI achieves this by prioritizing dynamically by root cause and urgency, using NLP summaries to improve speed and clarity and make recommendations based on continuous analysis of throughput and error (Table 1d).

3.1.5 Data intelligence and decision support

It is not always about faster execution, but better decisions. Operations and Product teams often have data but lack clarity. AI links signals, flags root causes, and answers 'why?' without needing a Data Scientist in every room. The shift is from dashboards to dialogue: systems that tell you what is going wrong and what to do about it.

AI allows payments providers to replace manual business intelligence dashboards with capabilities that identify cross-signal trends and make actionable suggestions. Static spreadsheets and siloed tooling can be replaced by assistants that respond to ad-hoc queries and multimodal models that merge operational, client, and financial data (Table 1e).

3.2 Risks and limitations of AI in payments operations

While AI adds power, it also introduces new risk classes. Unlike deterministic systems, AI operates probabilistically, which increases agility but reduces predictability. In financial operations this tradeoff that must be governed tightly.

Payment providers need to understand these trade-offs:

- **Hallucination and model uncertainty**: generative models sometimes return plausible sounding but incorrect outputs. In payments, this could mean false field mappings or misinterpreted regulations. No unsupervised AI should operate in a control-critical function without layered verification.
- **Opaque decision-making**: black-box models cannot easily explain themselves. If a routing engine or fraud filter behaves unexpectedly it erodes trust and may breach compliance requirements around explainability [FCA (2024)].
- **Data sensitivity and leakage**: broad data ingestion[1] means exposure. Without strong redaction and data isolation, sensitive information can leak, especially when integrating third-party models. Regulators such as the European Banking Authority [EBA (2024)] have expressed concerns about this issue and published guidelines for managing emerging AI risk.
- **Skill gaps and over-reliance**: teams may over-trust outputs or under-question results. AI becomes a risk if staff are not trained to challenge or correct it. Training in prompt design, model behavior, and override protocols, is essential.
- **Regulatory ambiguity and model risk**: model risk frameworks are evolving rapidly. Some AI tools will be reclassified as material models, requiring the same validation and oversight as credit or pricing models. The European Central Bank (ECB) and the Prudential Regulatory Authority (PRA) are expected to tighten expectations.

1. According to Tim Mucci of IBM: "Data ingestion is the process of collecting and importing data files from various sources into a database for storage, processing and analysis. The goal of data ingestion is to clean and store data in an accessible and consistent central repository to prepare it for use within the organization." https://tinyurl.com/y4pj6jnk

Table 2: Model classification and risk tiering

Tier	Characteristics	Use-cases	Controls
Tier 1: Critical	Client-facing or regulatory exposure	Routing logic, sanctions, fraud	Full validation, live monitoring, SME sign-off
Tier 2: Material	Supports decisions, not sole source	Liquidity forecasting, repair recommendations	Human-in-the-loop, traceability
Tier 3: Advisory	Internal efficiency, low risk	Summaries, knowledge retrieval	Sandboxed, lightweight QA

3.3 Controls and governance framework for AI in payments operations

AI cannot be managed like traditional technology. It needs oversight, validation, and clear accountability. In Table 2, we provide a simple classification framework for assessing the risk of deploying AI in payments systems and how banks might mitigate that risk. Below, we provide a proposed RACI framework (Table 3):

- **Expert-in-the-loop design**: subject matter experts must review high-stakes use-cases in a process where responsibilities are split between AI, which processes scale, and humans, who retain accountability. Exceptions should be logged and reused for retraining.
- **Validation and testing lifecycles**: models should be tested on historical cases before deployment, drift and false positive/negative rates must be tracked, and alerts must be set for out-of-pattern behavior post-deployment. Everything must be documented.
- **Data governance and input controls**: data must be validated before use, and access must provided on a role-based basis, with logs maintained of all access and training histories. Where possible, synthetic or anonymized datasets should be used.
- **Explainability and auditability**: where explainability is non-negotiable, interpretable models or overlays with post-hoc explanation tools should be used, with inference logs and rationales maintained.
- **Training and culture**: teams must be trained to challenge models, build muscle memory [2] around prompt testing, override logic, and escalation protocols, making AI augmentation, not automation, the norm.
- **Regulatory engagement**: AI usage should be tracked and documented, with models mapped to applicable regulations and a regulatory liaison designated for ongoing engagement.

This RACI framework for AI controls in payments operations will aid those who wish to effectively apply these to their operations.

4. The visibility gap: intelligence, resiliency, and the role of AI

Based on our experience, most providers tend to react to events, rather than be proactive. When a payment failure occurs, they find out about it in the same way that their clients do: the reconciliation does not balance, the service level agreement (SLA) breach email hits, or the regulator comes knocking. But by then, they are in damage control mode, not prevention.

The frustrating part of this is that it does not have to be that way, since the data required to prevent such failures already exists within the boundaries of these organizations. The problem, of course, is that

2. According to Cleveland Clinic, muscle memory is "the ability to recall and execute movements that have been learned through repetition." https://tinyurl.com/2tm8zzjy

Table 3: RACI matrix: AI controls in payment operations

Control Area	AI team	Ops	Risk	Tech	Audit	Model Risk	Legal/ Reg
Model tiering	R	C	A	C	I	C	I
Human-in-loop	R	A	C	C	I	C	I
Pre-deployment Testing	R	C	C	A	I	A	I
Live monitoring	R	A	C	R	I	C	I
False +ve/false -ve analysis	R	A	C	C	I	A	I
Input controls	A	C	C	R	I	C	I
Explainability logs	R	A	C	R	C	A	I
SME training	A	R	C	C	I	C	I
Docs and logs	R	C	A	C	I	A	C
Reg mapping	C	I	R	I	I	C	A
Audit alignment	C	I	A	C	R	C	C

Legend: R: responsible, A: accountable, C: consulted, I = informed

few have a holistic view of this data, since they tend to be scattered across legacy platforms, buried in regional systems, and/or fragmented across channels. The Operations teams have all the pieces but cannot see the whole picture until it is too late.

Applied correctly, AI can indeed help Operations teams solve such data challenges. And that is because when you pair AI with modern data flows, you are not just collecting information anymore, you are watching your payments systems come to life. You can see queue depths spike before they crash, you can catch exception patterns before they cascade, and you can spot routing delays that signal bigger problems coming down the line.

Imagine what would happen if Operations teams had access to real-time operational intelligence. It would mean they had access to live dashboards that identified and highlighted the health signals that mattered, be able to see queue depth, exception spikes, routing delays, and liquidity signals that told them when trouble was brewing, and receive predictive incident alerts that could catch the subtle patterns they knew about but could not monitor around the clock. It would also mean that they could see rising repair rates, channeling performance deviations and unusual straight-through processing drops that precede bigger failures.

And end-to-end transaction telemetry tracks payment velocity, interbank handoffs and forecast mismatches on inbound flows, before they become tomorrow's headaches.

The critical element that most banks are still not acting on is that their intelligence layer is only as good as the data foundation beneath it. This is where modernization efforts like ISO 20022 and unique end-to-end transaction references (UETRs) - a string of 36 unique characters attached to payment messages sent on the Swift network to help with transparency and tracking - become game-changers. ISO 20022 provides richer, more structured, data moving through systems, improving both interpretability and traceability. UETRs enable full end-to-end transaction tracking across correspondent chains, letting AI build a complete picture of every transaction's journey.

With the Digital Operational Resilience Act (DORA) pushing European banks toward stronger operational resilience, this shift from reactive to predictive operation has become a regulatory necessity. When regulators expect you to demonstrate operational resilience and business continuity, showing up with after-the-fact reconciliation reports is insufficient. DORA changes almost everything about how we think about payments resilience. AI integrated with real-time infrastructure and enriched

message formats delivers earlier detection, faster triage, and controlled recovery from operational disruptions.

The culture shift demanded is for payments providers to move from being reactive (cleaning up messes) to being proactive (preventing them).

The question that they, therefore, need to ask themselves is not any longer whether their payments infrastructures can handle always-on expectations, but whether they can monitor issues in real-time rather than having to continue to explain to clients why their monies have been lost in the system. In a world where payment delays make headlines and regulatory scrutiny is intensifying, we would argue that operational foresight is no longer optional.

5. Barriers to adoption

While we firmly believe that applying AI as the foundation upon which new payments operating models are based will have a transformational impact on how payments operations can, and should be structured, we are in no way underestimating the challenge. We are fully cognizant of the fact that AI momentum in payments tends to hit a wall when it meets organizational reality. The biggest barriers are seldom technical: they are predominantly human in nature, manifestations of which are visible in program delays, risk-averse governance, and missed opportunities to scale.

Nevertheless, despite challenges including the fact that there are still many organizations that are grappling with the basics of how to apply AI meaningfully, there are a number of leading banks that are today attempting to apply AI within their payments operations. To help them on this journey, we have highlighted below a number of the areas that could impede their progress. It is by no means exhaustive, but should spotlight what we believe to be some of the main issues that those aiming to execute such projects should be cognizant of.

- **Lack of executive familiarity with AI:** while AI makes the top ten list of concerns that keeps senior financial executives awake at night, few of these executives are actually as knowledgeable about its capabilities as they should be. They are certainly on the whole aware of AI's potential, but many still see it primarily as a tool (like a database) or a "futurist" concept (like blockchain), rather than as something that could, and should be embedded into core processes. It is certainly not viewed by enough executives as a capability that can have strategic implications. And until it is, the necessary investments in AI to make it a transformative capability across functions, will not be made.
  We are currently seeing a number of financial services organizations establish Chief AI Officer roles, but these tend to have very broad mandates, which makes instituting the kind of strategic analysis, investment, and granularity of execution that is necessary very difficult. To successfully execute on the agenda of applying AI to payments operations, you need experts who can make the strategic case necessary for senior executive buy-in, and there are few organizations that have these.
- **Governance**: financial services organizations operate in a highly regulated environment, which means they need to be able to explain what went wrong when regulators come knocking. Consequently, they are typically very careful about applying models whose decisions/recommendations they cannot easily explain to regulators. Given that AI does not behave like traditional software, and generates outputs that are probabilistic, not deterministic, it often makes banks very cautious about how they apply it. In the case of payments, fraud, or sanctions, the banks need to be absolutely certain that the algorithms make not only the correct decisions but also ones that can be justified in front of the regulators.
- **Team fragmentation**: talent gaps within and across silos, combined with fragmentation of teams, exacerbate the challenge of instituting AI within financial services organizations. AI ownership is often split across data science teams, business lines, IT, and Operations, with no single group clearly responsible for knowledge delivery. This fragmentation slows progress and increases the risk of misaligned or duplicated effort. Talent gaps persist not just in engineering, but in Product, Operations, and Risk functions, where the understanding of how to integrate AI into workflows is often still limited. Many banks experiment in silos then struggle with coherent adoption models. They are challenged to scale beyond proofs-of-concept and treat AI as a capability to be tested, not as an infrastructure layer to be deployed, governed, and iterated on, limiting its strategic value.

- **Data governance and integration:** a major challenge for most organizations, financial or otherwise, trying to apply AI to their operations is access to quality data. Without good data that is clean, structured, and accessible, AI will not deliver value. The old adage of "garbage in, garbage out" certainly applies to AI systems. Legacy systems often lock this data away, or present it in formats that are difficult for AI models to interpret, or in a chronically incomplete state with large gaps in the data. It is typical for AI projects to spend 50% of their time on data scrubbing and correction. Integration work further consumes time, money, and organizational patience.
- **Operational issues:** much of the infrastructure in place today, especially within mid-sized and/or traditional institutions, is not built to support real-time orchestration or event-driven triggers. This makes it difficult to deploy AI where it is needed most - in the transaction flow itself rather than around the edges.

In addition to the company-specific challenges, the technology itself also has some limitations that payments providers need to keep in mind. One such limitation is the fact that Large Language Models (LLMs) are not suitable, due to hallucinations, for deployment in precision-heavy (non-stochastic) environments, which might lead to payments data being predicted into existence. But foundation models are making progress, and with appropriate guardrails we expect to see improvements in reliability and predictability in the near term.

Of course, AI is more than GenAI, and financial services organizations should avoid equating all AI with LLMs. There are use cases where traditional machine learning, decision trees, or simple classifiers, outperform the latest foundation models. For example, most fraud engines have deployed AI models for years, but they are classifier rather than generative models. Choosing the right model for the job, rather than chasing the most advanced model, is the best route.

So, in summary, one of the biggest barriers to AI in payments is not the technology itself but the operating model around it. Moving past that will require not just better tools, but better structures, governance, corporate culture, and leadership alignment.

6. Our strategic recommendations

AI project failures rarely stem from bad technology; more likely they occur when technology enthusiasm collides with operational reality. For example, AI in payments is moving into the flow of funds, but implementations crash when they meet the on-the-ground complexity of this area.

We have found that the following seven approaches can deliver results, but each requires guard-rails, practicality, and adaptability.

6.1 Create living plans, not perfect documentation

Le parfait est l'ennemi du bien (Voltaire)

Many financial services organizations get bogged down trying to create perfect AI architecture documents, spending months debating where the models should live, agreeing what data they should consume, and deciding who will pay the running costs. Meanwhile, competitors are shipping their v0.9 and learning from real implementations.

Payments providers should start with good enough. They should document where each AI model sits in payments repair, sanctions, and treasury, present their data flows, and determine ownership. They then need to treat this as a living plan; review quarterly and update as they learn. Waiting for complete clarity will kill innovation faster than bad AI architecture ever could.

6.2 Avoid the hype

A common mistake that organizations make is trying to force every use case into whatever AI flavor is trending on social media. Needs should be classified honestly and the right technology applied to them. They should not apply the latest technologies simply because they are new. For example, LLMs should be used for free-text search, summarization, or dialogue, whereas deterministic logic should be applied for field checks or routing. Organizations should not over complicate the process, and should use simple rules when these work better.

Hybrid patterns should also be considered - allow LLMs to interpret intent, rule engines to handle processing and approval, and the LLMs to summarize the results. Forcing everything into a single bucket

will result in over-engineering and/or under-performance. The goal is solving problems, not showcasing technology.

6.3 Design for model decay

Frontier models will continue to be released at a furious rate; however, that does not mean that payments providers will need to deploy every single model immediately. They should by all means validate each model if it appears to offer business value, but being a fast follower might be better for the organization than being at the frontier of applying new technologies, unless, of course, the business model calls for it.

Internal models will also decay, be they rules-based, machine learning (ML)-based, deep learning (DL)-based, or LLM-based. The way that payments providers align internal data sources, such as through a retrieval-augmented generation (RAG) should also be maintained and upgraded regularly. Managing model decay will require constant attention.

6.4 Build governance that enables

Risk, compliance, operations, technology, and business should have joint ownership of model approval, drift monitoring, and kill-switch authority. Organizations will need to maintain a single automated inventory of every live model, but adopt time-bound reviews within fourteen days.

When governance becomes an obstacle, shadow models can emerge. Organizations should empower their Chairs to grant interim approvals with post-hoc validations. Speed matters almost as much as safety in competitive markets.

6.5 Invest in visibility

Building comprehensive telemetry from the start, with event streaming, lineage tracking, and real-time dashboards, is key. Models learn faster and break less when engineers can trace every step. However, payments providers should not insist on perfect observability everywhere before modeling anywhere.

Fast-track domains are needed where data is already healthy, while heavy telemetry spending is reserved for the genuine blind spots. Perfectionist approaches to monitoring slow momentum while adding limited value.

6.6 Measure what executives understand

Every deployment should be anchored to three indicators that executives typically recognize: (i) fewer manual interventions, (ii) higher straight-through processing, and (iii) lower avoidable errors. Release gates and bonuses should be connected to these metrics.

Domain-specific KPIs should be layered-in where they matter, such as in liquidity accuracy for Treasury, take-rate improvement for Merchant Services, etc. This will ensure that incentives are aligned with business unit P&L goals while maintaining enterprise-wide coherence.

6.7 Modernize through intelligent wrapping

Legacy functions should be exposed as representational state transfer (REST)[3] endpoints and should be wrapped back with task-specific agents the payments providers can switch on or off. Feature flags make rollbacks painless when something goes wrong.

Recognizing that some twenty-year-old cores will not wrap economically, a two-track approach should be used, with quicker wins obtained through API wrapping and deeper microservice carve-outs undertaken when wrapping costs approach rewrite costs. Perfect integration must not prevent good automation.

6.8 The reality check

These seven approaches can work in an environment that separates pilot cultures from AI-operated financial services organizations, but rigid adherence to this can be as risky as having no approach at all. Banks should build explicit agility into their approach: living plans that evolve, hybrid tooling that matches problems, time-boxed governance that enables progress, rich telemetry that focuses spending, domain KPIs that align incentives, and dual integration tracks that balance speed with architecture.

Organizations that get this balance right will scale AI safely and at market speed. The ones that do not will keep running expensive pilots that rarely, if ever, become operational reality.

3. REST is a software architectural style that was developed to enable interoperability between different internet systems.

7. Summary and Conclusion

The banking and payments industry is splitting into three camps: those building AI-operated infrastructure, those treating AI as just another tool (much like a new database), and those viewing AI as a distraction unlikely to have any impact. These different approaches will determine who survives the next competitive wave, and they distill into several realities.

AI is moving to the center of payments operations

Generative and traditional AI are no longer add-ons that automate isolated tasks. They're becoming the decision-making fabric of routing, risk, liquidity, and client experience. Stronger authentication at the front end, real-time fraud interdiction in the middle, and self-tuning liquidity management at the back end all draw on continuous-learning systems. Banks that fail to embed this layer will face the same margin and speed squeeze that mobile-first FinTechs triggered a decade ago.

Legacy architecture remains the binding constraint

Most large institutions still process high-volume flows on monolithic stacks designed for batch processing, not real-time events. Exception queues, low straight-through processing rates, and opaque status messages remain stubbornly high despite years of "digital transformation". Wrapping cores with middleware bought time but did not eliminate technical debt, AI-centric operations require deeper re-factoring, payment operations demand observability of every event, risk and compliance systems need to consume those events in real time, treasury and liquidity engines must predict funding needs seconds ahead, and data platforms need to broadcast ISO 20022-rich messages tagged with UETRs. Without this rewiring, AI will only operate at the edges.

Governance, not algorithms, creates the bottleneck

Probabilistic outputs, model drift, and opaque reasoning paths unsettle regulators and boards. Supervisory frameworks from the ECB, PRA, and DORA already require auditable controls around every production model. Institutions that scale safely implement cross-functional AI councils spanning Risk, Compliance, Operations, and Technology. They maintain single inventories that auto-record every model release through CI/CD pipelines. They use time-boxed approval cycles so governance doesn't become an organizational parking brake. And they embed human-override kill switches into workflow tools, not bury them in source code.

Execution follows seven practical rules

1. Publish living, AI-first blueprints for each domain and refresh them quarterly.
2. Match tool to task using lightweight rules or classic ML or other approaches where explainability matters, reserving LLMs for unstructured-text problems.
3. Design for model decay by assuming drift and baking re-training into sprint plans.
4. Implement time-bound governance so risk review keeps pace with agile delivery.
5. Invest in observability first; predictive power follows data clarity.
6. Measure what boards understand: intervention minutes, STP uplift, preventable losses.
7. Modernize through intelligent wrapping plus selective rewrites. Expose legacy functions as APIs and let modular agents orchestrate across them, carving out microservices only when wrapping costs exceed rewrite costs.

What comes next?

AI-operated payments infrastructure isn't theoretical. Every component already exists in production somewhere. Event streaming, ISO 20022 data, agent-based orchestration, and model telemetry. What differentiates leaders is treating AI as infrastructure, not experimentation. That means budgeting for plumbing with the same urgency as revenue features. Data quality, observability, controls these mean empowering a single steering forum to make trade-offs in near real time.

Banks that make this shift will slash cost-to-serve, raise reliability and resilience, and unlock revenue opportunities that deterministic workflows can't address. Those that keep layering brittle AI enhancements onto batch-era cores will watch their relevance erode.

The window for decisive action is narrowing. Institutionalize AI as your payments operating model, or watch competitors build insurmountable advantages while you're still running pilots or debating if AI is even real.

References

BCG, 2023, "A generative AI roadmap for financial institutions," Boston Consulting Group, https://tinyurl.com/4u5daxps

BoE/FCA, 2024, "Artificial intelligence in UK financial services – 2024," Bank of England and Financial Conduct Authority, https://tinyurl.com/57fyduhn

EBA, 2024, "Special topic – Artificial intelligence," European Banking Authority, https://tinyurl.com/yfhcpwbb

EPIF, 2017, "Money transfer process – flow of transaction information and funds," European Payments Institutions Federation, https://tinyurl.com/5n8bss4u

E.U., 2023, "EU AI Act: first regulation on artificial intelligence," European Union, June 8, https://tinyurl.com/3pnwctfz

Gartner, 2023, "Market guide for AI in financial crime risk management," https://tinyurl.com/y3zu38ak

GS, 2023, "Generative AI could raise global GDP by 7%," Goldman Sachs, April 5, https://tinyurl.com/bdh4sh4x

Hern, A., 2023, "OpenAI leaders call for regulation to prevent AI destroying humanity," The Guardian, May 24, https://tinyurl.com/2da3sdsa

J.P. Morgan, 2024, "J.P. Morgan payments expands biometric payments to U.S. clients," August 6, https://tinyurl.com/4s5ynduj

Marcus, G., 2025, "The most underreported and important story in AI right now is that pure scaling has failed to produce AGI," Forbes, Feb 19, https://tinyurl.com/466h7s7p

McKinsey, 2022, "The 2022 McKinsey global payments report," McKinsey & Co., https://tinyurl.com/mr282abm

Statista, 2025, "Estimated value of the financial sector's artificial intelligence (AI) spending worldwide from 2023 to 2024, with forecasts from 2025 to 2028," Feb 21, https://tinyurl.com/2ak38p94

Statista, 2025b, "E-commerce payment fraud losses worldwide 2020-2024, with a 2029 forecast," May 15, https://tinyurl.com/2bxb53m

Weaver, L., "Using AI to help fix wealth management," Forbes, May 16, https://tinyurl.com/28pu4x65

Future of Payments

Regulating retail Payments: balancing the **competing interest**

Emanuel van Praag,
Professor of Financial Technology (FinTech) and Law, Erasmus School of Law, and Counsel, Kennedy Van der Laan

ABSTRACT

This article examines the evolving regulatory landscape governing retail payments in the European Union (E.U.), with a focus on the competing legal and societal interests that payment service providers (PSPs) must meet. As digital payments accelerate and regulatory demands intensify, PSPs are increasingly expected to reconcile conflicting objectives across multiple domains. A combination of regulatory burdens, the need to continuously increase payment speed while preventing fraud, and the pressure to balance innovation with financial inclusion means that PSPs operate under persistent legal ambiguity and societal scrutiny. Their ability to navigate these competing demands with transparency, accountability, and fairness is critical to the integrity of the European payments ecosystem.

1. Introduction

In this paper, I discuss the major regulatory trends in European payments, focusing specifically on the competing interests at play.

Regulating payments involves balancing multiple, inherently valid, competing interests. Only through a deep understanding of these competing interests, can leaders in the payments industry, as well as regulators and legislators, fully grasp the complexities inherent within the payments sector and navigate their legal obligations with confidence.

This article is forward-looking, in the sense that I will also discuss trends that are expected to impact European payments in the future.

2. Anti-money laundering compliance versus privacy

The first, fundamental tension we observe in the payments world is between anti-money laundering compliance (and sanctions compliance) and the interest of privacy. This debate takes place at the legislative level, but also in the courts. Anti-money laundering (AML) compliance has an inherent tension with privacy. AML compliance requires a detailed knowledge of all the parties involved in a payment transaction, whereas privacy is the right not to be known, or, at least, not at such a granular level.

And although regulators have in recent years introduced more detailed rules in the Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML Regulation) [E.U. (2024a)], it is still left to the payment service providers (PSPs) to ensure the balance between these two competing demands is maintained.

2.1 Overview of AML requirements

PSPs are required to apply stringent AML compliance measures, including application of customer due diligence (CDD) measures at onboarding (AML Regulation article 20), updating customer due diligence information during the relationship (AML Regulation article 26 sub 2), and the monitoring of transactions (AML Regulation article 26 sub1).

This means that at onboarding and during their relationship, PSPs need to collect information from the payment services users (PSU) to undertake the following (AML Regulation article 20):

- Identify the customer and verify their identity.
- Identify the beneficial owners and take reasonable measures to verify their identity.
- Assess and, as appropriate, obtain information about, and understanding the purpose and intended nature of the business relationship.
- Determine whether the customer or the beneficial owners are subject to targeted financial sanctions.
- Assess and, as appropriate, obtain information on the nature of the customers' business, including the types of activities they are undertaking and their employment.
- Conduct ongoing monitoring of the business relationship, including the transactions undertaken throughout the course of the business relationship, to ensure that the transactions conducted are consistent with the PSPs knowledge of the customer, their business, and risk profile, including, where necessary, the source of funds.
- Determine whether the customer, the beneficial owner, and, where relevant, the person on whose behalf, or for the benefit of, a transaction or activity is being carried out is a politically exposed person, including their family members and close associates.
- Where a transaction or activity is being conducted on behalf of, or for the benefit of, natural persons other than the customer, identifying and verifying the identity of those natural persons.

The amount of information that needs to be gathered can be extensive. In some cases, it is limited to identification documents (AML Regulation article 22), but it can also require detailed information about the origin of someone's wealth and the nature of someone's business (AML Regulation article 25).[1] The transaction monitoring after

1. See more extensively the European Banking Authority (EBA) draft for a Commission Delegated Regulation on supplementing Regulation (EU) 2024/1624 of the European Parliament and of the Council with regard to regulatory technical standards specifying information and requirements necessary for the performance of customer due diligence for the purposes of Article 28(1) at page 34 of the EBA Consultation Paper Proposed Regulatory Technical Standards in the context of the EBA's response to the European Commission's Call for advice on new AMLA mandates, EBA/CP/2025/04, March 6, 2025.

onboarding can also be intrusive, as it requires understanding the underlying logic of transactions.

2.2 Challenging the AML requirements based on privacy protection

This tension between privacy and AML compliance has led to serious debates in courts, where PSUs, based on the General Data Protection Regulation (GDPR), wanted to withhold cooperation with the PSPs AML procedures or to better understand their logic [E.U. (2016)].

For example, in a recent Dutch court case the PSU objected to the PSP making a digital copy of his passport. The PSU suggested that he could present his passport himself to the PSP and that he would provide the PSP with a copy of his passport with a watermark that he made himself. The court reasoned that the PSP needed a copy of the passport in order to maintain evidence that verification of the identity of the PSU took place and that it was necessary for the PSP to have an automated process for this in which the PSP made the copy itself.[2]

In another case, a PSU wanted to understand why he was subjected to an enhanced customer due diligence (CDD) process and based his claim in court on the GDPR.[3] The PSP explained that some transactions triggered a flag under the automatic transaction monitoring system, but that it was an employee, who decided based on this flag and other information that enhanced CDD was required. The court ruled that this was not an automated decision making, because it was the human employee who decided to perform enhanced CDD. This is relevant, because in cases of automated decision-making, the PSU has the right to obtain meaningful information about the logic involved. Moreover, the court ruled that the PSU does not have a right to understand the underlying logic of the transaction monitoring system, because this would be at odds with the societal interest that "criminals" should not know how the transaction monitoring works (Based on GDPR article 23), since they could otherwise game the system.

However, despite these decisions, when a PSU asked the PSP to explain which personal data about him was processed without requiring insight into the underlying logic, this request was granted by the court.[4] Furthermore, at the E.U. level, numerous cases have been brought to the European Court of Justice to determine where the balance between the GDPR and the AML requirements should sit.[5] A really groundbreaking decision was issued in November of 2022, where the E.U. Court of Justice, acting as the plaintiffs, successfully challenged the fact that Ultimate Beneficial Owner register, which was established pursuant to the E.U. AMLD Directive IV (Directive 2015/849), was made publicly available. Basically, the E.U. Court of Justice considered the general objective to combat money laundering as an adequate justification for such a grave infringement on the personal lives and privacy of the persons involved.

In addition to the courts, the European data protection authorities have also become more involved in trying to determine the correct balance between GDPR and AML compliance. For example, the Dutch Data Protection authority issued a fine of €150,000 to International Card Service (the largest Dutch card issuer and a subsidiary of ABNAMRO Bank) for not performing a data impact assessment when remediating the identification of 1,500,000 PSUs.[6]

During the legislative process leading to the new AML package, the European Data Protection Board (EDPB) issued various statements demanding that a proper balance be found between privacy on the on hand and the requirements of AML compliance on the other hand, and especially that the AML legislation should institute adequate safeguards in relation to the processing of personal data and that the EDPB should be closely involved in all delegated rulemaking by the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) and the European Commission (EC).[7]

2. Appellate Court of Amsterdam April 30, 2024, ECLI:NL:GHAMS:2024:1165. A decision of the Dutch Supreme Court on the same question is expected shortly, see ECLI:NL:PHR:2025:260.
3. Based on GDPR article 15 and 22. District Court of the Hague 12 September 2024, ECLI:NL:RBDHA:2024:14477.
4. Appellate Court of Amsterdam July 26, 2020, ECLI:NL:GHAMS:2022:2192. A comparable case was District Court Gelderland November 1, 2022, ECLI:NL:RBGEL:2022:6145.
5. See Request for a preliminary ruling from the Riigikohus (Estonia) lodged on March 21, 2025 – X v Rahapesu Andmebüroo (Case C-222/25, Rahapesu Andmebüroo) and E.U. Court of Justice (Grand Chamber) November 22, 2022, C-37/20 and C-601/20.
6. See website of the Dutch Data Protection Authority, Boete voor creditcardbedrijf ICS na ontbrekende risicoanalyse, January 15, 2024, https://tinyurl.com/2s4yvpcd.
7. See EDPB letters of May 12, 2022 to the Council of the European Union (OUT2022-0030), the European Parliament (OUT2022-0036) and the EC (OUT2022-0035) and the EDPB Letter of May 19, 2021 to the EC (OUT2021-0088).

2.3 The balancing act in the AML regulation

Because of these societal interests, the AML Regulation has, especially when compared to its predecessor the AMLD IV directive [E.U. (2015)], more detailed prescriptions about privacy. For example, the AML Regulation enables obliged entities to enter into so called partnerships for information sharing to share information about "high risk customers", but it is also made explicit in the AML Regulation itself that (AML Regulation article 75):

- A data protection impact assessment is required.
- Obliged entities shall not solely rely on the information obtained but also use information obtained from other sources such as the customers themselves or their own observations.
- There is a need to assess the information obtained by themselves.
- The information obtained through the use of artificial intelligence, machine learning technologies, or algorithms may only be shared where those processes were subject to adequate human oversight.

Additionally, the AML Regulation enables that special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning health or a natural person's sex life or sexual orientation) (GDPR article 9), and personal data relating to criminal convictions and offences can be used for AML compliance (AML Regulation article 76). But this is subject to stringent conditions. It is only allowed, if it is strictly necessary for the purposes of preventing money laundering and terrorist financing. The data must originate from reliable sources, and be accurate and up-to-date. And the obliged entities must have procedures in place that make it possible to distinguish between, in the processing of such data, allegations, investigations, proceedings, and convictions, taking into account the fundamental right to a fair trial, the right of defense, and the presumption of innocence. PSPs may, based on the AML Regulation, also process these special categories of data with automated processes, including profiling or with processes involving AI systems.[8] But this requires that any decision taken based on this process is subject to meaningful human intervention and that the client may obtain an explanation of the decision reached by the obliged entity, and may challenge that decision except when the decision is to report a suspicious transaction with the financial intelligence unit (FIU).

Notwithstanding the efforts of the E.U. legislator to provide clarity to the market in the AML Regulation about the right balance between AML compliance and privacy, I still expect this to be an ongoing balancing act for PSPs. The key challenge for PSPs is that any processing of data based on the AML Regulation, is still only allowed when considered strictly necessary as defined in the GDPR. Evaluating necessity requires that PSPs can substantiate whether less privacy intrusive measures would not sufficiently mitigate AML risks and whether the overall balance between privacy and AML compliance is proportionate. Neither the AML regulation nor the GDPR does this balancing for the PSPs. Furthermore, the requirement of explainability when AI is used is challenging for PSPs, given the inherent complexities associated with explaining AI and the interest to keep internal AML monitoring rules confidential.

3. Speed in payments versus combating payment fraud

A second balancing act that PSPs need to manage is between speed in payment execution and combating payment fraud, especially since the less time it takes for the money to reach the fraudster the less opportunity there is to intervene in the process.

3.1 The balancing act between speed and combating fraud in the Instant Payments Regulation

In March 2024, the new Instant Payments Regulation was officially published in the official journal of the E.U. [E.U. (2024b)]. The Instant Payments Regulation requires all PSPs that offer regular credit transfers in euros to also offer instant credit transfers. These instant credit transfers are required to arrive at the payment account of the payee within ten seconds (Instant Payments Regulation article 5a sub 4 (c)). Even though it is not mentioned

8. As defined in article 3 (1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (the AI Act).

explicitly in the Regulation, one of the justifications for the Instant Payments Regulation is the strategic autonomy of the E.U. (Instant Payments Regulation recital 7).

Currently, it is mainly credit cards - except for some schemes that only have national reach - that immediately guarantee payment at the point of sale. And the card schemes are not E.U.-owned. When credit transfers arrive immediately into the payee's account, the payee immediately knows for certain that it has paid and can deliver the service. Instant payments could, therefore, offer an alternative to credit cards. However, with instant payments the payee can also instantly use the funds for onwards payment or draw them out in cash at an automated teller machine (ATM). Consequently, the nature of instant payments also creates opportunities for fraud to occur instantaneously.

In practice, therefore, we find that in order to combat fraud PSPs try to build-in deliberate delays (speedbumps) when transferring money. For example, some PSPs apply daily limits of €2,500. When a PSU wants to make a payment that is larger than the daily limit, the daily limit needs to be increased, which often involves a waiting period, of, for example, four hours. The regulators have been navigating this tension between speed and the need to delay payments to combat fraud initially in the Instant Payments Regulation and later in the draft Payment Services Regulation.

The Instant Payments Regulation requires that PSUs set a limit fixing a maximum amount that can be sent by means of an instant credit transfer (Instant Payments Regulation article 5a sub 6). That limit may be either on a per day or per transaction basis, at the sole discretion of the PSU. However, the Instant Payments Regulation also requires that PSUs are able to modify that maximum amount at any time prior to the placing of a payment order for an instant credit transfer. In a Q&A, the European Commission has clarified that pursuant to recital 19 of the Instant Payments Regulation the PSU should be able to change the limit with immediate effect.[9] In practice, this means that the fraudster first instructs the victim to change the limit - with immediate effect - and then the money is transferred instantly to the fraudster. Hence, this day limit does not really protect the PSU, as it can easily be circumvented.

3.2 The balance between speed and combating fraud in the draft Payment Services Regulation

During the ongoing negotiations for the new Payment Services Regulation (PSR), the workings of the daily limit is being discussed again and it is my expectation that the balance between speed and safety will be recalibrated towards safety across the whole of PSR [E.U. (2023)]. It is likely that the final text of this new Payment Services Regulation will be agreed upon around Christmas 2025 and that the Payment Services Regulation will be binding for PSPs as of beginning 2028. Strictly speaking, it means that until this date PSPs cannot apply the safety mechanisms set out below and from the beginning of 2028, they must apply them.

In the recent presidency compromise for PSR of June 13, 2025 the following is suggested.[10]

The PSU and the PSP shall agree in the framework contract on a maximum amount that can be set for each means of payment, including for credit transfers, and for each payment instrument (PSR article 51). It shall be possible for the PSU to modify limits for each means of payment and each payment instrument, which may be on a per-day or per-transaction basis, or both, at the sole discretion of the PSU. PSPs shall ensure that the PSU is able to modify the spending limits set prior to placing of a payment order. However, as opposed to the rules under the Instant Payments Regulation much more safeguards against fraud can be implemented. Firstly, it is made explicit that an increase of the spending limit by the payer, if done remotely, shall require the application of strong customer authentication (SCA).[11] Importantly, however, the increase in the spending limit shall not have immediate effect. Pursuant to PSR, if done remotely, PSPs shall require a delay of a minimum of four hours and maximum of twelve hours for any resulting increase in spending limits to come into effect. PSU may opt out of this waiting period, but also this requires SCA and will only take effect after the delay period. Hence, unless a PSU has already opted out of the delay period, the fraud-

9. EC QA Q&As on IPR implementation Q68, https://tinyurl.com/2kb226p3.
10. When the PSU is not a consumer, the PSP and the PSU can agree on less protection.
11. The Second Payment Services Directive (2015/2366) introduced the concept of strong customer authentication (SCA). SCA is used to verify that the customer has authorized a payment transaction. An example of SCA is a PSU authorizing a transaction by holding its card or smartphone against the card reader at a store and then entering his PIN.

ster will always have to wait at least four till twelve hours for "his" money to arrive. Furthermore, PSPs will need to notify PSUs in an agreed manner (for example a text message or push notification) when a spending limit is modified or when the opt-out is exercised.

However, in practice, the obligation to delay or block fraudulent transactions goes further. The presidency compromise of the PSR provides that PSPs must monitor for fraud (PSR article 83). It is required that PSPs base their transaction monitoring mechanisms on the analysis of previous payment transactions and access to payment accounts online. PSR prescribes that the processing of data by the PSP of the payer shall be limited to the following data and as far as necessary for combatting fraud:

- Information on the payer, including the environmental and behavioral characteristics that are typical of the payer in the circumstances of a normal use of the personalized security credentials.
- Information on the payment account, including the payment transaction history.
- Transaction information, including the transaction amount, payment instrument, if applicable, currency, date and time of execution, as well as unique identifier of the payee.
- Session data, including the device internet protocol address-range from which the payment account has been accessed, from which the transaction was initiated, and from which the transaction was authenticated.
- Device data, including device identifiers from which the transaction was initiated and from which the transaction was authenticated.

Processing of data by the PSP of the payee shall be limited to the following data and as far as necessary for combatting fraud:

- Information on the payee.
- Information on the payment account of the payee, including the payment transaction history.
- Transaction information, including the transaction amount, payment instrument, if applicable, currency, date and time of execution, as well as the name of the payer.
- Session data.
- Device data, including device identifiers.

Importantly, this draft of the PSR determines that if the PSP of either the payer or the payee fails to monitor transactions, that PSP shall bear liability for the losses incurred. The payer shall not bear any financial consequences from that specific transaction, except where the payer has acted fraudulently. The text is a bit ambiguous on whether this liability only applies when the relevant PSP does not perform any transaction monitoring at all, or also when the transaction monitoring that did take place was not sufficient. I would lean towards the latter, as only imposing liability for situations when something is not done at all, does not really make sense. Of course, this comes with its own difficulties since this would mean that financial institutions and, after the fact, courts and/or supervisory authorities need to determine whether transaction monitoring was performed to an acceptable level.

Moreover, PSPs need to act on the signals received from their transaction monitoring systems (PSR article 65). The payer's PSP must suspend any transaction if it has duly justified and has reasonable grounds to suspect that the transaction is fraudulent. For regular (meaning non-instant) payments, the PSP then needs to contact the payer without undue delay which information it needs to lift the suspension. Normally a payment must be credited to the payee's PSPs account by the end of the following business day (PSR article 69). PSR explicitly requires that within this one business day period the PSP of the payer shall make all reasonable efforts to contact the payer before taking a decision regarding the suspended transaction. If the payer has not yet been reached before this deadline, a decision must be made based on the limited information available. For instant payments, the decision on whether or not to block a payment based on strong suspicions of fraud needs to be made within ten seconds, which means that in practice this can only be a fully automated process. The payer must also be informed within the period of one business day for non-instant payments and within ten seconds for instant payments that the payment was blocked.

