Authorised Push Payment Fraud – The evolving landscape for the Compliance Professional

Author: Simon McFeely, Managing Director at Finvisor and Member of Compliance Institute's FinTech & Payments Working Group.

Imagine you're browsing a popular accommodation platform, excited to book your next holiday already dreaming of lying by the pool. You find the ideal location at an excellent price, proceed to book, and select the "pay later" option. Later that evening, you receive an email from the platform stating, "We're experiencing an issue with our payment gateway. Please click this link to complete your payment." Having used this platform for years, you don't hesitate. You click on the link, enter the bank account details provided, and make the payment through your banking app.

A few days pass, and you realise you haven't received a payment confirmation. It is only then that you understand that you've become a victim of an Authorised Push Payment (APP) scam—a form of fraud where a scammer manipulates an individual or business into transferring money directly into an account controlled by the criminal, either directly or via a "money mule."

Scammers are pervasive, experts at social engineering, and often ruthless. Everyone has encountered suspicious messages, emails, or calls apparently from trusted organisations, such as your bank, eFlow, the HSE, parcel delivery services, or other companies.

The Changing Face of Fraud in Payment Services

As the FinTech landscape has evolved, so have the strategies deployed by fraudsters. While traditional payment fraud methods such as card-not-present fraud and stolen financial information remain prevalent, the rise of Authorised Push Payment (APP) fraud has notably reshaped the fraud landscape in recent years. Strong Customer Authentication (SCA) requirements have brought substantial improvements in fraud prevention; however, fraudsters have adapted and are increasingly utilising social engineering tactics and bypassing controls to focus on bank-to-bank payment methods. Today, many fraud schemes rely less on exploiting technical vulnerabilities and more on manipulating human behaviour to initiate unauthorised transactions.

A major obstacle in addressing APP fraud is the lack of comprehensive and timely data regarding its costs and associated vulnerabilities. In August, the European Banking Authority (EBA) and the European Central Bank (ECB) published a joint report analysing payment fraud data from the latter half of 2022 to the first half of 2023. The report highlighted credit transfers and card payments as the most frequently exploited methods, reflecting the reliance on remote transactions in today's digital economy. In the first half of 2023, fraudulent credit transfers sent by European payment service providers (PSPs) reached €1.1 billion, while card-based fraud amounted to €633 million.

Despite periodic fraud reports from national and European bodies, the underlying data often lacks completeness, timeliness, and sufficient granularity to fully support anti-financial crime efforts. The EBA/ECB report itself notes data limitations, including incomplete submissions, methodological discrepancies, and data quality issues requiring ongoing review to improve the usability of the data. The report cautions against interpreting trends prematurely due to its limited three-period coverage.

What is clear, however, is that APP fraud continues to grow annually, with industry experts predicting a 25% increase year-over-year. In the UK, for instance, APP fraud losses from bank-to-bank transactions approached £500 million in 2023. Adjusting for population size, similar losses in Ireland could be estimated at approximately €35 million annually.

Fraud Enablement & Payment Innovation

The development of real-time or near-real-time payment networks and automated Know Your Customer (KYC) approvals has been a double-edged sword, facilitating rapid onboarding and seamless transactions while simultaneously creating new avenues for fraud. The speed and convenience of these systems allow fewer opportunities and less time to detect and prevent fraudulent activities effectively.

The joint EBA/ECB report underscores a significant contrast between remote and in-person transactions. Credit transfers and e-money payments, mostly initiated remotely, show a consistent trend where both legitimate and fraudulent transactions are primarily processed through online or mobile channels. In the first half of 2023, remote transactions accounted for 98% of the total fraudulent credit transfer value, with 57% of fraudulent activities stemming from the manipulation of unsuspecting payers into initiating these transactions. The remaining 43% involved fraudsters directly issuing payment orders, often using impersonation and coercion to facilitate account takeover.

Unlike other forms of criminality, the fraudsters involved here are typically highly organised, operate across multiple jurisdictions, and demonstrate considerable technical sophistication. They rely on networks of "money mules" and exploit data obtained through phishing attacks and corporate breaches. For instance, the organised crime syndicate known as the Black Axe gang gained notoriety in recent years for its extensive involvement in global financial fraud. Originally established in Nigeria, Black Axe expanded internationally and is heavily implicated in Business Email Compromise (BEC), romance scams, identity theft, and credit card fraud. Estimates indicate the gang may have collectively defrauded victims of up to $1 billion worldwide over the past decade.

The response from international law enforcement has become increasingly coordinated, leading to hundreds of arrests and substantial asset seizures. Closer to home, a recent Interpol operation targeting the Black Axe group led to the arrest of over 60 individuals, and more recently in October 2024, a former employee of an Irish bank was convicted and jailed for three years for his alleged involvement with the group.

