

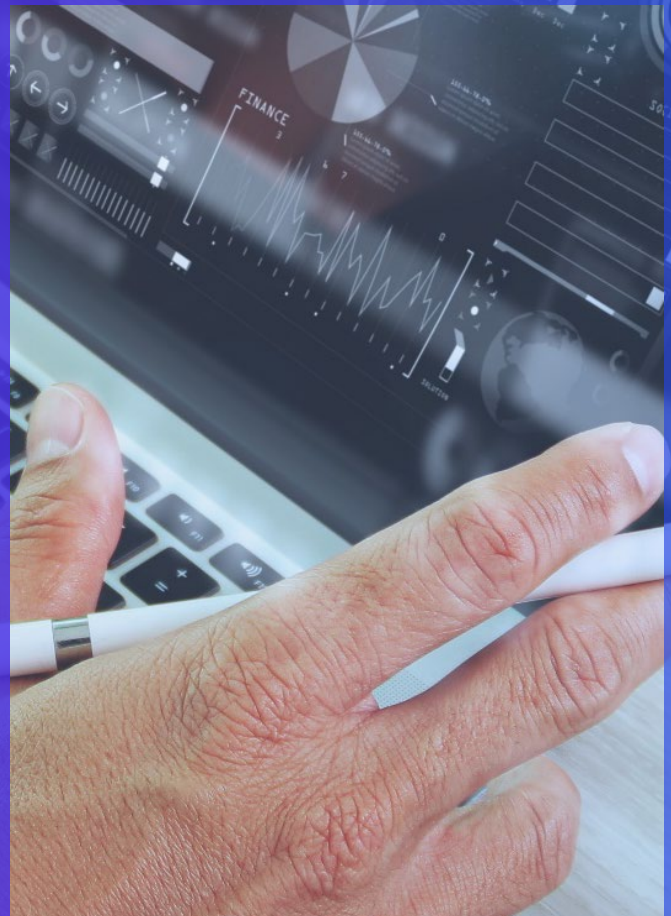


Mind the Fraud Gap:

Modernizing Fraud Prevention and Detection for the era of SEPA Instant Payments

Specialised White Paper

November 2025



KPMG in Ireland

Contents

01 **SEPA IP: A New Compliance Challenge**

02 **The Impact of Real-Time Payments**

03 **Modernizing Payment Fraud Prevention**

04 **Deep-Dive: AI In Action**

05 **From Readiness to Resilience**

06 **Contact us**



SEPA IP: A New Compliance Challenge

The Single Euro Payments Area (SEPA) Instant Payments Regulation (Regulation (EU) 2024/886) (IPR) entered into force on 8 April 2024. Established by the European Payments Council, the mandatory SEPA Instant Payments scheme aims to enhance the adoption, efficiency, speed, and accessibility of instant payments (IP), following the initial optional scheme that was launched in 2017, which resulted in poor adoption and execution success.

The IPR requirements are rolled out on a phased basis across the EEA, commencing in January 2025, with full compliance expected by July 2027.

CI: Credit Institution / Banks;
PI: Payment Institution;
EMI: E-money Institutions



Figure 1. Timeline for IPR implementation. From SEPA Instant Payments: Transforming the European Payments Landscape, KPMG 2024.

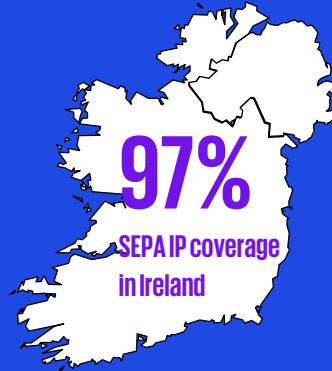


Figure 2. SEPA Instant Payment coverage in Ireland.

SEPA IP Coverage

Since January 2025, Ireland has seen a major shift in SEPA IP coverage among institutions. Ireland now leads in the EU with 97% coverage among scheme participants compared to 91% across the EU.