Moreover, the PSP of the payee may decide to suspend a transaction - meaning postpone making available the funds to the payee - when it suspects fraud. As opposed to the PSP of the payer, this is not a strict obligation but something the PSP can do, since the draft regulation states: "may postpone". It could be that this is merely an editorial mistake and this should be read as "shall postpone" too (PSR article 69). The PSP shall without undue

delay contact the payee and the PSP of the payer to allow them to express their views and where necessary, to contest the decision to postpone making the funds available.

Eventually, the PSP needs to decide within two working days to either make the funds available to the payee or to return the funds to the PSP of the payer. All these obligations of the PSPs require delicate balancing between combatting fraud for which the PSP may be liable towards the victim, when the PSP should have prevented the fraud but did not, and the need to have efficient and preferably instant payments.

But it gets more complicated, it is considered in the Payment Service Regulation that fraud is a predicate offense to the AML Regulation.[12] This means that if a PSP knows or suspects that a transaction is fraudulent this transaction must be reported to the Financial Intelligence Unit and the payment transaction may not be carried out for three days (AML Regulation article 71). During that three days, the FIU can instruct the PSP to suspend the payment transaction for longer or fully block it. If the PSP does not receive an instruction from the FIU, it still needs to evaluate whether it facilitates money laundering when it would let the transaction go through. It also means that in some cases the PSP cannot contact the parties involved as this may be considered tipping off. Lastly, a breach of the AML Regulation can be a reason for a significant fine, which makes striking the right balance between combatting fraud and instant arrival of funds even more pressing.

4. Sanctions compliance and anti-money laundering compliance versus discrimination

Another pressing dilemma that has recently received much attention in the Netherlands, but which I expect to become relevant in more E.U. countries, is the intersection between anti-discrimination law, and AML and sanctions compliance. There exists an inherent tension between both goals as AML and sanction compliance require that PSPs treat their clients differently, whereas anti-discrimination laws require justification when this difference in treatment affects certain protected groups, such as minorities, more significantly. This is even more pressing when some AML or sanction concerns are in fact more prevalent amongst specific groups, for example when cash usage or international payments are more common within an ethnic minority than in the general population. In that case, it cannot be avoided that more individuals from that ethnic minority are subjected to detailed screening and questions. But in such situations, the PSPs must be able to prove that they made sufficient efforts to evaluate the individual risk of each client in order to justify that prima facie discriminatory outcome.

A number of Dutch banking clients have complained about alleged discrimination with the Netherlands Institute for Human Rights (the Institute).[13] Similarly, the Court of Justice of the E.U. has been called upon to rule on the balance between AML and Sanction compliance and discrimination.[14]

An interesting example was a case with the Netherlands Institute for Human Rights where ING Bank suspended a payment of €100 between two accounts that belonged to the same client [NIHR (2024), van Praag (2024)]. The client transfers €100 from his account with Revolut to his ING account. In the description, he mentions the Arabic-sounding name of his brother. ING blocks the transaction and requests that the client provides the full name, address, and date of birth of his brother. The client asks for an explanation and files a complaint of discrimination with ING. According to the client, ING discriminates on the basis of race, as the Arabic-sounding name of his brother in the transaction description is the only reason for the blocks and checks. ING disagrees stating that ING must implement sanctions legislation and that this cannot be done in any other way than with the current screening method.

The Institute notes that ING blocked and checked the client's transactions due to a partial match of his brother's name with names on EU sanctions lists. Because the sanctions lists mostly contain names

12. PSR recital 69d and PSR article 65 where reference is made to article 71 of the AML Regulation.

13. Recent cases for the Netherlands Institute for Human Rights are February 13, 2025 nr. 2025-15, July 25, 2024 nr. 2024-63, February 28, 2023 nr. 2023-29, December 6, 2022 nrs. 2022-141 2022-142 2022-143 2022-144, February 22, 2023 nr. 2023-22, and June 22, 2020 nr. 2020-48.

14. E.U. Court of Justice 17 November 2022, C 562/20 and EU Court of Justice 6 April 2017, C 668/15.

that are of non-Dutch origin, people with non-Dutch sounding names will come up more often in the screening process. Consequently, people with non-Dutch sounding names who tend to be of non-Dutch origin will be blocked and checked more frequently. ING thus indirectly discriminates based on non-Dutch origin.

Indirect discrimination is in principle prohibited, unless there is an objective justification. This firstly requires that the indirect discrimination is caused by a legitimate purpose. The Institute rules that the purpose of ING's screening method is legitimate since ING screens its customers' transactions to prevent money from going to persons or entities on the sanctions lists and the transaction screening generally contributes to the goal. There is no information available on the effectiveness of the transaction screening, but the Institute considers it is plausible that blocking transactions with a name in the description or of the beneficiary that partially matches a name on the sanctions lists, and then requesting further information, generally contributes to preventing direct or indirect payments to persons on the sanctions list. Thus, the Institute ruled that ING's method is appropriate to contribute to the legitimate purpose.

The Institute then assessed whether the method of transaction screening is necessary for achieving the goal. ING states that it cannot achieve the goal with lighter means, as it must conduct extensive screening, because ING would be heavily penalized by the supervisory authorities if it would mistakenly allow a payment to go through. A more individual investigation of each transaction would be unworkable due to the large number of transactions to be checked. Finally, ING states that its method is proportionate. Although the interests of their customers are harmed by the blocks and checks according to ING, this serves a significant societal interest. The Institute, however, concluded that the transaction screening disproportionately harms the interests of people of non-Dutch origin. According to the Institute, it is clear that the consequences of the transaction screening are significant, both for the individual customer and for society. ING has not been able to convince the Institute that they have given sufficient weight to the interests of unjustly affected customers. Even though the decision of the Institute is not binding, it still carries great weight. It is expected that ING will need to recalibrate between sanction compliance and discrimination or alternatively invest more resources (for example, on manual checks) to make sure that less false positives are followed up upon.

Another important case with the Netherlands Institute for Human Rights concerns Rabobank, who refused to open a bank account for a Dutch charity foundation, because the statutory directors of the foundation did not have an address in the Netherlands [NIHR (2024)]. Rabobank as a matter of policy would only accept charities, if at least two of its statutory directors have an address in the Netherlands. The Institute considered this process indirectly discriminatory, because it would be in general individuals of another nationality than Dutch who would be living outside of the Netherlands. Rabobank contended that this policy was based on the consideration that charities with less connection to the Netherlands would have more international payment transactions, which would lead to increased AML risks. It would also be harder to understand the nature of the business. Rabobank's policy is intended to manage the costs and efforts of the AML process. The Institute did not consider this policy justified, because an outright rejection in the opinion of the Institute goes too far. The Institute concluded that Rabobank could also ask such charity foundation to substantiate its connection with the Netherlands. The Institute conceded that this would require more effort from Rabobank, but expected this additional effort to be relatively limited, and justified.

In the Netherlands, it is not only the Netherlands Institute for Human Rights, but also the Dutch Central Bank, as the regulator of the banks, and the Dutch Ministry of Finance, who have investigated complaints of discrimination. For example, on May 27, 2024 the Dutch Central Bank issued a guidance document encouraging banks to do more to combat discrimination [DNB (2024)], and the Ministry of Finance commissioned a report by KPMG into discrimination by banks and payment institutions [KPMG (2024)]. And in May 2025 ING Bank formally apologized in a public letter to its client for its discrimination of clients [ING (2025)].

We are also witnessing increased interest at the E.U. level to the tension between AML compliance and anti-discrimination law. For example, in the AML Regulation it is stated that "in accordance with Article 21 of the Charter, which prohibits discrimination based on any grounds, obliged entities should perform risk assessments in the context of customer due diligence without discrimination" (AML Regulation, recital 172). It is my expectation that this balance between discrimination and

AML compliance will continue to play a significant role and may become an explicit issue in other E.U. markets, especially since due to the increasing use of AI the risk of, and therefore attention to, discrimination will proliferate.

5. Innovation versus the cost of guaranteeing access to all consumers

The last balancing act that I would like to focus on is the one between innovation and the need to provide access for all consumers and the costs that are associated with that. A key priority of the European Commission (EC) is the twin transition: the digitalization and sustainability of the economy [E.U. (2020)]. As with any transition, there are not only winners but also those who are at risk to fall behind; those for whom the transition brings disadvantages. It is important from the perspective of society as a whole to take an extra step for these people so that they can also keep up. In my opinion, this is not only the morally right thing to do, but also wise. Transitions can only be successful if they have and maintain sufficient social support. However, individual PSPs that cater to customers with special needs will face additional costs and complexities. The European legislators pay special attention to the "consumer with special needs" in existing legislation and various legislative initiatives.

5.1 The Accessibility Act and accessibility requirements in the PSR and the Digital Euro Regulation

First, there is the Directive on accessibility requirements for products and services (the Accessibility Act) [E.P./E.C. (2019)]. The Accessibility Act aims to enable persons with disabilities to participate fully and effectively in society. The term "persons with disabilities" is defined as "persons who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others" (Accessibility Act article 3 (1)). All service providers must design their services in such a way that persons with disabilities can also use them. The Accessibility Act provides detailed rules regarding, among other things, the technical design of websites and apps and the information to be provided (Accessibility Act Annex 1 Section III). The Accessibility Act specifically focuses on the accessibility of "consumer banking services". Banking services include all payment, investment, electronic money, and credit services provided to consumers. A specific requirement for banking services is that the information must be provided at language level B2. This means that the information must be understandable for people with an average language proficiency level, ensuring that persons with disabilities can comprehend and use the provided information (Accessibility Act Annex 1 Section IV e). Moreover, the Accessibility Act introduces specific rules for the accessibility of payment terminals and ATMs (Accessibility Act Annex article 2 sub 1 (b) (i)). The payment terminals and ATMs must be accessible for "persons with disabilities" (Accessibility Act Annex 1 Section I 2 o (i)).

The proposal for the Payment Services Regulation contains similar requirements for SCA (PSR article 88 and recital 110). For some people, remembering their PIN and ensuring their debit card doesn't get lost is a challenge. For others, simply remembering the PIN itself can be easy, but entering it and reading it on the card reader can be difficult due to vision problems. New forms of SCA are currently being introduced that can be even more challenging, such as scanning a QR code or entering a specific code into a smartphone app connected to the payment account. Consequently, the PSR, with explicit reference to the Accessibility Act, instructs PSPs to ensure that all their customers, including persons with disabilities, the elderly, persons with low digital skills, and persons without access to digital channels or payment instruments, have at least one tool tailored to their specific situation that enables them to perform SCA.

Accessibility for consumers with special needs is also considered important for the digital euro. Postal services of Member States or their regional or local authorities (when not acting in their capacity as public authorities) are also required to offer basic payment services in the digital euro and to provide face-to-face digital inclusion support to persons with disabilities, functional limitations, or limited digital skills, and to older people [E.P./E.C. (2023), Article 14 sub 3]. These parties and standard credit institutions must provide digital inclusion support to persons with disabilities, functional limitations, or limited digital skills, and to older people. Digital inclusion support includes specific assistance in

opening a digital euro account and using all basic digital euro services [E.P./E.C. (2023), Article 14 sub 4]. Furthermore, the digital euro must have usage and service features that are simple and easy to handle, including for persons with disabilities, functional limitations or limited digital skills, and older persons; and be accessible to persons with disabilities by complying with the accessibility requirements laid down in the Accessibility Act [E.P./E.C. (2023), Article 2 sub 1].

5.2 Availability of cash

The second development is the draft Regulation on the legal tender of euro banknotes and coins [E.P./E.C. (2023)]. In the recitals, the European legislator specifically emphasizes the importance of cash for vulnerable groups, including the elderly, persons with disabilities, and people with limited digital skills. Special attention is also given to people with lower incomes and financially excluded individuals, such as those without a bank account, asylum seekers, and migrants [E.P./E.C. (2023), recital 14]. The regulation requires, among other things, that member states ensure that cash is sufficiently available for these vulnerable groups throughout the entire territory of the member state and that they intervene if this availability is at risk [E.P./E.C. (2023), Article 8].

The Netherlands is at the forefront of digital payments, which has led to a decrease in the use of cash. The Netherlands is, therefore, not waiting for this regulation and a draft law (**Wet chartaal betalingsverkeer**) has been submitted to address this situation [Tweede Kamer (2024-2025a)].[15] Under this draft law, major Dutch banking institutions must maintain their cash infrastructures. According to the proposed law, the cash infrastructure consists of nationwide and adequate facilities for the withdrawal and deposit of euro banknotes and coins. A major bank is defined as a bank with more than three million payment account holders residing or established in the Netherlands. Currently, this includes only ABN AMRO, ING, and Rabobank. The Wet chartaal betalingsverkeer requires each major bank to cooperate with the other major banks. This legislation formalizes the current structure, where the three major banks collaborate through the joint venture Geldmaat.

All banks with more than five hundred thousand payment account holders in the Netherlands must enable these account holders to use the facilities of the cash infrastructure for the unwrapped deposit of euro banknotes.

Banks with more than fifty thousand payment account holders in the Netherlands must enable these account holders to use the facilities of the cash infrastructure for the withdrawal of euro banknotes.

The major banks must ensure that the cash infrastructure is available to smaller banks under fair, reasonable, and non-discriminatory conditions and rates. Additionally, rules will be established by General Administrative Order regarding the fees a bank charges customers for using the cash infrastructure and the conditions the bank applies. These fees can be set to zero, which is what the legislator plans for withdrawals and deposits by individuals [Tweede Kamer (2024-2025b)].

5.3 Evaluation

The main issue with these measures is the extent to which individual (financial) institutions can be required to adapt their services to ensure everyone can use them, while this investment is not cost-effective from the financial institution's perspective. The Accessibility Act addresses this by requiring adaptations, only if they are proportionate. An adaptation is only necessary if it does not require a substantial change to a product or service, resulting in a fundamental change to its essential nature, and does not impose a disproportionate burden on the (financial) institutions involved (Accessibility Act article 14 (2)). This requires an assessment in which the additional costs of making a product or service more accessible are weighed against the total costs incurred by the (financial) institution, against net turnover, and the estimated benefits to persons with disabilities, taking into account the number and frequency of use of the specific product or service.[16] Incidentally, this is not really new, at least not in the Netherlands. The Dutch Equal Treatment on the Grounds of Disability or Chronic Illness Act already requires (financial) institutions to ensure, at least gradually, general accessibility for people with disabilities or chronic illnesses, unless this would

15. I am also aware of cases at the Dutch Institute for Financial Disputes where consumers argued that it was insufficiently possible for them to withdraw money close to their homes. See the rulings of January 30, 2025 nr. 2025-0077 and June 15, 2022 nr. 2022-0840.

16. Accessibility Act Annex VI. In accordance with Accessibility Act Article 14 (8) this consideration must be shared with the regulator.

place a disproportionate burden on them,[17] and there is already some case law from the Netherlands Institute for Human Rights on when a burden is disproportionate [NIHR (2017, 2018, 2021, 2022)]. Based on this case law, a financial institution that wants to invoke proportionality is required to factually substantiate how much the adaptations would cost and why this cannot reasonably be demanded from the financial institution.

The Accessibility Directive (and also the accessibility provisions of the digital euro) essentially covers three interests. First, the interest of consumers with special needs who should have a real choice of various financial institutions to offer them services. If many financial institutions fail to make adjustments based on proportionality, the range of options for this group of consumers will diminish. Second, there is the interest of the financial institution to limit costs, which is why they may be keen to invoke proportionality. Third, there is the interest of other financial institutions that do make adjustments. There is a risk that smaller institutions will cherry-pick the lucrative opportunities, while larger financial institutions incur the costs of fulfilling their social obligation to ensure that everyone can continue to bank.

The digital euro adopts a partially different approach. Here, postal services and Giro services of Member States or their regional or local authorities are given special responsibilities for caring for consumers with special needs [E.P./E.C. (2023), recital 29]. Apparently, the European government – unlike the Dutch government, for example, with the basic cash infrastructure (see paragraph 5.2 above) – believes that a publicly financed solution is preferable.

PSPs for their part need to evaluate whether they can credibly invoke proportionality, but also whether they want this given their role in society and their reputation.

17. Artikel 2a Wet gelijke behandeling op grond van handicap of chronische ziekte.

6. Conclusion

PSPs, given their specific role of facilitating payments, face numerous demands from society and the law. Unfortunately, these expectations are sometimes conflicting. Legislators, regulators, as well as the courts have tried to provide guidelines on how this balancing act should be managed in practice. However, these guidelines are never really conclusive, which in the end means that it is up to the PSPs to manage these differing demands on their own. Obviously, mistakes have been made and continue to be made, but by at least being aware of what is at stake PSPs can manage this so-called balancing act in a more controlled manner. This article aims to facilitate this process.

References

DNB, 2024, "Gerichtere maatregelen nodig om discriminatie bankklant tegen te gaan," May 27, https://tinyurl.com/w6fvdyt7

E.U., 2015, "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC," European Union, May 20

E.U., 2016, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," European Union, April 27

E.U., 2020, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU," September 24

E.U., 2023, "Proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010," European Union, June 28

E.U., 2024a, "Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," May 31

E.U., 2024b, "Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro," European Union, March 13

E.P./E.C., 2019, "Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services," European Parliament and European Council, April 17

E.P./E.C., 2023, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro," European Parliament and European Council, June 28

ING, 2025, "ING luistert, leert en handelt om ervaren discriminatie te voorkomen," May 27, https://tinyurl.com/y48vc5kf

KPMG, 2024, "Onderzoek naar ervaren discriminatie van burgers bij de dienstverlening door banken en betaalinstellingen," April 19, https://tinyurl.com/jze4bska

NIHR, 2017, nr. 2017-107, Netherlands Institute for Human Rights, October 4

NIHR, 2018, nr. 2018-46, Netherlands Institute for Human Rights, May 8

NIHR, 2021, nr. 2021-120, Netherlands Institute for Human Rights, September 7

NIHR, 2022, nr. 2022-53, Netherlands Institute for Human Rights, May 17

NIHR, 2024, nr 2024-63, Netherlands Institute for Human Rights, July 25

Tweede Kamer, 2024-2025a, "Wijziging van de Wet op het financieel toezicht, de Bankwet 1998 en enige andere wetten in verband met de goede werking van het chartale betalingsverkeer (Wet chartaal betalingsverkeer)," , vergaderjaar, 36 711, https://tinyurl.com/bdzn62db

Tweede Kamer, 2024-2025b, "Memorie van Toelichting bij de Wet chartaal betalingsverkeer,"vergaderjaar, 36 711, nr. 3, p. 16.

van Praag, E. J., 2024, "Sanctiecontroles: het middel is erger dan de kwaal. Terechtwijzing van de wetgever, Rondom het nieuws," Tijdschrift voor Financieel Recht, 201-204

Future of Payments

From bottleneck to breakthrough: transforming payment investigations into **competitive advantage**

Galitchenko Iouri,
Products and Market Manager, SWIFT

ABSTRACT

This article explores how financial institutions can transform their exceptions and investigations (E&I) processes in cross-border payments to reduce cost, improve customer satisfaction, and meet new compliance requirements. While payments have become faster, investigations are still taking a long time to be resolved; mostly due to manual interventions and old messaging formats. By using tools like SWIFT Case Management, ISO 20022, and AI technologies, banks can reduce costs and gain competitive perspective. Using real industry data and examples, this article explains why modernizing E&I is not just good idea, but a business imperative.

1. Introduction

In today's interconnected financial landscape, cross-border payments have accelerated dramatically, yet handling exceptions and investigations remain stuck in past.

Although payments can now cross continents in seconds, resolving issues still require days or even weeks, leading to inflated operational costs, customer frustrations, and missed opportunities.

Given the immediacy and transparency pressures that banks are currently facing from both customers and regulators, transforming management of exceptions has become an imperative for success.

A question most financial institutions need to ask themselves is whether they are willing to fall behind their peers within a payments ecosystem that reward efficiency and punishes complexity, or are they ready to embrace change and seize new competitive advantage? The aim of this article is to help financial executives to make an informed decision in this regard.

2. The current state of exceptions and investigations in payments

Despite dramatic improvement in cross-border payments efficiency, the handling of exceptions and investigations (E&I) remains problematic and costly. According to SWIFT's 2025 industry report, average payment settlement times have decreased significantly, from four days in 2019 to just one day in 2024, yet average investigation resolution times remain unchanged at approximately 8 days. Between 1% and 3% of cross-border payments result in inquiries, mainly due to missing information, compliance checks, and inaccuracies; resulting in substantial delays and operational overheads [(SWIFT (2025)].

This critical inefficiency stems from heavy reliance on manual processes, requiring on average five to ten manual interactions per case. Adding to the challenge, 71% of the data elements used in E&I-related MT messages, such as MT199 and MT299, are free-format, making the information difficult to interpret, prone to error and a major cause of delayed responses (SWIFT, 2025). Consequently, operational costs spiral with larger financial institutions facing annual penalties, fees and additional costs of up to U.S.$20 million due to inefficient E&I processes.

Moreover, this operational bottleneck significantly impacts customer experience.

Industry surveys reveal that more than 3% of customers switch banking relationships as a result of frustrations over poor transparency and slow investigations [BNY Mellon (2024)]. These statistics underline an urgent need for transformative changes in managing payment exceptions.

3. Why E&I transformation matters

Transformation of E&Is in payment system is not just option, but a necessary measure due to severe consequences that institutions are facing today. According to SWIFT 2025 report, inefficient investigation processes cost the global banking industry approximately U.S.$602 million annually; included within this figure is U.S.$332 million for operational costs and an additional U.S.$270 million related to liquidity costs associated with unresolved payments. And this numbers relates only the payments processed via SWIFT rails, if other type of transfer are added, the number is likely to be much higher.

Banks suffer substantial financial penalties and high operating costs when investigations remain manual and delayed. Apart from the financial implications, customers experiencing poor transparency and frequent delays are moving their business to competitors who offer superior E&I processes.

Moreover, the ongoing migration to ISO 20022 standard is creating additional urgency. According to BIS (2024), failure to comply with structured message requirements leads to higher rejection rates for cross-border payments. SWIFT's 2025 industry report suggests that around 30-35% of corporate clients are willing to redirect their payment volumes to banks that support structured data standards.

In summary, neglecting investments in E&I transformation will not only increase operational costs but it will also have a significant impact on customer retention and the long-term competitiveness of banks.

4. Leading Solutions to Improve E&I

As inefficiencies in E&I continue to cause operational delays and financial losses, banks are increasingly turning to technology-driven solutions to modernize their E&I handling. At the center of this transformation is the shift toward centralized orchestration platforms such as SWIFT Case Management, which enables structured, automated and trackable exception processing. According to SWIFT industry report (2025), banks using such tools can reduce investigation times by up to 80% for non-complex cross-border cases, freeing up resources and improving transparency.

Equally important, real-time case tracking using End-to-End Investigation References (EIRs) brings visibility and accountability to the process. Clients and compliance teams can follow progress live, addressing one of top pain points cited in BNY Mellon (2024).

One of the most impactful changes is the adoption of ISO 20022 structured messaging, which replaces ambiguous free-text formats like MT199/299 with rich, machine-readable data formats [BIS (2024)]. Over 70 countries are now adopting or mandating ISO 20022, and platforms like Fedwire and CHAPS have deadlines set for 2025 and 2026 respectively [SWIFT (2025)]. Structured messages improve automation, reduce manual touchpoints, and eliminate the need for constant clarification between correspondent banks.

Additionally, advanced platforms such as Pega Smart Investigate (PEGA TM), SmartStream TLM Aurora, and others offer pre-check validation, duplicate request prevention, and internal smart routing logic to ensure investigations are handled only when needed, and by the correct parties. Such solutions can integrate with banks' internal CRMs and compliance systems via API, allowing case data to be managed within existing operations workflows [Pega (2024)].

Emerging technologies are also playing an important role. For example, AI-powered anomaly detection is increasingly used to identify transaction risks early. Yu et al. (2024) find that neural network models like CNN-GRU can detect compliance red flags or suspicious patterns, preventing exception cases before they even arise.

These technologies not only improve operational efficiency but also customer trust. According to PYMNTS (2025), faster E&I resolution directly correlates with improved satisfaction, and banks with superior exception handling enjoy better client retention.

To succeed in today's payments environment, banks must move beyond reactive case-by-case resolutions. They need scalable, automated E&I solutions that can integrate seamlessly with compliance, operations, and customer service. Investing in the right tools, technology and data models now will help them not just catch up, but leap ahead.

5. Benefits of implementing an effective E&I strategy

For financial institutions, the benefits of transforming E&I processes go far beyond cost cutting, they extend into customer satisfaction, compliance agility, and long-term strategic positioning. As already mentioned, traditional E&I processes are slow, expensive, and opaque. But when banks invest in modern, centralized solutions, the return is measurable and immediate.

According to SWIFT industry report (2025), early adopters of its SWIFT's Case Management platform may benefit a revenue increase of between 3 and 5 percent, driven by new transaction flows, improved foreign exchange margins, and better use of operational liquidity. This is due to enhanced customer experiences, as well as operational efficiencies. In an environment where 30–35% of corporations are willing to move their banking flows to institutions offering better transparency and structured messaging [SWIFT (2025)], this is not an issue that banks can afford to ignore.

And as was mentioned above, the customer impact must not be ignored. PYMNTS (2025) found that poor E&I processes result not only in financial losses but in brand damage and client churn. When a client has to wait for a week to get any kind of explanation about a missing payment, and hears

nothing in the meantime, this creates frustration. When case updates are real-time, and resolution is fast, trust grows.

In summary, implementing a structured and tech-enabled E&I strategy helps banks reduce friction, satisfy clients, ensure compliance, and boost the bottom line. Not upgrading is no longer just a missed opportunity, it is a strategic risk.

6. Conclusion

In an era where speed, transparency, and reliability define competitive advantage in financial services, outdated approaches to exceptions and investigations (E&I) are no longer acceptable. As payments become faster and more complex, institutions must modernize their E&I capabilities to avoid operational bottlenecks, rising costs, and client dissatisfaction. Technologies such as ISO 20022 messaging, centralized case management, and AI-driven anomaly detection are no longer "nice-to-haves", but essential tools for efficiency and trust. As industry data shows, banks that act early benefit from increased revenue, reduced costs, and stronger relationships. The question is no longer whether to transform, but how soon can you begin.

References

BNY Mellon, 2024, "Payment investigations: from evolution to revolution," November, https://tinyurl.com/54w3x7mb

BIS, 2024, "Harmonised ISO 20022 data requirements for cross-border payments," Bank for International Settlements, Committee on Payments and Market Infrastructures, February, https://tinyurl.com/2k7mj9he

Kapronasia and SmartStream, 2024, "Driving operational excellence in payment exceptions," https://tinyurl.com/ypf346k9

Kochhar, M., and S. Ghosh, 2022, "Going straight for smooth cross-border payments," Infosys BPM, https://tinyurl.com/bddd742w

PYMNTS, 2025, "How payments investigations can cement bank relationships," PYMNTS Editorial Staff, January, https://tinyurl.com/4f9svru3

Pega, 2023, "Smart investigate for payments: streamlining exceptions and investigations," https://tinyurl.com/mtjuknhe

SWIFT, 2025, "It's time to transform exceptions and investigations," SWIFT, April, https://tinyurl.com/muyn2p93

Tookitaki, 2025, "Fraud protection solution for cross-border payments," Tookitaki Compliance Hub, February, https://tinyurl.com/ms2fs7rf

Yu, Q., Z. Xu, and Z. Ke, 2024, "Deep learning for cross-border transaction anomaly detection in AML systems," 6th International Conference on Machine Learning, Big Data and Business Intelligence MLBDBI2024, https://tinyurl.com/ffss3wnf

2. https://tinyurl.com/5ankvdt5

Future of Payments

Towards **European sovereignty** in retail Payments

Diederik Bruggink, Senior Director, Payments, Digital Finance and Innovation, European Savings and Retail Banking Group (ESBG)

Douglas Lockhart, Payments and Digital Finance Advisor, European Savings and Retail Banking Group (ESBG)[1]

ABSTRACT

This article explores ongoing efforts to establish European sovereignty in retail payments amidst increasing geopolitical pressures and regulatory advancements. It highlights the rise of non-cash payments in the euro area, with card payments being the most prevalent method. Regulatory measures such as the Instant Payments Regulation and the proposed digital euro are being designed to promote innovation, efficiency, and European independence in payment systems. It points out concerns over Europe's reliance on international card schemes and foreign-owned processing infrastructure, which underscores the pressing need for strategic autonomy in this sector. Private-sector initiatives like the European Payments Initiative (EPI) and EuroPA focus on developing pan-European payment solutions, leveraging technologies such as SEPA Instant Credit Transfers. These initiatives aim to reduce fragmentation and enhance interoperability within the European payments landscape. The collaboration between EPI and EuroPA demonstrates promising advancements toward achieving seamless cross-border payment solutions. Despite these efforts, challenges remain in public and private approaches, particularly regarding cost efficiency and adaptability. Questions linger over the feasibility of proposed solutions, including the digital euro, in meeting diverse policy objectives and market demands. In conclusion, this article underscores the complexities and challenges involved in creating a unified European payments system. While significant progress has been made, achieving a comprehensive solution will require balancing public institutional oversight with private-sector innovation and adaptability, all while addressing the various policy issues and technical challenges at hand.

1. The views expressed in this paper are those of the authors and do not necessarily represent the views, the official policy, or the position of the associations or the members they represent.

1. Introduction

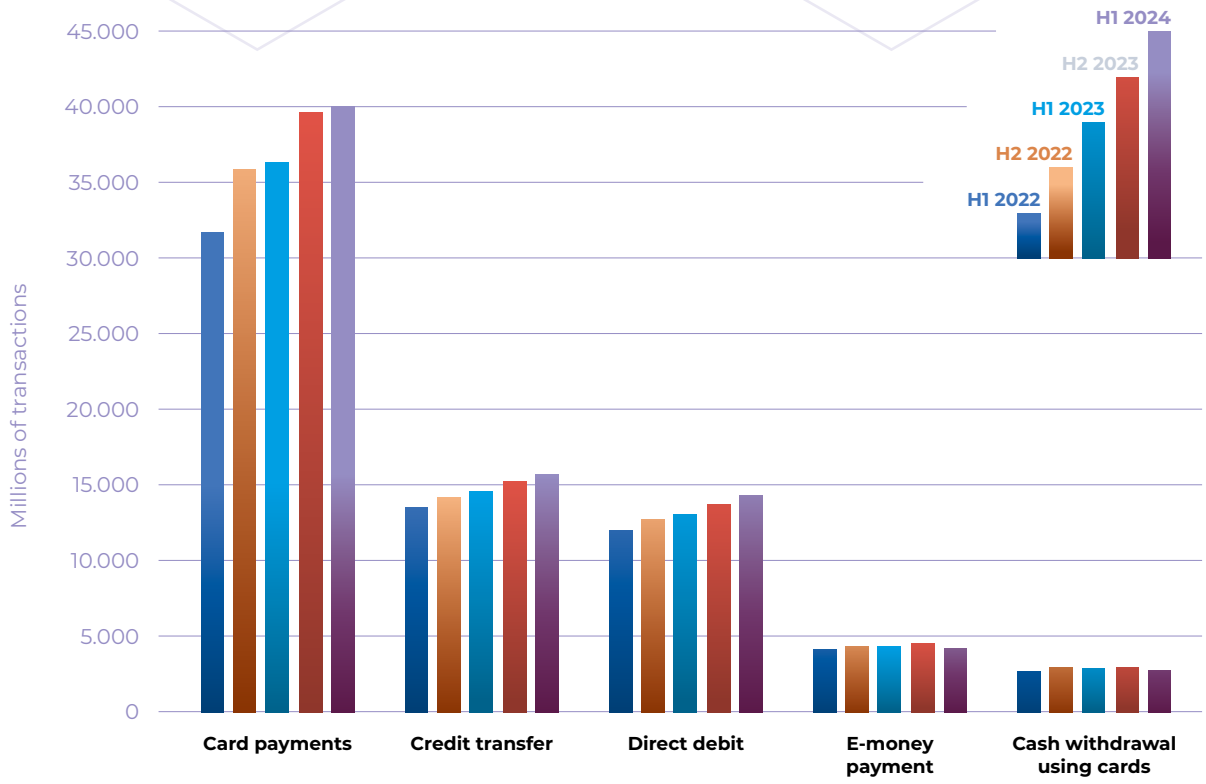
Following increased political pressure at a European level, both from the Commission and the European Central Bank, significant strides have been taken to achieve the long-term goal of a European Sovereign Payments Union. Since the inception of the Single Euro Payments Area (SEPA) in 2002, the private sector has experienced several stages of increased openness and integration in European payments. However, with the continued prevalence of international card schemes, an increasingly fraught geopolitical context has focused the minds of policymakers and key European payment actors alike to work towards a truly European payments solution.

With the decline of cash neither accelerating or showing signs of stopping, there is also a growing sense by central bankers that the role of the euro, both at home and internationally, can only be secured by a digital equivalent. Quite how parallel public and private initiatives will be reconciled remains a principal question, but progress on several fronts continue at pace. With a recent landmark commitment by home-grown, European digital payments solutions to work together for a common acceptance framework, and upcoming political discussions over what a digital euro would look like, now seems an important moment for a stock take and reflection on the progress already made.

2. Retail payments in the euro area: state of play

Non-cash payments are now extremely pervasive in the euro area, with the number of these types of transactions increasing year-on-year. Payment statistics collected for the first six months of 2024 (ECB Data Portal) show that 72.1 billion non-cash payments were made in the euro area, an increase of 7.4% over the same period in 2023. 40.1 billion (56%) of these transactions were made with cards, which

Figure 1: Number of cashless transactions in the euro area (2022-2024)



Source: ECB Data Portal

experienced an even higher rate of growth (10.3%) than the previous year. Credit transfers and direct debits accounted for 22% and 15% respectively. These figures cover the entire euro area. Figure 1 presents a graphical representation of these ECB statistics.

Card transactions continue to be the predominant form of cashless payments, while cash is (still) used for the bulk of point of sale (POS) and person-to-person (P2P) payments [ECB (2024)]. In terms of payment trends, consumer preferences are reportedly unchanged. Over half of euro area consumers prefer to use cards and other digital payment methods. However, a majority of consumers consider it important to have the option to pay with cash. This cognitive dissonance between the purported value of cash to consumers and its real-life application is a growing obstacle to policymakers and the banks facilitating both cash and alternative payment provision.

At the start of the current decade, payments were described [Bruggink (2020)] as the oil that lubricates the European economy. However, if not organized properly, it can also act like the first barrier to the creation of internal markets. Payments are also one of the tools that strengthen the international role of the euro, for example, when international trade and international financial contracts are cleared in euros. Given the significant role that it performs in the economy, payments has been, and always will be, under the scrutiny of regulators.

2.1 Regulatory retail payments strategies

Regulatory initiatives can help regulators achieve their geopolitical agenda. They can also foster innovation and competition, impact end-user protection, pricing, and transparency, and be applied in the fight against financial crime. With several policy objectives inspiring regulatory initiatives on several fronts, Payment Service Providers (PSPs) will have to stay abreast of such developments and be sufficiently flexible to cope with diverse future regulatory initiatives. If the mix of objectives is applied correctly, it can certainly contribute to a European payments ecosystem that is fit for the digital economy.

At the end of 2019 and in the Summer of 2020, the Eurosystem [Cœuré (2019)] and the European Commission [E.C. (2020a)] presented their respective Retail Payments Strategies. The key themes of these strategies are summarized in Table 1. Both strategies highlighted the importance of retail payment solutions being rooted in the E.U. for European consumers. As instant payments are home grown in Europe, the European Commission sees these as one of, if not the, building blocks for the creation of a European champion in payments.

The Eurosystem updated its Retail Payments Strategy in 2023 [Eurosystem (2023)], and remains focused on strengthening the European payments market by developing a pan-European retail payment solution at the point of interaction and enhancing SEPA. Its digital euro project, launched in 2021, supports this strategy by aiming to boost efficiency, autonomy, resilience, and innovation. Designed to align with industry standards and complement private solutions, the digital euro

Table 1: Key Themes within the Retail Payments Strategies of the Eurosystem and the European Commission

Eurosystem	European Commission
Pan-European reach and customer experience	European payment solutions that work cross-border
Convenient and cost-efficient	Competitive and innovative payments market
Safety and security	Payment and other support Infrastructures: unrestricted access and interoperability
European identity and governance	Improved International payments supporting the international role of the euro
Global acceptance	

would help unify payments across Europe. Recent global events - like the war in Ukraine, rising cyber threats, and increased reliance on digital payments - have underscored the need for more resilient retail payment systems.

2.2 Call for strategic autonomy in retail payments

In a recent report, the ECB found that card payments have become the leading form of electronic transactions in the E.U., reaching 70 billion payments transaction - or 54% of all non-cash transactions - in 2023. In 2022, international card schemes processed about 61% of euro area card payments, while national schemes handled the remaining 39%. Including transactions beyond the euro area, the market share of national schemes dropped slightly to 36–37%.

Today, only nine national card schemes remain active in the E.U. - fewer than in 2018, following the reclassification of one Spanish scheme and the exclusion of some minor French ones. In thirteen euro area countries, card payments rely entirely on international schemes. In the rest, national schemes are steadily losing market share.

Card processing is also concentrated. While 80 providers operate across E.U. countries (not counting subsidiaries), just four cross-border companies dominate the market. Most processors are owned by entities based in E.U. Member States, though Germany and Sweden host several controlled by U.S. investors. Domestic-only processors are generally E.U.-owned, but those working across borders are often held by non-E.U. shareholders.

These dynamics raise concerns about the E.U.'s strategic autonomy in payments. The continued decline of national schemes, coupled with foreign ownership in processing infrastructure, points to growing dependence on external players. This reinforces the need for careful oversight to safeguard Europe's sovereignty in point-of-interaction payments.

2.3 Achieving strategic autonomy in retail payments – institutional efforts

This call for E.U. strategic autonomy in payments was also a driving factor of two recent regulatory initiatives. The Instant Payments Regulation [E.U. (2024)] states in its first recital that to create favorable conditions for increased competition, in particular for payments at the point of interaction (POI), the SEPA project should be continuously updated to reflect innovation and market developments in payments, promote the development of new Union-wide payment products, and facilitate access for new market entrants. The proposed Regulation for the digital euro [E.U. (2023)] in its first recital states that the Commission emphasized in its Retail Payments Strategy of September 2020 that a digital euro, as a retail central bank digital currency, would act as a catalyst for innovation in payments, finance, and commerce in the context of ongoing efforts to reduce the fragmentation of the Union retail payments market. The Eurosummit of March 2021 called for a stronger and more innovative digital finance sector and more efficient and resilient payment systems. The Eurogroup also acknowledged, in its statement of 25 February, the potential of a digital euro to foster innovation in the financial system. In that context, both the European Parliament and ECOFIN Council welcomed in February and March 2022 the European Central Bank's decision to launch a two-year investigation phase of a digital euro project, starting from October 2021.