Increasing Regulatory Obligations & Shifting of Liability

Since 2020, the UK's Payment Systems Regulator (PSR) has implemented a phased strategy requiring financial institutions to adopt Confirmation of Payee (CoP) and the APP Fraud Reimbursement Model. These changes were introduced through directions by the PSR and changes to the Financial Services (Banking Reform) Act of 2013.

- **CoP** was introduced to mitigate fraud by requiring payers to verify payee identities before transactions are completed, aiming to reduce misdirected payments and prevent unauthorised transactions. This process involves matching payee names with account numbers and alerting users to any discrepancies. However, CoP has notable limitations; it applies only to specific UK domestic transactions and does not return a usable payee name result if the receiving Payment Service Provider (PSP) utilises a 'pooled account' infrastructure.
- **APP Fraud Reimbursement Model**, which became mandatory as of 7th of October 2024 replacing a previous voluntary code, requires sending PSPs to compensate victims of APP fraud unless the consumer acted with gross negligence. This model shifts significant liability for fraud losses to PSPs and is intended to incentivise the introduction and usage of stronger anti-fraud measures. Like CoP, it has limitations, and it applies only to UK domestic payments, excludes 'on-Us'[1] transactions, and covers only certain consumer types within its definition of "consumer".

The UK's CoP and the Reimbursement Model are in their early stages, however, new trends in "friendly fraud" are evident, and there is an adaptation of other scams like sextortion and romance fraud already emerging. Fraudsters are reportedly leveraging the reimbursement approach to manipulate victims further, resulting in the unintended consequence of escalating fraud risk.

The role of the Compliance Officer is becoming increasingly complex, requiring continuous monitoring of regulatory developments and fraud trends across Europe to detect and deter evolving fraud typologies. Given the dynamic regulatory landscape, Compliance Officers should ensure visibility into key regulatory changes expected over the next 18 months and prepare their organisations accordingly.

SEPA Instant Payments Regulation (IPR)

Regulation (EU) 2024/886, The Instant Payment Regulation (IPR), requires payment service providers (PSPs) who provide standard credit transfers in Euros, to offer the service of sending and receiving instant payments in Euros. Effective from the 8th of April 2024, the IPR has a phased implementation timeline, with distinct deadlines for compliance depending on institutional type and location within or outside the Eurozone when handling euro transactions.

Under the regulation, credit institutions and banks (CIs) must be able to receive SEPA instant payments by the 9th of January 2025 and must implement sending capabilities by the 9th of October 2025. Payment institutions and e-money institutions (PIs/EMIs) in the Eurozone have until the 9th of April 2027 to establish both sending and receiving functionalities. The IPR requires PSPs to process payments around the clock, with a 10-second settlement window, ensuring near-immediate fund availability post-transaction initiation. Furthermore, SEPA Instant payments are required to incorporate Verification of Payee (VoP) services, closely aligning with the UK's Confirmation of Payee (CoP) approach and adding a robust layer of security to the instant payment infrastructure.

While this regulation is a significant advancement, particularly in markets like Ireland, where SEPA Instant coverage is currently limited to around 5%, it also introduces considerable operational demands. Compliance Officers will face increased challenges in managing real-time fraud risks, given the cross-border and 24-hour nature of SEPA Instant transactions.

Evolving Payment Services Regulation

In June 2023, the European Commission released its proposal for the Payment Services and Electronic Money Services Directive (PSD3) and the Payment Services in the EU Regulation (PSR). Currently, PSD2 provides a right to refund only for unauthorised payment transactions, leaving a significant portion of fraud unaddressed i.e. when fraudsters manipulate users into authorising payments themselves.

The initial PSR proposal introduced additional refund rights under two specific circumstances:

- Consumers experiencing financial loss due to a VoP service failing to detect a mismatch between the payee's name and IBAN.
- Consumers fall victim to "spoofing" fraud, in which fraudsters impersonate a PSP employee and deceive the consumer into actions that lead to financial loss.

In recent drafts, the scope of vulnerabilities eligible for refunds expanded to include fraudsters impersonating trusted entities, such as central banks or government authorities. This amendment reflects a regulatory shift towards closer alignment with the UK framework, while the PSR proposal further enhances consumer protections by introducing mandatory information-sharing mechanisms among PSPs, requiring PSP-led user training on fraud awareness, and mandating prompt reporting of fraudulent sites to host providers.