While Credit institutions in the Eurozone had to already adapt their operations to the new IPR requirements, Payment Institutions, E-Money Institutions in the Eurozone as well as institutions outside the Eurozone still have a long journey ahead. The main challenges to be overcome by institutions include:

1. Upgrading IT Infrastructure and Monitoring systems, to support real-time processing and settlement of transactions.

- 24/7 system availability
- Individual transaction process within 10 seconds (no longer batch process)
- No room for error with direct impact on customer experience and failure of systems leading to reputational risks
- Real-time (instant) fraud monitoring systems
- Proactive fraud risk management, requiring integration of advanced fraud prevention tools and robust customer due diligence measures

2. Reviewing Liquidity Management, driven by the move from limited fund settlement operating hours under Target 2 to the future requirement to avail of 24/7 settlement for IP in TIPS or RT1 systems.

The European Payments Council (EPC) has unveiled the 2025 version of the SEPA Instant Credit Transfer (SCT Inst) Rulebook, with key updated requirements which went live on October 5, 2025.

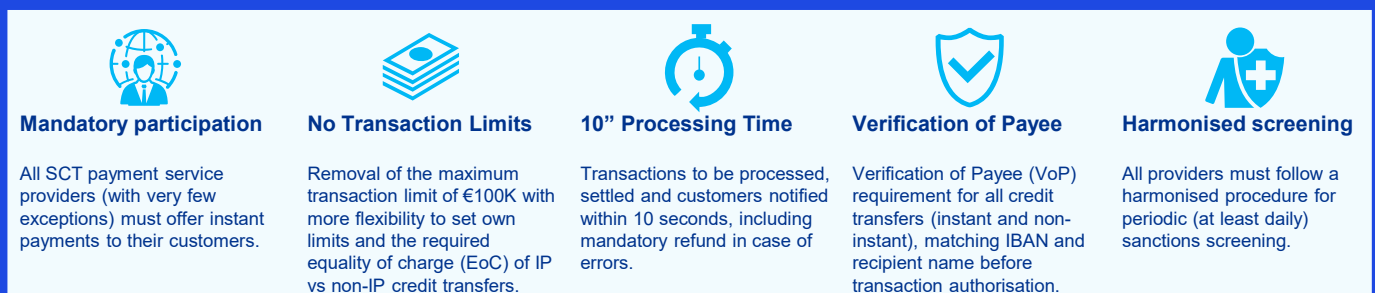


Figure 3. Key requirements for financial institutions addressed in the SEPA Instant Credit Transfer Rulebook.

The Impact of Real-Time Payments

The implementation of the SEPA Instant Payments Regulation (IPR) represents a seismic shift in the European payment ecosystem. While this regulation promises positive outcome for customers in the form of enhanced speed of transactions, greater accessibility, and market competitiveness, it also introduces new risks, specifically in the area of payments fraud. Institutions that fail to act proactively and decisively by increasing their fraud prevention efforts will be faced with the risk of increasing fraud losses, due to the irrevocable nature of instant payments.

The Fraud Loss Formula

The fraud loss formula offers a structured approach for financial institutions to assess the true impact of the IPR. The formula expresses total financial fraud losses as the sum of bank and customer losses, offset by fraud prevented and recouped value.

Assuming IP do not change the volume of transactions, bank losses as a result of unauthorized payment fraud (e.g. due to weak security systems) are likely to remain stable at current levels. However, changes in regulations may require banks to reimburse customers for additional losses not yet covered under the current framework. The recent introduction of the failure to prevent fraud offence in the UK has broad applications for institutions in Ireland. Furthermore, the EU has proposed similar, though more limited, rules that would require reimbursement for impersonation fraud (a type of APP fraud). These initiatives will drive an increase in bank losses in the medium term. In countries where IP have seen widespread adoption, in-app scams leading to authorized push payment (APP) fraud have spiked, leading to an increase in customer losses.

With transactions processed in less than 10 seconds, the window for fraud detection and intervention is significantly shortened, reducing fraud prevented value unless action is taken to upgrade systems and processes. The instant nature of transactions allows funds to be quickly moved onwards, from the receiving institution to a third party, making tracing and recovery more cumbersome. This could essentially reduce recouped value (close) to zero.

Bank Loss:

Direct financial losses absorbed by the institution. This includes liability for unauthorised payment fraud losses due to weak security systems.

Customer Loss:

Financial loss incurred by the customer, for which the institution is not liable. Losses often result from authorised push payment (APP) scams.

Fraud Prevented Value:

The estimated value of fraudulent transactions successfully blocked before completion, typically through real-time detection and intervention.