The European Central Bank states that a digital euro would make the euro area more robust. It would support Europe's strategic autonomy and monetary sovereignty, making our payments landscape more competitive and resilient to non-European payment providers. A digital euro would also offer a foundation for further innovation by private payment service providers.

These calls for Europeanisation of payments are not new. Such calls were also made in the past, and the sector has made efforts to respond to these calls. Despite past initiatives such as EAPS, Monnet, and PayFair, during 2006 - 2016, the European payment industry has failed to create an independent pan-European alternative payment scheme. Thus, although Europe enjoys a unified payments market, with well-functioning domestic cards markets, pan-European cards acceptance across the Single Euro Payments Area is entirely reliant on cobranding with international (i.e., non-European) card schemes. While cards have become the most commonly used cashless payment product in the European internal market, so far, the European payments industry has failed to deliver on policy objectives regarding sovereignty in the European payments market [Bruggink (2022)].

2.4 Achieving strategic autonomy in retail payments – private sector efforts

In 2020, a group of major European banks announced the launch of the implementation phase of the European Payments Initiative (EPI), which aims to create a pan-European payment solution leveraging notably instant SEPA credit transfers. EPI aims to become the new standard of payments for European consumers and merchants in all types of payment transactions. This announcement was welcomed by both the European Central Bank [ECB (2022)] and the European Commission [E.C. (2020b)]. In their announcements, both institutions view EPI as a strategic response to the persistent fragmentation in Europe's retail payments landscape. While previous efforts like the SEPA initiative laid important groundwork for infrastructure integration, practical adoption across borders remains inconsistent – especially with national card schemes and mobile wallets still dominating domestic markets. The ECB specifically underscores how EPI aligns with its retail payments strategy and emphasizes the opportunity to build on existing platforms like the SEPA Instant Credit Transfer scheme and the Eurosystem's TIPS infrastructure.

The European Commission, for its part, hails EPI as a "ground-breaking" project that can deliver fast, reliable, and competitive payment options to European citizens and businesses. It also sees the initiative as a pillar in its forthcoming retail payments strategy and encourages broader participation from banks, FinTechs, and third-party providers across the E.U. Both texts converge on a shared vision: EPI is not just a technical upgrade, it is a bold step toward strengthening Europe's financial autonomy, fostering innovation, and boosting global competitiveness in the digital payments arena.

In 2023, EPI announced that it would use "Wero" as the commercial name for its innovative digital wallet. In the same year, it also acquired iDEAL (Netherlands) and Payconiq (Belgium and Luxembourg), giving it a head start in the Benelux, whilst its German and French shareholders committed to bring in their Giropay and Paylib volumes respectively. This makes EPI the first European private provider of a regional (i.e., multiple markets) payment solution.

EPI combined some existing domestic solutions under the new wero brand. Other domestic payment solutions felt the need to combine forces too, and in 2025 three of them – Bancomat (Italy), Bizum (Spain), and MB WAY (Portugal) announced [EPA (2025)] that they will be bringing European payments to the next level through EuroPA, the European Payments Alliance, by achieving a significant milestone in cross-border payments in Europe, by enabling interoperability between the three solutions. Recently, other similar solutions - Blik (Poland), IRIS (Greece), and Vipps MobilePay (Nordic countries) - have joined the initiative and will gradually be integrated into operations.

2.5 Towards pan-European retail payments?

On June 23rd, 2025, the two private sector initiatives, EuroPA and EPI, announced that they plan to collaborate to expand sovereign Pan-European payments [EuroPA and EPI (2025)]. The EuroPA alliance (European Payments Alliance) – represented by Bancomat, Bizum, MB WAY (SIBS), and Vipps MobilePay – and EPI announced that they are exploring solutions to rapidly address Europe's sovereignty challenge in payments, especially with regards to cross-border transactions. Via this initiative, the two consortia aim to enable European citizens to send and receive payments seamlessly across the continent, for the benefit of both consumers and merchants, via their existing channel. This announcement was later followed by a support statement by the three European Credit Sector Associations (ECSAs, or as the European Savings and Retail Banking Group – ESBG, the European Association of Co-operative Banks – EACB, and the European Banking Federation – EBF are called together) [Bruggink (2025)]. In their statement, the ECSAs state that initiatives such as these demonstrate the importance that private solutions attach to the need to strengthen Europe's capacity to operate its own payments, based on Europe's best-in-class payment solutions and increased mutual acceptance. Solutions that are user-centric, collaborative, and aim to enable interconnectivity, can support innovation, and help shape Europe's future in alignment with European objectives.

The existing European solutions are making efforts to reduce fragmentation through interoperability and integration between the different players. Such interoperability could be achieved through a common switch, whilst the option of a joint payment acceptance network could be also

explored. Such collaborative efforts would leverage existing solutions that European citizens are already familiar with: EuroPA and EPI are collaborating on a joint solution that builds on their existing strengths and widespread user adoption through improved interconnectivity. Their goal is to support all types of payments - whether person-to-person or commercial, online, or in-store - across the markets their platforms serve. The current study exploring this integration is set to conclude by the end of summer. Initially, the agreement will cover 15 European countries, representing over 382 million people - around 84% of the E.U. population including Norway. This will allow users to continue using their trusted digital payment solutions both at home and throughout Europe, while also providing a blueprint for regions lacking such options. By connecting established systems, this initiative offers a swift route to greater European sovereignty and independence - objectives shared by both the European Commission and the Eurosystem. Rooted in Europe's technological strengths and diversity, the approach is poised to enhance innovation, ease of use, and efficiency for both consumers and businesses.

3. Quo vadis?

While not new, the call for E.U. strategic autonomy in payments has grown louder than before, driven by the current geopolitical circumstances. At this point in time, the private sector has clear incentives to deliver, though significant obstacles still remain. The only viable alternative to a private-sector-led solution would be a digital euro, which has its own benefits and drawbacks. A recent study estimated that the cost of implementing the digital euro showed an average outlay of €110 million per bank - with European citizens ultimately footing both the public and private bills for a digital euro, of course [PwC (2025)]. Clearly, as a financial instrument, the economics of both options must be front of center of this discussion. Policy objectives must be considered with regards to both associated costs and how effectively and efficiently they can be achieved (by European payment options).

There are a variety of design options for both the digital euro and private market proposals. From the payment solutions on offer at a European scale, to the specifics required for interoperability (e.g., centralized or common risk management rules, acceptance standards etc.). Both proposals have their pros and cons. With regards to the former, a private solution has the clear advantage of agility. Payments continue to rapidly evolve and (as can be seen with payment cards, for example) the market is incentivized to innovate to keep up with market demand and potential opportunities. The same flexibility applies to private offering regarding allowing for variations in consumer demand across European member states. Meanwhile, while any central bank will always struggle to challenge the agility of market players, it benefits from the capacity to resolve design and standardization issues through pan-EU edicts. The ECB is in a position to ensure a pan-European solution more than the market due to its supervisory position and relationship with the co-legislators – not least via its planned "mandatory acceptance" from merchants via its legal tender status. Quite what the implications, or scrutiny, of this muddled combination of market participant, rule-maker, and supervisor will be, remains unclear.

The ECB and co-legislators have presented a number of policy considerations not normally front-of-mind for payment scheme developers. These include the strategic autonomy of the Union, preservation of public money, privacy, and financial inclusion. These objectives are traditionally, and in all likelihood will remain, the preserve of public bodies. However, that is not to say that a public product can achieve the objectives any more efficiently than a private solution (with the notable exception of public money). Strategic autonomy ultimately requires a European solution, independent of foreign actors or technology. This is a significant challenge made more difficult by the inherent requirement that the product is one that Europeans will actually use. There is, as yet, little indication that an online digital euro will be any more private than a market solution (in neither case will the ECB be able to see customers' transaction data, purportedly). The offline digital euro has been proposed as the private, digital solution but it can only be at best "cash-like", which leaves one to expect that those seeking privacy will continue to rely on cash. Similarly, few instances have yet been provided of financial inclusion being available for digital euro where the individual is unable (and willing) to avail themselves of currently available services.

The propositions remain too broad, there are too many objectives being discussed and too many options on the table to be clear on the best or most likely path forward. However, given the policy issues at the heart of the initiatives and the technical com-

plexity in resolving them, it is difficult to foresee an end result in which there is no public institutional direction over private design and operational decision making. Quite what the balance will be is the critical question. But, with the motivating geopolitical factors only intensifying, pressure to find a balance, too, can be expected to increase.

4. Conclusion

In conclusion, achieving European sovereignty in retail payments is essential for reducing reliance on international card schemes and foreign-owned processing infrastructure. This strategic autonomy is crucial for enhancing Europe's independence and resilience in the payments sector. Various regulatory measures, such as the Instant Payments Regulation and the proposed digital euro, aim to promote innovation, efficiency, and European independence in payment systems. Additionally, private-sector initiatives like the European Payments Initiative (EPI) and EuroPA are working towards developing pan-European payment solutions to reduce fragmentation and enhance interoperability.

Despite significant progress, challenges remain in both public and private approaches, particularly regarding cost efficiency and adaptability. Questions linger over the feasibility of proposed solutions, including the digital euro, in meeting diverse policy objectives and market demands. The collaboration between EPI and EuroPA demonstrates promising advancements toward achieving seamless cross-border payment solutions. This integration aims to support all types of payments across the markets their platforms serve, enhancing innovation, ease of use, and efficiency for both consumers and businesses.

Ultimately, achieving a comprehensive European payments system will require balancing public institutional oversight with private-sector innovation and adaptability. This balance is essential for addressing the various policy issues and technical challenges involved in creating a unified European payments system.

References

Bruggink, D., 2020, "European payments regulation: state of play at the start of the new decade," Journal of Payments Strategy and Systems 14:1, 32-39

Bruggink, D., 2022, "The internal cards market in Europe from 2002 to 2020: A success or a failure?" Journal of Payments Strategy and Systems 16:3, 265-276

Bruggink, D., 2025, "European Credit Sector Associations welcome efforts to strengthen European retail payments," Statement, July 1, World Savings and Retail Banking Institute - European Savings and Retail Banking Group (WSBI-ESBG), https://tinyurl.com/msb8b3he

Cœuré, B., 2019, November 26, "Towards the retail payments of tomorrow: a European strategy," speech at Joint Conference of the ECB and the National Bank of Belgium on "Crossing the chasm to the retail payments of tomorrow, https://tinyurl.com/4hntvt6r

E.C., 2020a, "Communication from the Commission to the European Parliament, the Council, the European

Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU," European Commission, COM(2020) 592 final, https://tinyurl.com/2hyywcbd

E.C., 2020b, "European payments: The European Commission welcomes the initiative by a group of 16 banks to launch a European payments initiative (EPI)," European Commission, July 2, https://tinyurl.com/yc6y542s

ECB Data Portal, European Central Bank, https://data.ecb.europa.eu

ECB, 2022, "ECB welcomes initiative to launch new European payment solution," European Central Bank, July 2, https://tinyurl.com/msrkdcwj

ECB, 2024, "Study on the payment attitudes of consumers in the euro area (SPACE)," European Central Bank, https://tinyurl.com/y5d2ben7

EPA, 2025, "EuroPA: The future of payments is here," European Payments Alliance, March 31, https://tinyurl.com/5xtepz4k

E.U., 2023, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro," European Union (COM/2023/369 final), https://tinyurl.com/2an6zn4y

E.U., 2024, "Regulation (EU) 2024/886 of the European Parliament and of the Council," European Union, March 13, https://tinyurl.com/5y56d6v8

EuroPA and EPI, 2025, "EuroPA and EPI launch collaboration to expand sovereign Pan-European payments," June 23, https://tinyurl.com/2uuuyu9v

Eurosystem, 2023, "The Eurosystem's retail payments strategy – priorities for 2024 and beyond," https://tinyurl.com/bp595sf4

PwC, 2025, "Digital Euro Cost Study - From concept to implementation: evaluating some economic implications of the digital euro for European retail banks," Commissioned by the European Association of Co-operative Banks (EACB), the European Banking Federation (EBF) and the European Savings and Retail Banking Group (ESBG), https://tinyurl.com/4t5v3jaf


LG

Future of Payments

The future of Payments: **quo vadis Europe?**

Christophe Bonte,
Senior Policy Adviser,
European Banking Federation

ABSTRACT

Europe's payments sector is facing significant and unprecedented changes. With the constant emergence of new technologies, payments are probably the financial activity most affected by innovation. Furthermore, regulation continues to impact all aspects of payments. With the fast geopolitical changes and considering the crucial role it plays in the economy, the payments sector is increasingly driven by political imperatives. Sovereignty, competitiveness, and resilience have become key issues that strongly influence the future of payments in Europe. In this article, I examine the challenges and opportunities associated with the accelerating digitalization of the payments landscape in Europe, a trend intensified by the rollout of instant payments. I will also discuss the European authorities' plan to create a state-backed retail digital euro, in contrast with most other jurisdictions across the world, and how this may impact the functioning of the European payments market, the innovation capacity of banks, and potentially financial stability if the project is not properly framed. All these developments lead to increased pressure on security of payments, which with fraud levels remaining high, has become an issue that must be combated by all relevant actors.

1. The digital (r) evolution of European payments

The European payments industry is undergoing a period of radical transformation. Digitalization is profoundly reshaping the payments sector in Europe, with the emergence of new technologies that are improving the user experience, expanding the offerings of payment service providers (PSPs), streamlining the operations of commercial banks, and impacting up to the role and activities of central banks.

1.1 Digital payments are on the rise

For some time now, and much more clearly since the COVID-19 pandemic, we have observed a significant decline in the use of cash for retail point-of-sale (POS) payments and a growth in digital payments, particularly online and mobile. Today, payments are no longer only digital, but solutions are increasingly mobile. The wallet is the phone and vice versa. There has been a clear shift towards digital payments in the euro area, although these have not yet overtaken cash payments whose attractiveness is intact and which will likely remain a preferred payment option [ECB (2024a)], especially in extreme scenarios such as war, a massive cyber-attack, or a major power outage.

With the acceleration of innovation, payments are fundamentally becoming more instantaneous, frictionless, and integrated into the customer journey. While they are often invisible, yet payments remain a vital aspect of the economy and the systems and networks that support it.

Another feature is that the world of payments is now expanding well beyond its traditional boundaries and integrating into other services. Open Banking and Open Finance, "Buy Now, Pay Later", the emergence of digital wallets and super apps provided by big techs [BdF (2024)], embedded payments, Central Bank Digital Currencies (CBDCs), crypto assets, to name just a few, are all important developments that are reshaping the payments sector like never before.

Clearly, payments are no longer the preserve of banks just as they are not characterized by the predominance of cash anymore. Many other players are involved in facilitating transactions, from the initial purchase to the final settlement. This is referred to as the payments ecosystem made up of infrastructure and technology providers, financial institutions, and third-party service providers, only to name the main actors.

1.2 Banks will continue playing an important role

While the payments (r)evolution challenges the role of banks, they will remain a major player in an increasingly digital and diversified payments sector. Not only have banks always been present in payments and in technology - think of online banking – but they are also well-established, safe, and trusted institutions. Moreover, banks are becoming even more digital in response to new competition from essentially non-financial institutions whose core business often lies outside the financial services sector, such as large online platforms that have built their success and attractiveness on the collection and processing of massive amounts of personal and commercial data.

Competition is positive if it contributes to further innovation and improves the user experience in a meaningful and accessible way. But it also implies that the principle of "same activity, same risks, same rules" applies to all companies that provide or offer payment services regardless of their qualification as PSP under the relevant legislation. Competition also implies enhanced cooperation and a clear allocation of liabilities particularly in terms of preventing, mitigating and combating payments fraud.

The European payments landscape has evolved significantly since the European Commission published its first Strategy for Retail Payments in the EU in 2020 [E.C. (2020)]. This action plan has been largely implemented and one of its key pillars, the generalization of instant payments, has been enforced.

2. The future is instant

In the age of social media where communication is instant, customers expect payments to be just as digital and fast. The COVID-19 pandemic only accelerated this trend. Within the Single Euro Payments Area (SEPA), standard credit transfers typically take one or two days to process, especially if they are cross-border. This will change with the implementation of the European Union (E.U.)'s Instant Payments Regulation (IPR).

2.1 The pioneering role of banks

In 2017, several European banks began implementing instant payments solutions after the European Payments Council (EPC) developed a common scheme, the SEPA Instant Credit Transfer (SCT Inst), at the request of the Euro Retail Payments Board (ERPB) [ECB (2015)], a high-level body chaired by the European Central Bank (ECB) and tasked with addressing strategic issues related to retail payments. At the time, it was felt that only a pan-European approach would contribute to a single market for payments, similar to what had been achieved with the SEPA Credit Transfer (SCT) scheme, which provides a common set of rules and standards for regular credit transfers.

The uptake of SCT Inst was, however, slow and very uneven across European countries, not only because the scheme was voluntary, but several obstacles prevented its widespread adoption. This is where the European Commission stepped in and proposed, in October 2022, legislation requiring all PSPs, such as banks, that offer their users a service of sending and receiving credit transfers in euro to also offer a service of sending and receiving instant credit transfers, for domestic and cross-border payments, at a cost no higher than that of standard credit transfers.

2.2 The operational challenges of IPR implementation

Regulation (E.U.) 2024/886 amending SEPA Regulation (E.U.) 260/2012 as regards to instant credit transfers in euro entered into force on April 8, 2024 [E.U. (2024)]. The new requirements of the Instant Payments Regulation will apply progressively and to PSPs located in the euro area first. Since January 9, 2025, euro area-based PSPs must be able to receive instant credit transfers.

The big bang date is, however, October 9, 2025, by which time euro area-based PSPs must be able to send instant credit transfers in euro and provide a service of Verification of Payee (VoP) for all credit transfers, whether instant or standard. As per this service, which must be free of charge, the payer's PSP must verify that the beneficiary's IBAN and name match, and to alert the payer of possible mistakes or fraud before authorizing a transaction. VoP must be performed across all initiation channels used by PSPs with their customers. PSPs located in an E.U. country outside the euro area must comply with the same obligations, but only from July 9, 2027.

The EPC developed a VoP scheme in record time. Published in October 2024 [EPC (2024a)], it will be operational on October 5, 2025, alongside the updated SCT Inst scheme rulebook, compliant with the IPR, and just days before the VoP service becomes mandatory under the new Regulation. With a few exceptions in the E.U., such as the Netherlands and Portugal, where VoP service already exists, VoP is a new service for all users.

Given that millions of transactions - both instant and non-instant credit transfers - will be subject to the new checks from the first day of application, PSPs are actively communicating the objectives and characteristics of the VoP service to their customers. It is in this context that the European Banking Federation (EBF) and several national banking associations have joined forces with consumers organizations. A dedicated Task Force of the ERPB has also defined a high-level, principles-based and non-binding guidance as well as a set of examples for possible use by PSPs, to facilitate a smooth introduction of VoP for end-users.

According to the IPR, an instant credit transfer implies that the funds must be on the beneficiary's account within 10 seconds. Today, technology has made it possible to process 99% of successful instant payment transactions in less than 5 seconds [ECB (2024b)]. The challenges lie more in the numerous obligations that must be fulfilled before the transaction is released, in the first place VoP.

An instant credit transfer can be initiated 24/7 via all the channels that can be used to place standard credit transfers, such as online or at a bank branch. However, if it is initiated through a non-electronic channel, it will be executed immediately after being entered into the PSP's electronic system. In addition, it will be possible to submit multiple payment orders for instant credit transfers in euro as a package, where PSPs already offer this possibility for standard credit transfers (bulk payments). In this case, if the payer is a corporate (not a consumer), it can decide to opt out from the VoP service.

Finally, the Instant Payments Regulation also implies significant changes to banks' financial sanctions operations. Since January 9, 2025, a new financial sanctions screening regime applies whereby all E.U.-based PSPs, regardless of their location, must check their customer records immediately after the publication or update of a new E.U. sanctions list, and at least once a day. This system thus moves away from transactions screening, which would have prevented frictionless instant

payments. However, this does not exempt banks from continuing to perform transactions screening to ensure compliance with non-E.U. sanctions lists, such as the one of the U.S. Office of Foreign Assets Control (OFAC), in addition to customer screening. This may result in a lot of false positives and delays in the processing of instant payments.

2.3 Towards potential market shifts and new business opportunities

While adapting to the new rules, PSPs are integrating instant payments into their business strategy to take advantage of the opportunities and economies of scale created by the new Regulation, as eventually instant payments will become the new normal across Europe.

The rollout of instant payments is a powerful driver for the emergence of European-grown cross-border payment solutions, which have the potential to become pan-European champions. The success of SEPA demonstrates that Europe can build a private system that makes the E.U.'s Single Market a reality, including in payments.

Leveraging on the SCT Inst, the European Payments Initiative (EPI) - whose membership comprises more than 20 European banks - launched Wero in 2024. It is a unified account-to-account (A2A) private instant mobile payment wallet solution rolled out by banks in France, Germany, and Belgium to enable cross-border instant payment transactions. Luxembourg and the Netherlands will follow in 2026.

Likewise, the EuroPA initiative will make the mobile payment services of Bizum (a particularly popular solution in Spain and owned by the country's major banks), Italy's Bancomat, and MB Way from Portugal interoperable to the benefit of their users. Vipps MobilePay in the Nordic countries, Poland's Blik, and IRIS in Greece have recently joined the initiative and will gradually be integrated into operations.

Together, these countries account for the majority of digital payments in the euro area. While these solutions were launched with a focus on person-to-person (P2P) payments, they will gradually extend to e-commerce and eventually in-store payments (in 2026 for Wero, for example).

A mapping of European payment solutions carried out by the EBF shows that 20 of the 27 E.U. countries have an A2A private instant mobile payment solution, and only 7 have neither a domestic card scheme nor a mobile payment solution and rely entirely on the payment infrastructure of international card schemes such as Visa and Mastercard.

More recently, EuroPA and EPI launched a collaboration and announced their intention to work together towards interconnecting their solutions. The aim is to extend existing solutions beyond their national or regional markets to facilitate cross-border payments in Europe across all use cases (P2P and commercial payments both online and in-store) [EPI (2025)].

These solutions and initiatives respond not only to the changing needs of users in an increasingly digital payments market, but also to the heavy reliance on non-E.U. payment providers and the emergence of technological solutions offered by foreign companies. Despite having different infrastructural setups, these initiatives share the same goal and aim to expand to more countries, contributing to an even more integrated and sovereign pan-European payments market. But there is an elephant in the room: the digital euro.

3. The digital euro

In June 2023, the European Commission published a legislative proposal to establish a digital euro [E.C. (2023)]. The proposal was released after the Eurosystem launched an investigation phase on introducing a digital euro in October 2021. Two years later, the ECB's Governing Council decided to move to the next phase of the digital euro project, the preparation phase, which will last until October 2025. The Governing Council will then decide on the potential launch of the next phase, or the continuation of the current preparation phase. The decision by the ECB's Governing Council on whether to issue the digital euro is subject to the adoption of the legislative act currently being negotiated by the European co-legislators.

The digital euro will be a retail CBDC, and as such would be a form of central bank money that is directly accessible to the public, like cash, and with the status of legal tender.

3.1 The rise of CBDCs

CBDCs have become a major topic of discussion among policymakers, central banks, and financial institutions worldwide, spurred by Facebook's

announcement of Libra (later renamed Diem) in 2019. The proposed stablecoin aimed to create a global private digital currency outside the control of central banks, prompting widespread concerns about monetary sovereignty, financial stability, and regulatory oversight.

This development, combined with the accelerating digitalization of finance and declining use of cash, has prompted central banks to legitimately explore digital currencies. While some countries have made significant progress in launching a CBDC, many others are still in the research phase, weighing the potential benefits and risks.

CBDCs can be broadly categorized into two categories: retail CBDCs (designed for use by the general public) and wholesale CBDCs (intended for financial institutions to settle large-value transactions). Different countries have pursued work on CBDCs for varying reasons, ranging from improving financial inclusion to strengthening monetary policy effectiveness and enhancing cross-border payments.

To date, only a handful of countries have fully launched a retail CBDC, with limited success. The Bahamas launched the Sand Dollar in 2020, Nigeria the e-Naira in 2021, and Jamaica JAM-DEX in 2022. Most larger economies have questioned the need for such an initiative at this stage. In several countries, the central bank or ministry of finance has stopped the project (Sweden, U.S.), is reevaluating its plan (U.K.), or concluded from the outset that there is currently no need nor genuine interest in a retail CBDC (Switzerland).

3.2 The European approach

In contrast, Europe, and the euro area in particular, has taken a different direction and chosen a distinct approach by positioning the digital euro as more than just a digital equivalent of cash. Unlike other CBDCs around the world, the digital euro is linked to a digital wallet and instant payments infrastructure, raising fundamental questions about its impact on banks, financial stability, and competition within the European payments ecosystem.

The reasons and objectives for launching a digital euro have evolved over time. According to the ECB and the Commission, the main rationale for the digital euro stems from the declining use of cash, the increasing digitalization of finance, and concerns about monetary sovereignty.

Since work on the digital euro began, Europe has faced a changing geopolitical landscape, with the emergence of new political priorities, such as competitiveness, strategic autonomy, and resilience. In this context, the sovereignty of retail payments has gained importance and attention from European policymakers. Furthermore, the ECB's digital euro project has evolved, and so have the perspectives of the banking sector. Meanwhile, the legislative process has advanced at a slow pace.

As currently designed by the ECB, the digital euro risks duplicating existing private payment solutions, already being developed and scaled to address the legitimate need for greater sovereignty in European retail payments, which are currently too dependent on foreign actors. This duplication could result from the digital euro's potential to offer similar functionalities to existing private instant payment solutions, such as mobile wallets or online payment platforms. Moreover, it could impose an overly prescriptive and complex set of requirements, hindering the innovation capacity and thus the competitiveness of European banks, as well as the European Commission's simplification objectives. Finally, it imposes high costs on intermediaries and potentially also undermines financial stability. These three areas of possible impacts are detailed below.

3.3 Impact on the role of banks and risks to financial stability

One of the most pressing concerns about the digital euro is the risk of bank disintermediation. If consumers and businesses shift deposits from commercial banks to digital euro accounts, which will constitute a liability of the central bank and therefore not appear on banks' balance sheets, banks could experience a decline in their deposits. This, in turn, could reduce their lending capacity and increase the cost of credit. In times of financial stress, a rapid shift of deposits into digital euro holdings could exacerbate liquidity shortages, potentially creating systemic risks.

It is encouraging that the ECB is putting in place safeguards, such as holding limits, to prevent the digital euro from being used as a store of value. A study published by Copenhagen Economics in December 2023 examined four different holding limit scenarios and their impact on financial stability and consumer welfare. It concluded that the lower the holding limit, the more limited the loss of deposits [Copenhagen Economics (2023)].[1] Low

holding limits that are stable over time are necessary to prevent the digital euro from altering the traditional bank funding model, making it more difficult for banks to fulfil their strategic role in meeting Europe's financing gap and contributing to the massive investment needs triggered by the green and digital transition and increased security spending.

3.4 Impact on the innovation capacity of banks

The potential rollout of the digital euro entails significant costs for the banks that will be mandated to distribute it.[2] By having to commit high resources into its implementation, banks risk missing out on their own innovation and losing competitiveness.

Furthermore, a digital euro will likely absorb all the necessary resources that have not yet been deployed to meet the large number of regulatory obligations that require considerable investment in the coming years (Instant Payments Regulation, Anti-money Laundering Regulation, Digital Operational Resilience Act, European Accessibility Act, Digital Identity Regulation, Payment Services Regulation, ...).

In reality, the generalization of instant payments will largely achieve the same political objective as the digital euro, i.e., enhancing European competitiveness and strengthening sovereignty in payments, most likely at a much lower cost. The European payments industry cannot afford two major and competing mandatory projects. If the digital euro requires duplicative investments in parallel infrastructures, banks could face prolonged periods of reduced funding for innovation and financial pressure.

3.5 Overlap with existing payment solutions

Unlike other CBDCs designed to complement existing payment methods, the digital euro is positioned as a payment instrument that could interact directly or even unfairly compete with existing European payment solutions. These solutions are increasingly exploiting the opportunities and economies of scale created by the deployment of instant payments to expand reachability and better compete with non-E.U. providers, as explained above. This risk will be accentuated by the mandatory acceptance of the digital euro, which will become legal tender.

The E.U. already has a dynamic, secure, and well-functioning electronic payments market. Today, for their retail payments, European consumers and businesses have access to a variety of methods and instruments to meet their different needs, including (instant) credit transfers and direct debits, debit and credit cards, and cash. They can initiate payments through a multitude of solutions and channels, such as mobile banking, digital wallets, mobile payments, contactless payments, through payment initiation service providers (PISPs), and more. This reflects an active, competitive, and constantly evolving sector, with new business models and new players entering the ecosystem. If the digital euro fails to integrate seamlessly with existing banking and payment solutions, it could inadvertently drive users toward large non-E.U. digital wallet providers and international card schemes, whose dominance it is intended to reduce.

A key concern is whether the digital euro will create an uneven playing field, where banks that will be mandated to distribute the digital euro bear the costs of implementation while large non-E.U. platforms benefit from the new payment infrastructure without contributing to liquidity, security, or fraud prevention. Such a scenario could fundamentally alter the retail banking model, with a consequent erosion of related revenue streams that may affect banks' profitability, which is essential for their resilience.

3.6 A case for a wholesale digital euro

Given the concerns raised above, the approach of prioritizing a wholesale CBDC over a retail digital euro is preferred. A wholesale CBDC could improve the efficiency of interbank settlements, strengthen the resilience of financial markets, and contribute to monetary sovereignty without displacing bank deposits, affecting retail banking models, or disrupting established payment systems.

1. With a holding limit at €3,000, the study finds that the digital euro could lead to an outflow of up to €739 billion of bank deposits in the euro area. This corresponds to a loss of 10% of the total household deposit base and 3% of the total bank liabilities. With a holding limit of €500, the loss of deposits would be limited to €139 billion, a decrease of 81% compared to a €3,000 holding limit.
2. A recent study by PwC estimates that banks would face initial costs for the implementation of the digital euro - excluding an offline functionality, multiple accounts and running costs - that could exceed €2 billion, with an average outlay of €110 million per bank. When extrapolated to the entire euro area, the total change costs could reach €18 billion; available at https://tinyurl.com/3kejfupr.

Additionally, a wholesale digital euro would be a real CBDC and align with broader political objectives, such as increasing the international role of the euro, strengthening financial sovereignty, and enhancing global cross-border payments in line with the G20 Roadmap [FSB (2024)]. It would have obvious use-cases and add value to its participants, the banks.

It is not surprising to see a rise in wholesale CBDC projects around the world, both domestically and across borders, including in Europe. In this regard, the ECB's recent announcement that it will provide an interoperable solution in the short-term and look into providing an integrated solution in the medium- to long-term is a step in the right direction [ECB (2025)].

3.7 A collaborative approach to strengthen the sovereignty of European payments

Strengthening the sovereignty of European payments is a strategic objective shared by the banking sector, the ECB, and the European co-legislators. All options should be explored, taking into account the deployment of European private instant payment solutions that take full advantage of the generalization of instant payments, and close the gaps where no such solutions exist.

If a digital euro is to emerge, it is essential that it leverages on investment made to build private solutions and reuses, where possible, infrastructures, processes, and industry standards already in place to minimize costs for PSPs that will be mandated to distribute the digital euro. It should also cater for a viable business and compensation model and preserve the stability and resilience of banks and their role in the European economy. This means that its introduction should be a simple value proposition that is released gradually to add clear value to all stakeholders. It is in this context that the EBF considers it essential to continue the close and constructive dialogue with the ECB and the co-legislators.

4. The changing nature of fraud

Finally, with the radical changes that characterize the payments sector as described above - the emergence of new technologies, the increase in digital payments, the speed of payments - also arises the fundamental question of payments security, and more specifically of cybercrime and fraud.

4.1 Fighting online fraud

Although fraud levels are declining thanks to effective measures such as strong customer authentication (SCA) and the implementation of a risk-based approach by PSPs [EBA/ECB (2024)],[3] new types of fraud are on the rise with techniques constantly evolving, such as those resulting from social engineering, which uses psychological manipulation to push users into making payments they would not have otherwise made. Social engineering increasingly leads to fraudulent authorized push payments (APP) [EPC (2024b)]. A typical example is bank employee impersonation when a customer receives a phone call, text message, or email appearing to come from a bank.[4]

These new forms of fraud highlight that digital fraud and scams affect a much broader and more complex matrix than just the point of payment but involve electronic communication channels and the widespread use of social networks. It is, therefore, more appropriate to refer to online fraud than payments fraud, as most fraud is enabled outside the banking system and, more generally, the payments value chain.

Effective action against fraud driven by social engineering is crucial to maintaining secure, trustworthy, and competitive payment systems. Banks invest heavily in fraud prevention and control, but banks alone cannot combat fraud and be solely responsible for phenomenon that occurs outside their sphere of competence and of which they are also victims.

4.2 A holistic approach is required

A collective, multi-stakeholder approach, based on cross-sectoral collaboration, is needed, as high-

3. There is no detailed statistics as regards to payment fraud in the E.U. apart from this report whose scope is limited to PSD2 and the methodology used raises questions that we do not address here.
4. Revolut's "Consumer security and financial crime report" shows that, in the second half of 2024, over half of APP cases were purchase scams (56%), followed by job scams (20%), investment scams (10%). Impersonation scams, romance scams or invoice scams are other sources of fraud; available at https://tinyurl.com/3vjvapp5.

lighted in a recent ERPB report on fraud to retail payments [ERPB (2024)]. It is essential that all actors – beyond banks - involved in the fraud chain share responsibility, including through the introduction of legal obligations for fraud prevention measures by telecom operators and online platforms, where most fraud originates, and a fair allocation of liability that would make everyone involved part of the solution.[5]

Other jurisdictions, such as Australia and its innovation Scam Prevention Framework, are already taking steps in this direction. The E.U. could draw inspiration from this initiative. Currently, its regulatory response is fragmented across different pieces of legislation dealing with payments, primarily the review of the Payment Services Directive (PSD2), but also the activities of very large online platforms, via the Digital Services Act. A holistic approach is urgently needed to combat fraud.

With the gradual adoption of instant payments, the risk of fraud may even increase, simply due to the ability to transfer money in seconds, which could lead to higher fraud losses and lower recovery.

4.3 Avoiding that instant payments become instant fraud

The new VoP service introduced by the Instant Payments Regulation aims precisely at preventing instant payments from turning into instant fraud. However, this mechanism cannot replace the technical measures taken by PSPs to protect customers against potential fraudulent payment orders. These measures include the application of a cooling-off period (or a delay applied by the PSP) when users increase their spending limits, which they can do at their sole discretion and with immediate effect under the IPR. This mechanism has proven very effective in fraud prevention in countries such as the Netherlands. In the extensive Q&As published in July 2024 to clarify the requirements of the IPR [E.C. (2025)], the European Commission acknowledged that such measure - which is part of sound risk management - does not violate the obligations of the new Regulation.

Increased sharing of fraud information and data, in line with the E.U.'s General Data Protection Regulation (GDPR), transaction monitoring (e.g., using artificial intelligence to detect fraud patterns), and customer education through fraud awareness campaigns are also important and useful tools to complement SCA and ensure reliable and secure payments while avoiding friction in the user experience. These measures are most effective when industry and authorities join forces through a public-private partnership.

The economic, societal, and security impacts that result from online fraud and its consequences for payments require a collective effort and a broader approach covering the entire chain of a fraudulent conduct and not just PSPs. Failure to do so would put European payment services competitiveness at risk and the European economy with it.

5. Conclusion

The Retail Payments Strategy for the E.U., published by the Commission in September 2020, is already five years old. It may need to be revised. Since then, the objective of strategic autonomy has come to the fore with the alteration of the geopolitical environment.

The sovereignty of payments has undoubtedly gained in importance and attention among European policymakers. The emergence of big techs in the payments sector has also been confirmed, as has the increase in online fraud and the use of new technologies such as digital identity and artificial intelligence, which can both help reduce fraud and generate new types of fraud. The CBDC debate has also evolved, with jurisdictions adopting sometimes radically different approaches, such as the decision by the euro area to develop a retail digital euro.

It is, therefore, essential that Europe has a strategic vision and a clear path for its payments sector, and banks must be part of this vision and this future. Indeed, because the banking sector is essential for financing the substantial investments needed to meet the immediate and long-term challenges, Europe needs a competitive, resilient, and profitable banking and financial sector.

This is where innovation plays a key role. While payments remain fundamentally a domestic activity, the digitalization of payment solutions has the potential to create a truly cross-border, pan-Euro-

5. PSR (2024) found that Meta platforms were linked to 54% of scam incidents (119,338 cases) and 18% of total losses (£62.7 million) in 2023. These observations are confirmed by the Revolut study as well.

pean retail payments market. Because digitalization knows no border, it can contribute to greater integration, thereby strengthening Europe's competitiveness and strategic autonomy. To achieve this, Europe needs simpler rules and an effective and balanced regulatory framework that fosters innovation, not hinders it, while also addressing the risks associated with the emergence of new technologies.

References

BdF, 2024, "The growth of big techs in the financial sector: which risks, which regulatory responses?" Banque de France, October

Copenhagen Economics, 2023, "Effects of a digital euro on financial stability and consumer welfare," December

EBA/ECB, 2024, "2024 report of payment fraud," European Banking Authority/European Central Bank

E.C., 2020, "Communication from the Commission on a Retail Payments Strategy for the EU (COM(2020) 592 final)," European Commission, September 24

E.C., 2023, "Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro," European Commission, June 28

E.C., 2025, "Clarification of requirements of the Instant Payments Regulation," European Commission, July 28

ECB, 2015, "Instant payments across Europe by November 2017," European Central Bank, November 27

ECB, 2024a, "Study on the payment attitudes of consumers in the euro area (SPACE)," European Central Bank

ECB, 2024b, "High-level communication strategy with end users on instant payments: final report by the ERPB workstream," European Central Bank, ERPB/2024/003, May 29

ECB, 2025, "ECB commits to distributed ledger technology settlement plans with dual-track strategy," European Central Bank, July 1

EPC, 2024a, "Verification of Payee Scheme Rulebook," European Payments Council, October 10

EPC, 2024b, 2024 payment threats and fraud trends report," European Payments Council, EPC162-24/Version 1.0, November 22

EPI, 2025, "EuroPA and EPI launch collaboration to expand sovereign Pan-European payments," European Payments Initiative, June 22

ERPB, 2024, "Report of the ERPB Working Group on fraud related to retail payments," Euro Retail Payments Board, September

E.U., 2024, "Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro," European Union, March 19

FSB, 2024, "G20 roadmap for enhancing cross-border payments: consolidated progress report for 2024," Financial Stability Board, October 21

PSR, 2024, "Unmasking how fraudsters target UK consumers in the digital age," Payment Systems Regulator, December 17

Future of Payments

Tackling **authorized push payment (APP)** fraud: a challenging and evolving Payments environment

Piers Reynolds,
Partner, Freshfields LLP

Laura Feldman, Barrister, Freshfields LLP, and Lecturer in Law, University of Oxford[1]

ABSTRACT

The U.K. Payment Systems Regulator (PSR) has introduced significant changes to the U.K. payments landscape. The recently introduced mandatory reimbursement regime (the Scheme) allows victims of "authorized push payment" (APP) fraud to reclaim fraudulently transferred funds from the sending payment system provider (PSP) that processed the payment unless certain limited defenses apply. This novel Scheme, which is unique globally, aims to redistribute the burden for fraud between PSPs and consumers, encourage PSPs to introduce greater measures to tackle fraud, and curtail disputes in this area. We explain the Scheme, assess its operation to date, explore potential difficulties, and conclude with practical guidance for PSPs managing the new measures.