PSD3/PSR is now expected to become law in 2025 with an anticipated 2-year transition period. Although this timeline may seem extended, Compliance Officers should proactively track the developments in PSD3 and PSR, ensuring their

Board is informed and a firm action plan is in place. It is also advisable to incorporate a comprehensive review of fraud risk management strategies in their 2025 or multiyear compliance plans to ensure readiness for these regulatory changes.

Irish National Policy

In October, the Department of Finance introduced the National Payments Strategy (NPS), outlining 16 "future outcomes" and 26 associated "actions". These outcomes span six chapters, with chapter five dedicated to payment fraud–a term mentioned over 200 times throughout the NPS document.

The NPS is well-received by the industry, with anticipated benefits including the development of a "shared fraud database," legal avenues to flag illegal online content, and the establishment of formal cross-sector initiatives.

In Ireland, there are over 270 entities–including payment firms, credit unions, virtual asset service providers, and e-money institutions–face inherent exposure to payment fraud risks (excluding traditional credit institutions). Compliance Officers within these firms should prioritise alignment with the NPS initiatives in 2025, tracking its progress closely and identifying proactive ways to support its outcomes.

Changes to Visa's Risk Management Policies

Many FinTechs in Ireland are acquiring firms or are acquiring merchants receiving card funds from payment service users for onward transmission, or e-money issuance. Most if not all these firms will have a direct or indirect relationship with Visa.

Effective from the 31st of March 2025, Visa will retire both the Visa Dispute Monitoring Program (VDMP) and the Visa Fraud Monitoring Program (VFMP), consolidating them into a streamlined framework known as the Visa Acquirer Monitoring Program (VAMP). VAMP will incorporate a new transaction count-based metric that aggregates both fraud and non-fraud disputes, reflecting Visa's evolving risk appetite. From the 1st of January 2026, VAMP will significantly tighten tolerance levels, lowering the "Above Standard" threshold for Acquiring entities from 0.9% to 0.3% and for Merchant entities from 1.5% to 0.5%.

Failure to stay within Visa's risk appetite could lead to expensive penalties, and in a worst-case scenario, de-risking.

Compliance Program Readiness

Compliance Officers should keep the Board and key internal stakeholders informed, ensuring they are fully supportive and aware of the shifting landscapes. As we design and implement the annual compliance plan, Compliance Officers could consider the following key priorities:

1. A Comprehensive Fraud Risk Assessment: The issue is often that firms conduct high-level reviews rather than deep-dive assessments. As a rule of thumb, the risk assessment should consider the market threat landscape, and payment fraud typologies inherent to the firm considering its customers, markets, and the

nature of its business. The risk assessment should also assess the specific controls in place to identify and prevent fraud, be that as a send, or receive-side payment service user customer. Firms should encourage further collaboration within their firm and at an industry level to share best practices on fraud risk assessment methodologies and to learn about control frameworks that work well at other firms.

2. Enhanced Fraud Detection and Monitoring: During the risk assessment process, the Compliance Officer should look deeply into the fraud detection system in place. As real-time payments will become more prevalent, the level of required sophistication in compliance technology will increase both in terms of rule design, and level of performance:

   - Many payment firms in Ireland operate skeleton staff at the weekend or outside of office hours, the Compliance Officer will need to evaluate how the fraud detection system can deter, detect and manage fraud risk scenarios 24/7.
   - Rules-based approaches to control design no longer work and smarter real-time transaction monitoring, machine learning, and behavioural analytics are needed to swiftly identify unusual or high-risk transactions.
   - Transaction monitoring systems of the future need to utilise more KYC profile information and leverage external data points such as geo-location identifiers, IP addresses and device usage.

3. Consideration to implement VoP / CoP: While it is not yet a regulatory obligation within the EU, some firms are implementing VoP controls and triggering it as part of a firm's enhanced due diligence control system, for example when there is a higher likelihood of social engineering fraud associated with a payment instruction.

4. Training Employees and Educating Customers: Approaches vary massively across the industry and many firms could do better. The Compliance Officer should review their firm's website, walkthrough fraud signposts during the onboarding and payment journeys, and assess the triggering points for fraud-awareness notifications to customers.

Wrapping Up

If you feel overwhelmed after reading this piece, that is natural, the pace and extent of changes can appear overwhelming. There is still time to prepare, and the emerging requirements and best practices should be factored into your risk assessment and compliance plan. Recent events in the UK provide key lessons, firms were aware of the implementation dates for CoP and the Reimbursement Model well in advance. Many firms were well prepared, had full support from the Board, invested resources into fully understanding how the new requirements would impact their business model, and made improvements to their fraud risk management frameworks. On the other hand, some firms were less organised, not ready, and remain potentially exposed to the cost of fraud.

REFERENCE

1 transactions where the acquirer and card issuer are the same entity