Recouped Value:

The value of fraud-related funds successfully recovered post execution of the transaction.

$$\text{Net Fraud Loss} = \text{Bank Loss} + \text{Customer Loss} - \text{Fraud Prevented Value} - \text{Recouped Value}$$

Impact under IPR:



Figure 4. The fraud loss formula and impacts under SEPA Instant payments regulation in the European market.

Customer Impacts

Potential negative customer outcomes are intrinsically linked to the customer experience and the heightened potential for fraud under IPR.

With payments processed in seconds and often irreversible, customers are more vulnerable to fraudulent scams stemming from social engineering tactics.

The rapid evolution and ease of access to generative AI has further intensified this threat. The impact of IPR, when institutions do not appropriately strengthen their fraud prevention measures, not only causes direct monetary harm but also erodes trust and diminishes the overall customer experience.

Operational Impacts

Operational impacts under IPR arise as banks must identify and block fraudulent transactions within seconds.

This demands high-performing fraud detection systems that operate 24/7, increasing operational complexity and cost.

Integrating legacy core banking systems with modern real-time payment engines, Verification of Payee (VoP) tools, and AI powered detection algorithms introduces architectural complexity and increases the likelihood of integration failures or bottlenecks.

Regulatory Impacts

Under the new IPR, regulatory impacts can be substantial and multifaceted.

Financial institutions that fail to meet key implementation milestones face not only financial penalties but also heightened regulatory scrutiny and reputational exposure. A single failure to detect a sanctioned entity in a live transaction could result in severe penalties, regulatory action, and long-term damage to institutional credibility.

In a payments ecosystem where speed, transparency, and trust are paramount, regulatory missteps are not just operational setbacks, they are strategic liabilities.

Modernizing Anti-Fraud Programs

While the implementation of SEPA Instant Payments introduces a range of risks in relation to payment fraud, it also generates opportunities for financial institutions to bridge gaps in their fraud prevention frameworks by acting proactively to modernise and strengthen their existing capabilities across several key areas. By focusing on each of these, institutions can better balance the fraud loss formula and increase fraud prevented value.

Customer Focus

Customer education

Well-informed customers are essential to preventing scams before money ever leaves their accounts. Increasing awareness through campaigns, case studies, proactive messaging, and app notifications empowers individuals to recognize and avoid scams, stopping fraud attempts before they succeed.

Friendly Friction

Introducing dynamic, risk-based interventions such as prompts, short delays, and layered authentication tools can stop fraudulent transactions before funds are irretrievably transferred, while maintaining a smooth customer experience. The key challenge is balancing strong security with seamless usability.

Operations Focus

Employee Education

In the context of IP, where transactions are processed in seconds and are generally irreversible, well-trained staff serve as the first and most effective line of defence against fraudsters. Structured training programs, scam typologies, and strong soft skills can significantly improve detection and response, reduce fraud losses and protect customer trust.

Customer Profiling & Behavioural Analytics

Instant payments demand accurate customer profiles and advanced behavioural analytics to detect and stop fraud in real-time. Traditional, post-transaction reviews will no longer be sufficient to prevent losses and minimize financial impacts.

Real-Time Anomaly Detection

Next to behavioural analytics, continuous real-time anomaly detection will become essential to detect fraud in IP. Only immediate identification and intervention can prevent fraudulent transactions. The complexity lies in deploying advanced models that maintain low latency and high accuracy in real time.

Intelligence Sharing

Collaborating with a wide network of banks, telecommunication providers, social media platforms, and regulators to establish real-time intelligence sharing across institutions will become vital as coordinated fraud attacks can spread even more rapidly with real-time payments.

The Role of AI

Similar to almost all other areas of business, (agentic) AI is starting to rapidly become a cornerstone of effective fraud prevention, especially in the era of instant payments. The focus on customers and operations can be underpinned by AI to empower financial institutions to respond to new threats with greater speed, accuracy, and adaptability. Leveraging AI in these domains not only strengthens defences against sophisticated fraud tactics but also supports regulatory compliance, operational efficiency, and customer trust. In doing so, it allows to an institution transform its fraud prevention approach from reactive to proactive and future-proof its operations.