1. This article was finalized on July 30, 2025 and reflects the position at that point in time.

1. Introduction

There are two main avenues of recourse that victims of APP fraud may pursue in the U.K.: the "mandatory reimbursement scheme" for payments using the faster payment system (FPS), or through the courts. The Scheme, which has applied since October 7th, 2024, allows victims of APP fraud to make a claim from the sending PSP (the Sending PSP) for reimbursement in most cases. APP fraud arises where the victim "authorizes" the payment but under false pretenses. The new reimbursement requirement does not apply to international payments, payments made for unlawful purposes, payments across other payment systems (a separate scheme exists for CHAPS), civil disputes, and where the customer has acted fraudulently or with gross negligence. Claims falling outside the scope of the Scheme may be subject to litigation. There are limited grounds to challenge APP fraud in the courts because of the bank's obligations to execute customer instructions unless exceptional circumstances arise. This article will focus on the Scheme as opposed to the common law as that currently covers most payments in the U.K.

2. The Scheme

The Scheme operates as follows:

- PSPs must provide mandatory reimbursement in most cases of a payment scam where a claim is made within 13 months of the final payment. There are two exceptions: where the PSP can show that the customer has acted fraudulently, or with gross negligence (known as the "customer standard of caution").
- A Sending PSP (a PSP, which holds the customer's account) must reimburse the victim within five business days, except where they "stop the clock". Sending PSPs can "stop the clock" by investigating further, for example by gathering additional information.
- The cost of reimbursement, which is capped at £85,000, is shared equally between the Sending and receiving payment service providers (the Receiving PSP). The Sending PSP can levy an optional claim excess of £100.
- Pay.UK oversees the Scheme,[2] but the binding legal instruments that implement the requirements envisage that the PSR can undertake enforcement action where necessary.
- Additional care is required for "vulnerable consumers", as defined in accordance Financial Conduct Authority (FCA) standards.

2.1 The Scheme in operation

Six months after the Scheme was introduced, the PSR published a thought piece providing a snapshot of its operation [PSR (2025)]. It notes that during the first three months since implementation, around £27m was returned to victims via in-scope claims (which represents 86% of funds lost) and the overwhelming majority of claims (98%) were awarded without resort to the customer standard of caution.[3] More recently, PSR consumer research reported that most consumers surveyed were unaware of the Scheme. We may, therefore, see an increase in claims with expected growing awareness of the reforms.

PSPs are closely scrutinized for their management of the Scheme as Pay.UK is required to collate comprehensive data on performance.[4] We were expecting the publication of the data but this has not as yet materialized. This may mean that Pay.UK is struggling to process that data and/or that there are issues with PSPs providing the information.

Where a fraud claim cannot be resolved between a PSP and the consumer, it can be referred to the Financial Ombudsman Service (FOS). There is currently limited insight available into the volume of fraud and scam claims with the FOS following the implementation of the Scheme, though it has reported a steady increase in complaints in relation to APP fraud. Shortly before the introduction of the Scheme, the data for the three-month period between July and September 2024 indicated circa.

2. Pay.UK is a corporation that manages membership of the FPS used to process most payments in the U.K.
3. The PSR published further data in July 2025 (available at: https://tinyurl.com/mkm4t5wf), indicating that during Q1 2025 87% of the money lost to APP scams was returned to victims, 86% of claims were closed within 5 business days, and 3% of claims were rejected due to the consumer not taking enough care over the transaction or their claim. Notably, around third of claims during Q1 2025 were not within the scope of the Scheme with many likely falling within the category of civil disputes as opposed to fraud.
4. PSPS must retain and report on the total volumes and value of APP fraud claims that: have been reported; that are reimbursable and those that are not reimbursable; closed within the 5 business day and 35 business day deadlines; claims where the Sending PSP has informed the Receiving PSP of the claim within the notification period; where the Receiving PSP has responded to a Sending PSP's information requests in a timely and accurate manner; where the consumer standard of caution has been applied; where the customer is assessed as vulnerable; as well as the total number and value of claims reimbursed and the total volumes and values of claims where the Sending PSP received the reimbursable contribution amount within 5 business days.

9,000 complaints about fraud and scams [FOS (2024)], which is significantly higher than in the same period the previous year and an increase on the previous quarter in 2024.[5]

Of these complaints, around 55% related to APP fraud. The FOS has not published specific fraud and scam data for the period from October to December 2024 but noted 8,830 current account complaints compared to 7,804 complaints in the same period during 2023 and that "[f]raud and scams continues to be the main driver of these complaints". The FCA's recent annual report notes 28% more cases about fraud and scams in 2024/25 than in the previous year (35,416 up from 27,675) [FCA (2025)]. Despite the introduction of the Scheme, the FOS has predicted that it will receive almost 37,000 fraud and scam complaints for the 2025-26 fiscal year, which would represent a notable increase in claims compared to the previous year. Nonetheless, the annual report finds that for the initial six months of the Scheme, there was a low volume of complaints relating to the Scheme. This likely reflects the time-lag between a claim for reimbursement, attempts to resolve the dispute between the consumer and retail, and referral to the FOS. The annual report also finds that there has been an increase in cases where there is an ongoing civil dispute about the suspected underlying fraud or scam or investment. This suggests that uncertainty regarding the line between civil disputes and fraud remains challenging (see further section 3.1.3 below).

The fact that the Scheme is not predicted to have any impact on cases reaching the FOS raises questions. It could imply that many of the claims caught by the Scheme were previously covered by the voluntary CRM (Contingent Reimbursement Model) code of practice for APP scams. The CRM arrangement accepted by many PSPs allowed victims to reclaim funds transferred fraudulently in many cases.[6] A further reason could be that the complexities of the Scheme may simply lead to disputes between consumers and PSPs to ascertain the interpretation of many aspects of the regime (discussed below in section 3). If we do see escalating APP fraud claims reaching the FOS, it may call into question the benefits of introducing the Scheme.

5 6,264 complaints reported in the same period the previous year.

6. Under the CRM, which has since been retired following introduction of the Scheme, signatories committed to (inter alia) protect customers with procedures to detect, prevent, and respond to APP scams; provide a greater level of protection for customers considered to be vulnerable to fraud; respond effectively to the receipt of funds from this type of fraud; and reimburse customers who were not to blame for the scam.

3. The challenges

There are a number of challenging aspects to the Scheme.

3.1 Uncertainty

There are several facets of the regime that are inherently uncertain, such as the gross negligence customer standard of caution and the definition of vulnerable consumers, the extent to which PSPs can "stop the clock" in a "proportionate" and "reasonable" manner, and the line between fraud and civil disputes. These issues are likely to lead to an escalation of referrals to the FOS and litigation to ascertain how these facets of the Scheme should apply in practice.

3.1.1 Customer standard of caution

The PSR has published additional guidance on the customer standard of caution but there remains further areas of uncertainty. In summary, the guidance provides that the standard has four aspects:

- A requirement for consumers to have regard to specific, directed warnings.
- A prompt reporting requirement.
- An information sharing requirement necessitating that consumers respond to "reasonable and proportionate requests".
- Reporting to the police where requested.

If it can be demonstrated that the consumer has been grossly negligent in not meeting one of more of these requirements, then they may not be reimbursed. The PSR has explained that "gross negligence is a very high bar which will critically depend on the individual circumstances of each case". It is unclear how these four points should apply in practice. For example, the extent to which warnings may be considered in assessing the customer's fault.

A further area of difficulty is ascertaining vulnerable consumers that are not subject to the customer standard of caution and the claims excess. The problems identifying and managing vulnerable consumers are evident from a recent FCA review that has presented a mixed picture of outcomes by firms.

Based on the high standard of negligence and the vulnerable consumer carveout, consumers only have to exercise limited care in processing payments and the primary burden is on PSPs to expand warnings to tackle fraud and request and respond to information provided by the consumers in a proactive manner. This is evident from the PSR figures showing that firms have been reluctant to rely on the gross negligence/consumer standard, with only a 2% rejection rate on this ground. The high standard is in marked contrast to the more limited grounds for a claim that has evolved under the common law. In this respect, we may see an awkward tension arise where claims above £85,000 result in reimbursement under the Scheme up to £85,000, with the remainder of the sums dissipated subject to litigation in the courts on potential breaches of bank's duties when executing payment. In turn, the Scheme may send misleading messages to consumers on the extent to which they can claim compensation for losses flowing from fraudulently induced transactions.

3.1.2 Stop the clock

Although the "stop the clock" provisions allow Sending PSPs to conduct further investigations, consumers only need to respond to "reasonable and proportionate requests for information" [PSR (2023a)]. Receiving PSPs are also not permitted to engage with the defrauded customer but are still liable for 50% of the costs. This may place an unfair burden on Receiving PSPs, particularly where a Sending PSP has not exercised adequate skill and care in identifying and preventing fraud. There are currently limited ways to deal with failing PSPs to ensure a fair distribution of liability based on the steps taken by the relevant PSPs to tackle fraud (see, section 3.3 below). The PSR has confirmed that they have no plans to provide any additional guidance on the meaning of "proportionate" use of stop the clock provisions, which leaves scope for differing interpretations of the provisions.

3.1.3 Civil disputes

Victims of APP fraud may not rely on the Scheme where the claim relates to a civil dispute. This may be an important defense to many APP fraud claims that are more appropriately addressed via civil dispute mechanisms and not mandatory reimbursement. There has been recent guidance on this issue, which focuses on assessing the nature of the relationship with the purported scammer to ascertain whether the case is more akin to a business dispute on the provision of goods/services than to a fabricated business transaction that has duped

the consumer.[7] However, the line between civil disputes and fraud claims remains unclear and is likely to lead to disputes. This is supported by the PSR figures indicating a third of recent cases fell outside of the Scheme mainly due to the matter being a civil dispute and the FOS concerns with managing claims with other agencies due to this issue (see Section 2.1 above).

3.1.4 The consequences of uncertainty

Due to the vagueness around these and other features of the Scheme, the PSR accepted that there may be a degree of uncertainty during the implementation stages that could lead to increases in disputes referred to the FOS [PSR (2022a)]. We may, therefore, see FOS complaints driven significantly higher as customers and PSPs attempt to navigate the interpretation of the Scheme.

Unfortunately, the nature and structure of the FOS system results in limited scope for regulatory or judicial authority to provide for consistency or guidance in future cases and there is a lack of alignment between FOS and FCA expectations. There are expected reforms to the FOS to address the way it manages cases to address these and other shortcomings. It will be important to monitor how these proposals are implemented to assess whether it will result in meaningful changes.

As well as concerns with the ability of the FOS to oversee the Scheme, similar fears have arisen on the extent to which Pay.UK and the PSR can effectively oversee the implementation of the measures. The PSR will be absorbed into the FCA later this year. The Government plans to consult on the details of the proposals and will legislate to formalize the changes shortly thereafter.[8] The consolidation of the PSR into the FCA is part of the government's broader Plan for Change and Industrial Strategy, which aims to create a regulatory environment that supports economic growth and increases living standards by reducing unnecessary regulatory burdens on businesses.

The concerns around the operation of the Scheme were reflected in an April 2025 report by the All-Party Parliamentary Group on Fair Banking. The report concluded that complaints relating to APP fraud and scams have "rocketed" during recent years and names and shames specific banks that are purported to be failing to address complaints correctly; noting "[a]necdotal evidence suggest that some firms are either not responding to fraud reports and compensation requests, or taking far, far longer than the five days now mandated by the MRR" [APPG (2025)]. This illustrates how scrutiny of Scheme will likely be placing increasing public pressure on banks to ensure they react appropriately to claims. A further report was published in July 2025 indicating further concerns with the Scheme. Consequentially, the reports recommend several changes to the Scheme, including:

- Extend the Scheme to international payments and crypto-asset fraud.
- Increase the £85,000 cap on claims.
- Introduce a levy on other businesses outside the finance sector that may contribute to the underlying fraud.
- Greater disclosure of the specifics of fraud (including number of complaints relating to non-payment of reimbursements referred to the FOS).
- Clearer pathways for reporting and claiming.
- Improved compliance with the five-day target for compensation under the Scheme.
- Improved warnings.

We are awaiting the Government's response to these proposals.[9]

It will be important to monitor the outcome of these expected policy developments to assess whether we will see changes to the regulatory oversight of the Scheme (including on how the FOS, PSR, and Pay.UK operate), as well as the operation of the Scheme. It seems likely that we will at least see an increase in the type of data that PSPs will need to provide. Pending reforms, there will remain difficulties for financial institutions assessing the appropriate response to the more difficult cases potentially falling outside the Scheme. Ultimately, this may cause a continued steady stream of cases reaching the FOS and court for resolution, which does not align with the objective of the reforms.

7. On 23 September 2024, the PSR published its policy statement [PSR (2024a)] and final guidance [PSR (2024b)] to help PSPs assess whether an APP fraud claim raised by a customer relates solely to a civil dispute and is, therefore, excluded from the reimbursement requirement.
8. https://tinyurl.com/4fdy76cx
9. The second report confirmed there will be an independent review into the Scheme during the next year and has urged the Government to introduce reforms as part of an updated Fraud Charter that will be published in late 2026.

3.2 Balancing payment friction and protecting consumers

An overarching practical difficulty with the regime is how PSPs can balance the importance of protecting consumers from fraud and not causing excessive friction when processing payments. Although the PSR has indicated it expects additional payment friction, this may be at odds with FCA requirements in relation to the Consumer Duty to ensure customers are satisfied with services offered, including speed and compliance with instructions. For example, the FCA has warned firms that they should not be creating excessive friction in processing payments when looking to act in compliance with the new Duty. In a "Dear CEO" letter to Payment Firms, the FCA criticized "poor financial crime controls," adding that some firms were failing to combat fraud and choosing to "freeze a disproportionate number of accounts, for too long, and without adequate explanation" in response to potential threats [FCA (2023)]. The letter urges firms to take better care of their customers by freezing accounts less frequently, investigating possible fraud faster, communicating better with affected customers, and supporting those "put in acute financial difficulty" after having their accounts frozen. Similar sentiments were expressed in the FCA's multi-firm review of anti-fraud controls and complaint handling in firms with a focus on APP fraud; which reiterated concerns over firms' account freezing practices.

Despite FCA statements warning against excessive frictions, recent amendments to the Payment Services Regulations allow PSPs to adopt a risk-based approach to processing payments to provide more time to assess potentially fraudulent payments where needed. In November 2024, the FCA published its final guidance for payment services and electronic money to explain how PSPs should apply the legislative changes to minimize the impact on legitimate payments [FCA (2024)]. The final guidance provides further details on how PSPs can use the payment delay window to investigate fraud where there are reasonable grounds to suspect fraud. It indicates that PSPs have a wide degree of discretion to freeze customer accounts in the case of fraud even where this may result in friction in payment processing.

The conflicting messages on how to manage fraud prevention and customer expectations creates challenges for PSPs acting consistently with regulatory expectations. The complexities are illustrated by the U.K. Finance statistic that 31% of financial institutions are having difficulty measuring and understanding effective ways of combatting scams [U.K. Finance (2023)]. As to the former, the PSR reimbursement framework aims to protect consumers by encouraging PSPs to implement fraud prevention measures, including expanding the use of warnings to allow customers to exercise adequate caution. However, measures are not watertight because of the widespread nature of APP fraud in circumstances where PSPs cannot readily identify victims. Low value purchase scam payments are extremely problematic for PSPs to detect and prevent because they are not easily differentiated from other low-value payments. Even when established, it is often problematic to determine if they fall within the scope of a scam or a dispute, as there is often very limited evidence available.

Given the evolving picture of the Scheme, the safest course for many PSPs will be to err on the side of caution and freeze payments where there are fears of fraud. This would be consistent with the common law position, where it is rare to see a customer successfully claim against a bank for loss caused by freezing an account due to fraud. In light of this context, systems and controls should be designed to slow or freeze transactions in a wide range of cases. Likewise, frontline staff should be vigilant and encouraged to intervene wherever suspicion of fraud arise, although the level of intervention ought to be case-specific. A further tool that can be used is that Sending PSPs can agree to indemnify Receiving PSPs for losses arising from freezing a customer account. This may allow the quick retrieval of funds even after fraudulent transactions are processed. Information sharing to prevent and tackle fraud is also helpful. There have been efforts to facilitate voluntary information sharing by financial services firms under the Criminal Finances Act 2017 and Economic Crime and Corporate Transparency Act 2023 (ECCTA). The ECCTA recently extended the instances when regulated firms can share data to go beyond Anti-Money Laundering to cover preventing economic crimes. It also allows the sharing of data outside the AML regulated sector in certain instances.

3.3 Compliance

Although Pay.UK is responsible for monitoring compliance with the reimbursement rules, enforcement remains the responsibility of the PSR. This division of monitoring and enforcement arises because of the nature of FPS, which operates via

contractual arrangements between Pay.UK and members, i.e., PSPs, as opposed to authorization via regulation. Where Pay.UK considers that further action is necessary to address non-compliance, it will initiate a series of management steps, which may involve implementing a mitigation action plan, enhanced monitoring, and engagement of senior level executives.

Initially, the PSR envisages that Pay.UK should take steps to address failings, which if unresolved should be referred to the PSR. The statutory instruments implementing the Scheme allow the PSR to intervene where necessary. The integration of the PSR into the FCA also suggests that there are efforts to expand the enforcement capabilities of the regulator. A Memorandum of Understanding between the FCA and PSR and other regulators also facilitates the sharing of information with a view to improving enforcement outcomes. Examples where the PSR expects Pay.UK to refer a case include:

- A consistent failure by a PSP to abide by the new reimbursement requirement.
- Data collection failings.
- An extreme compliance failure by a PSP to abide by the new reimbursement requirement [PSR (2023b)].

In the past, the PSR has issued directions for operational resilience failings, such as the direction implementing a fine for 2.4 million as a result of declined customer transactions in a six-hour period due to a system breakdown [PSR (2019)]. We have also seen fines for overcharging customers due to the incorrect application of payment rules to consumer credit card customers [PSR (2022b)]. We may see similar action depending on how the Scheme is managed by PSPs. In the future, the PSR may also look to hold senior managers accountable in line with its legislative Regulatory Principle to ensure "[t]he responsibilities of the senior management" for compliance with PSR requirements, including general directions. It is, therefore, important that those supervising implementation have adequate measures in place to exercise adequate oversight.

4. Preparing for developments

Given the complex and emerging aspects of the Scheme, financial institutions need to employ bespoke approaches for different categories of customers and react to a developing legal framework. In circumstances where firms cannot easily predict which regime applies as part of a multi-tiered and inconsistent legal and regulatory environment, this can result in significant challenges for the sector. Particularly as claims in relation to the Scheme are likely to increase and we may also see greater reporting requirements.

To ensure PSPs adequately implement the new measures, they ought to consider the following steps as appropriate in light of existing safeguards:

- Expand investigations of the threats to customers and align protection accordingly.
- Increase fraud awareness initiatives.
- Identify transactions at higher risks of APP fraud (e.g., large and unusual transaction in light of customer's banking history).
- Identify at-risk accounts to fraud and increase additional safeguards.
- Identify vulnerable consumers and contact this group with further information on how to protect themselves against fraud.
- Train staff on the changes.
- Implement additional methods where possible to freeze and recover fraudulently transferred funds.
- Use risk-based, tailored, and effective warnings to help prevent fraud.
- Continually re-evaluate and return to previous plans to reflect ongoing developments.
- Information sharing to tackle fraud.
- Develop a functioning data collection and filtration system to adhere to new disclosure requirements.

With expected publication of data on the Scheme and anticipated reforms to the financial services regulatory architecture predicted, PSPs should monitor anticipated developments closely and react appropriately as information materializes.

References

APPG, 2025, "Authorised push payment fraud – who bears the burden?," All-Party Parliamentary Group, March, https://tinyurl.com/3cyfywx3

Bank of England, 2025, "The Bank of England, Financial Conduct Authority, Prudential Regulation Authority, and Payment Systems Regulator revise Memorandum of Understanding in relation to payments in the UK," June 24, https://tinyurl.com/mpw7k5nd

FCA, 2023, "Dear CEO letter: implementing the consumer duty in payment firms," Financial Conduct Authority, February 21, https://tinyurl.com/mrhbc5rm

FCA, 2024, "Guidance for firms that enables a risk-based approach to payments," Financial Conduct Authority, finalized guidance FG24/6, November 22, https://tinyurl.com/bdd6esth

FCA, 2025, "Annual Report and Accounts: for the year ended 31 March 2025," Financial Ombudsman Service, https://tinyurl.com/4dz9h5fr

FOS, 2024, "Quarterly complaints data: Q2 2024/25," Financial Ombudsman Service, November 27, https://tinyurl.com/8m8auwnd

PSR, 2019, "PSR PS19/3 - Specific Direction 9 (Crisis Communications: Visa)," Payment Systems Regulator, May 30, https://tinyurl.com/4etxfrau

PSR, 2022a, "Consultation paper CP22/4: authorised push payment (APP) scams: requiring reimbursement," Payment Systems Regulator, September 29, https://tinyurl.com/5x3s2m3j

PSR, 2022b, "PSR fines £1.82m for overcharging interchange fees on credit cards," Payment Systems Regulator, May 12, https://tinyurl.com/3v4z2hvd

PSR, 2023a, "PSR Consultation paper CP 23/7: APP fraud: the consumer standard of caution," Payment Systems Regulator, August 15, https://tinyurl.com/fcfcwkrp

PSR, 2023b, "Policy statement PS23/3: fighting authorised push payment fraud: a new reimbursement requirement, Response to September 2022 consultation (CP22/4)," Payment Systems Regulator, June, https://tinyurl.com/mv7wahp4

PSR, 2024a, "PS24/6 Supporting the identification of APP scams and civil disputes," Payment Systems Regulator, September 23, https://tinyurl.com/bdfywnfd. PSR, 2024b, "Authorised push payment scams reimbursement requirement: supporting the identification of APP scams and civil disputes," Payment Systems Regulator guidance, September, https://tinyurl.com/2kkd2rj2

PSR, 2025, "The story so far: a snapshot of what we've seen since our APP scams reimbursement requirement went live," Payment Systems Regulator thought pieces, May 15, https://tinyurl.com/mryu8rtn

U.K. Finance, 2023, "Scams legislation and prevention: understanding the human factor," online event, July 6, https://tinyurl.com/26cu3prk

Future of Payments

Challenges for banks: e-wallets and the application of strong customer authentication

Jan Jans,
Partner, RegCounsel Financial Services

ABSTRACT

The digitalization of payments has elevated the role of technical service providers (TSPs), such as e-wallet providers, in the client-facing layer of the payment chain. Their growing involvement poses challenges for card-issuing banks, particularly regarding their obligation to apply strong customer authentication (SCA) under the Revised Payment Services Directive (PSD2). This article argues that TSPs involved in the authentication process act as outsourced service providers for the purposes of SCA, triggering compliance with the broader outsourcing framework - including the EBA Guidelines on Outsourcing and DORA. As TSPs are not typically subject to direct supervision by financial regulators, banks may struggle to enforce the contractual safeguards required by outsourcing rules. This tension raises questions about enforcement and accountability in the current regulatory architecture.

1. Introduction

In the past decades, the digitalization of the European retail payment market has resulted in a significant increase in the development of new and innovative payment products, including the introduction of contactless payment methods [E.U. (2023)]. While payment products were initially primarily offered by banks, non-regulated service providers are increasingly taking part in the payment chain. Some of these service providers develop client-facing interfaces that enable payment service users (PSUs) to use their bank issued debit or credit cards to make payments. For example, BigTechs, such as Apple, Google, and Samsung, offer digital wallets that are used by PSUs to make contactless payments with tokenized debit and credit cards using the Near Field Communication (NFC) chip installed on their smartphone (e-wallets). The services offered by e-wallet providers are typically in support of the payment services offered by banks and do not in themselves qualify as regulated payment services, as described by PSD2, as these e-wallet providers are never in possession of the funds that are transferred. Consequently, these service providers, also referred to as technical service providers (TSP) under PSD2, are not required to obtain payment service provider (PSP) licenses and are, therefore, not subjected to the PSD2 framework.

With the increasing participation of unregulated service providers in the payment chain, banks are facing additional challenges when trying to safeguard the security of their electronic payment offerings. In addition to adding layers of complexity to the payment process, banks are also facing additional challenges when trying to meet their own legal obligations. One area where this is causing concern for banks is the undertaking of strong customer authentication (SCA) while having to rely on the e-wallet providers even though they are not mandated to undertake such authentication by PSD2.[1]

In June 28, 2023, the European Commission (Commission) published a proposal for a payment services regulation (PSR Proposal) as part of the Financial Data Access and Payments Package,[2] which, amongst others, aims to strengthen PSU protection as well as the confidence in the use of payment products by introducing improvements to the application of SCA involving e-wallets. The PSR Proposal was amended by the European Parliament (EP) on April 23, 2024 (EP Amendment) and by the Council of the European Union (Council) on June 13, 2025 (Council Amendment) and has entered the trilogue negotiations at the moment of writing.

This article analyses the proposed amendments to the PSD2 SCA requirements for banks in the context of e-wallets under the PSR Proposal, thereby taking into account the practical challenges banks are facing as a result of their interactions with TSPs offering e-wallets.

2. Strong customer authentication (SCA) under PSD2

When a bank receives a payment order from a PSU, the PSD2 authentication obligation requires it to verify the identity of the PSU and the use of the payment instrument by the PSU (Article 4(29) PSD2). SCA is an enhanced form of authentication that requires a combination of at least two authentication elements categorized as knowledge, possession, and inherence (Article 4(30) PSD2). The "knowledge" element relates to information that only the PSU has (e.g., PIN code or password). The "possession" element refers to something that only the PSU possesses (e.g., a random reader or a smartphone). The possession element does not have to be something physical but can also be non-physical such as an app, provided there is a unique connection between the possession element and the PSU [EBA (2020)]. The "inherence" element reflects something that the PSU is (e.g., fingerprint scanning, facial recognition, or behavioral biometrics) [EBA (2019a)]. For online card payments, the technology most used by banks to conduct SCA is 3D Secure,[3] which involves a security protocol to confirm the PSU's identity using, for example, the PSU's fingerprint [E.U. (2023)].

1. It should be said that while they are not covered by PSD2, e-wallet providers are subject to the Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA) as part of their role as "arrangement providing functionalities supporting the use of electronic payment instruments".
2. Further to the PSR Proposal, the Financial Data Access and Payments Package also includes a proposal for the Third Payment Services Directive (PSD3) and a Financial Data Access (FiDA) Regulation.
3. 3D Secure was introduced in 2018 by EMVCo, which is a consortium between Visa, American Express, Mastercard, China UnionPay, Discover, and JCB.

The two elements used for the SCA process must be mutually independent, meaning that a security breach of one element should not result in a breach of the other element.[4] The requirement that the authentication elements must be mutually independent means, according to the European Banking Authority (EBA) PSD2, that the two elements have to belong to two different categories [EBA (2020)].

A valid combination of two authentication elements results in the generation of a unique authentication code, which is accepted only once by the bank for the execution of a payment (Art. 4(30) PSD2 jo. art. 4(1) Delegated Regulation (EU) 2018/389). In the event that SCA is applied for a so-called remote payment (i.e., payment initiated via the internet or a device for distance communication), the bank must apply dynamic linking, which involves the generation of a unique authentication code specific to both the transaction amount and the identity of the beneficiary) (Article 97(2) PSD2.). It should be noted that even contactless payments via a QR code qualify as remote payment transactions because they are initiated via the internet, and, therefore, require dynamic linking as part of SCA.

2.1 When is strong customer authentication (SCA) required?

PSD2 requires banks to apply SCA in the event that the PSU: (i) accesses its payment account online, (ii) initiates a payment in the capacity as payer,[5] (iii) creates a list of trusted beneficiaries (i.e., businesses assigned by the PSU to a whitelist of trusted beneficiaries), or (iv) carries out an action through a remote channel which may imply a risk of payment fraud (Article 97(1) PSD2).

In order to help with the development of user-friendly and low-risk payment services, banks are allowed to disapply SCA in certain circumstances (Recital 11 Delegated Regulation (EU) 2018/389). For example, an acquirer can request that the bank applies a transaction risk-based exemption for SCA for low-risk transactions if the acquirer's or bank's fraud rates are below certain thresholds (Article 18 Delegated Regulation (EU) 2018/389). Furthermore, in order to establish some kind of balance between enhanced security and user-friendliness in remote payments, the bank can decide to disapply SCA for remote low value payments (i.e., transactions that do not exceed €30), provided that the total transaction amount initiated with a particular payment instrument since the last time SCA was applied does not exceed €100 and that there have not been more than 5 consecutive transactions since the last application of SCA (Article 16 Delegated Regulation (EU) 2018/389). Banks can also choose not to apply SCA for recurring fixed-amount transactions from the second transaction onwards, provided that the beneficiary and the transaction amount do not change (Article 14 Delegated Regulation (EU) 2018/389).

It is important to note, however, that the decision not to apply SCA is not risk free, since under PSD2 the bank remains liable for any unauthorized transaction, unless the payer has acted fraudulently (Article 74(2) PSD2).

3. E-wallets and the obligation to conduct strong customer authentication (SCA)

With an e-wallet, the PSU can use its bank-issued payment instrument (e.g., debit- or credit card) to make online or contactless payments (i.e., remote payments) via its smartphone through a process called tokenization [E.C. (2023a)]. Tokenization involves the replacement of the PSU's primary account number (PAN) with a unique algorithmically generated number referred to as the payment token (Token).[6] According to the Commission, the Token itself is not to be considered a "payment instrument "within the meaning of PSD2 but merely a "payment application" within the meaning of article 2(21) of the Interchange Fees Regulation [E.U., 2015)] (Recital 24 PSR Proposal). According to EBA, the Token can qualify as a "possession element" for SCA purposes provided that the card issuer is involved in the issuance of the Token [EBA (2020)]. A PSU that wishes to use an e-Wallet for making payments, must first add one of its payment instruments to its e-wallet.

4. Article. 9(1) Delegated Regulation (EU) 2018/389. If a PSU uses a multipurpose device for conducting SCA, such as a smartphone, article 9(3) Delegated Regulation (EU) 2018/389 requires the PSP to use separated secure execution environments via the software installed on such device.
5. SCA is required for online European payments. This means both the merchant's and cardholder's Bank are established in Europe.
6. The main difference between tokenization and encryption is that with tokenization the original data cannot be recovered from the Token.

3.1. Adding a payment instrument to an e-wallet

When a PSU adds a debit or credit card to its e-wallet, the card details (including the PAN) are shared with the TSP offering the e-wallet, which subsequently identifies the bank who issued the respective card. Upon receipt of the PAN related to the card that is to be added to the e-wallet, the bank requests a so-called token service provider, such as Visa Token Service or American Express Token Service, to issue a Token for the relevant card. Both the Token and PAN are stored by the token service provider and the Token is shared with the bank. Subsequently, the Bank shares the Token with the TSP offering the e-wallet, which stores the Token in the secure element of the PSU's smartphone (secure element).[7]

The process of tokenization, where the PAN is replaced by a Token, is considered by PSD2 to constitute an "action through a remote channel which may imply a risk of payment fraud or other abuse," which means that if a PSU adds a card to its e-wallet, the card issuing bank is obligated to conduct SCA as part of this process. In fact, Article 85 of PSR Proposal explicitly states that SCA must be applied at the moment of a Token creation or replacement. Consequently, the PSU is directed to the online interface of the bank to complete SCA before the bank requests the token service provider to issue the Token.

3.2. Initiating a payment with a tokenized card

If a PSU wishes to initiate a payment via its e-wallet, the "authentication" obligation under PSD2 requires the bank to verify the identity of the PSU (also referred to as customer authentication) as well as the details of the transaction (also referred to as transaction signing) (Article 4(29) PSD2). With ordinary card payments, these processes are both completed by the card issuing bank, whereas with e-wallets, customer authentication takes place within the e-wallet interface instead of the bank's interface. In other words, if a payment is initiated with an e-wallet, it is the TSP, rather than the bank, who verifies the identity of the cardholder.

Thereafter, the Secure Element generates a cryptogram for the transaction, which is based on the transaction information and Token. The cryptogram is sent together with the transaction information and Token to the acquirer via the merchant's Point of Sale (PoS) device. The cryptogram and Token are then sent to the card network, which validates the cryptogram and de-tokenizes the Token. Subsequently, the card network sends the PAN and transaction data to the bank, which is responsible for the verification of the payment instruction initiated with its card (i.e., the transaction signing) and the transfer of the corresponding funds to the acquirer.

3.3. Interplay between the bank and TSP

Given that under PSD2 the bank is responsible for both customer authentication and transaction signing, the question arises as to whether the customer authentication conducted by the TSP as part of an initiated payment via an e-wallet qualifies as the outsourcing of an element of the SCA requirement to the TSP [Jans (2024)].

Given that the bank receives confirmation from the TSP that the PSU's identity has been verified instead of the bank actually verifying its identity, the bank relies on the correctness of input provided by the TSP in order to complete the "authentication process".

In my opinion, the involvement of the TSP in the authentication process constitutes outsourcing, as outlined by the regulatory framework, which means that the bank must comply with numerous legal requirements applicable to outsourcing arrangements, in particular if the involvement of the TSP constitutes critical outsourcing.

This implies that the bank will not only be required to meet the outsourcing requirements under the EBA Guidelines on outsourcing [EBA (2019b, 2025)] but also the outsourcing requirements imposed under the Digital Operational Resilience Act (DORA).[8] For example, the bank will have to ensure adequate oversight of the performance of the TSP's outsourced functions and enter into an outsourcing agreement with the relevant TSP that

7. For example, iPhones have a "secure element" in their NFC chip where the Token is stored. The PAN is never stored on the device.
8. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. DORA forms part of the broader Digital Finance package of the Commission and seeks to bring harmonization of the rules relating to operational resilience for the financial sector. The European Supervisory Authorities (ESAs) are currently preparing to designate critical third-party service providers (CTTSP) under DORA. Given the important role of certain TSPs in the SCA process, it is likely that (some of) these TSPs will be designated as CTTSP under DORA.

allows the bank to have a certain level of control over the outsourced function, such as the bank's audit rights. Before signing such an agreement, DORA requires the bank to conduct a thorough risk assessment, which includes, amongst others, an assessment of operational, legal, ICT-related, reputational, and data protection risks. If the TSP does not meet the agreed key performance indicators (KPIs) and no other remedy is available, the bank must either transfer the outsourced function to a third party or conduct this process itself.

Given that the current PSD2 framework does not explicitly consider such TSP involvement as outsourcing, legal outsourcing requirements have typically not been made part of any contractual arrangement between banks and TSPs offering e-wallets. Offering e-wallet solutions, therefore, gives rise to regulatory concerns since banks are not able to apply any controls or checks on the security measures and their compliance with the requirements of PSD2, Delegated Regulation (EU) 2018/389 and DORA. Moreover, given that the PSD2 framework for SCA is not directly applicable to TSPs, there is no regulatory incentive for TSPs to assist the banks in meeting their regulatory obligations.

4. The PSR Proposal

In its evaluation of PSD2, the Commission concluded that the application of SCA by PSPs has been very successful in reducing payment fraud (Recital 107 PSR Proposal). This view is also supported by other evaluations, such as the joint report on payment fraud in the European Economic Area published by the EBA and the European Central Bank in August 2024 [EBA/ECB (2024)]. Although the security of payment transactions has improved as a result of the SCA requirement, the Commission's evaluation also shows that the obligation to conduct SCA has made the customer journey for certain PSUs more difficult [E.C. (2023b)]. For example, the fact that there is still a significant number of PSUs who do not, or cannot, use smartphones for online and contactless payments imposes barriers for these persons to complete the SCA process. To improve financial inclusion, the Commission, therefore, stresses, in line with the European Accessibility Act [E.U. (2019)], the importance of banks facilitating all PSUs, including those who do not have access to digital devices such as smartphones, to benefit from protections against fraud that are provided by SCA [E.C. (2023a)].[9]

Generally, however, the use of the smartphone as part of the SCA process has taken a prominent role in the payment chain. With the increasing use of e-wallets by PSUs and the lack of a clear legal framework covering the interplay between banks and TSPs, the Commission considered it essential to address TSP involvement in the SCA process in the PSR Proposal [E.C. (2023a)]. The Commission takes the view that the involvement of e-wallet providers in the SCA process constitutes outsourcing and that such TSPs should, therefore, be subject to the legal requirements covering outsourcing arrangements by PSPs. Although the Commission recognizes the importance of TSPs as part of the payment chain, it does not want to go as far as bringing these service providers within a PSP license regime at this point in time [E.C. (2023a)].

4.1. E-wallets and the outsourcing of part of the SCA process

The Commission suggests in the PSR Proposal that TSPs that verify elements of the SCA will be required to enter into outsourcing agreements with the banks regarding their involvement in the SCA process, and liable for failure to support the application of SCA (Article87 PSR Proposal). As with outsourcing in general, it is explicitly mentioned in the PSR Proposal that in case of outsourcing the bank remains fully liable *vis-à-vis* the payer for any failure to apply SCA (Article 87(2) PSR Proposal). To ensure that this legal obligation can be enforced in practice, the Commission suggests that the competent authorities overseeing compliance with the payments framework shall have the power to require all the information from TSPs that it considers necessary to carry out any investigation of potential breaches of the law (Article 91(5) PSR Proposal). The PSR Proposal does not, however, seem to allow competent authorities to also impose administrative measures or sanctions on TSPs in case of a breach of law.

The EP appears to take a different view regarding the qualification of TSP involvement in the SCA process given that the requirement for the bank to have an outsourcing agreement in place with the TSP has been deleted in the EP Amendment.

9. According to Recital 110 PSR Proposal, PSPs must ensure that their customers can benefit from various methods to perform SCA which are adapted to their needs and situations, which should not depend on one single technology, device or mechanism, or on the possession of a smartphone or another smart device.

This deletion has, however, been reversed by the Council, which suggests that there is a lack of agreement between the European institutions on how to best address this topic (Article 87(1) Council Amendment). It remains to be seen which position will make it to the final text of the PSR Proposal after the trilogue negotiations.

Further to the legal qualification of TSP involvement in the SCA process, the Commission takes the view that the TSP is to be held liable in case of failure to support the SCA process. To this end, the Commission included in the PSR Proposal that TSPs offering e-wallets are to be held liable for failure to support the application of SCA *vis-à-vis* the bank within the remit of their contractual relationship (Article 58 PSR Proposal). Although the EP does not require the bank and the TSP to enter into an outsourcing agreement, it does maintain this liability provision, albeit with the limitation that the TSP is only to be held liable in these circumstances for "direct" financial damages whereby the liability should be proportionate to the shortcoming and the amount of the transaction (Article 58 EP Amendment). It strikes me as odd that the EP does not recognize the TSP involvement as outsourcing and at the same time wants to hold the TSP liable if it falls short in its involvement in this process. In line with the Commission, the Council suggests to broaden the scope of the TSP's liability by stating that the TSP is to be held liable for "any financial damage" rather than "direct financial damage" (Article 58 Council Amendment). Furthermore, the Council aims to make this requirement directly applicable to TSPs under the Council Proposal (Article 1a PSR Proposal).