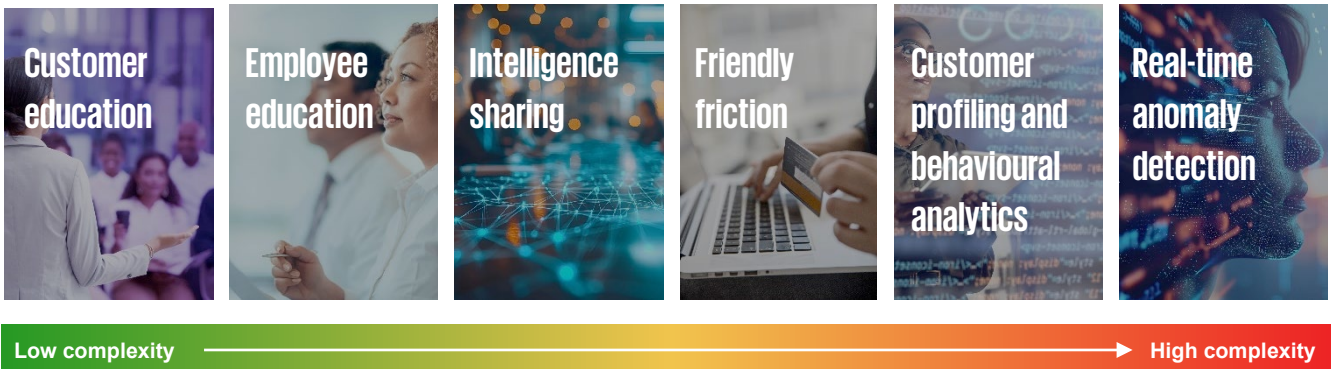


Figure 5. Opportunity areas for payments fraud prevention under IPR, order from low to high technical complexity

Deep-Dive: AI In Action

AI in Payment Fraud Prevention

The customer benefits from AI-driven fraud prevention through enhanced protection, reduced false positives, and a safer, more seamless banking experience.



Customers

AI supporting both customers and institution to detect and prevent payments fraud



AI

AI helps banks reduce fraud losses, cut operational costs, and respond to threats faster. It improves customer trust by enhancing security and enables smarter risk management through continuous learning and real-time detection.



Operations

Agentic AI to support AML and fraud prevention teams

AI for customer/employee education

Real-time anomaly detection

Customer profiling and behavioural analytics

AI-Driven Identity Security Controls

Adversarial AI

Figure 6. AI enhances fraud prevention by directly protecting customers and augmenting traditional anti-fraud systems within institutions.

Real-Time Anomaly Detection

Unlike traditional rule-based monitoring, deep learning architectures can ingest vast volumes of transaction data and autonomously learn complex, non-linear patterns. This enables dynamic risk scoring and continuous monitoring of payment flows, safeguarding instant payments with limited manual intervention. These models deliver low-latency, high-accuracy fraud detection.

Agentic AI

Agentic AI is transforming AML and fraud prevention by automating investigations, case management, and workflow orchestration. Beyond reducing manual effort, it enables faster intelligence sharing and integration of real-time anomaly detection into operational workflows. By handling routine and repetitive tasks it frees analysts to focus on complex decision-making and high-risk cases.

Profiling & Behavioural Analytics

AI can help institutions predict customer behaviour by analysing transaction patterns, device usage, and channel preferences to build behavioural baselines. Using supervised machine learning, real-time monitoring of login habits and transaction velocity detects anomalies that may indicate fraud. When risks arise, AI triggers interventions like short delays or layered authentication, adding “friendly friction” to block fraud while preserving a smooth experience.

AI-Driven Identity Security

AI-powered Identity Verification and adaptive Strong Customer Authentication (SCA) strengthens digital transaction security by detecting forged IDs, synthetic identities, and deepfake attempts. It enables dynamic, risk-based authentication, adjusting requirements in real time based on behavioural anomalies, geolocation, and device recognition, reducing fraud while maintaining a seamless customer experience.

Adversarial AI

Adversarial AI strengthens fraud defences by simulating attack scenarios and probing system vulnerabilities. This approach is critical for stress-testing real-time risk scoring models, VoP mechanisms, and adaptive transaction limits before deployment. By mimicking sophisticated fraud patterns, adversarial testing ensures that behavioural analytics and machine learning detection systems remain resilient against evolving threats.