It is also helpful for banks that from a competition law perspective steps have been taken regarding third party access to the NFC antenna installed on smartphones. On March 19, 2025, the Commission ruled that Apple, acting in the capacity of "gatekeeper" under the Digital Markets Act (DMA) [E.U. (2022)], must open up iOS connectivity features to third-party devices [E.C. (2025)]. Initially, smartphone producers that also operate as e-wallet providers did not provide third-party access to these devices, which meant that banks could not develop their own e-wallet solutions to be installed on a smartphone. Furthermore, because of the lack of access, banks were not able to transfer the outsourced SCA process to themselves or another service provider if the KPIs were not met by the e-wallet provider that also produced the smartphone on which the e-wallet is installed. With the Commission's decision, an important step is made to help banks meet their legal obligations when their cards are being used for making payments via an e-wallet.

5. Conclusion

With the further digitalization of the payments market, TSPs offering e-wallets have acquired a prominent role in the payment chain. It has, therefore, become even more important to have clear rules on the interplay between card issuing banks and TSPs when it comes to TSP involvement in the SCA process.

With the PSR Proposal, the Commission has taken an important step towards recognition of the role of e-wallet providers and the legal challenges that they impose on banks under the PSD2 framework. Although the EP appears to take a different view, the Commission and Council clearly recognize the involvement of these service providers in the SCA process as outsourcing by the card issuing bank. This means that the bank is obligated to implement the legal outsourcing requirements *vis-à-vis* the TSP, which is currently difficult given that PSD2 does not explicitly recognize this legal qualification and does not impose any requirements in this regard on TSPs. Although I welcome the steps that are suggested by the Commission and the Council with the PSR Proposal, these amendments do not, in my view, fully take away the practical challenges that banks face in this regard. Although the outsourcing requirements should theoretically be complied with when the bank and TSP have an outsourcing agreement in place, the fact that the competent authorities supervising the payments sector cannot impose enforcement measures or administrative sanctions on TSPs regarding their involvement in the payment chain, may in practice result in a lack of incentive for these TSPs to ensure that individual banks can comply with the regulatory framework. In practice, this means that it is not unlikely that individual banks may encounter difficulties in agreeing on the required documentation with TSPs, in particular when these TSPs have a dominant market position. The fact that the Council suggests to explicitly apply the PSR outsourcing requirements to TSPs does not, in my view, alter these practical concerns given that the Council Amendment does not seem to allow competent authorities for the payments sector to impose enforcement measures or administrative sanctions on TSPs in case of a breach of law.

Although it remains to be seen how the Digital Markets Act (DMA) and the critical third-party service providers (CTTSP) designations by the ESAs under DORA will impact compliance by TSPs with these requirements, it might help to consider the option of bringing TSPs that support the authentication process within the remit of supervision by these competent authorities, even if it is merely a registration requirement. Better supervision of TSP compliance with the outsourcing requirements could in my view be provided for when these TSPs are brought under the supervision of the competent authorities for the payments sector.

References

EBA, 2019a, "EBA publishes an Opinion on the elements of strong customer authentication under PSD2," European Banking Authority, June 21

EBA, 2019b, "Final report on EBA Guidelines on outsourcing arrangements," European Banking Authority, EBA/GL/2019/02, February 25

EBA, 2020, "Strong customer authentication and common and secure communication (incl. access)," European Banking Authority, July 24

EBA, 2025, "The EBA launches consultation on its draft Guidelines on third-party risk management with regard to non-ICT related services," European Banking Authority, July 8

EBA/ECB, 2024, "The EBA and ECB release a joint report on payment fraud," European Banking Authority and European Central Bank, August 1

E.C., 2023a, "On the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market," European Commission, June 28

E.C., 2023b, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)," European Commission, February 2

E.C., 2025, "Commission provides guidance under Digital Markets Act to facilitate development of innovative products on Apple's platforms," European Commission, March 19

E.U., 2015, "Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (Text with EEA relevance)," European Union, April 29

E.U., 2019, "Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance)," European Union, April 17

E.U., 2022, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)," European Union, September 14

E.U., 2023, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)," European Union, FISMA/2021/OP/0002

Jans, J. A., 2024, Electronic payments in the European market: creating a level playing field between banks and non-banks, EBI Studies in Banking and Capital Markets, Palgrave Macmillan

Future of Payments

Data management and its impact on industry

John A. Bottega,
President, EDM Association

ABSTRACT

For the past 20 years, data management has transformed from a back-office function into a core strategic capability across industries. The 2008 financial crisis accelerated this transformation by exposing the risks associated with failing to properly curate and understand our critical information assets. It pushed data management to the forefront, and today, all industries are recognizing how improved data management disciple will not only avoid risk but create competitive opportunities and improved operational efficiencies. In this paper, we explore, through the exploration of a number of real-world case studies, how deploying improved data management capabilities are helping to improve corporate efficiency. Across all industries, data management is now a critical function and key factor in the success of organizations competing in an ever-increasing digital economy. And to be competitive in this new world of AI, data is the fuel that feeds our AI programs and proper data management will increase the probability that our AI implementations will be accurate, ethical, and trusted. Data integrity is critical in complex business systems where any weakness in data quality or security threatens the entire process. This paper underscores the need for disciplined data management practices, ethical standards, and investment in data-centric leadership to support a stable and innovative global economy.

1. Introduction

If you go back 20 years, you would be hard pressed to find organizations with dedicated data management organizations. Data management was either a function of technology, or it lived in the back-office, largely driven via manual processes. The emergence of formal data management titles really did not appear until the mid-2000s, when organizations started to recognize data as a critical corporate function, rather than a stepchild of technology.

But it was not until data and data management rose to the C-Suite of the financial services industry, largely driven by the financial crisis of 2008, that suddenly data management was on the agenda of every senior executive and every corporate Board of Directors. Regulatory pressure stemming from the financial crisis took a magnifying glass to how organizations were collecting, curating, maintaining, utilizing, and protecting their data assets. The crisis brought scrutinous attention to the impact and risks associated with making critical business decisions without accurate, timely, and trusted data. The financial services industry was amassed in data but lacked a structured data management discipline.

Today, data management is no longer an afterthought, but one of the most important activities of an organization, impacting every aspect of a company's operation. No longer just a financial services industry focus, data management has become the focus across all industries. It has become the backbone of decision-making, innovation, and operational efficiency, woven into the fabric of every business function.

As a society, we are constantly generating new data. This has exploded in our increasingly digital world. Information captured and collected from our mobile phones, personal devices, and online and social media sites provide retailers, manufacturers, technology firms, and even federal, state, and local governments with insights into our movements, habits, likes, and dislikes. Cloud adoption has made massive amounts of data easy to store and even easier to access and retrieve. Regulations such as GDPR and the numerous privacy laws put the demand on organizations to ensure data is protected, privacy laws are respected, and data is being used in an ethical manner. Data management has become one of the most important activities that determines a company's success or failure in our digital economy.

2. AI for data for AI

Today, with the advent of AI and machine learning, data management is even more important. There is no debate that AI is the future. AI, agentic AI, and AI agents are appearing in every aspect of our lives and our businesses. Simply put, what feeds these technologies is data. But it cannot be done passively. Data must be properly curated and managed to ensure positive outcomes from our AI agendas. Data that feed these technologies must be accurate, timely, and unbiased, else the results that these technologies produce will be compromised.

If there was not enough focus on data management already, AI has dramatically increased the pressure that we are now putting on data management professionals to deliver trusted data to these technologies. But we have a problem. Traditional data management (those methodologies we depended on in 2008) cannot keep pace with the "three v's" – volume, velocity, and variety. In order to keep pace with the explosive growth of data, data professionals must now depend on AI to curate the data needed to feed AI. We need "AI for data for AI." And thus, this new trend is emerging.

At data events and conferences across the globe, the AI agent is the hot topic. How are these technologies being used, deployed, and leveraged? For the data management professional, AI agents are a welcomed approach to solving the "AI for data for AI" problem. AI agents are even appearing in company organizational charts, sitting beside the data management professional. AI agents are being deployed to perform data architecture, data quality, and data governance functions. Instead of being threatened by these technologies for fear of losing one's job, AI agents are being embraced by the data management community – a welcomed addition to assist in achieving data management excellence!

3. Data management case studies

The EDM Association (formerly the EDM Council; edmcouncil.org) is advocating this trend. The EDM Association is an international data management trade association dedicated to advancing trusted data, analytics, and technology standards across industry. With more than 375 corporate member

organizations across financial services, manufacturing, healthcare, telecom, public sector, and technology, the EDM Association provides globally recognized data management frameworks, standards, technical specifications, and professional certification programs that enable organizations to innovate their data management programs. It serves as a global hub for professionals and organizations focused on advancing best practices in data management.

The following case studies highlight where members of the EDM Association have effectively embraced and deployed effective data management programs in their organizations, utilizing industry best practices to position themselves to take on this new era of AI-driven data management and innovation.

3.1 Manufacturing/Automotives

TVS Motor Company (tvsmotor.com) is a multinational automotive manufacturer based in Chennai, India, specializing in two-wheelers and three-wheelers. It is the third-largest motorcycle company in India by revenue and the second-largest two-wheeler exporter in the country.

TVS Motor's aim is to become a data-driven organization to support their growth and innovation. But they realized that their organization had a limited focus on data. Across their businesses, data was not being used effectively, nor was it being recognized as an important asset that could carry the company forward. Data was underutilized and siloed across departments. There was no cohesive governance, poor data quality, and limited metadata management.

TVS embarked upon a journey to establish a Data Management & Governance program, utilizing the EDM Association's Data Management Capability Assessment Model (DCAM; dmcouncil.org/frameworks/dcam), as the basis of their program. DCAM identifies data management best practices across key data management capabilities: strategy, program, governance, architecture, data quality, data governance, and data enriched analytics.

By following these best practices, TVS Motors transformed their data management program across their enterprise:

- They established improved data governance processes to better control, protect, and utilize their information assets.
- They improved their metadata management, ensuring consistent semantic definitions across all data assets.
- They established a stronger data quality program building confidence and trust in their data and data usage.

Through the adoption and use of data management best practices, TVS has positioned themselves to achieve greater value out of their data. They have established an information infrastructure that can leverage the benefits of AI and innovation. They have successfully established data as core to their operations – today and for the future.

3.2 Consumer Cyclical/Restaurants

McDonald's is one of the best-known, most recognized brands in the world. Kantar, one of the world's leading marketing data and analytic companies, ranked McDonald's one of the top ten valuable brands globally in the Kantar BrandZ 2025 rankings,[1] and ranked McDonald's the #1 fast food brand worldwide.

McDonald's supports their franchise restaurants with data platform products and services that help their teams gain business insights. They rely heavily on data collected from thousands of sources across the globe. In order to provide critical insights, the data collected and aggregated must be of the highest quality, with consistent adherence to data standards in order to provide trusted analytics. The challenge arises from the vast scope of their operations – managing over 43,000 restaurants in over 100 countries!

At the end of 2024, McDonald's adopted the DCAM best practice framework and joined the EDM Association's Data Excellence Program[2] to enhance their data management and data governance programs and improve their analytic capabilities to generate valuable business insights for their restaurants.

The first steps of their data excellence journey began with an evaluation of their data management capabilities against the industry standard. By performing this evaluation, McDonald's was able to establish a baseline capability benchmark from

1. https://tinyurl.com/vmj5sskm
2. edmcouncil.org/data-excellence-program/

which they could plan improvements and measure the impact on their business.

All of the capabilities needed to improve their data management and governance objectives were evaluated. The outcome of these assessments provided a clear understanding of the current state of their data management program and an understanding of the strengths and weaknesses of their data infrastructure. In performing this evaluation, McDonald's then turned to their trusted partners and together, built a prioritized roadmap of improvements needed to achieve their data and analytic objectives.

Mark Twain said, "The secret of getting ahead is getting started." By starting their data management improvement journey aligned to industry standards, McDonald's created the awareness and the vision for enhancing their data management and governance programs, generating valuable business insights for their franchises and corporate management. And like other organizations that are driving their data management programs, McDonald's has positioned themselves to take advantage of the latest advances in AI and machine learning to drive their analytic programs.

3.3 State Government

In 2014, the State of Indiana, through executive order from the Governor, established the **Indiana Management Performance Hub (MPH)**, to address cross-agency data sharing needs. In 2017, the Indiana Open Data Act officially codified the MPH as a standalone State Agency within the Office of Management and Budget, giving the MPH the authority and agility to lead Indiana's data transformation.

Working together with the **Indiana Department of Workforce Development (DWD)**, they embarked on a data management transformation program aimed at improving data integration across agencies, developing advanced analytic solutions, and developing AI policy and training, offering data proficiency programs for State employees.

To achieve these objectives, MPH and DWD embraced the EDM Association's DCAM framework, driving consistent and scalable data management processes across the State. By raising the awareness of their data management programs and identifying specific areas of improvement, MPH and DWD were able to promote consistent, scalable data practices across state agencies, translate conceptual data governance goals into actionable strategies and enhance cross-team communication and data literacy to foster a unified data culture.

4. The impact of data management on the payments industry

Data management not only impacts public and private entity operations but also has a profound impact on industry-wide infrastructures that are key to economic efficiency. One such infrastructure is the payments industry. The payments process is much more complicated than simply tapping your credit card at the point of sale. That tap initiates a complex interconnected and coordinated dance of functions that must operate without delay or error to safely and effectively move payments across the system. The payment process is made up of customers, businesses, banks, payment gateways, providers, facilitators, and oversight regulators, all working together to achieve this objective.

In Bottega (2024), I highlighted how the payments industry is undergoing rapid change due to technologies like AI and machine learning, and how data is now the fuel.[3] Every step of a payment transaction relies on accurate, timely data, making data the essential element powering the process. For this process to work, embracing data management is not optional; it is vital for the efficient movement of information across the payment system.

The payment process is made up of a number of interconnected steps:

- **Transaction**: initiating a transaction requires numerous data elements, including customer and identification details, product and merchant information, pricing, inventory, and more. Each of these data categories must meet rigorous standards of accuracy and completeness. Effective data management enhances the likelihood that transactional data will be of the highest quality, thereby facilitating a successful start to the payment process.

3. Bottega, J. A., 2024, "The importance of data management for the payments industry," Journal of Payments Strategy & Systems 18:4, 357-365

- **Payment**: the payment gateway connects merchants and financial institutions. With new participants and data handoffs, use of industry-standard identification codes is now required.
- **Authorization**: the issuing bank verifies the transaction by checking the payer's account information and then approves or rejects the transaction. Incorrect data during this process may lead to the rejection of valid transactions or approval of invalid ones, which can affect customer experience or revenue.
- **Settlement**: settlement is the transfer of funds from payer to payee, requiring accurate data from both parties to ensure success and prevent fraud.
- **Reconciliation**: in this step, businesses align their records with payment process data and generate reports for accounting, audit, and financial analysis.

Data management enhances the entire payment lifecycle. Each capability of an effective data management program needs to be examined with respect to its impact on the payment system, focusing on how data strategy, business, data and technology architecture, data quality, data governance, and advanced analytics impact the process.

As the expression goes, "a chain is only as strong as its weakest link." This is especially true for payments. In the payment chain, every step, from transaction to reconciliation, relies on secure, accurate and timely data. The weakest link is the point where data is most exposed, or poorly managed, where security is weakest, where human error or fraud is most likely to occur, and where systems are least integrated or standardized.

Each stakeholder in the chain has a responsibility to ensure they are managing their portion of the data flow accurately and effectively. Each stakeholder has the responsibility of adhering to best practices while driving automation in order to ensure data integrity is maintained. Modern data management methodologies such as data tokenization and encryption, real-time monitoring, auditing and zero-trust architectures must be part of the data management support processes. A single weak point, such as an unsecured endpoint or a misconfigured API, can jeopardize the entire payment chain.

5. Conclusion

In these examples, I have described case studies of how data management best practices are driving better business outcomes and referred, with some detail, to an article describing the impact of data management on the payments industry, in an attempt to highlight the impact that data management has on businesses and organizations – and on our own personal lives. The expression, "data is the fuel", is admittedly overused, but is spot-on accurate. Data dependency can no longer be minimized. Data risk cannot be ignored. Data programs funding cannot be compromised. The opportunity of "AI for data for AI" as well as the role of agentic AI and AI agents cannot be denied. And most importantly, organizations must respect and fully support the data executives and professionals who are tasked with managing this important asset. The future of all industries, and the customers they serve, are dependent on it for a secure and stable global economy.

Future of Payments

Cashless future – reality or fiction?

Tobias Trütsch,
Managing Director and Head of the Center for Financial Services Innovation (FSI-HSG), University of St. Gallen (HSG), Switzerland

ABSTRACT

While cash use is steadily declining in favor of digital payments, its societal relevance remains strong. This paradox reflects cash's enduring role as a store of value, symbol of financial autonomy, and trusted medium in times of crisis. Although fewer transactions involve cash, public resistance to its abolition is growing. Declining access and acceptance risk triggering a self-reinforcing downward spiral, raising concerns about inclusion and resilience. Maintaining cash as a public good may require legal and policy measures. The debate over cash's future, therefore, transcends technology, touching on fundamental issues of trust, equity, and systemic stability.

1. Note: This article is partly based on an earlier German version from April 2025.

1. Introduction

The means of payment market is in constant evolution. In the earliest days, transactions were made using natural money such as shells or salt. These were gradually replaced by coins made of gold and silver, which in turn gave way to paper money (Figure 1). In recent decades, paper has been supplemented – and in some cases overtaken – by plastic money in the form of payment cards. Initially, the form of money and the method of payment were inseparable. Over time, however, a decoupling occurred: while physical means of payment are becoming less prevalent, electronic forms of money are on the increase.

History shows that new payment methods – cash included – were always developed with the goal of simplifying the transfer of value. The payment forms that succeeded were those that enhanced the efficiency of economic exchange and reduced transaction costs. This historical trajectory raises a pressing question: is cash on the verge of disappearing?

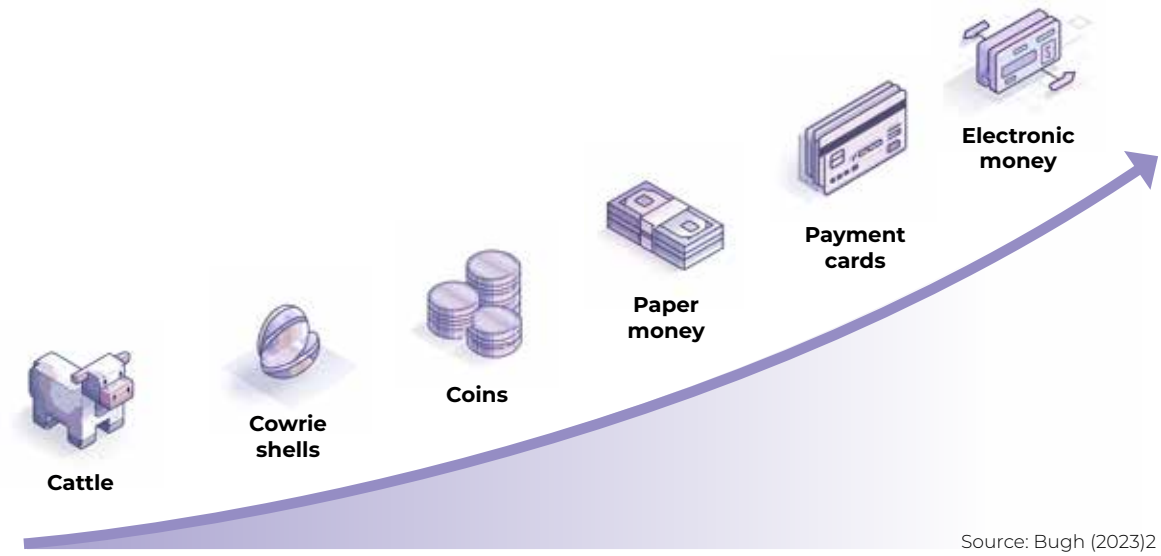
2. The use of cash is declining

In Switzerland, the trend is clear – cash is being used less frequently. Around one in six people no longer carry cash on a regular basis. Payment cards and mobile payment apps, especially Twint (the Swiss mobile payment app), are seeing widespread adoption.[3] The coronavirus pandemic served as a powerful accelerator of this shift. Similar developments are evident across other European countries.

The decline in cash use is driven by both supply and demand factors. On the supply side, there are now more opportunities to pay electronically in places where cash once dominated – such as vending machines, parking meters, and farm stands. At the same time, the growing presence of digital platforms has created new use cases where cash is simply no longer viable.

From the demand perspective, consumers are increasingly opting for digital payment methods because they are fast, convenient, and easy to use. In particular, contactless mobile payments have proven to be more attractive than cash for many daily transactions.

Figure 1: Evolution of means of payment and forms of money



Source: Bugh (2023)2

2. Bugh, J., 2023, "The evolution of the payment method: barter to e-payments," Pathquest, February 8, https://tinyurl.com/bdzkp6mc.
3. swisspaymentmonitor.ch

Yet despite this decline, three paradoxes surrounding cash have emerged. The first paradox is that, even as people use cash less often, the total value of cash in circulation – particularly in Switzerland and the eurozone – reached historic highs in early 2021, relative to GDP. Since interest rates have started to rise again after the coronavirus pandemic, this ratio has begun to fall. Notably, the CHF 1,000 note makes up about half the total value of cash in circulation in Switzerland. Demand for high-denomination notes tends to spike during crises – such as the financial crisis or the coronavirus pandemic – suggesting that they are increasingly used as a store of value rather than as a means of payment.

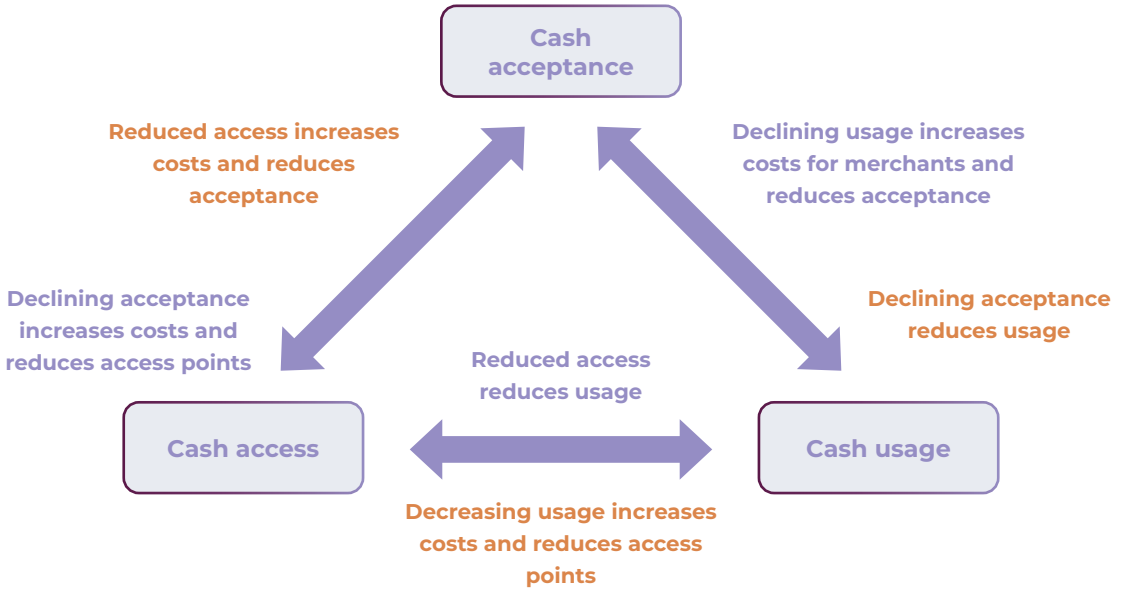
The second paradox is how public opinion has remained resolute in support of cash. Although the use of cash is decreasing, resistance to its abolition is growing. In Switzerland, 70 percent of the population are somewhat or clearly opposed to getting rid of cash, even though most of them are using it less frequently. Emotional attachment, perceived privacy, and other attributes of cash likely contribute to this stance.

The third paradox relates to individual behavior. While cash is used less frequently in daily transactions, people are holding more of it – both in their wallets and at home. Fewer cash withdrawals are being made, but when they do occur, the amounts tend to be larger. This may be linked to a perceived decline in the accessibility of cash withdrawal points such as ATMs and bank branches. Objective analyses for Switzerland confirm this perception.[4]

3. A vicious circle of decline?

These developments raise concerns about the emergence of a self-reinforcing downward spiral. Cash usage, access, and acceptance are interlinked and can influence each other in ways that accelerate the decline of cash (Figure 2). As consumers and businesses use less cash, they withdraw it less often, making ATMs less economically viable. Some ATMs are also being removed due to increased incidents of physical attacks, which drive up insurance and operating costs. For banks, maintaining cash infrastructure is largely a cost factor without the corresponding revenue. Consequently, retailers are more likely to limit or phase out the option of cash payments.

Figure 2: Potential vicious circle in the use of cash



4. Swiss Money Map, "Monitoring Cash Access Points in Switzerland," moneymap.ch.

As consumers encounter more barriers to using cash, they naturally shift further toward digital alternatives – further reducing demand for cash and, by extension, reducing access points like ATMs. A vicious cycle begins. This trend is noticeable in Switzerland and Germany, though a full-scale negative spiral has not yet taken hold. In contrast, countries such as Sweden, the Netherlands, and the U.K. have already experienced strong feedback loops that significantly accelerated the decline of cash's importance.

4. Alternative cash withdrawal points

Alternative options for withdrawing and depositing cash at retail points of sale are best understood as complements to traditional cash access channels, such as ATMs and bank branches. These new forms of access can enhance convenience, but they cannot fully replace established infrastructure. Retail outlets, for instance, often lack the capacity to meet demand for specific banknote denominations, and they are generally not equipped to verify the authenticity of cash or manage its recycling in a secure and systematic way. These functions remain core responsibilities of traditional banks, which continue to play a central role in maintaining the integrity of the cash cycle.

The central bank is also indispensable in this system. It ensures the authenticity of banknotes, removes those unfit for circulation, and issues new, high-quality currency. This "fresh" cash typically enters the economy via the banking sector – distributed as change by retailers or accessed directly by consumers through withdrawals. Without the support of both central banks and commercial banks, the reliability, security, and efficiency of the cash supply chain would be compromised.

5. The unique properties of cash

Cash occupies a unique and enduring position within the monetary system. Unlike digital payment methods, which are based on commercial bank money and thus entail counterparty risk, cash is central bank money – backed by the central bank and free from debtor risk. It represents the foundation of the financial system, offering an unmediated form of payment that is both tangible and widely accepted.

What sets cash apart is not just its physicality but the social, economic, and psychological functions it serves. It enables participation in the financial system without requiring access to digital infrastructure or banking services, thereby promoting inclusion. It also ensures a high level of privacy and anonymity, which many people still value in an increasingly data-driven world. In times of crisis or technical failure, cash remains a reliable fallback, independent of power supplies, internet access, or digital platforms. For many, it also facilitates more conscious spending, offering a clear sense of how much money is being used.

Efforts to develop a retail Central Bank Digital Currency (CBDC) aim to replicate many of these advantages. However, digital money – no matter how sophisticated – cannot fully reproduce the tactile and trust-based qualities of physical cash. Complete anonymity, for instance, is difficult to guarantee in a digital format, and no technology can entirely replicate the sense of control that comes with handling physical money. For this reason, a retail CBDC is likely to serve as a complement to, rather than a replacement for, cash.

6. Future trends in payment method solutions

The future of payment method solutions remains uncertain. However, some key trends are already emerging: First, mobile phones are likely to become the primary interface for payments, integrating all individual payment flows within their own ecosystems (e.g., Alipay and WeChat Pay). Physical payment cards are being phased out in favor of digital versions stored on smartphones or other mobile devices. Payment providers are shifting from offering "payment as a pain" to delivering "payment as a service". The most successful solutions are smooth, easy to use, and embedded within comprehensive ecosystems that deliver high individual value. Optimal analysis of transaction data will be key to delivering these tailored experiences.

Second, payments are likely to increasingly rely on biometric and behavior-based identifiers. Transactions may be authorized using unique features such as voice, eyes, facial recognition, fingerprints,

gait, or even digital behavior like browsing patterns. Real-time (instant) payments will become the norm, enabling transfers at any time, from any location.

Third, the payment process could become fully integrated into the purchasing experience, making it essentially invisible – whether during in-app purchases, online shopping, or at unmanned retail outlets. The traditional experience of making a payment will disappear. As a result, the psychological "pain of paying", especially associated with cash, will be reduced. This may lead to increased consumer spending, along with a higher risk of indebtedness.

Fourth, AI agents are poised to take over the entire shopping journey – from product search and selection to automated purchasing and payment processing. Beyond simply completing transactions, these agents can intelligently choose the most suitable payment method by factoring in fees, bonus programs, account balances, and available bank details. By leveraging liquidity forecasts, AI can also optimize the timing of payments and debits such as direct debits or invoice settlements. Unlike human consumers, AI agents operate with pure rationality, always aiming to maximize individual benefit. Trained on billions of real transactions, these agents develop a detailed semantic understanding of personal payment behavior in real time. They can detect patterns and contextual signals, enabling not only automated payment authorization but also significantly reducing fraud risk. Their capacity to process vast amounts of data in real time opens the door to innovative financial services – such as dynamic credit models or context-aware "buy now, pay later" offerings – tailored to the consumer's current payment behavior.

Fifth, the foundation for future payment systems is likely to be blockchain technology, enabling automated transactions through smart contracts. Stablecoins and central bank digital currencies (CBDCs) will become the new standard, while existing cryptocurrencies will mostly serve as collector's items. The dominance of a few global card issuers will diminish, giving central banks a more finely tuned monetary policy toolkit. However, this also paves the way for increased surveillance and data control – turning citizens into transparent individuals and making surveillance capitalism a tangible reality.

7. Conclusion

Despite the ongoing decline in its use as a means of everyday payment, cash remains deeply embedded in society - particularly as a store of value. It is unlikely to disappear in the foreseeable future. Many people continue to hold onto cash, not only out of habit but because of the trust, security, and autonomy it provides. However, this continued relevance will not come without challenges.

If the use of cash continues to decline, questions will arise about how to maintain access and ensure that the infrastructure supporting it remains financially viable. Sustaining cash as a public good may eventually require legal safeguards to preserve its acceptance and availability. In addition, targeted measures – such as optimizing the efficiency of the cash cycle and considering public or subsidized funding – may become necessary to support its continued circulation.

In light of these dynamics, the debate about the future of cash is not merely about convenience or technology. It touches on broader issues of social equity, resilience, and trust in the financial system. As such, decisions about how to manage and maintain access to cash will remain a matter of public interest for years to come.

Future of Payments

Preparing for October 2025: implementation and impact of the EPC's **Verification of Payee** scheme

Dominique Allebroeck,
Product Manager, The European Payments Council

ABSTRACT

As the European Payments Council (EPC) prepares to launch its Verification of Payee (VOP) scheme in October 2025, this article explores the scheme's implementation, regulatory background, and broader implications for fraud prevention, user experience, and financial interoperability across the Single Euro Payments Area (SEPA). Introduced in response to the E.U. Instant Payments Regulation (IPR), the scheme aims to reduce fraud and misdirected payments by enabling name-IBAN verification before transactions are authorized. The article explains how the scheme functions, including the role of Routing and/or Verification Mechanisms (RVMs) and the EPC Directory Service (EDS), which together enable real-time verification and secure data exchange between Payment Service Providers (PSPs). It also outlines the responsibilities of payers, payees, and PSPs in adapting to the new process, along with the compliance steps required from PSPs. Finally, the article considers future developments for the VOP scheme, positioning VOP as a key pillar for safer, more trustworthy digital payments in Europe.

1. Introduction

Combating fraud and improving security in digital payments are top priorities for consumers, businesses, Payment Service Providers (PSPs), and governments alike. The Verification of Payee (VOP) scheme about to be launched by the European Payments Council (EPC), is a key measure to reinforce trust and enhance the overall safety of payment transactions. As a direct response to the E.U. Instant Payments Regulation (IPR), which mandates that PSPs offer name-IBAN verification services, the VOP scheme provides the framework to meet this requirement across the Single Euro Payments Area (SEPA). By establishing standardized rules, practices, and interoperability protocols, the VOP scheme seeks to minimize fraud and misdirected payments - ultimately boosting user confidence in both SEPA Credit Transfers (SCT) and SEPA Instant Credit Transfers (SCT Inst).

As things stand, when a payer initiates a credit transfer, their PSP is not required to verify whether the account holder's name matches the beneficiary name provided in the payment instruction. This lack of verification leaves room for fraud or errors. Starting from October 9, 2025, under the new IPR, this verification will become mandatory, and payers will be informed of the outcome before proceeding. While the final decision to complete the payment will still rest with the payer, the introduction of this step marks a significant shift in the payment experience and will require users to adopt new habits. The VOP scheme supports this transition by automatically checking payee details, helping to prevent fraud, enhancing confidence that funds are being sent to the correct recipient, and reducing human errors - all while strengthening the overall security of credit transfers.

The E.U. IPR, officially published in March 2024 in the E.U.'s Official Journal, establishes the legal framework for implementing VOP services across the euro area. Under the regulation, all PSPs must offer VOP services free of charge, ensuring the verification occurs before the payer authorizes a credit transfer. In cases of a close match, PSPs are required to share the registered name associated with the provided IBAN, enabling the payer to make an informed decision. PSPs must also clearly inform customers about the consequences of ignoring VOP alerts, including potential impacts on liability and refund rights. The regulation acknowledged the need for harmonization and encouraged PSP-led organizations - such as the EPC - to develop E.U.-wide standards, leading to the creation of the EPC VOP rulebook. While consumers must receive the VOP service by default, business payers submitting batch payments may contractually opt out. The regulation mandated the full implementation of VOP services within 18 months of its entry into force, setting a compliance deadline on October 9, 2025.

2. About the VOP Rulebook

Following a public consultation on the proposed VOP scheme rulebook and the proposed EPC recommendations for the matching processes under the VOP scheme rulebook, the EPC has launched the first version of the VOP scheme rulebook in October 2024. The EPC scheme has been developed to support the PSPs in the European Economic Area (EEA) that will be required to comply with legal obligations on the verification of a payee, as outlined in the proposed E.U. IPR[1] amending the SEPA Regulation.[2]

This version 1.0 of the VOP scheme rulebook focuses to predominantly fulfil the E.U. legislative requirements set out by the IPR. This means that for the time being, and to allow PSPs in the EEA time to comply with the new regulatory requirements within the given deadlines, the rulebook limits itself to verifications of a payee related to a SCT or a SCT Inst. Future versions of the VOP scheme rulebook could cover other payment instruments as well, depending on market needs or interest.

The VOP scheme allows the PSP of the payer (the Requesting PSP) to instantly send to the PSP of the payee (the Responding PSP), a request to verify the International Bank Account Number (IBAN) and the name of the payee as given by the payer (the Requester), or in case the payee is a legal entity, an identification code that unambiguously identifies that payee [e.g., Value-Added Tax (VAT) number or Legal Entity Identifier (LEI)]. The reason for this request is that the payer intends to initiate an SCT or an SCT Inst transaction to the payee.

The Responding PSP promptly checks whether the

1. https://tinyurl.com/mrxmjbt5
2. https://tinyurl.com/yck62ft5

received information aligns with the corresponding data it holds for the intended payee. It then sends a VOP response back to the Requesting PSP - indicating whether the details are a match, no match, close match (including the name on record), or if the verification could not be completed. The Requesting PSP must then immediately relay this response to the payer. The VOP scheme rulebook will go live on October 5, 2025.[3]

3. How the VOP scheme works?

Figure 1 provides a high-level representation of how the VOP scheme works, including key actors and flows.

The VOP scheme enables the payer's PSP (requesting PSP) to instantly send a verification request to the payee's PSP (responding PSP) to confirm the accuracy of the IBAN and payee name provided by the payer. This request may also include additional unique identification codes, such as a VAT number or Legal Entity Identifier (LEI).

Figure 1: VOP scheme, high-level overview

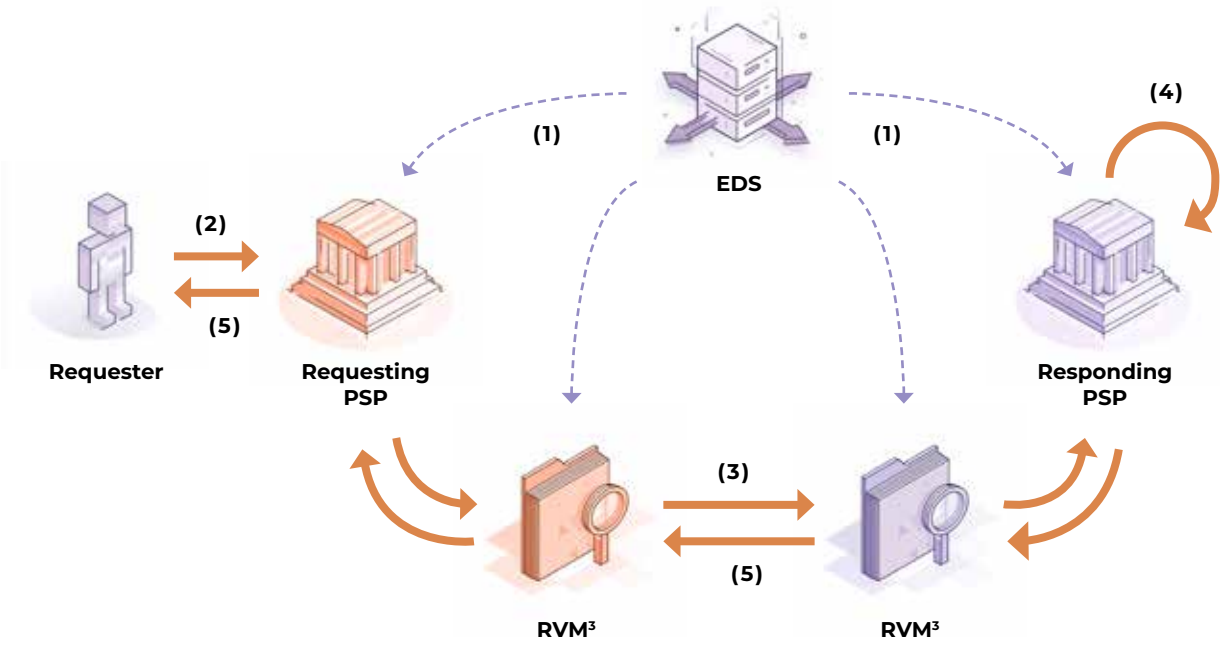
(1) EDS local file downloaded daily and cached by PSPs and/or RVMs

(2) Before authorizing an (instant) credit transfer, the requester inserts IBAN and name[2] triggering a VOP request

(3) Requesting PSP[1] sends the VOP request to the responding PSP

(4) Responding PSP[1] authenticates and authorizes requesting PSP[1] using the EDS local file

(5) Responding PSP[1] provides VOP result (match, no match, close-match, etc.)



Notes:

1. Or a Routing and/or Verification Mechanism (RVM) acting on behalf of the PSP
2. Or another identifier, for business users.
3. Requesting and/or Responding side RVM may or may not be present (or also be one and the same, e.g. for domestic transaction)

3. More information about the rulebook can be found on the EPC website: https://tinyurl.com/2nnka23j.

The purpose of this verification is to support the initiation of a SCT or SCT Inst. Upon receiving the request, the responding PSP immediately checks the data against its records and sends back a response indicating whether the details match, do not match, are a close match, or if verification is not possible. The requesting PSP then promptly relays this response to the payer.

3.1 Possible outcomes of a VOP check:

- **Match**: the name provided in the payment by the payer, corresponds exactly to the name of the holder of the account indicated in the payment.
- **No match**: the name provided in the payment by the payer, does not correspond at all with the name of the holder of the account indicated in the payment.
- **Close match**: the name provided in the payment by the payer, almost corresponds with the name of the holder of the account indicated in the payment, with some slight differences. In this case, the correct name will be included in the response as well.
- **Verification check not possible**: it was not possible to perform the VOP (due to a technical reason, or the payee's account is closed, or no answer was received on time...).[4]

3.2 RVMs play a key role in the VOP scheme

In the EPC's VOP scheme, the Routing and/or Verification Mechanisms (RVMs) play a vital role in ensuring payments reach the correct recipient by verifying the payee's details. Requesting and responding PSPs can either manage VOP interactions directly or rely on RVMs to route requests, return responses, and access the EPC Directory Service (EDS). Acting as intermediaries, RVMs securely forward VOP requests and responses between requesting and responding PSPs, ensuring all data is transmitted accurately and without alteration. This flexible approach supports interoperability and enables PSPs to streamline their technical operations.

Subject to prior agreement, RVMs may also perform the verification process on behalf of responding PSPs, providing additional operational support. Beyond routing and verification, RVMs offer essential risk management services and other related functions that help maintain the security and integrity of the VOP process.

To manage routing data effectively, RVMs receive delegation from the PSPs they serve. This authorization enables them to update and maintain the PSPs' routing information within the EPC Directory Service (EDS), which is critical for accurate and secure message routing across the VOP network.

3.3 VOP RVM qualification process

Recognizing the crucial role RVMs play within the VOP scheme, and anticipating that many PSPs will rely on one or more RVMs, the EPC requires all RVMs to undergo a formal qualification process. This process aims to ensure that there is a high level of interoperability, security, and compliance across the scheme. It includes a self-certification of the RVM's VOP APIs against the EPC's API Reference Toolbox (ART) test platform, which assesses both functional and technical compliance through a set of standardized test cases.

Organizations wishing to provide services as VOP RVMs can initiate the qualification by submitting a completed and signed RVM Agreement to the EPC. This structured process ensures that only qualified, scheme-compliant RVMs participate in the ecosystem, fostering trust and reliability for all VOP participants.

4. The EDS: the backbone of VOP routing

In API-based schemes like VOP, two scheme participants communicate via APIs either directly or through a proxy, such as an RVM. Before this communication can occur, all participants must know how to reach each other - that is, the network address of their counterpart - and have the necessary information to ensure interoperability, such as supported protocol options.

To address this need, the EPC introduced the EDS. The EDS acts as the default, centralized platform that facilitates reachability and interoperability

4. To support a better understanding of how the scheme works, the EPC has also created a video, which can be viewed on its website: https://tinyurl.com/4ud23eka.

across all API-based EPC scheme participants. It securely stores essential identification, routing, and interoperability data, including BICs, LEIs, National Authorization Numbers, and API endpoints, ensuring participants can identify and connect with one another within the VOP scheme.

To avoid operational bottlenecks and ensure high availability, participants can download and locally cache the EDS data, removing the need for real-time queries. Importantly, the EDS does not hold any personal data of individual or corporate end-users - only institutional information related to PSPs - thereby protecting privacy while enabling seamless interoperability across SEPA.

The EDS is scheduled to go live on September 2, 2025, ahead of the VOP scheme's official launch on October 5, 2025. Participants onboarded during the pilot phase will automatically be recognized in the live environment.

4.1 Supported functions of the EDS

The EDS has been designed with functionality and efficiency in mind. First, it automatically imports scheme participants' adherence data from the EPC's official Register of Participants, ensuring accuracy and alignment with scheme governance. Authorized users - whether PSPs or approved intermediaries - can access the EDS via a user-friendly Web GUI or through EDS APIs, allowing them to manage and update participant data seamlessly. Additionally, users have the option to download the EDS dataset and store it locally, which supports smooth operations without relying on real-time lookups.[5]

4.2 Impacts for the customers

The introduction of the VOP service will bring noticeable changes to the customer experience, especially for payers. They will begin seeing new warning messages when the beneficiary name does not fully match the account details. While PSPs are working to harmonize these notifications, slight differences may remain between PSPs and national communities. Clear communication and familiarization with the process will be key to ensuring a smooth transition and maintaining trust in digital payments.

4.3 Recommendations for payers

To make the most of the VOP service, payers should be informed about how it works and why it is important. Entering the full, correct name of the beneficiary helps avoid unnecessary alerts. If a warning appears, it is a good idea to double-check the IBAN details and/or contact the beneficiary, as it could signal a mistake or potential fraud. Regular, trusted recipients are generally not affected, but updating saved contacts with official names will help ensure smooth and secure payments going forward.

4.4 Recommendations for payees and their PSPs

To ensure smooth implementation of the VOP service, payees - particularly legal entities and corporations - are advised to clearly display their official legal or commercial names, as well as unambiguous identifiers supported by their PSP (e.g., VAT number and/or LEI) on all invoices. It is equally important for PSPs to verify that these identifiers and names are accurately recorded and maintained in their PSPs' databases. Additionally, payees should take proactive steps to ensure their payers are familiar with and use the correct identifier or name when initiating payments, helping to minimize mismatches and reduce payment delays or rejections.

5. What's next for the VOP scheme?

The immediate priority is to ensure the VOP scheme is fully up and running by October 2025, in line with the implementation deadline of the IPR. This means achieving seamless interoperability among all PSPs in the euro area, each of which must either build their own VOP service or partner with an RVM. For the moment, early testing results are promising, and several countries are already preparing for the transition. Some national communities (e.g., Belgium) even anticipated the launch of VOP at national level, to secure a smooth transition to the EPC VOP scheme in October 2025.

Communities with existing VOP solutions are now working on connecting with PSPs across all eurozone markets. Beyond that, discussions will begin in 2026 on potential enhancements to the scheme,

5. More information about EDS can be found on the EPC website: https://tinyurl.com/42a75u4x.

with a view to incorporating new features into the next version of the EPC VOP scheme rulebook - planned for release in 2027 - starting from the evaluation of a possible extension of VOP scheme to bulk payments.

Importantly, the next phase of EPC's VOP scheme will extend interoperability to non-EEA PSPs, further broadening the scope and impact of the scheme. Meanwhile, existing RVMs will be allowed to offer additional value-added services tailored to specific market needs, e.g., in the form of Additional Optional Services (AOS) on top of VOP scheme.

Looking ahead, wider adoption of the VOP scheme could open the door to new innovations within the payments ecosystem. Future versions of the rulebook may extend beyond credit transfers to include other payment instruments, depending on market needs and regulatory changes. The scheme also lays the groundwork for more advanced anti-fraud measures, such as layered risk assessments powered by data analytics, machine learning, and stronger identity verification. Ultimately, VOP marks a major step toward safer digital payments - boosting trust, compliance, and efficiency across Europe's evolving financial landscape.

6. Conclusion

With its implementation scheduled for October 2025, the EPC's VOP scheme represents a significant step forward in the E.U.'s efforts to enhance payment security, reduce fraud, and strengthen user confidence in digital transactions. By mandating name-IBAN checks before authorizing SCT and SCT Inst, the VOP scheme introduces a crucial layer of protection for consumers and businesses alike. The initiative's technical framework - underpinned by the EDS and the RVMs - ensures seamless interoperability and real-time communication among PSPs. As PSPs work to meet the deadline, clear instructions, good preparation, and customer awareness will be essential for a smooth launch. After 2025, the VOP scheme could lead to new features, such as support for more payment types and better fraud prevention tools. Ultimately, VOP is more than a regulatory requirement, it is a transformative measure that will help shape a safer, more transparent, and more resilient European payments landscape.

Future of Payments

Protecting self-hosted payment systems against **ransomware**: a comprehensive guide

Buck Rogers,
Professor in Cyber Security, University of Gloucestershire, and Cyber Advisor, Projective Group

Scott Beange,
Head of Data Management and Cyber Strategy, Projective Group

ABSTRACT

This paper explores the growing threat of ransomware to self-hosted payment systems, which are increasingly targeted due to the sensitive financial data they handle and their operational importance. It examines the evolving tactics used by ransomware actors, including double extortion and backup destruction, and identifies common vulnerabilities in payment infrastructure such as weak access controls, unpatched systems, and insufficient segmentation. Drawing on industry best practices and peer-reviewed research, this article outlines a multi-layered defense strategy incorporating strong access controls, endpoint protection, immutable offline backups, staff training, and incident response planning. It also stresses the importance of threat intelligence and compliance with standards like PCI DSS. The paper concludes with actionable recommendations to help financial organizations enhance resilience, minimize operational disruption, and reduce the likelihood of ransom payments.

1. Introduction

The evolving sophistication of ransomware tactics necessitates a proactive approach, including strategies for mitigating cloud-based ransomware threats [Dopamu (2024)].

Ransomware, a form of malicious software that operates by encrypting data on a computer system, rendering it inaccessible to the legitimate users, has become a prevalent and increasingly sophisticated cyber threat [CSBS (2023)]. Following encryption, attackers demand a ransom payment, often in cryptocurrency, in exchange for providing a decryption key to restore access to the compromised data. The tactics employed by ransomware actors have evolved considerably over time. Initially, the primary goal was data encryption and ransom payment for recovery. However, a significant shift has occurred with the emergence of "double extortion" tactics [CSBS (2023)]. In these scenarios, attackers not only encrypt the victim's data but also exfiltrate sensitive information before encryption. They then leverage this stolen data, threatening to release it publicly if the ransom demands are not met. This dual approach significantly increases pressure on victim organizations to comply with ransom demands, as the potential consequences now include not only the loss of data availability but also the risk of sensitive data exposure.

Self-hosted payment systems, which are crucial for businesses to conduct transactions, face unique risks and challenges in the context of this evolving ransomware threat [Dispensa (2023)]. These systems are often directly connected to financial processing and handle highly sensitive information, including cardholder data [Dispensa (2023)]. This makes them particularly attractive targets for cybercriminals seeking financial gain through ransomware attacks. The compromise of a self-hosted payment system can lead to an immediate halt in payment processing capabilities, directly impacting an organization's revenue streams [Dispensa (2023)]. Furthermore, the sensitive nature of the data stored and processed by these systems means that a successful ransomware attack can easily escalate into a significant data breach, with severe consequences for the organization and its customers.

The potential impact of a successful ransomware attack on a self-hosted payment system can be far-reaching and devastating [IPC (2022)]. The most immediate consequence is often a significant loss of revenue due to being unable to process payments [Dispensa (2023)]. Beyond this, organizations face substantial costs associated with responding to the incident, including engaging forensic experts to investigate the breach, legal counsel to navigate data breach notification requirements, and specialized services to attempt data recovery [IPC (2022)]. In cases where personal or financial data is compromised, organizations may also incur legal fees and face regulatory fines due to non-compliance with data privacy laws [IPC (2022)].

The reputational damage resulting from a ransomware attack and subsequent data breach can be severe and long-lasting, leading to loss of customer trust and potentially impacting future business [IPC (2022)]. Moreover, ransomware attacks can sometimes lead to direct financial fraud, resulting in further monetary losses for the affected organization [IPC (2022)].

While cyber insurance policies can help offset some of these costs, obtaining and maintaining such coverage involves premiums and potential deductibles [IPC (2022)]. Downtime caused by ransomware can also lead to substantial financial losses due to disrupted operations and lost sales [Vanover (2023)].

2. Understanding ransomware tactics and techniques targeting payment systems

Ransomware attacks targeting self-hosted payment systems typically follow a predictable lifecycle, often beginning with gaining initial access to the network. Common attack vectors include phishing emails, which may contain malicious attachments or links designed to trick users into downloading malware or revealing credentials [PTP Cloud (2023)]. Exploiting vulnerabilities in exposed and poorly secured Remote Desktop Protocol (RDP) services is another frequently used method for initial intrusion [CISA (2025)]. Attackers also actively seek out and exploit known vulnerabilities in unpatched software and operating systems running on systems connected to the payment infrastructure [CISA (2025)].

Once attackers have successfully gained initial access to a system within the network, they often

engage in lateral movement [CISA (2025)]. This involves navigating through the network infrastructure to identify and compromise other systems, with the ultimate goal of reaching critical assets such as payment processing servers and databases [CISA (2025)]. Attackers utilize various tools and techniques to facilitate lateral movement, including leveraging compromised credentials obtained during the initial breach or through other means, and using protocols like RDP to remotely access other systems [CISA (2024)]. Privilege escalation is another common tactic employed during this phase, where attackers attempt to gain higher levels of access and control within the compromised systems and the network environment [CISA (2025)]. This allows them to perform actions that a standard user would not be authorized to do, such as disabling security controls or accessing sensitive data.

The core objective of a ransomware attack is to encrypt data, rendering the targeted payment systems and their associated data unusable [CSBS (2023)]. Many modern ransomware groups have adopted a "double extortion" strategy [PTP Cloud (2023)]. In addition to encrypting the data, they also exfiltrate sensitive information, such as cardholder data, before initiating the encryption process [PTP Cloud (2023)]. This stolen data is then used as additional leverage to coerce victims into paying the ransom, with the threat of public release if the demands are not met [PTP Cloud (2023)]. Given the highly sensitive nature of payment card information, preventing data exfiltration from these systems is of paramount importance [CISA (2023a)].

The act of data exfiltration itself constitutes a data breach, which carries significant legal and regulatory obligations for organizations, including mandatory reporting requirements in many jurisdictions [IPC (2022)]. Furthermore, ransomware attackers often target an organization's backup systems and recovery mechanisms [CISA (2025)]. By compromising or deleting backups, the attackers aim to eliminate the victim's ability to restore their systems and data without paying the ransom, thereby increasing the likelihood of payment.

3. Key vulnerabilities in self-hosted payment systems prone to ransomware attacks

Several key vulnerabilities commonly found in self-hosted payment systems make them susceptible to ransomware attacks. Insecure remote access configurations, particularly the exposure of RDP services with weak passwords or without the protection of multi-factor authentication (MFA), are frequently exploited by attackers to gain initial access to the network [CISA (2025)]. The use of weak or default credentials across various system components and applications also provides a simple yet effective entry point for malicious actors [CISA (2025)]. Inadequate access controls, where users are granted permissions beyond what is necessary for their roles, can further facilitate lateral movement and access to sensitive payment data once an attacker has compromised an initial account.

Outdated and unpatched software and operating systems represent another significant vulnerability [CISA (2025)]. Known vulnerabilities in these components are actively targeted by ransomware exploits, providing attackers with readily available pathways into the system.

Insufficient network segmentation and poorly configured firewall rules can also leave self-hosted payment systems exposed. A lack of network segmentation allows ransomware to spread rapidly from an initially compromised system to the critical payment processing environment, while inadequate firewall rules might permit unauthorized traffic to and from the payment system, creating opportunities for attackers [CISA (2025)].

The absence of robust backup and disaster recovery plans is a critical vulnerability that can significantly increase the impact of a ransomware attack [CSBS (2023)]. If backups are not performed regularly, stored offline in a secure manner, and thoroughly tested, organizations may find themselves unable to recover from a ransomware attack without resorting to paying the ransom. Finally, inadequate endpoint security measures, such as the lack of up-to-date antivirus and anti-malware software on servers and workstations that interact with the

1. A comprehensive overview of current ransomware mitigation techniques, including multi-layered defenses such as robust backups and employee training, is provided by Ojo (2025).

payment system, can allow ransomware to execute and spread within the environment [CISA (2025)].1

4. Comprehensive strategies for protecting self-hosted payment systems against ransomware

Protecting self-hosted payment systems from ransomware requires a comprehensive and proactive approach that encompasses multiple layers of security controls [Google Cloud (2023)]. Adopting a defense-in-depth strategy, which involves implementing a combination of technical, administrative, and physical safeguards at various levels, is crucial [IPC (2023)]. This ensures that if one security measure fails, others are in place to provide continued protection.

Establishing robust backup and recovery procedures is paramount [NCSC (2021). Organizations should regularly create offline backups of the entire payment system and all associated data, storing these backups in a physically separate location or an isolated cloud environment [NCSC (2021). Implementing immutable backups, which cannot be modified or deleted by ransomware, provides an additional layer of protection [Vanover (2023)]. Encrypting backups is also essential to safeguard against unauthorized access in the event that the backup storage itself is compromised [Cynet (2023)]. Crucially, the entire backup and recovery process should be regularly tested to ensure its effectiveness and reliability when needed [Vanover (2023)].

Implementing strong access controls and adhering to the principle of least privilege are fundamental

Table 1:
Recommended preventive measures against ransomware for self-hosted payment systems

Preventive measure	Description	Reference
Implement offline backups	Regularly create and store backups offline or in isolated environments.	11
Enforce MFA	Require multi-factor authentication for remote access and administrative accounts.	10
Regular patching	Establish a process for timely patching of operating systems, software, and firmware.	11
Network segmentation	Isolate the payment system within the network using firewalls and segmentation.	5
Endpoint security	Deploy and maintain up-to-date antivirus, anti-malware, and EDR solutions.	7
Security awareness training	Conduct regular training for personnel on phishing and social engineering risks.	10
Incident response plan	Develop and regularly test a ransomware-specific incident response plan.	10
Data encryption	Encrypt sensitive data at rest and in transit within the payment system environment.	6
Compliance adherence	Ensure compliance with relevant industry standards like PCI DSS and data privacy regulations.	9

Source: CSBS (2023)

security practices [Vanover (2023)]. Organizations should enforce strong password policies, including complexity requirements and regular password changes, and grant users only the minimum level of access necessary to perform their job functions [CISA (2025)]. Regular reviews and audits of user accounts and their associated access permissions are also necessary to identify and rectify any potential security gaps [NCSC (2021)].

Establishing a rigorous vulnerability management program is vital for proactively identifying and mitigating security weaknesses [PCI Security Standards (2018)]. This includes conducting regular vulnerability scans on all components of the payment system infrastructure. A timely patching process for operating systems, payment processing software, and all other applications must be implemented, with a priority placed on patching known exploited vulnerabilities [CISA (2025)].

Network security hardening measures are essential for protecting the payment system from unauthorized access. Implementing strong firewall rules to control both inbound and outbound network traffic is critical. Network segmentation should be implemented to isolate the payment system from other, potentially less secure, parts of the organization's infrastructure. Any unnecessary network services and ports should be disabled to reduce the attack surface. Hardening the Server Message Block (SMB) protocol can also help prevent lateral movement of ransomware within the network [CISA (2025)].

Enforcing multi-factor authentication (MFA) for all remote access points to the payment system and for all administrative accounts adds a significant layer of security. It is crucial to ensure that MFA is implemented using strong and reliable authentication methods. Deploying and maintaining up-to-date antivirus and anti-malware solutions on all servers and workstations that interact with the payment system is a fundamental security measure. Organizations should also consider implementing Endpoint Detection and Response (EDR) tools for more advanced threat detection and analysis capabilities [CISA (2025)]. Application whitelisting can further enhance endpoint security by restricting the execution of only authorized software [Google Cloud (2023)].

Conducting regular security awareness training for all personnel who have access to, or interact with, the payment system is essential for mitigating the risk of social engineering attacks like phishing [CISA (2025)]. Training should emphasize the importance of recognizing and reporting suspicious emails and other potentially malicious activities. Developing and regularly testing a comprehensive incident response plan specifically tailored for ransomware attacks targeting the payment system is crucial for ensuring a swift and effective response in the event of an incident [CISA (2025)]. This plan should clearly define roles, responsibilities, and step-by-step procedures for detection, containment, eradication, and recovery. Encrypting sensitive data both at rest and in transit within the payment system environment provides an additional layer of protection, safeguarding the confidentiality of data even if it is exfiltrated [CISA (2025)]. Finally, organizations handling payment card information must ensure compliance with all applicable industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS) [PCI Security Standards (2018)]. Staying informed about, and adhering to, relevant data privacy laws and regulations is also critical [IPC (2023)].

5. Responding to a ransomware incident affecting a self-hosted payment system

In the event that a ransomware attack successfully breaches preventative security measures, a well-defined and practiced incident response plan is critical for minimizing the impact and ensuring a swift recovery. The initial step upon suspecting a ransomware incident is detection and immediate isolation. All affected systems, including those hosting the payment system and any connected workstations or servers, should be promptly disconnected from the network to prevent the ransomware from spreading further. For payment systems hosted in cloud environments, taking snapshots of the affected volumes can be valuable for later forensic analysis [CISA (2025)].

Communication during this phase should ideally occur through out-of-band channels, such as phone calls, to avoid alerting the attackers that their presence has been detected [CISA (2025)].

The next phase involves containment and eradication. The specific ransomware strain involved should be identified to understand its behavior and

Table 2:
Key steps in responding to a ransomware incident affecting a self-hosted payment system

Incident response step	Description	Reference
Detection and initial response	Identify the attack, isolate affected systems from the network, and initiate communication.	5
Containment and eradication	Research the ransomware, terminate malicious processes, delete associated files, and secure the entry point.	5
Recovery and restoration	Restore the payment system and data from clean, offline backups, prioritizing critical systems. Do not pay the ransom.	11
Post-incident analysis and lessons learned	Determine the root cause of the attack, identify vulnerabilities, and update security policies and procedures.	11

Source: Google Cloud (2023)

potential removal methods. Any identified ransomware processes running on the affected systems should be terminated or disabled. All associated files and registry entries related to the ransomware should also be deleted from the compromised systems. It is crucial to identify the initial point of entry that allowed the ransomware to infect the system and to secure this vulnerability to prevent future reinfections [CISA (2025)].

Recovery and restoration are the subsequent critical steps. The payment system and its associated data should be restored from clean, offline backups. It is essential to prioritize the restoration of critical systems and functionalities first to minimize business disruption [CISA (2025)]. After restoration, the integrity and functionality of the recovered systems must be thoroughly verified [Vanover (2023)]. Under no circumstances should the ransom be paid to the attackers [CISA (2025)]. Paying the ransom does not guarantee data recovery and only serves to encourage future attacks.

The final stage of the incident response process is post-incident analysis and lessons learned. A detailed analysis should be conducted to determine the root cause of the attack and identify any security weaknesses that were exploited. Based on the findings of this analysis, security policies, procedures, and training programs should be updated to prevent similar incidents from occurring in the future [CISA (2025)].

6. The role of threat intelligence in protecting against ransomware

Threat intelligence plays a crucial role in bolstering an organization's defenses against ransomware attacks targeting self-hosted payment systems. By continuously monitoring threat intelligence sources, organizations can stay informed about emerging ransomware variants, the latest attack techniques, and indicators of compromise (IOCS) [Google Cloud (2023)]. This proactive awareness of the evolving threat landscape enables organizations to adapt their security strategies and remain ahead of potential attackers. Integrating threat intelligence feeds into existing security tools and processes can significantly enhance an organization's ability to identify and block known malicious actors and infrastructure [Google Cloud (2023)]. Leveraging threat intelligence resources provided by government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) [CISA (2023b)], and national cybersecurity centers [NCSC (2021)] can provide valuable insights and actionable data to strengthen preventative and detective security controls.

7. Conclusion

The global financial ecosystem we operate in today is a rapidly changing landscape that is a very attractive target for attackers who are utilizing increasingly sophisticated techniques.

Protecting self-hosted payment systems against the persistent and evolving threat of ransomware requires a holistic and multi-layered security approach. Organizations must prioritize the implementation of robust preventive measures, including establishing reliable backup and recovery procedures, enforcing strong access controls and the principle of least privilege, maintaining a rigorous vulnerability management and patching program, hardening network security, enforcing multi-factor authentication, deploying comprehensive endpoint security measures, and conducting regular security awareness training for all personnel.

In the unfortunate event of a successful attack, having a well-defined and regularly tested incident response plan is crucial for ensuring a swift and effective containment, eradication, and recovery process. Furthermore, staying informed about the latest ransomware threats and tactics through continuous monitoring of threat intelligence sources is essential for adapting security strategies and proactively defending against emerging risks. By diligently implementing these recommendations, organizations can significantly enhance their resilience against ransomware attacks and safeguard their critical self-hosted payment infrastructure.

References

CISA, 2023, "Understanding ransomware threat actors: LockBit," Cybersecurity and Infrastructure Security Agency, June 14, https://tinyurl.com/mt4bbzsp

CISA, 2023b, "Stop ransomware guide," Cybersecurity and Infrastructure Security Agency, October 19, https://tinyurl.com/zh5ryvjw

CISA, 2024, "#StopRansomware: Blacksuit (Royal) Ransomware," Cybersecurity and Infrastructure Security Agency, August 27, https://tinyurl.com/ms8ubn84

CISA, 2025, "Stop ransomware guide," Cybersecurity and Infrastructure Security Agency, October 19, https://tinyurl.com/zh5ryvjw

CSBS, 2023, "Ransomware self-assessment tool 2.0 (R-SAT)," https://tinyurl.com/tdrf5w9k

Cynet, 2025, "6 ransomware protection strategies you must know," May 8, https://tinyurl.com/3bbkm99z

Dispensa, B., 2023, "Ransomware mitigation: top 5 protections and recovery preparation actions," AWS Security Blog, September 1, https://tinyurl.com/55pbn7su

Dopamu, O. M., 2024, "Cloud-based ransomware attack on US financial institutions: an in-depth analysis of tactics and counter measures," International Journal of Science and Research 13:2, 1872–1881

Google Cloud, 2023, "Best practices for mitigating ransomware attacks using Google Cloud,"

IPC, 2022, "How to protect against ransomware," Information and Privacy Commissioner of Ontario, October, https://tinyurl.com/4dwd5zxv

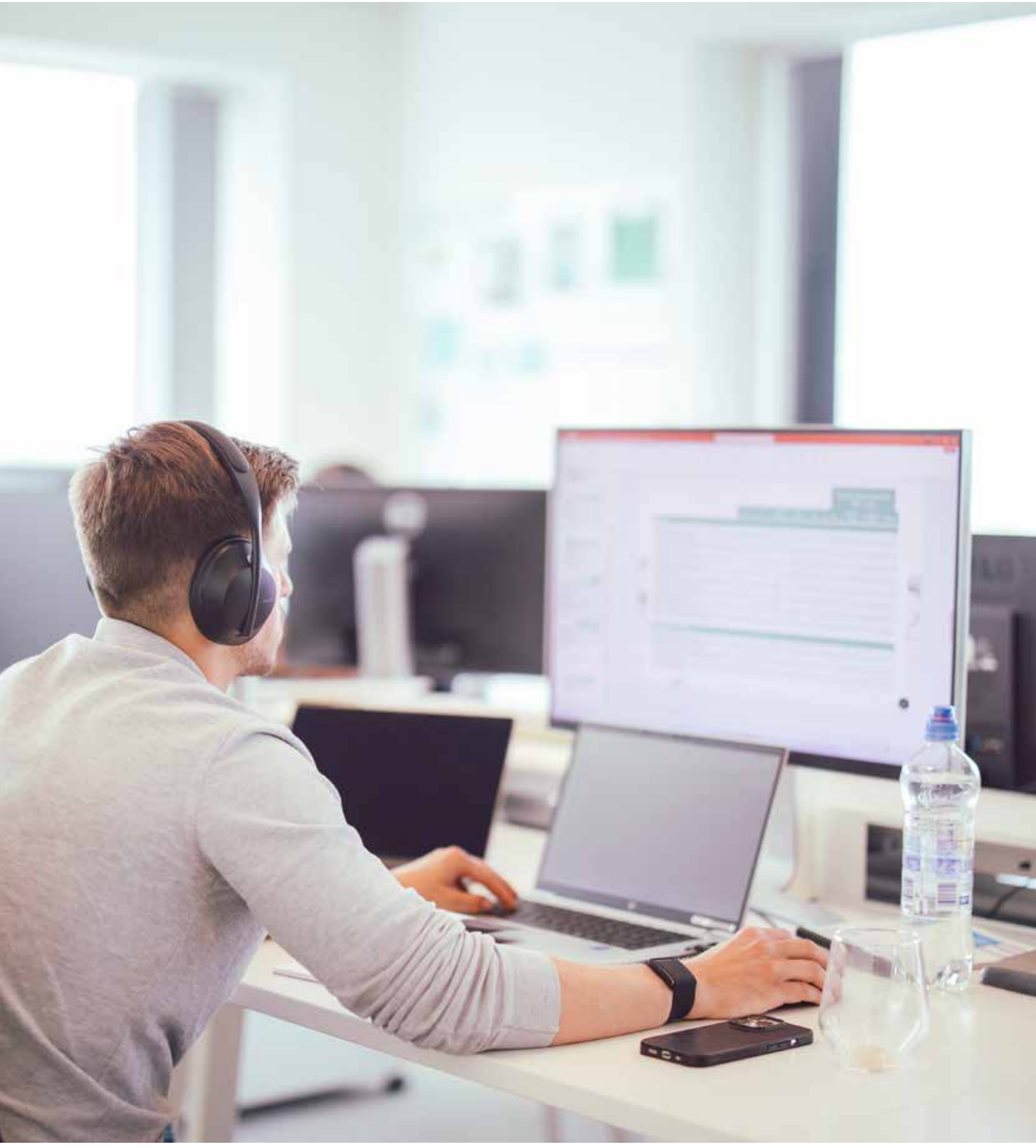
NCSC, 2021, "Mitigating malware and ransomware attacks," National Cyber Security Centre, September 9, https://tinyurl.com/3ttr783r

Ojo, A. O., 2025, "Ransomware trends and mitigation strategies: A comprehensive review," Global Journal of Engineering, Technology and Agriculture 22:3, 9-16

PCI, 2018, "PCI DSS Quick Reference Guide," PCI Security Standards Council, July, https://tinyurl.com/2nf3xdpd

PTP Cloud, 2023, "Protecting against ransomware," April, https://tinyurl.com/5crfzr8v

Vanover, R., 2023, "How to protect against ransomware: 6 best practices," Veeam, July 27, https://tinyurl.com/m5ysz7m



Future of Payments

Transforming **cross-border Payments**: navigating technological innovation, geopolitical fragmentation, and auditing challenges

David S. Krause, Emeritus Associate Professor of Finance, Marquette University

Eric P. Krause, Assistant Professor of Accounting, Iowa State University

ABSTRACT

This paper explores the transformation of global cross-border payments at the intersection of technological innovation, geopolitical fragmentation, and auditing complexity. It evaluates the limitations of legacy infrastructures, such as SWIFT and correspondent banking, and examines the emergence of distributed ledger technologies (DLT), central bank digital currencies (CBDCs), and newly institutionalized stablecoins. Special attention is given to the implications of the U.S. GENIUS Act, which provides regulatory clarity for fiat-backed stablecoins and has catalyzed issuance by major financial institutions. While these digital assets promise faster, lower-cost, and more transparent cross-border transactions, they also raise new challenges regarding taxation, custody, interoperability, and auditability. This paper analyzes how programmable financial architectures alter compliance and assurance dynamics and how stablecoins may support geopolitical objectives by reinforcing dollar dominance in digital networks. It concludes with policy recommendations focused on technical standardization, regulatory harmonization, and modernization of auditing practices to enhance the resilience, integrity, and inclusivity of the evolving global payments ecosystem.

1. Introduction

The cross-border payments ecosystem is undergoing a profound transformation driven by technological innovation, geopolitical fragmentation, and evolving auditing frameworks. Historically dependent on legacy infrastructures such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and complex correspondent banking networks, international payments have long suffered from inefficiencies related to cost, speed, and transparency. In response, a new generation of financial technologies, including distributed ledger technologies (DLT), central bank digital currencies (CBDCs), and regulated stablecoins, has begun to reshape the global payments landscape. The 2025 passage of the GENIUS Act, which provides a regulatory foundation for fiat-backed stablecoins, signals an important institutional shift in this domain. Together, these innovations promise faster and more interoperable cross-border transactions but introduce new complexities in legal harmonization, data governance, and financial assurance.

Cross-border payments remain foundational to global commerce, investment, and remittances. In 2022, such payments exceeded U.S.$150 trillion in volume, involving businesses, governments, financial institutions, and individuals [McKinsey & Co. (2022)]. Yet despite their scale, the underlying infrastructure remains fragmented and opaque. High transaction costs, delayed settlements, and limited visibility across intermediated systems persist - challenges that disproportionately affect individuals in developing economies, small and medium-sized enterprises, and remittance-dependent households [BIS (2023b)].

Efforts to modernize these systems have accelerated. Legacy models such as SWIFT are increasingly regarded as inadequate for the real-time demands of a digital economy. New architectures, including blockchain-based platforms, tokenized payment rails, and CBDC pilots, are being tested as alternatives [BIS (2022)]. These technologies offer potential gains in speed, cost-efficiency, and auditability. However, they also present new sources of operational and legal uncertainty, including risks related to consensus protocols, smart contracts, and enforceability across jurisdictions.

This technological shift coincides with rising geopolitical tensions that are reshaping financial infrastructure. The exclusion of Russian banks from SWIFT following the Ukraine invasion has exemplified the strategic use of financial networks as tools of national power. In response, countries such as China and Russia have accelerated efforts to build sovereign or regional alternatives to Western-dominated systems (Nölke (2022), Ballis (2025)]. The risk of a fragmented or multipolar payments architecture is thus increasing, with implications for systemic coherence and global coordination.

These dynamics also challenge traditional audit and compliance frameworks. Assurance practices developed for centralized institutions and document-based trails are increasingly strained in environments that rely on decentralized ledgers and programmable transactions. Issues such as data provenance, cross-border regulatory arbitrage, and the reliability of external data inputs (oracles) now complicate oversight and assurance processes. Furthermore, the emergence of risks such as smart contract vulnerabilities and algorithmic consensus failures demand a rethinking of financial risk modeling [FATF (2021), IAASB (2023)].

This paper examines the convergence of technological innovation, geopolitical realignment, and audit complexity in the transformation of global payments. It compares legacy and emerging infrastructures, evaluates the implications of increasing geopolitical bifurcation, and assesses how financial assurance must evolve to address digitally native risks. It concludes with policy recommendations to enhance interoperability, regulatory coherence, and audit resilience in the evolving global payments ecosystem.

2. Evaluating current cross-border payment systems

2.1 Traditional systems and their limitations

The global cross-border payments ecosystem has long relied on correspondent banking relationships and financial messaging services such as the SWIFT network. Historically rooted in bilateral trust arrangements, correspondent banking evolved into a multilayered system in which financial institutions maintain accounts with each other to settle international transactions [Cheng et al. (2024)]. While this infrastructure enabled the expansion

of international finance throughout the twentieth century, its limitations are increasingly evident.

Between 2011 and 2024, active correspondent banking relationships declined by more than 20%, with emerging markets disproportionately affected [BIS (2024b)]. This decline reflects a combination of rising compliance burdens, de-risking practices by global banks, and the emergence of more agile digital alternatives. Cross-border transactions conducted through traditional channels often involve multiple intermediaries, each contributing to cost, processing time, and opacity. Settlement periods typically span 2–5 business days, and fees accrue at every step, particularly for currency conversions and intermediary charges [EY (2024)]. According to the World Bank (2024), average global remittance costs remain at 6.2%, more than double the United Nations Sustainable Development Goal (SDG) target of 3%.

Liquidity management adds another layer of inefficiency. Financial institutions are required to pre-fund nostro accounts in multiple currencies, resulting in trapped capital and opportunity costs. The World Bank (2024) estimates that these costs exceed U.S.$5 billion annually for large global institutions. Moreover, the legacy infrastructure suffers from limited end-to-end visibility. Once a transaction enters the correspondent chain, it becomes difficult for originators to track progress, complicating compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) standards [FATF (2024), BIS (2024a)].

Auditors face corresponding challenges. Fragmented transaction trails, inconsistently maintained logs, and jurisdiction-specific data retention rules hinder oversight and elevate the risk of regulatory non-compliance. These weaknesses have prompted calls for renewed investment in digital audit infrastructure and cross-border data sharing protocols [Arman (2023)].

2.2 Modernizing legacy infrastructure: SWIFT gpi and CLS

In response to growing inefficiencies, SWIFT launched its Global Payments Innovation (gpi) initiative in 2017 to enhance transparency and reduce settlement times. As of 2025, over 65% of gpi payments reach their destination within five minutes, and more than 90% are credited within 24 hours [SWIFT (2024)]. SWIFT gpi allows institutions to trace payments in real time and identify delays attributable to specific intermediaries, offering a marked improvement over legacy systems.

Nevertheless, structural inefficiencies persist. SWIFT remains a messaging platform rather than a settlement mechanism, and its reliance on underlying correspondent banking relationships means that frictions, liquidity constraints, and compliance burdens are not fully resolved. Interoperability between jurisdictions remains a significant challenge, particularly for transactions involving smaller financial institutions or emerging market currencies.

Continuous Linked Settlement (CLS) represents another advancement in global payment infrastructure. CLS mitigates foreign exchange (FX) settlement risk through payment-versus-payment (PvP) mechanisms, eliminating the risk that one party delivers funds without receiving the corresponding currency in return - commonly referred to as “Herstatt risk” [Miller (2002)]. As of 2022, CLS processed approximately one million transactions per day across 18 currencies and more than 70 directly connected financial institutions, with indirect benefits extending to over 30,000 market participants [CLS Group (2021)].

Despite its benefits, CLS has notable limitations. Participation costs are high and coverage is limited to major currencies. Consequently, many FX trades involving emerging markets fall outside its scope. Efforts are underway to expand PvP access through public-private partnerships and regulatory support, particularly for high-risk corridors where settlement risk remains acute [Bayle de Jessé (2021), Heller (2024)].

2.3 Fintech and non-bank alternatives

A growing array of fintech companies and non-bank financial intermediaries are offering cross-border payment services that seek to bypass the inefficiencies of traditional rails. These include digital wallets, real-time gross settlement platforms, push-to-card solutions, and crypto-native remittance services. Such alternatives offer lower costs and faster speeds for retail and small-business users by leveraging pre-funded local accounts and digital integration layers [Derviz (2023)].

While fintech providers have achieved notable success in retail markets, particularly in remittance corridors and emerging economies, they are not without limitations. Pre-funding requirements and

reliance on fragmented domestic networks introduce inefficiencies, especially for large or complex transactions. Currency conversion fees often range from 1% to 4%, and exchange rate spreads further increase costs [EY (2024)]. Moreover, regulatory requirements, particularly around KYC, AML, and cross-border data transmission, vary widely across jurisdictions, complicating compliance for non-bank operators.

Major card networks have expanded their role in cross-border payments through push-to-card services, allowing for near-instant fund transfers to eligible debit or credit cards. Visa and Mastercard have leveraged their global networks to offer these services across increasingly diverse corridors. Transaction costs typically range between 0.6% and 1.4% [Nawrocki (2024)], making them competitive for smaller payments, though adoption remains uneven across regions. The International Monetary Fund (2024) reports that mobile money and digital wallet usage for cross-border transactions has increased by over 200% in Africa and Southeast Asia since 2020. Nevertheless, it is estimated that 1.4 billion adults remain unbanked globally, limiting access to such solutions [World Bank (2024)].