AI for Customer/Employee Education

AI-driven education tools, such as interactive chatbots, adaptive learning modules, and behaviour-based alerts, can deliver personalized, real-time learning experiences for both customers and employees. For customers, this means proactive messaging and app notifications that empower individuals to recognize scams before they occur. For employees, AI supports structured training programs that stay relevant as fraud tactics evolve, improving frontline detection and response while reducing operational burden.

From Readiness to Resilience

SEPA Instant Payments has caused a pivotal shift in the European payments landscape, one that demands financial institutions to significantly innovate and modernize their payments accounts, services and infrastructure. With real-time payments settling in under 10 seconds and operating 24/7/365, traditional fraud detection methods are no longer sufficient and institutions must radically modernize their approach to payment fraud prevention in order to avoid increased fraud losses and maintain customer trust. To move from basic readiness to true resilience, financial institutions must identify existing and potential future weakness in their fraud detection and prevention frameworks and integrate these insights into a cohesive strategy: proactively strengthening fraud controls, leveraging data and (gen)AI, and embedding agility into their processes. This should go beyond just meeting regulatory requirements, and also focus on building robust fraud defences that protect customers and sustain trust in a fast-moving payments environment.

How KPMG can help

With over 150 years of experience in financial services, broad industry insights, and deep data & technology and regulatory expertise, KPMG is uniquely positioned to help financial institutions bridge gaps in their anti-fraud frameworks, specifically in response to the increased risks and regulatory demands introduced by the SEPA Instant Payments Regulation. Our approach is focused on protecting institutions and their customers from the heightened vulnerability while ensuring regulatory compliance and maintaining a positive customer experience.



Health Check

A rapid, structured review of your current capabilities, controls, data, and operating model across the payment journey, benchmarked against regulatory requirements and peer organizations to ensure a comprehensive view of your strengths and vulnerabilities.

The outcome is a clear list of gaps, recommendations, and a high-level roadmap for remediation, giving you the clarity and direction needed to move beyond basic compliance and lay the foundation for sustainable and resilient fraud prevention.



Control Design

Building on the results from our Health Check, we will work with you to design and implement robust, future-ready controls tailored to your risk profile and business needs, and to implement a solid robust framework to proactively manage fraud.

Our approach leverages advanced data enrichment and AI-driven solutions to maximize effectiveness and ensure regulatory alignment, helping you achieve both compliance and a consistently safe and seamless customer experience.



Deliver with AI

Our experts can support you transforming your existing IT landscape into an intelligent, scalable fraud prevention architecture, powered by AI. Our Trusted AI team will ensure that your solutions are ethical, secure and compliant.

By prioritizing customer protection and operational agility, we help you move from readiness to resilience, empowering your organization to thrive in the era of real-time payments while maintaining public trust and regulatory confidence.

Contact us



Owen Lewis

Partner,
Head of AI & Velocity and
Banking & Capital Markets
E: owen.lewis@kpmg.ie



Ian Nelson

Partner,
Head of Financial Services
and Regulatory
E: ian.nelson@kpmg.ie



Rory Timlin

Partner,
Technology Consulting
E: rory.timlin@kpmg.ie



Niamh Lambe

Managing Director,
Head of Financial Crime
E: niamh.lambe@kpmg.ie



Niclas-Andreas Mueller

Director, Risk Consulting and
KPMG AMLA Office Liaison
E: niclas-andreas.mueller@kpmg.ie



Harshal Suthar

Associate Director,
Management Consulting
E: harshal.suthar@kpmg.ie



Tony Smith

Associate Director,
Management Consulting
E: tony.smith@kpmg.ie



Jochem Schrijvers

Manager,
Management Consulting
E: jochem.schrijvers@kpmg.ie



Kate O'Riordan

Consultant,
Management Consulting
E: kate.e.oriordan@kpmg.ie



Oscar Blood

Consultant,
Management Consulting
E: oscar.blood@kpmg.ie



[kpmg.ie](https://www.kpmg.ie)

© 2025 KPMG, an Irish partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks of KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

If you've received this communication directly from KPMG, it is because we hold your name and company details for the purpose of keeping you informed on a range of business issues and the services we provide. If you would like us to delete this information from our records and would prefer not to receive any further updates from us please contact unsubscribe@kpmg.ie.

Produced by: KPMG's Creative Services. Publication Date: June 2025