2.4 Performance benchmarks and regional disparities

The efficiency of cross-border payment methods varies by transaction size, currency pair, and geographic corridor. Traditional bank remittances under U.S.$200 average 10.5% in fees, compared to 5.9% for money transfer operators [BIS (2024b)]. For wholesale transactions, SWIFT payments of U.S.$100,000 may incur U.S.$25–U.S.$100 in fees, plus a 0.5%–3% FX markup, resulting in total costs of U.S.$500–U.S.$3,000 depending on the corridor. Transactions involving major currencies (e.g., USD/EUR, USD/JPY) benefit from liquidity and direct routing, while exotic currency pairs often require multiple conversions and intermediary banks, raising both cost and latency [FSB (2024)].

Although significant progress has been made, with average global remittance costs falling from 9% in 2015 to approximately 6% in 2024, efficiency gains have not been evenly distributed [IMF (2024)]. High-cost corridors, especially those involving low-income or politically unstable regions, remain underserved. These disparities highlight the urgency of global regulatory coordination and infrastructure modernization to ensure inclusiveness and resilience in cross-border payments.

3. DLTs and CBDCs

Emerging technologies are rapidly transforming cross-border payments by addressing long-standing inefficiencies in speed, cost, transparency, and accessibility. CBDCs and DLT offer innovative frameworks for payment processing, settlement, and compliance. While these tools promise major efficiency gains, they also introduce new challenges for monetary policy, regulatory coordination, and auditability. This section evaluates the evolving role of these technologies and highlights recent case studies that illustrate their global implementation.

3.1 CBDCs

CBDCs, which are digital forms of central bank liabilities, are at the forefront of payment innovation. Unlike cryptocurrencies, which are decentralized and often volatile, CBDCs are issued and backed by central banks and designed to preserve monetary sovereignty. By enabling direct settlement between central banks or commercial financial institutions, CBDCs can eliminate multiple intermediaries in cross-border transactions and significantly reduce transaction costs and settlement times [BIS (2023b), Krause (2024)].

Despite these advantages, implementing CBDCs for cross-border use presents substantial technical and governance challenges. Jurisdictions must establish shared protocols for data access, interoperability, transaction validation, and settlement finality. Privacy protections, cybersecurity risk management, and monetary policy coordination also remain unresolved [IMF (2022)].

3.1.1 CBDC case studies

Projects such as Agorá, mBridge, and the Sand Dollar highlight the range of applications and challenges in deploying CBDCs. Project Agorá, a BIS-led collaboration among several central banks, explores shared multi-CBDC platforms with built-in compliance features [BIS (2023c), EY (2024)]. China's e-CNY trials in trade with Belt and Road partners aim to reduce dollar dependence through integrated cross-border infrastructure [Atlantic Council (2025), IMF (2022)]. Meanwhile, the Bahamas' Sand Dollar illustrates how small jurisdictions can extend financial inclusion through retail CBDCs with potential for regional use [BIS (2023b)].

3.2 DLTs

DLTs underpin many of the innovations in digital payments. By enabling direct peer-to-peer transfers across distributed systems, DLTs reduce settlement times from days to seconds and can lower transaction costs to less than 0.1% [BIS (2024c), EY (2024)]. Moreover, DLT enhances auditability by creating immutable records of payment events, allowing for transparent compliance checks and real-time reconciliations.

Yet significant barriers remain. Integration with existing financial infrastructure is complex, and legal recognition of blockchain-based settlement finality varies by jurisdiction. Interoperability among different blockchains and traditional systems also presents challenges. Moreover, public blockchains raise privacy and scalability concerns, while permissioned networks require trusted governance arrangements [IMF (2022), FSB (2023c)].

3.2.1 DLT case studies

Ripple/XRP: Ripple seeks to improve cross-border settlement by using its XRP token and ledger to facilitate instant transactions between financial institutions. Its global expansion has been tempered by regulatory scrutiny. A 2020 lawsuit by the U.S. Securities and Exchange Commission (SEC) alleging that XRP was an unregistered security initially limited adoption. A 2023 ruling partially in Ripple's favor has revived interest in the platform, though full legal clarity remains pending [Handagama (2023), Yaffe-Bellany (2023), BIS (2024a)]. In 2025, the SEC dropped the lawsuit, but Ripple's broader adoption continues to hinge on regulatory harmonization and integration standards [Nguyen (2025), WEF (2024c)].

Enterprise Blockchain Initiatives: financial institutions are increasingly deploying permissioned DLT networks for payments, trade finance, and securities settlement. These systems prioritize privacy, compliance, and auditability. Several banks are now tokenizing fiat deposits to facilitate intraday liquidity and FX transactions with enhanced transparency. The Financial Stability Board (FSB) and Basel Committee are monitoring these developments to ensure adequate reserve management and oversight [FSB (2020), BIS (2024c)].

Tokenization trends: tokenization of real-world assets enables fractional ownership and 24/7 cross-border transferability through smart contracts. These programmable assets reduce operational costs and settlement risk while improving market accessibility. Tokenization complements the use of CBDCs and stablecoins by creating a broader ecosystem of digitally native instruments [Nawrocki (2024), BIS (2024b)].

4. Stablecoins and the GENIUS Act era

The landscape of cross-border payments has been reshaped by the passage of the U.S. Guaranteeing Essential, Neutral, and Interoperable Ubiquitous Stablecoins (GENIUS) Act in 2025. This legislation has introduced clear regulatory standards for stablecoin issuance, including requirements for 1:1 fiat backing, public audits, capital buffers, and oversight by federal regulators [U.S. Congress (2025)]. The GENIUS Act has catalyzed a wave of stablecoin development by financial institutions and technology firms seeking to modernize international payments.

Stablecoins are digital assets designed to maintain a stable value relative to fiat currencies. Unlike CBDCs, which are public liabilities, stablecoins are typically issued by private entities and backed by reserve assets. They offer programmable features, near-instant settlement, and compatibility with blockchain infrastructures. These characteristics make them well-suited for remittances, B2B transactions, and dollar access in emerging markets [Catalini and de Gortari (2021)].

The passage of the GENIUS Act significantly accelerated stablecoin development among major financial and fintech firms. Companies like PayPal, Visa, Mastercard, and Fiserv are at the forefront of this push, demonstrating a clear commitment to integrating stablecoins into their operations. PayPal's PYUSD, launched in 2023, is already a significant player in the market. As of June 2025, it holds the position of the seventh-largest stablecoin globally with a market capitalization of U.S.$1 billion. This early success highlights the growing acceptance and utility of stablecoins within established financial ecosystems.

Beyond PayPal, other prominent financial institutions and fintech companies are actively exploring and implementing stablecoin solutions. Many have announced pilot programs for dollar-backed stablecoins across various blockchain networks [Lang (2025)]. These widespread initiatives underscore the increasing institutionalization of stablecoins

and reinforce their potential to become efficient and scalable tools for facilitating cross-border fund movements.

4.1 Benefits for cross-border payments

Stablecoins are transforming cross-border payments by reducing reliance on correspondent banking, enabling 24/7 transfers, and significantly cutting transaction costs. While average global remittance fees are over 6%, stablecoins can bring these costs below 1% depending on the corridor and infrastructure. Their programmability also allows for smart contract-based compliance checks, automated reconciliation, and transparent audit trails [Carballo (2025)].

The U.S. Treasury has also recognized stablecoins as instruments of soft power. By embedding the dollar in global blockchain infrastructures, U.S.-regulated stablecoins may help sustain dollar hegemony in a multipolar financial system [U.S. Treasury Department (2024c)].

4.2 Remaining barriers

Despite regulatory advances, several issues remain unresolved. Tax treatment of stablecoin transactions in the U.S. may still trigger taxable events unless legislative reforms introduce de minimis exemptions [Tax Policy Center (2024)]. Custody, insolvency protections, and legal status of stablecoin holdings under bankruptcy law are also evolving concerns.

Interoperability is another challenge. As stablecoins are issued across multiple platforms (Ethereum, Solana, and proprietary chains), cross-chain bridging remains complex. The Bank for International Settlements emphasizes the need for global technical standards to prevent fragmentation [BIS (2023b)]. In addition, fees - whether platform-based or network-imposed - can fluctuate unpredictably, potentially limiting use in micro-transactions.

4.3 Performance comparison

Table 1 summarizes key performance features across traditional systems, stablecoins, and CBDCs.

The GENIUS Act marks a significant inflection point in the development of stablecoins, anchoring them within the regulatory perimeter while preserving their technical advantages. As institutions invest in issuance, custody, and interoperability frameworks, stablecoins are likely to play a foundational role in the next generation of cross-border payment systems. If global alignment on tax, custody, and technical standards is achieved, stablecoins could offer an efficient, accountable, and inclusive infrastructure for international finance.

4.4 Integrating CBDCs, DLT, and stablecoins

The convergence of CBDCs, DLT, and stablecoins is reshaping the architecture of global payments. Hybrid models combining these technologies offer new pathways for interoperability, compliance, and resilience. For example, stablecoins pegged to CBDCs could act as intermediaries between public and private networks, allowing for seamless integration of retail and wholesale ecosystems.

Project Dunbar, a BIS-led initiative, exemplifies this integration. The project explores the use of unified ledgers to settle transactions involving multiple CBDCs, stablecoins, and tokenized commercial bank money. Early findings suggest that such platforms could reduce costs by up to 70% and improve compliance monitoring through built-in audit features [BIS (2023b), FSB (2023b), IMF (2023)]. However, success depends on developing common

Table 1: Comparative performance of cross-border payment systems

Feature	SWIFT (traditional)	Stablecoins	CBDCs (pilot stage)
Settlement speed	2–5 days	Seconds	Near-Instant
Cost per transaction	3–7%	<1%	0.1–1%
Transparency	Low	High	Medium–High
Intermediaries	3–5	0–1	1–2

technical standards, cross-border regulatory frameworks, and real-time auditing tools.

As digital currencies evolve, their long-term success will depend not only on technical scalability but also on regulatory clarity, institutional adoption, and global coordination. Ongoing research and pilot programs will be critical to validating use cases and mitigating risks before these technologies scale to systemic levels.

5. Geopolitical and regulatory influences on cross-border payments

As cross-border payment systems become more central to financial stability and economic policy, their geopolitical relevance has intensified. In recent years, governments have increasingly treated payment networks not only as tools for financial integration but also as instruments of national security and economic influence. The imposition of sanctions, the exclusion of financial institutions from SWIFT, and the pursuit of regional alternatives to dollar-based payment rails reflect a broader strategic decoupling of financial infrastructures.

5.1 Sanctions and trade disputes

The use of global payment systems as tools of geopolitical leverage reached a new level of intensity following Russia's invasion of Ukraine in 2022. In response, the United States, European Union, Japan, and allied countries imposed sweeping sanctions that included disconnecting several major Russian banks from the SWIFT messaging network [Zorthian (2022)]. This move significantly impaired Russia's ability to settle international transactions in major currencies and access global financial markets [CEIP (2022)].

However, these measures were not uniformly applied. Financial institutions deemed critical to energy-related transactions were initially exempt to minimize collateral disruptions in global energy markets, especially in Europe. This selective enforcement highlighted the strategic trade-offs inherent in weaponizing financial infrastructure and underscored the constraints of multilateral coordination in sanction regimes.

Beyond their immediate economic impact, SWIFT-related sanctions reverberated through global trade networks. Russian firms struggled to access liquidity in foreign currencies, while key trading partners, including China and India, accelerated efforts to establish alternative bilateral payment arrangements. These developments catalyzed a broader reassessment of dependence on dollar-centric systems and prompted a renewed push for financial sovereignty through regional or national payment alternatives.

5.1.1 Evolution of sanctions enforcement

The Russia sanctions episode also revealed both the strengths and weaknesses of existing enforcement mechanisms. Unlike the Iran sanctions of the previous decade, which included far-reaching secondary sanctions targeting non-compliant third parties, the initial Russian measures largely avoided penalizing indirect counterparties. This more limited approach reflected the complexity of disentangling global trade relationships and highlighted the need for real-time, precise enforcement tools.

Traditionally, sanctions enforcement has relied on batch processing and periodic updates to restricted-entity lists using extract, transform, and load (ETL) processes. These systems are often ill-equipped to keep pace with the speed of digital payments. Delays between policy announcements and effective enforcement create vulnerabilities that sanctioned entities can exploit [Hughes (2025)].

To address these challenges, regulators and financial institutions are deploying more advanced sanctions screening tools capable of real-time updates and analytics integration. These tools seek to reconcile the need for speed in payment processing with the obligation to screen counterparties against dynamically evolving sanctions lists, improving accuracy without imposing undue latency on transactions.

5.2 Circumventing sanctions through digital assets

As restrictions on traditional banking channels expanded, Russia and its trading partners increasingly turned to digital assets, particularly cryptocurrencies and stablecoins, to facilitate international trade. According to U.S. Treasury reports, digital currencies such as Bitcoin and Tether (USDT) have been used to conduct transactions in energy, commodities, and dual-use goods, particularly in trade

with China and India (U.S. Treasury Department (2023), Fabrichnaya and Marrow (2024)].

In response to these pressures, the Bank of Russia introduced legislation in 2022 authorizing the use of digital financial assets for cross-border payments. The policy shift reflects a broader strategic goal of reducing exposure to Western-controlled payment infrastructure and building alternative rails for international trade [Bank of Russia (2022)].

Western regulators have responded by enhancing scrutiny of digital asset transactions. The U.S. Treasury sanctioned several crypto-related entities in 2024 for facilitating sanctions evasion using stablecoins [U.S. Treasury Department (2024b)]. These actions signal a growing regulatory consensus that the decentralized nature of digital payments must not undermine international sanctions enforcement.

Nevertheless, the use of digital assets for large-scale sanctions circumvention remains limited by practical constraints. Public blockchain transactions can be monitored using advanced analytics tools, such as those developed by Chainalysis, enabling law enforcement to trace suspicious flows [Chainalysis (2024)]. Moreover, the relative illiquidity and volatility of most cryptocurrencies restrict their usability for high-value, time-sensitive commercial transactions [Adrian and Weeks-Brown (2022)].

5.3 Geopolitical realignment and alternative payment systems

The strategic weaponization of global payment networks is accelerating a trend toward geopolitical realignment and financial fragmentation. The increasing use of non-dollar bilateral payment arrangements and local-currency settlement mechanisms reflects growing efforts by states to insulate their economies from external pressure.

For example, more than 90% of bilateral trade between Russia and China is now settled in renminbi or rubles, circumventing the dollar altogether [McDowell (2024)]. China has also promoted the internationalization of the renminbi through expanded use of its Cross-Border Interbank Payment System (CIPS), which processed over 5 quadrillion renminbi in 2019. While CIPS continues to rely on SWIFT messaging for certain functions, it provides a foundational layer for renminbi-based cross-border clearing [CEIP (2022)].

China's efforts to reduce dollar dependence extend beyond bilateral trade. In Southeast Asia and Central Asia, Beijing is encouraging broader adoption of CIPS and bilateral swap arrangements, while also participating in multi-CBDC initiatives such as Project mBridge. Although these efforts are unlikely to displace the U.S. dollar in the short term, they mark a decisive shift toward multipolarity in global finance.

5.4 Russia's SPFS and Direct Settlement Mechanisms

In parallel, Russia has expanded its own domestic alternative to SWIFT - the System for Transfer of Financial Messages (SPFS). Although more limited in scope and reach, SPFS allows Russian banks to communicate payment instructions without relying on foreign infrastructure. Russian institutions have also deepened their integration into China's National Advanced Payment System (CNAPS) and pursued direct settlement arrangements through Chinese state-owned banks.

These mechanisms have enabled continued trade in energy and essential goods despite international sanctions. However, they also raise concerns about the emergence of parallel payment ecosystems that may be less transparent, more difficult to audit, and harder to regulate. The proliferation of such alternatives risks further fragmenting the global financial architecture and reducing the effectiveness of multilateral financial governance.

5.5 Regulatory divergence and jurisdictional fragmentation

The rapid growth of digital asset usage in cross-border contexts has exposed stark differences in national regulatory approaches. While some jurisdictions have adopted comprehensive regulatory frameworks, such as the European Union's Markets in Crypto-Assets (MiCA) regulation, others remain in early stages of policy development or rely on enforcement-based models [WEF (2024a)].

The Financial Stability Institute (FSI) highlights material differences in how countries define, license, and oversee stablecoin issuers [Ledger Insights (2024)]. These include variations in reserve composition requirements, redemption rights, capital buffers, and disclosure obligations. Inconsistent definitions of digital assets - as either securities, payment instruments, or commodities - further complicate efforts to build a unified regulatory approach [FSB (2023c), BIS (2023b)].

This divergence not only increases compliance costs but also enables regulatory arbitrage, as issuers may domicile in jurisdictions with weaker oversight while offering services globally. For regulators, auditors, and financial institutions, the absence of a harmonized framework impedes efforts to assess systemic risk and ensure consistent consumer protection.

5.6 KYC, AML, and cross-border compliance gaps

The complexity of regulatory compliance is compounded by the lack of consistent KYC and AML standards across jurisdictions. Legacy compliance systems, many of which rely on static databases and manual reporting, are ill-suited for the real-time, dynamic nature of digital transactions [Hughes (2025)].

Real-time sanctions screening and enhanced due diligence requirements are placing new demands on compliance infrastructure. Institutions must now balance operational efficiency with regulatory precision, often in environments where regulatory obligations diverge significantly across borders. Inconsistencies in enforcement increase not only legal risk but also the risk of inadvertently facilitating illicit activity.

Institutions such as the International Organization of Securities Commissions (IOSCO), Financial Action Task Force (FATF), BIS, and FSB are actively working to close these gaps. In 2022, the FATF reaffirmed that systemically important stablecoins must comply with its updated AML/CTF standards, including the "Travel Rule" and enhanced reporting obligations [FATF (2022)]. Similarly, the FSB has called for global alignment of oversight practices and emphasized that no stablecoin with systemic importance should operate without meeting robust legal and audit standards [FSB (2023a)]. These efforts reflect an emerging consensus that digital innovation must be accompanied by strong governance, compliance, and auditability to prevent fragmentation and ensure long-term financial stability.

6. Transformation of cross-border payments auditing

The digital transformation of cross-border payments - driven by stablecoins, CBDCs, and DLTs - is fundamentally reshaping the auditing and assurance landscape. While these innovations enhance speed, efficiency, and transparency, they simultaneously introduce new risks and complexities for auditors, regulators, and compliance professionals. This section examines how auditing standards, assurance practices, and accounting frameworks are evolving to meet the challenges of an increasingly decentralized and digitally native payments ecosystem.

6.1 Auditing in distributed ledger and stablecoin systems

DLTs offer a theoretically immutable and transparent transaction history, which holds promise for improved auditability. However, these benefits often fail to extend fully into practice due to the continued existence of opaque, off-chain components. In the case of stablecoins, for instance, reserve management, issuance governance, and redemption operations frequently occur outside the ledger, where traditional audit limitations persist [Derviz (2023)].

Stablecoin issuers vary widely in the rigor and frequency of their reserve disclosures. Tether, the largest stablecoin by market capitalization, has historically relied on attestations rather than comprehensive independent audits. This practice has drawn regulatory and market criticism due to ongoing questions about the adequacy, liquidity, and transparency of its reserve assets [Torpey (2023)]. In 2025, Tether entered discussions with a major global accounting firm to explore formal audits, signaling an acknowledgment of the growing demand for assurance standards in digital asset markets [Lang and Howcroft (2025)].

By contrast, Circle's USD Coin has built its brand on transparency, issuing monthly attestations by Deloitte and publishing reserve breakdowns. However, it has not released a full-scale audit since 2021, highlighting the broader industry's struggle to adopt comprehensive assurance frameworks [Khalili (2024)]. This inconsistency undermines trust and raises broader concerns about systemic risk

should stablecoin issuers face redemptions during periods of market stress.

Regulators are responding by introducing legal mandates for standardized audits. In the U.S., the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act of 2025 imposes a suite of requirements: monthly public reserve disclosures, third-party attestations by registered public accounting firms, annual audits for issuers with more than U.S.$50 billion in circulation, and executive certifications attesting to the accuracy of reserve reports [Krause (2025a), Olmem et al. (2025), Sullivan & Cromwell (2025)]. These provisions seek to align stablecoin auditing with public company financial reporting norms and mitigate risks associated with opaque reserve structures.

Professional bodies are also updating technical guidance. The American Institute of CPAs (AICPA) published criteria in 2025 for stablecoin reserve attestations, while international regulators such as the European Securities and Markets Authority (ESMA) have enacted MiCA-compliant audit standards requiring 1:1 reserve backing, verification by licensed auditors, and the prohibition of algorithmic stablecoins [AICPA (2025), ESMA (2025)].

6.2 Accounting considerations for CBDCs

CBDCs introduce novel accounting challenges. Under current U.S. Generally Accepted Accounting Principles (GAAP), digital assets are generally treated as indefinite-lived intangibles, subject to impairment when market value declines, but not eligible for upward revaluation [ISDA (2022), Dale (2022)]. This model, however, may be inappropriate for CBDCs, which are state-issued instruments designed to maintain a stable nominal value and function as legal tender.

The International Financial Reporting Standards (IFRS) framework may offer more flexibility, potentially allowing CBDCs to be classified as cash equivalents depending on their maturity, liquidity, and functional use [IFRS (2022), Wytenburg et al. (2021)]. However, this would likely require an update to existing IFRS standards, such as IAS 7, to clarify the accounting treatment of sovereign-backed digital currencies and prevent misclassification.

Commercial banks participating in CBDC pilots must also determine how to report CBDC holdings on balance sheets. Key questions include whether CBDCs held for customers should be treated as liabilities, whether direct retail CBDC accounts displace deposit liabilities, and how central bank reserve requirements apply to CBDC balances. Projects like Aber, a joint CBDC experiment between the central banks of Saudi Arabia and the UAE, highlight the need for standardized reporting of cross-border CBDC liquidity and settlement activity [BIS (2021)].

Both the BIS and the IMF have called for globally coordinated approaches to accounting classification and financial disclosures. Consistent reporting would not only improve comparability across jurisdictions but also support macroprudential oversight of emerging digital liabilities [BIS (2025), Wytenburg et al. (2021)].

6.3 Auditing and sanctions enforcement

Digital payment systems intersect increasingly with global sanctions regimes, AML compliance, and CTF efforts. Effective enforcement of these frameworks depends on real-time transaction monitoring, due diligence, and independent audits.

As digital assets are increasingly used to evade sanctions - particularly in high-risk jurisdictions such as Russia, North Korea, and Iran - auditors are being called upon to verify not only financial records but also compliance with sanctions laws and data transparency obligations [U.S. Treasury Department (2024a)]. Modern audit techniques now include blockchain analytics, risk-scoring algorithms, and AI-based behavioral pattern detection to identify illicit activities and support law enforcement [Chainalysis (2024), Arctic Intelligence (2025)].

Auditors also serve a vital function in providing documentation for asset seizure proceedings and criminal investigations involving cross-border digital payments. The Financial Crime Academy (2025) emphasizes that advanced data analysis tools are essential for identifying shell entities, typologies of sanctions evasion, and anomalies in transaction flows. Moreover, independent audits serve as a key safeguard against institutional blind spots or deliberate circumvention of reporting requirements.

6.4 Global harmonization of audit standards

Fragmentation in national auditing and accounting practices presents a substantial barrier to the development of interoperable, trustworthy global payment systems. To mitigate this risk, global stand-

ard-setters have launched new initiatives to adapt assurance practices to the digital era.

In 2024, the International Auditing and Assurance Standards Board (IAASB) adopted a new Strategy and Work Plan for 2024–2027, with a core focus on elevating audit trust in a rapidly evolving technological landscape. One of its key pillars is supporting the audit profession's ability to respond to digital transformation, including challenges associated with auditing DLT-based transactions, digital assets, and algorithmic financial systems [IAASB (2024b)].

Complementing this, the IAASB released a Technology Position Statement emphasizing the need to embrace innovation and remove barriers within existing standards that may hinder the effective use of emerging technologies. The statement outlines eight action areas, including revising guidance, integrating technology-focused terminology, and promoting consistency across jurisdictions to ensure that auditors are equipped to evaluate next-generation financial systems [IAASB (2024a)].

These developments reflect a broader recognition that technology is not a peripheral consideration but a central component of future assurance. A durable foundation for digital payments depends not only on cryptographic consensus or protocol efficiency, but also on confidence in the institutions and standards that govern them. That confidence, in turn, relies on audit frameworks that are global, rigorous, and adaptable.

7. Conclusion and recommendations

The ongoing transformation of global cross-border payments - driven by emerging technologies, shifting geopolitical alliances, and evolving regulatory expectations - requires a coordinated policy response to preserve financial stability, integrity, and inclusiveness. This section outlines actionable recommendations across four stakeholder groups: central banks, international standard-setters, regulatory bodies, and private-sector participants. These recommendations are designed to further interoperability, strengthen auditability, and mitigate the risks associated with systemic fragmentation.

Central banks and monetary authorities

- **Developing interoperable CBDC frameworks:** central banks should prioritize the development of CBDC systems that are interoperable across jurisdictions. This includes agreeing on messaging protocols, legal standards for settlement finality, and privacy safeguards. Projects such as mBridge and Agorá demonstrate the potential of shared platforms, but broader adoption requires multilaterally agreed frameworks [BIS (2023a), IMF (2023)].
- **Strengthening coordination on FX liquidity and settlement risk:** to avoid new forms of systemic risk, central banks must expand PvP arrangements and liquidity backstops for CBDC and tokenized FX settlements. Lessons from CLS and Project Dunbar suggest that PvP integration into CBDC infrastructure can reduce settlement risk while preserving monetary sovereignty [Bayle de Jessé (2021), BIS (2023b)].
- **Supporting harmonized accounting treatment for CBDCs:** central banks should work with global accounting bodies to clarify the classification and treatment of CBDC balances under IFRS and national standards. A coordinated approach will improve comparability and prevent regulatory arbitrage across jurisdictions [Wytenburg et al. (2021), BIS (2025)].

Global regulatory and standards

- **Establish baseline global audit standards for stablecoins and digital assets:** the FSB, IAASB, and IOSCO should coordinate to define minimum audit requirements for stablecoin issuers. This includes standards for reserve verification, redemption rights, and off-chain governance disclosures [FSB (2023d), IAASB (2024b)].
- **Expand real-time compliance infrastructure for sanctions and AML/CTF:** regulatory authorities and supranational bodies such as FATF should invest in tools and mandates that support real-time monitoring of cross-border payments. This includes transaction-level visibility, dynamic sanctions list integration, and digital identity verification tools [FATF (2022), Hughes (2025)].
- **Promote equivalence frameworks for regulatory recognition:** to reduce market fragmentation, regulators should negotiate bilateral and multilateral "equivalence" regimes that recognize compliance standards across jurisdictions. This is particularly relevant in the EU–U.S. and ASEAN–China corridors, where divergent rules create legal uncertainty and increase compliance costs [ESMA (2025), Ledger Insights (2024)].

Private sector and financial intermediaries

- **Build auditable, tokenized payment infrastructure:** financial institutions and fintechs should adopt permissioned DLT platforms with integrated compliance and audit layers. These systems should support real-time transaction reporting, embedded rule enforcement (e.g., smart contract-based AML), and compatibility with existing enterprise resource planning systems [Derviz (2023), Chainalysis (2024)].
- **Partner with reputable audit firms for transparency assurance:** stablecoin issuers and digital asset custodians must elevate transparency through regular third-party audits conducted by accredited public accounting firms. Monthly attestations should be complemented by annual full-scope audits, as contained within the GENIUS Act and MiCA [Krause (2025b), AICPA (2025)].
- **Invest in compliance-driven innovation:** private sector actors should prioritize the development of tools that combine regulatory technology (RegTech) and financial technology (fintech). These include AI-powered transaction monitoring, anomaly detection, and cryptographic attestations of compliance. Enhanced due diligence at the technical layer can reduce the burden on front-line compliance personnel while improving outcomes [Arctic Intelligence (2025)].

Multilateral institutions and development banks

- **Support technical assistance for low-income countries:** the World Bank, IMF, and regional development banks should expand technical assistance programs to support digital payments infrastructure in low- and middle-income countries. This includes capacity-building in regulatory compliance, digital identity systems, and audit readiness for central banks and financial institutions [World Bank (2024), IMF (2023)].
- **Pilot inclusive cross-border payment systems:** development finance institutions can play a catalytic role by funding pilot projects that test low-cost, cross-border payment corridors using CBDCs or compliant stablecoins. These should be designed with interoperability, privacy, and user protections built in from inception, with an emphasis on remittance and SME use cases [BIS (2023c), WEF (2024b)].

Taken together, these recommendations underscore the need for a balanced approach - one that embraces innovation while reinforcing trust, governance, and systemic resilience. The future of global cross-border payments will not be defined solely by technological breakthroughs but by the quality of the legal, regulatory, and institutional frameworks that underpin them.

References

Adrian, T., and R. Weeks-Brown, 2022, "Cryptoassets as national currency? A step too far," International Monetary Fund (IMF), https://tinyurl.com/4wnyz9jy

AICPA, 2025, "AICPA publishes comprehensive criteria for reporting on stablecoins," March 26, https://tinyurl.com/4wytcj3d

Arman, D., 2023, "Considering IT risk during audit risk assessment procedures," Journal of Accountancy, November 1, https://tinyurl.com/b8dbr6pa

Arctic Intelligence, 2025, "Technology and automation in AML compliance for gatekeepers," February 27, https://tinyurl.com/yc7jwu89

Asian Banking & Finance, 2024, "How 2024 will spark financial services innovation in Southeast Asia. Correspondent banks raise costs in cross-border payments," https://tinyurl.com/49n72aax

Atlantic Council, 2023, "Standards and interoperability: the future of the global financial system," https://tinyurl.com/vthd8nv9

Atlantic Council, 2025, "CBDC tracker: global trends in central bank digital currency development," https://tinyurl.com/3f5hcrbj

Ballis, A., 2025, "Geopolitical tensions and financial networks: strategic shifts toward alternatives," arXiv, https://tinyurl.com/mr2w8x2y

BIS, 2021, "CBDC and its associated motivations and challenges – Saudi Arabia," Bank for International Settlements, https://tinyurl.com/35jwb8s7

BIS, 2022, "Implementation monitoring of the PFMI: Level 3 assessment on financial market infrastructures' cyber resilience," Bank for International Settlements, https://tinyurl.com/2b9z5w6j

BIS, 2023a, "Crypto crashes and stablecoin runs: economic and policy responses," Bank for International Settlements, https://tinyurl.com/2tbxaewc

BIS, 2023b, "The future monetary system: cross-border payments," Bank for International Settlements, https://tinyurl.com/3d8srtpa

BIS, 2023c, "Considerations for the use of stablecoin arrangements in cross-border payments," Bank for International Settlements, https://tinyurl.com/422jpr2b

BIS, 2024a, "FSB proposed framework for crypto-asset regulation," Bank for International Settlements, https://tinyurl.com/wyj7vxc3

BIS, 2024b, "Statistics on payment, clearing and settlement systems in the CPMI countries," Bank for International Settlements, https://tinyurl.com/53bc8ax4

BIS, 2024c, "Distributed ledger technology in payment systems: implementation challenges and operational impacts," Bank for International Settlements, https://tinyurl.com/2hnc24fr

BIS, 2025, "2025 triennial central bank survey of foreign exchange and OTC derivatives markets," Bank for International Settlements, https://tinyurl.com/99ench55

Bank of Russia, 2022, "On the use of digital financial assets in international trade, https://tinyurl.com/52khs5fa

Bastion, 2025, "State of stablecoins, part 3: the U.S. regulatory shift," April 3, https://tinyurl.com/tj86nedw

Bayle de Jessé, M., 2021, "Settlement risk: addressing the key issue in cross-border payments," CLS Group, October 15, https://tinyurl.com/43zjtxcs

BNP Paribas, 2023, "The benefits of Continuous Linked Settlement (CLS) in today's foreign exchange market," November 20, https://tinyurl.com/55p2a5xe

Carballo, I., 2025, "Stablecoins and cross-border payments: what banks must do," https://tinyurl.com/3mhn4zmb

Catalini, C., and A. de Gortari, 2021, "On the economic design of stablecoins," MIT working paper, https://tinyurl.com/32b5m8ye

CEIP, 2022, "How sanctions on Russia will alter global payments flows," Carnegie Endowment for International Peace. https://tinyurl.com/muc8u439

Chainalysis, 2024, "The 2024 geography of cryptocurrency report," https://tinyurl.com/yutuj5ab

Cheng, K., Z. Liu, S. Pezzini, and L. Yu, 2024, "Correspondent banking: origins, evolution and reglobalisation," Bank for International Settlements (BIS), https://tinyurl.com/udtsh5s5

Circle, 2023, "Circle announces cross-border transfer partnerships for USDC," https://tinyurl.com/3ebmm2zu

CLS Group, 2021, "CLS welcomes FSB Progress Report on Cross-Border Payments Roadmap," November 2, https://tinyurl.com/ms2zfbps

Crystal Intelligence, 2024, "Beyond borders: mapping the global digital asset regulatory landscape," https://tinyurl.com/mv5xrmzz

Dale, B., 2022, "The risk of bitcoin on a public company's balance sheet," Axios, July 29, https://tinyurl.com/ytp7bsb7

Darbyshire, R., 2020, "Accounting issues for central bank digital currencies," Long Finance, https://tinyurl.com/c758x7t6

Derviz, A., 2023, "Cross-border payments at a crossroads between SWIFT and DLT," Czech National Bank, July 7, https://tinyurl.com/3w9scbm6

ECB, 2020, "Exploring the anonymity properties of a CBDC," European Central Bank, https://tinyurl.com/yha9ccds

ESMA, 2025, "ESMA and the European Commission publish guidance on non-MiCA compliant ARTs and EMTs," January 17, https://tinyurl.com/33suz7my

EY, 2024, "Global payments outlook: navigating the next frontier," Ernst & Young, https://tinyurl.com/yy8jxuaf

Fabrichnaya, E., and A. Marrow, 2024, "Russia, China turn to digital payments as sanctions hamper bilateral trade settlements," Reuters, July 25, https://tinyurl.com/jx3fdmb4

Faster Payments Council, 2024, "Cross-border faster payments: a framework for successful implementation," https://tinyurl.com/4w84jstm

FATF, 2021, "Guidance on risk-based supervision," Financial Action Task Force, https://tinyurl.com/3ee3atyf

FATF, 2022, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," Financial Action Task Force, https://tinyurl.com/2bmn4vf6

FATF, 2024, "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation," Financial Action Task Force, https://tinyurl.com/2bmn4vf6

Financial Crime Academy, 2025, "Advanced data analysis in AML," March 14, https://tinyurl.com/2psbkavy

FSB, 2020, "Regulation, supervision and oversight of "global stablecoin" arrangements," Financial Stability Board, https://tinyurl.com/5nb4shde

FSB, 2021, "Targets for addressing the four challenges of cross-border payments: final report," Financial Stability Board, https://tinyurl.com/yz26ufmy

FSB, 2023a, "Global regulatory framework for crypto-asset activities," Financial Stability Board, https://tinyurl.com/4rf2pm8c

FSB, 2023b, "Regulatory approaches to cryptoassets in cross-border payments," Financial Stability Board, https://tinyurl.com/4x2jm76n

FSB, 2023c, "Enhancing cross-border payments: stage 3 roadmap," Financial Stability Board, https://tinyurl.com/5ycj4vat

FSB, 2023d, "High-level recommendations for the regulation, supervision and oversight of global stablecoin arrangements: final report," Financial Stability Board, https://tinyurl.com/8udhvxeu

FSB, 2024, "Recommendations to promote alignment and interoperability across data frameworks related to cross-border payments: final report," Financial Stability Board, https://tinyurl.com/7d485t59

FXC Intelligence, 2024, "New Data: cross-border payments market now worth over $194tn and is forecast to reach $320tn by 2032," https://tinyurl.com/yc22bnvx

Gitau, P., 2024, "AML/CTF audit for regulatory and best practices compliance," October 18, https://tinyurl.com/8rc6nydr

Handagama, S., 2023, "Ripple vs. SEC: a timeline of the legal battle," CoinDesk, https://tinyurl.com/k8dhyxsp

Heller, D., 2024, "Fixing cross-border payments: the essential steps," Fnality, December 3, https://tinyurl.com/2w47zfud

Hughes, C., 2025, "Payments industry: the impact of dynamic global sanctions," London Stock Exchange Group (LSEG), https://tinyurl.com/3xtfk3jv

IAASB, 2023, "Digital technology market scan: digital assets," International Auditing and Assurance Standards Board, https://tinyurl.com/4vhus6tx

IAASB, 2024a, "Elevating trust in audit and assurance: IAASB's strategy and work plan for 2024-2027," International Auditing and Assurance Standards Board, April 11, https://tinyurl.com/j3658kmz

IAASB, 2024b, "Technology position," International Auditing and Assurance Standards Board, October 3, https://tinyurl.com/5dy5frnz

ICAEW, 2024, "FASB issues crypto asset standard," https://tinyurl.com/yjsmedff

IFRS, 2022, "FASB-IASB joint meeting on digital assets," International Financial Reporting Standards Foundation, https://tinyurl.com/49j42pk7

IMF, 2022, "The rapid growth of fintech: vulnerabilities and challenges for financial stability," International Monetary Fund, https://tinyurl.com/573w4kvz

IMF, 2023, "Geopolitics and fragmentation emerge as serious financial stability threats," International Monetary Fund, https://tinyurl.com/38xdzwta

IMF, 2024, "Global financial stability report: digital assets and financial stability," International Monetary Fund, https://tinyurl.com/kjsmcnfr

ISDA, 2022, "Accounting for digital assets: key considerations," https://tinyurl.com/5btszz8w

Khalili, J., 2024, "Flush with cash, Tether has got Microsoft, Google, and Amazon in its crosshairs," Wired, August 12, https://tinyurl.com/4xfayhpx

Krause, D., 2024, "The future of global payments: the convergence of CBDCs, cryptocurrencies, AI, and DeFi," SSRN, https://tinyurl.com/yfksjd79

Krause, D., 2025a, "The implications of a U.S. ban on central bank digital currencies: global financial dynamics and the future of payments," SSRN, https://tinyurl.com/mtjx27ac

Krause, D., 2025b, "The GENIUS Act: a new era of U.S. stablecoin regulation," SSRN, https://tinyurl.com/5f74rd6c

Lang, H., 2025, "Visa and Bridge partner to launch stablecoin-linked cards," Reuters, https://tinyurl.com/bds2ca27

Lang, H., and E. Howcroft, 2025, "Tether is in talks with 'Big Four' firm about reserve audit, CEO says," Reuters, March 21, https://tinyurl.com/y4275akn

Ledger Insights, 2024, "Financial Stability Institute calls for more consistent stablecoin regulation globally," https://tinyurl.com/2ktx9e69

McDowell, D., 2024, "McDowell explains how US sanctions boost China's cross-border currency use," The Diplomat, Syracuse University, October 11, https://tinyurl.com/bdh5hbb5

McKinsey & Co., 2023a, "The 2023 McKinsey global payments report," https://tinyurl.com/bddyu3af

McKinsey & Co., 2023b, "Blockchain implementation in banking: costs, challenges, and transformation strategies," https://tinyurl.com/r6ks23jc

Miller, P., 2002, "CLS Bank: managing foreign exchange settlement risk," Bank of Canada Review, Bank of Canada, https://tinyurl.com/4ew7694w

Moody's, 2024, "What businesses need to know about sanctions compliance," April 9, https://tinyurl.com/mur7fz7z

Mural Pay, 2025, "The evolution of cross-border payment systems: from SWIFT to digital solutions," https://tinyurl.com/yc2jhv35

Nawrocki, T., 2024, "Cross-border payments: trends, challenges, and solutions," Payments Journal, https://tinyurl.com/ycy68uuh

Nölke, A., 2022, "The weaponization of global payment infrastructures: a strategic dilemma," SAFE white paper no. 89, Leibniz Institute for Financial Research SAFE, https://tinyurl.com/4njat8yp

Nguyen, V., 2025, "SEC is dropping Ripple lawsuit: CEO Brad Garlinghouse," Crypto Briefing, March 19, https://tinyurl.com/2rc52d8a

Olmem, A., J. A. Castelluccio, M. Bisanz, K. F. Truesdale, and J. P. Taft, 2025, "Congress moves forward on stablecoin legislation: the US Senate Banking Committee approves the GENIUS Act," Mayer Brown, March 17, https://tinyurl.com/38ju62ar

Reuters, 2025, "Study: 130 countries exploring digital currencies," April 11, https://tinyurl.com/pjjcr954

Roth, R., and W. Davis, 2024, "PayPal launches its own stablecoin, PYUSD," The Verge, August 15, https://tinyurl.com/585fn7hf

Sullivan & Cromwell, 2025, "Stablecoin legislation," March 19, https://tinyurl.com/2wscmdxf

SWIFT, 2024, "Global payment trends and market share analysis: annual report," https://tinyurl.com/3485pe9z

SWIFT, 2025, "SWIFT gpi: transforming cross-border payments," https://tinyurl.com/42eupda2

Tax Policy Center, 2024, "How is cryptocurrency taxed?" https://tinyurl.com/mth9fb54

Torpey, K., 2023, "Tether's ability to maintain dollar peg 'constrained' says S&P Global," Investopedia, December 12, https://tinyurl.com/576ske8n

U.S. Treasury Department, 2023, "Treasury sanctions Russian illicit procurement network," April 18, https://tinyurl.com/ykp4z9p7

U.S. Treasury Department, 2024a, "U.S. Treasury deputy secretary warns "malign" actors are using virtual assets," Reuters, April 8, https://tinyurl.com/bdcumufh

U.S. Treasury Department, 2024b, "Treasury sanctions facilitators of Russian sanctions evasion through the use of virtual currency," April 12, https://tinyurl.com/y5j5t9us

U.S. Treasury Department, 2024c, "2024 National strategy for combating terrorist and other illicit financing," May 16, https://tinyurl.com/dm6snyjc

WEF, 2024a, "Digital assets regulation: Insights from jurisdictional approaches," World Economic Forum, https://tinyurl.com/4dnmn3d2

WEF, 2024b, "Central bank digital currency (CBDC) policy-maker toolkit," World Economic Forum, https://tinyurl.com/y6vfzdth

WEF, 2024c, "Digital currency competition: assessing alternative cross-border payment solutions," World Economic Forum, https://tinyurl.com/3226tdfc

World Bank, 2024, "Remittance prices worldwide report," https://tinyurl.com/yx7wry2b

Wytenburg, R., R. V. Darbyshire, and A. Beja, 2021, "A central bank's guide to international financial reporting standards," International Monetary Fund, https://tinyurl.com/bdec2929

Yaffe-Bellany, D., 2023, "Federal judge rules XRP is not inherently a security in victory for Ripple," New York Times, https://tinyurl.com/2xb5sddz

Zorthian, J., 2022, "What are the new SWIFT sanctions and their impact on Russia?" Time, https://tinyurl.com/mdfrn52k

Future of Payments

CBDCs and the digital euro: AML compliance moves closer to the end-user

Christian Sillaber,
Senior Researcher, Department of Private Law, University Bern

ABSTRACT

The emergence of CBDCs, and specifically the development of the digital euro, presents a complex landscape of challenges and opportunities within the AML/CFT framework. This article provides an analysis of the bifurcated AML/CFT approaches embedded within the digital euro's design, highlighting the tension between legacy compliance models and novel privacy considerations. The online variant of the digital euro showcases enhanced KYC, continuous transaction monitoring, and robust digital identity integration, with oversight centralized under the recently established AMLA. These mechanisms promise to exceed traditional banking surveillance and traceability, leveraging real-time data and audit trails to set new benchmarks for AML efficacy. Conversely, the digital euro's offline variant - intended to emulate the anonymity and immediacy of cash - depends primarily on transaction limits, presenting intricate calibration challenges. This paper argues that the digital euro's AML/CFT regime is poised to serve as a regulatory bellwether for broader E.U.-wide adaptation to rapid technological change. As public attitudes and stakeholder resistance evolve in response to policy trade-offs, it is essential that AML/CFT objectives are pursued without compromising innovation, fundamental rights, or equitable economic participation.

1. Introduction

The monetary landscape is undergoing a radical transformation with the advent of Central Bank Digital Currencies (CBDCs).[1] These government-issued digital currencies promise to reshape our digital economy by offering a secure, efficient, and real-time means of payment that integrates seamlessly into the digital fabric of everyday life.

Unlike cryptocurrencies, which are often associated with volatility and regulatory uncertainty, and private digital payment systems such as WERO or Venmo, which are backed by debt issuance, CBDCs are issued through sovereign authority. Amid increasing interest in CBDCs [Bidder et.al (2025)],[2] the digital euro emerges as a particularly noteworthy initiative, distinguished by its regional scope and its intended use for augmenting [E.C. (2023a)] retail cash transactions [Armelius et al. (2021)]. Pursuant to European Union regulation [E.C. (2023b)], the European Central Bank (ECB) is actively exploring the viability of a digital form of cash intended to coexist with physical euro banknotes and coins.

One of the distinctive characteristics of the digital euro - and, by extension, other central bank digital currencies, such as the recently announced e-rupee project [Reserve Bank of India (2025)] as well as the Bank of Japan's CBDC pilot program [Bank of Japan (2025)] - is its potential to enable direct peer-to-peer (P2P) payments, akin to transactions conducted with cash but within a digital framework [Sillaber et al. (2024)]. This feature is particularly interesting, as it responds to an increasing demand for privacy in financial transactions, an essential aspect of personal finance in an age with increasing concerns regarding data privacy.[3]

The aforementioned anonymity features, while appealing to users and beneficial from a resilience standpoint, raise significant concerns for regulatory authorities tasked with preventing illicit financial activities. Money laundering, terrorist financing, and other criminal enterprises could take advantage of features that provide anonymity, thereby posing substantial risks to the integrity of financial systems and eroding public confidence. Accordingly, achieving an appropriate balance between user privacy and effective anti-money laundering protections represents a critical challenge that must be addressed as policymakers and regulators develop legal frameworks for CBDCs [Lagarde et al. (2022)].

This paper explores the intricate relationship among CBDCs, privacy, and anti-money-laundering/combating the financing of terrorism (AML/CFT) measures. Using the emerging digital euro as an example, it discusses how anti-money laundering compliance can be seamlessly integrated into the technical design of central bank digital currencies without compromising their potential to facilitate private P2P financial transactions. The paper highlights that a promising solution lies in technologically advanced methods that embed AML/CFT measures directly within the mechanisms governing access to, and use of, the digital euro.

2. The design of CBDCs: The digital euro

The European legislative initiative to introduce a digital euro is regarded as a pivotal step in adapting the euro monetary system to the digital age [Panette (2023), Miha (2025)]. This project, as first formalized in the European Commission's draft regulation [E.C. (2023a)], seeks to establish a CBDC as a digital version of the euro, with the stated objective of designating it as legal tender throughout the Eurozone. The central policy objective is to ensure that public money remains accessible, trusted, and competitive within the rapidly evolving landscape of private digital currencies [Auer et al. (2023)], emerging stablecoins [Aldasoro et al. (2025)], and technology-driven alternative means of online payment [ECB (2024)].

According to Article 7(1) of the draft regulation, the digital euro is equal to non-digital euros and physical cash, thus anchoring its role as a complementary - and expressively not substitutive - instru-

1. As of July 31, 2025, according to CBDCTracker.org reports, four central banks have officially launched a CBDC, while approximately 30 other national banks are either developing proof-of-concept projects or are in the pilot phase.
2. Wholesale CBDCs are gaining significant attention for their potential to enable efficient, high-value settlements, especially in light of the growing adoption of tokenized deposits and atomic settlement applications. On the other hand, retail CBDCs face obstacles, as evidenced by countries like Sweden, Canada, and the U.K., which have scaled back their initiatives due to limited public interest and challenges in adoption. It should be noted that while both types of CBDCs are under development, this paper focuses specifically on retail CBDCs.
3. The European Commission identifies privacy as the most significant risk noted in the Eurosystem report on the public consultation regarding a digital euro; ECB (2021).

ment within the existing monetary system [Lemke (2024)]. The ex-lege legal tender status further obligates acceptance of the digital euro for the settlement of debts and transactions across member states' territories, meaning it must be accepted under the same conditions and with the same finality as cash or non-digital central bank money.[4]

The legislative framework envisions the digital euro as comprising two distinct variants: the **online** and **offline** forms (Recitals 17 and 34 of the draft digital euro regulation). This approach acknowledges the varied payment environments and use-cases present in contemporary digital economies.

The online variant is designed for transactions executed through internet-connected devices, contingent upon stable network connections and supporting IT infrastructure (Recital 4 of the draft digital euro regulation). The design of this system is intended to align with workflows and conveniences established in prevailing commercial banking and private payment platforms. In contrast, **the offline variant** features a limited set of functions focused on facilitating direct value transfers between individuals in physical proximity, without involving intermediating infrastructure or requiring continuous Internet connectivity (Recitals 58, 69 of the draft digital euro regulation). Its purpose is to provide a "cash-like" experience within the digital landscape, thereby ensuring resilience during instances of network unavailability, safeguarding privacy for low-value transactions, and promoting inclusivity for individuals who have restricted access to the broader online environment (Recitals 5, 6, 16 of the draft digital euro regulation).

The essential role of access to both online and offline digital euro ecosystems is reserved for supervised PSPs, which serve as the primary entry and exit points for end-users (PSPs as defined in Article 4, point (11) of Directive 2015/2366). Entry into either ecosystem, whether through the establishment of an online account or by provisioning an offline device, requires a contractual relationship between the user and a PSP.[5] By design, this relationship is contingent upon the completion of "know your customer" (KYC) procedures [ECB (2025)]. Whether the user chooses an online account - managed and authenticated by their PSP of choice - or opts for the additional provisioning of an offline-capable digital euro device (incorporating secure hardware features), the foundational logic remains consistent: all individuals must successfully undergo rigorous identity verification procedures before being granted access.

The stated goal of requiring strong (digital) identities has direct consequences for the inclusion of underbanked or unbanked individuals, a concern expressly acknowledged in the legislative proposal (Recital 5 of the draft digital euro regulation). While special onboarding mechanisms may be introduced to facilitate access for these groups, the minimum threshold, KYC-compliant onboarding, remains (Recital 29 of the draft digital euro regulation). Any participation in the digital euro ecosystem (whether online or offline) is, therefore, by legislative design, irreversibly linked to the user's verified real-world identity.

Direct access to the online digital euro without intermediaries, analogous to self-custodied wallets in decentralized cryptocurrencies, is not foreseen [ECB (2025)].[6] The offline variant, notwithstanding its infrastructure-light transactional mode, requires that user devices undergo enrollment and, potentially, periodic synchronization via PSP infrastructure,[7] if only to ensure compliance with global account limits and to potentially facilitate risk-based AML/CFT controls whenever the device is connected (Recitals 25, 32 and 33 of the draft digital euro regulation). For funding and defunding operations, transfers between both systems will be permissible (Article 23(2) of the draft digital euro regulation). To bridge the operational gap between these systems, the legislative draft also outlines hybrid transaction models, wherein a single transaction process may be divided between online and offline components (Recital 40 of the draft digital euro regulation on "waterfall" and "reverse waterfall" functionalities).

While much of the technological implementation details of these systems remain to be defined, the two variants are not only technologically dis-

4. Article 9 of the draft digital euro regulation stipulates several important exceptions to the obligation to accept the digital euro, most notably for small businesses, for good faith reasons, for non-business transactions, and pursuant to party agreement.
5. Compare Article 13(6) of the draft digital euro regulation: "[..] users shall only enter into a contractual relationship with [PSPs]. Digital euro users shall not have any contractual relationship with the [ECB] or the national central banks."
6. While not a decentralized means of access, integration into the EDI wallet could render access more transparent and ubiquitous (cf. Article 25 of the draft digital euro regulation).
7. Although the progress report lacks specificity, it suggests a significant capacity for programmability and updateability functionality of the offline devices [ECB (2025)].

tinct but also differ fundamentally in their environmental assumptions and AML/CFT expectations. The online version assumes an omnipresent, robust network environment and can, therefore, support real-time compliance monitoring and transaction screening. In contrast, the offline digital euro's independence from network infrastructure presents unique technical challenges.

The digital euro proposal introduces an "overlay network", a regulatory compliance layer connecting individual PSPs (Recital 25 of the draft digital euro regulation: "[..] by establishing alone or jointly with national central banks a single access point of digital euro user identifiers and the related digital euro holding limits"). This network, which may be directly accessible to regulatory and oversight bodies, is tasked with ensuring that system-wide account and transaction limits are enforced, regardless of the specific infrastructure of individual PSPs or the delineation between online and offline access (Recitals 31 and 34 of the draft digital euro regulation). Although much remains unknown at present, the overlay network could prove instrumental in monitoring aggregated transaction behavior, enforcing global caps - for example, the maximum amount an individual may hold across all accounts - and detecting anomalous usage patterns indicative of illicit finance, though the specific limits and conditions have yet to be determined. While technical standards for this overlay network are still under development, the architectural principle remains clear: compliance is embedded not only at the user onboarding and access layers, but also at the systemic level.

In summary, the approach to the digital euro seeks to reconcile two primary objectives: ensuring a high degree of transactional freedom, privacy, and resilience for end users - particularly in offline contexts - while simultaneously embedding AML/CFT requirements as non-negotiable prerequisites for both entry into, and use of, the digital euro ecosystem.

3. AML/CFT risks

This subsection presents a systematic analysis of the AML/CFT risks and challenges inherent in CBDCs, using both the online and offline versions of the digital euro as examples. The discussion is organized across several key dimensions: (i) KYC procedures and onboarding, (ii) transaction monitoring, (iii) beneficiary and counterparty identification, (iv) record-keeping and auditability, as well as (v) jurisdictional and other legal considerations.

3.1 KYC and onboarding

As outlined, the online digital euro serves as the entry point to the broader digital euro ecosystem. Its issuance and distribution are conducted primarily through existing intermediaries, such as banks and regulated financial institutions, all of which are already subject to established AML/CFT frameworks (Article 4, point (11) of Directive 2015/2366). As a result, the additional KYC risk introduced by the online digital euro into the financial system is largely confined to those existing intermediaries. This model has also been applied by the Bank of England in its Digital Pound project [BoE (2025a)]. These entities maintain primary responsibility for customer onboarding and identity verification, utilizing existing AML/CFT infrastructures and prudential protocols (Recital 79 draft digital euro regulation).

However, significant uncertainty exists regarding access pathways for unbanked and underbanked populations. At present, the mechanisms through which these groups will access the digital euro remain undefined.[8] The absence of clear onboarding processes for this demographic risks the emergence of a parallel, less regulated channel for digital euro acquisition, which could be exploited for illicit financial activity.

In conclusion, although the online digital euro's KYC risks are largely comparable to those present in traditional commercial banking systems, the unresolved onboarding processes for underbanked and unbanked individuals present a material - but not insurmountable - anti-money laundering challenge. Whether process differences and risks will emerge between populations utilizing strong dig-

8. The Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA) and the European Banking Authority (EBA) are tasked to "...issue guidelines specifying the interaction between AML/CFT requirements and the provision of basic digital euro payment services with a particular focus on financial inclusion of vulnerable groups including asylum seekers or beneficiaries of international protection, individuals with no fixed address or third country nationals who are not granted a residence permit but whose expulsion is impossible for legal or factual reasons." (Article 14(5) draft digital euro regulation).

ital identities and those relying on traditional identification methods remains to be seen.

3.2 Transaction monitoring

Turning to transaction monitoring, the online digital euro is expected to replicate traditional banking payment flows. Under the envisioned architecture, transactions pass through regulated intermediaries with full visibility into each transaction. Thus, the risk profile closely mirrors that of existing systems [Sillaber et al. (2024)]. Efforts related to AML/CFT, including transaction screening, pattern recognition, and suspicious activity reporting, will largely remain functionally analogous to current practices. Transactions conducted through the online digital euro will provide compliance teams with granular data points, facilitating the application of analytical tools and thresholds consistent with prevailing banking standards (Recital 65 draft digital euro regulation). Because both the sender and the receiver will be robustly identified, the quality of data available for analysis is expected to surpass that of current systems. The Bank of England also adopts a similar strategy, emphasizing its objectives for interoperability [BoE (2025a)].

In contrast, the offline digital euro presents significant monitoring challenges. Designed for P2P transactions without the involvement of intermediaries, offline digital euro transfers do not generate centralized - or for that matter any - records or allow for validation through regulated entities (Recital 71 draft digital euro regulation). As a result, neither real-time nor retrospective transaction surveillance is possible due to the cryptographic and technological structure powering offline transfers, such as secure devices or wallets capable of independent communication. The detection of illicit transactions is comparable to the risks associated with the use of cash, in which anonymity and the lack of a structured audit trail undermine the effectiveness of law enforcement and compliance efforts.

3.3 Beneficiary and counterparty identification

With respect to beneficiary and counterparty identification, the digital euro benefits from a foundational design principle: account holders must be linked to a robust, verifiable digital identity (Recital 58 draft digital euro regulation). The optional use of the European digital identity (EUDI) wallet has the potential to increase the quality of record-keeping and traceability beyond current standards [E.U. (2024)]. Consequently, the risk of misidentifying counterparties or obscuring payment recipients is reduced, if not eliminated.

By contrast, offline digital euro transactions are conducted on a P2P basis.[9] In the absence of intermediary validation or recipient identification, counterparty risk is analogous to that encountered with conventional currency. Tracing recipients or confirming their legitimacy remains virtually impossible using standard compliance tools. Consequently, beneficiary risks in offline scenarios are comparable to those associated with cash.

3.4 Record keeping and auditability

From a record-keeping and auditability perspective, the contrast between the two variants is pronounced. The online digital euro, linked to digital identities and intermediated transaction flows, inherently generates comprehensive records of transaction histories.[10] This connection greatly facilitates audit trails, compliance verification, and forensic investigation, as digital footprints are readily available for regulatory examination. The design contemplates the capacity to maintain immutable, tamper-evident ledgers, thereby supporting enhanced auditability and accountability [FIU (2023)].

By contrast, the offline digital euro does not incorporate any record-keeping or data retention features within P2P transfers (Recitals 34 and 35 of the draft digital euro regulation). Transactions in this environment are, in effect, private and transient exchanges between end-users. The absence of record retention significantly impairs retrospective auditability and complicates the enforcement of AML/CFT requirements. Without centralized or decentralized logs, compliance becomes reliant on downstream detection, often occurring only when transactions are converted back into the regulated financial system, thereby introducing potentially significant delays and enforcement blind spots.

9. This may not apply to transactions exceeding certain thresholds, where the infrastructure automatically divides the transaction into online and offline components ("waterfall").
10. See Annexes II through V of the draft digital euro regulation regarding the data that the ECB, PSPs, and Support Service Providers may collect.

3.5 Jurisdictional and other legal considerations

While broader jurisdictional and legal issues extend beyond the scope of this analysis, a significant benefit of the digital euro in the context of AML/CFT laundering is instantaneous settlement (Recital 64 of the draft digital euro regulation). The design enables immediate finality of transactions, in stark contrast to otherwise multi-day settlement cycles. This immediacy significantly reduces counterparty settlement risk, thereby indirectly supporting AML/CFT regimes by enhancing transactional certainty, minimizing avenues for fraud, and constraining opportunities for layering or complex structuring schemes intended to obscure illicit provenance [FIU (2023)].

Additionally, the digital euro's cross-border interoperability and the integration in divergent legal and technical systems remain unresolved challenges [FIU (2023)]. Potential fragmentation could hinder AML/CFT efforts by enabling regulatory arbitrage and creating inconsistencies in the application of identification and monitoring standards. If left unaddressed, such jurisdictional heterogeneity risks undermining the coherence and effectiveness of AML/CFT controls that are critical to digital currency systems.

3.6 Summary

The AML/CFT risks inherent in the digital euro differ substantially between its online and offline forms. The online version allows for the adoption of existing KYC and transaction monitoring frameworks, bolstered by enhanced digital identity integration and comprehensive recordkeeping, thereby providing a more robust foundation compared to legacy bearer and banking instruments. In contrast, the offline digital euro raises classic challenges associated with cash-like anonymity and transactional opacity, further complicated by the absence of oversight and recordkeeping. Systemic considerations help mitigate these risks, as settlement finality and technological robustness contribute positively to AML/CFT controls. However, the unresolved question of access for unbanked and underbanked populations presents a potential vulnerability that requires further examination to prevent the emergence of blind spots in AML/CFT compliance.

4. Regulatory balancing and AML/CFT measures

The effective implementation of AML/CFT is a stated design goal of the digital euro (Recital 78 of the draft digital euro regulation). The draft regulation attempts to balance robust AML/CFT controls with the preservation of user privacy.[11] It delegates to the EBA and the AMLA the critical task of formulating guidelines to define the relationship between AML/CFT obligations and inclusive access to basic digital euro payment services (Article 14(5) draft digital euro regulation). This governance arrangement seeks to harmonize regulatory oversight across Member States while ensuring access, particularly for unbanked and underbanked populations (Article 14(5) draft digital euro regulation).

The draft regulation's approach is explicitly risk-based, reflecting the organizing principles of the E.U.'s AML framework. Notably, it expressly precludes full anonymity - an alignment with the Commission's comprehensive AML/CFT package [E.U. (2024b)]. Simultaneously, it innovates by suggesting heightened privacy for offline, cash-like digital euro payments, while subjecting online transactions to the same data protection, privacy, and AML/CFT requirements that govern private digital instruments.

The analysis of the preceding section has highlighted several technical and operational challenges that may complicate AML/CFT compliance, notably P2P transfers and onboarding processes designed to accommodate users outside traditional banking channels. The discussion that follows will address the issues along the already introduced axes of (i) KYC and onboarding, (ii) transaction monitoring, (iii) beneficiary and counterparty identification, (iv) recordkeeping and auditability, and (v) jurisdictional and ancillary legal considerations.

4.1 KYC and onboarding

AMLA, established in July 2025 as a central supervisory actor (Recital 86 AMLA regulation), is charged with developing guidance on KYC requirements and rules for onboarding to the digital euro. Notwithstanding the absence of finalized guidance on

11. See "Stakeholder consultations" of the draft digital euro regulation: "Privacy was considered the most important feature of a digital euro by both citizens and professionals participating in the consultation" [Brunnermeier and Landau (2022)].

onboarding (see, for example, the open regulatory questions reflected in Article 14 of the digital euro proposal), emerging publications and the draft digital euro regulation advocate for the application of risk-based measures to KYC and onboarding procedures.

The digital euro ecosystem is planned with the rollout of the European Digital Identity and its wallet (EUDI Wallet) in mind [E.C. (2021)]. Under the proposed regulatory regime, PSPs are required to accept the EUDI Wallet for customer identity verification, encompassing both new and existing customers (Recital 58 draft digital euro regulation). The wallet will facilitate access to digital identity attestations and enable remote customer due diligence (Article 25(1) draft digital euro regulation). Notably, this identity solution is anticipated not only for remote onboarding but also to extend to all payment devices in retail contexts (Article 25(2) draft digital euro regulation).

Crucially, the draft regulation highlights an explicit distinction between privacy interests and supervisory obligations by providing that users' identities remain with the PSPs (Article 34 draft digital euro regulation). Both the ECB and PSPs are required to implement "state-of-the-art technical and organizational safeguards" to shield user identities from access by the ECB at the front-end level, thereby seeking to reconcile privacy-by-design imperatives with AML/CFT objectives (Article 32 draft digital euro regulation).

As a logical consequence, in instances where an online euro wallet is linked to payment accounts at other PSPs, those providers assume the status of joint data controllers, thereby bearing heightened obligations under the General Data Protection Regulation (Article 26 GDPR "Joint controllers").

For the envisaged offline variant of the digital euro, the efficacy of AML/CFT laundering controls is primarily derivative of the online onboarding process. Offline wallets are based on digital identity attestations previously validated in an online environment, implying a necessary, albeit indirect, dependency on robust online onboarding and verification practices (Recital 69 of the draft digital euro regulation). The integration of risk-based KYC procedures thus extends de-facto into the offline sphere, although the technical implementation of offline KYC surveillance is limited to core safeguards relying on trusted hardware.

4.2 Transaction monitoring

Transaction monitoring regimes for CBDCs frequently aim to strike a careful balance between the objectives of preventing illicit finance and respecting data minimization and privacy principles [ECB (2025)]. Transaction monitoring, continuous assessment for suspicious activities, predicate offenses, and sanctions screening are core expectations, drawing directly from established best practices within the traditional payments ecosystem.

The digital euro's online variant will be, by design and necessity, congruent with existing payment rails regarding transaction monitoring surveillance. Full transaction monitoring, leveraging artificial intelligence/machine learning (AI/ML) based systems and network analytics, will be facilitated by persistent ledger connectivity, enabling advanced pattern recognition, real-time flagging of suspicious activities, and extensive checking against EU/OFAC sanctions [FIU (2023)]. Article 32 of the proposal envisions a centralized (potentially federated) transaction monitoring mechanism (Article 32 draft digital euro regulation: "General fraud detection and prevention mechanism"), operated either by the ECB or designated support service providers, to assess real-time fraud risks and provide post-settlement detection support to PSPs. Importantly, while the detection mechanisms are expected to leverage identifiers such as unique account numbers and session metadata (e.g., IP address ranges), Article 32(6) imposes explicit privacy requirements, precluding direct user identification by support service providers: "The providers of support services will be subject to contractual safeguards that prevent the linking or onward transmission of any personal data that can only be processed for specific purposes, and when strictly necessary" [ECB (2025)]. Furthermore, for the enforcement of holding limits and exceptions in emergencies, Recital 77 foresees the establishment of a single access point for user identifiers and holding limits. The regulation frequently emphasizes that this must respect the GDPR's mandates for data minimization and security by design, possibly incorporating decentralized storage to mitigate data breach risks. Upon request from a competent authority (FIU), PSPs must furnish collected data to support AML/CFT investigations (Article 37).

Distinctly, the digital euro's offline mode intentionally mirrors certain privacy attributes of cash (Recital 71 digital euro proposal). The disconnected operation of the offline wallet precludes imme-

diate transaction-level monitoring; data retention is expressly forbidden for offline transaction flows (Article 37(2)), except for PSPs' record-keeping related to funding and defunding events, in accordance with Article 40 of Directive (EU) 2015/849. To mitigate resulting risks, the regulation authorizes the European Commission to impose transaction and holding limits on offline balances (Article 37(5)), a risk-based tradeoff justified by the limited exposure at stake [Brunnermeier and Landau (2022)]. Furthermore, periodic synchronization, for updating balances and monitoring compliance with limits, may supplement supervisory mechanisms without undermining privacy.

4.3 Beneficiary and counterparty identification

Beneficiary and counterparty identification represent foundational concerns in AML/CFT compliance frameworks. Effective identification is central to robust transaction monitoring, profiling, and the prevention of illicit financial flows.

The digital online euro aligns with the trend of traditionally account-based systems[12] by requiring strong, verifiable (digital) identity linkage for all account holders. In particular, the standardized user identifier and user alias association improves the quality and granularity of record-keeping, offering regulators and intermediaries deterministic identification of both counterparties and beneficiaries in electronic transactions. As a result, the risks of misattributing transaction parties, creating false identities, and obscuring payments are expected to be significantly reduced; though it remains to be seen how the creation of aliases will be harmonized and practically implemented in practice. PSPs can leverage these identity guarantees to develop high-integrity profiles for both payers and payees.

Conversely, digital offline euro transactions, which occur through P2P exchanges in close physical proximity (e.g., near field communication (NFC) based device-to-device transactions), recreate the practical anonymity of cash. During offline transfers, no personal or transactional data are exchanged or monitored, and counterparty identification is neither feasible nor required (Recital 75 draft digital euro regulation). PSPs handle personal data only when digital euros are moved between online digital euro payment accounts and local storage devices, similar to personal data processing associated with ATM cash withdrawals.

Thus, while digital online euros advance AML/CFT objectives through robust identity binding, offline functionalities require an adaptation of existing risk-based AML frameworks to address the persistence of anonymity similar to that of physical currency [Lemke (2024)]. To mitigate the risks previously described, the Regulation authorizes the European Commission to impose transaction and holding limits on offline balances (Article 37(5)), a risk-based tradeoff again justified by the limited exposure at stake. Additionally, periodic synchronization, intended for updating balances and monitoring compliance with caps, may enhance supervisory mechanisms without compromising privacy.

4.4 Record keeping and auditability

AML compliance for CBDCs hinges on robust mechanisms for record-keeping and auditability, which facilitate both real-time monitoring and ex-post investigation.

As outlined, the digital euro draft proposal envisions robust digital identifiers as foundational to both its online and offline variants. Central to this framework are "user identifiers", unique pseudonymous strings assigned to clearly distinguish each user in online transactions (Article 2(27)), and "user aliases", which provide an additional layer of pseudonymity to protect user identities, visible only to PSPs and the users themselves (Article 2(28)). The regulatory structure mandates that audit trails must, at a minimum, include these identifiers along with transactional metadata and session details, such as IP address ranges.

PSPs processing online transfers, therefore, maintain detailed transactional records. Under the proposed regulations, each transaction generates immutable, tamper-evident records that are closely associated with user identifiers or their aliases. These logs, which document account numbers, timestamps, and session metadata, are designed to fulfill strict privacy-by-design requirements, preventing identification of users by any party other than the responsible PSP, explicitly excluding the ECB and national banks (Recital 71 draft digital euro regulation).

12. Not to be confused with the question of whether transactions themselves are account-based or value-based at the technical level [Armelius et al. (2021), Brunnermeier and Landau (2022)].

From an AML/CFT perspective, this architecture enables granular auditability: it supports compliance verification, suspicious activity reporting, and forensic investigations, thanks to the ready accessibility and integrity of the records. Nevertheless, ensuring interoperability with legacy financial audit systems will likely remain a significant priority [Lemke (2024)].

In contrast, the P2P nature of the offline digital euro is intentionally designed without detailed record-keeping. Transactions in this mode are ephemeral: no persistent audit logs or user linkages are maintained on the device or card during transfers, in line with privacy-enhancing protocols [Armelius et al. (2021)]. For AML/CFT efforts, this design introduces significant auditability gaps, as transactional data is absent - with the exception of balance information - until a wallet synchronizes with a PSP or the central system (for example, during recharging or conversion of funds). Legal obligations for PSPs arise at the moment of synchronization, when balances must be verified against minimum audit trail requirements. While this process partially addresses audit blind spots, delays and technical contingencies (such as device loss or theft) remain unresolved risks for continuous AML compliance.

4.5 Jurisdictional and other legal considerations

As previously discussed, AML/CFT compliance in the context of cross-jurisdictional CBDC operations is dominated by the need to ensure that digital currencies do not become vectors for illicit finance across borders [FIU (2023)]. AML regimes for CBDC systems reflect a movement toward centralized oversight, with the proposed establishment of the AMLA as the central supervisory and coordinating authority. AMLA's federated operational approach aims to harmonize supervision, impose uniform sanctions, and centralize information flows across PSPs and intermediaries facilitating or processing CBDC transactions, especially where cross-border operations are involved.

For the online digital euro, stringent AML compliance obligations are imposed on PSPs, and intermediaries, regardless of the cross-border nature of transactions.[13] Distribution of the system to third-country persons is contingent on a formal agreement of their countries with the E.U., as set forth in Article 19 of the digital euro proposal [FIU (2023)]. Such agreements require third-country national banks and competent authorities to abide by ECB rules, disclose relevant usage information, and adopt regulatory standards that are materially equivalent to those in the Union, particularly regarding AML obligations (Article 10 draft digital euro regulation). Failure to maintain equivalency or to address strategic AML deficiencies can result in the suspension or termination of access, with the ECB exercising oversight on foreign PSP compliance (Article 20 draft digital euro regulation).

Offline functionality, while technically distinct, does not circumvent AML requirements in cross-border settings. Offline devices physically moved to third countries distributing offline digital euro must also uphold ECB-imposed limits and adhere to substantive AML controls, as stipulated in Article 19(5).[14] The legal framework is designed to allow restriction, suspension, or termination of third-country participation in cases of inadequate AML frameworks, grounding operational risk mitigation in binding intergovernmental agreements and enforceable regulatory standards.[15]

4.6 Summary

In summary, the digital euro presents differentiated responses to AML/CFT risks depending on its mode of use. The online variant essentially builds upon and enhances existing KYC and transaction monitoring frameworks, with the digital E.U. identity wallet expected to significantly improve data quality and accessibility for AML compliance. In contrast, the offline variant requires an explicit policy decision: permitting full transactional anonymity, albeit limited by transaction and holding caps, which entails accepting a residual level of AML risk. This tiered approach represents carefully calibrated trade-offs between AML safeguards and user privacy, aligning legal compliance with the realities of practical implementation.

13. Access to foreign nationals, however, is possible, as Article 13 of the draft digital euro regulation explicitly allows visitors to the E.U. to onboard.
14. Recital 47 of the draft digital euro regulation emphasizes the objective of aligning with the G20 agenda concerning cross-border payments and remittances.
15. It remains to be seen whether blacklisting will be possible (and effective) for foreign nationals' devices, especially if those devices do not, or may never, reconnect to the online environment.

5. Conclusion

A closer examination of the complex AML/CFT challenges and opportunities arising from the ongoing development and anticipated deployment of CBDCs, particularly with regard to the digital euro, reveals an interesting balancing act. The analysis reveals that the AML/CFT framework for the digital euro is inherently bifurcated, reflecting not only legacy compliance models but also novel privacy considerations and risk-based trade-offs. The online variant emphasizes well-established KYC procedures, continuous transaction monitoring, and integration with digital identity infrastructure: features that are likely to surpass the surveillance and traceability capabilities of traditional banking or physical cash. This approach, overseen by the recently created AMLA, may represent a watershed moment for the effectiveness of AML/CFT measures by leveraging high-quality, real-time data and robust audit trails.

Nevertheless, the digital euro carries significant operational and systemic risks. Real-time settlement centralized at the ECB or designated intermediaries introduces new centralization risks and the possibility of operational single points of failure. By contrast, the offline functionality, designed to mimic the privacy and immediacy of cash, relies on restrictive transaction limits as its primary AML safeguard. Calibrating these limits involves significant systemic repercussions: if set too low, they may undermine the public's ability to access resilient offline liquidity during crises, potentially encouraging capital flight or substitution with physical cash or alternative emerging stablecoin alternatives [Lagarde and Panetta (2022)].

In light of these findings, the importance of robust and adaptive AML frameworks in the context of the digital euro cannot be overstated. AML/CFT policies must do more than merely extend existing standards; they must address the paradigm shifts brought about by programmable and data-rich digital money. Innovations in AML, including machine learning-based anomaly detection, privacy-preserving analytics (e.g., enabled by zero-knowledge proofs), and dynamic risk scoring, should be prioritized for pilot implementation, supported by rigorous transparency and oversight arrangements. Policy developments must anticipate and specifically regulate technological and operational barriers to AML/CFT compliance, such as cross-jurisdictional data fragmentation, identity portability, and resistance to surveillance from both public and private actors. Legal and ethical considerations require renewed focus on proportionality, necessity, and accountability as core principles, to ensure that AML/CFT measures do not become overreaching, erode civil liberties, or exacerbate financial exclusion.

The trajectory of CBDC adoption suggests that public perception and stakeholder resistance will continue to evolve partially in response to the perceived trade-offs between privacy and transparency. Ultimately, the AML/CFT framework for the digital euro will serve as a bellwether for broader regulatory and technological adaptation within the E.U. Policymakers must ensure that AML objectives are neither compromised in the name of innovation nor used as tools to undermine fundamental rights and economic inclusion.

References

Aldasoro, I., M. Aquilina, U. Lewrick, and S. H. Lim, 2025, "Stablecoin growth – policy challenges and approaches," Bank for International Settlements, https://tinyurl.com/yc52ka2j

Armelius, H., C. A. Claussen, and I. Hull, 2021, "On the possibility of a cash-like CBDC," Sveriges Riksbank

Auer, R., G. Cornelli, and J. Frost, 2023, "Rise of the central bank digital currencies," International Journal of Central Banking 19, 185-214

Bank of Japan, 2025, "Central bank digital currency experiments progress on the pilot program (May 2025)," Payment and Settlement Systems Department Bank of Japan

Bidder, R., T. Jackson, and M. Rottner, Matthias, 2025, "CBDC and banks: disintermediating fast and slow," BIS working papers no. 1280, Bank for International Settlements

BoE, 2025a, "Product Strategy," Bank of England, https://tinyurl.com/stdhf75d

BoE, 2025b, "Interoperability models for UK based payments," Bank of England, https://tinyurl.com/5n869hwu

Bidder, R., T. Jackson, and M. Rottner, 2025, "CBDC and banks: disintermediating fast and slow," Bank for International Settlements

Brunnermeier, M. K. and J.-P. Landau, 2022, "The digital euro: policy implications and perspectives," European Parliament

E.C., 2021, "Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity," June 3, European Commission

E.C., 2023a, "Proposal for a Regulation of the European Parliament and of the Council on the legal tender of euro banknotes and coins, COM/2023/364 final," European Commission, June 28

E.C., 2023b, "Proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro, COM(2023) 369 final," European Commission, June 28 (cited as: Digital Euro Proposal)

ECB, 2021, "Report on the public consultation on a digital euro," European Central Bank

ECB, 2024, "Study on the payment attitudes of consumers in the euro area (SPACE)," European Central Bank

ECB, 2025, "Progress on the preparation phase of a digital euro: third progress report," European Central Bank

E.U., 2024a, "Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro (Text with EEA relevance)," European Union, March 19

E.U., 2024b, "Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance)," European Union, June 19

FIU, 2023, "The AML/CFT implications of central bank digital currency and the digital euro," Financial Intelligence Unit of Latvia

Jenko, M., 2025, "Interview with Piero Cipollone," conducted by Miha Jenko on July 10, 2025

Lagarde, C., and F. Panetta, 2022, "Key objectives of the digital euro," The ECB blog, 13/2022

Lemke, C., 2024, "Function follows form or form follows function – the legal nature of CBDC," European Property Law Journal 12:2-3, 211-279

Panette, F., 2023, "Shaping Europe's digital future: the path towards a digital euro," speech to the Committee on Economic and Monetary Affairs of the European Parliament, September 4, 2023, available at https://tinyurl.com/3d4ub76d

Reserve Bank of India, 2025, "Report of the Central Board of Directors on the working of the Reserve Bank of India for the year ended March 31, 2025," Reserve Bank of India.

Sillaber, C., and M. Eggen, 2024, "Privacy in payments: what a CBDC can do better than commercial bank money," https://tinyurl.com/4h4hbpsr

WE MAKE THINGS HAPPEN.

Leading change in Financial Services.

BELGIUM
UNITED KINGDOM
THE NETHERLANDS
FRANCE
GERMANY
SWITZERLAND

www.projectivegroup.com

Projective INSTITUTE