

Authorised Push Payment Scams

An assessment of reimbursement requirements for victims of online fraud

In 2022, Authorised Push Payment (“APP”) fraud losses were valued at €9.9 million in Ireland. In a world where digital transactions dominate and the border between convenience and vulnerability becomes increasingly blurred, the UK have introduced new legislation to reimburse victims of APP scams, championing the customer. Yvonne Kelleher and Niamh Lambe from our Risk & Regulatory Consulting team explain below the complex world of electronic payments and examine the significance of this pivotal legislation for the customer’s financial independence in an Irish context.

INTRODUCTION

In its Consumer Protection Outlook Report 2023, the Central Bank of Ireland outlined its expectation of firms to have effective measures to mitigate the risk of fraud, be proactive in identifying and dealing with cases of fraud and engage effectively with consumers who have been the victim of fraud. This includes taking steps to support the victims of APP scams to retrieve their funds where possible.

Prior to the publication of this report, The UK Treasury had unveiled plans to support victims of APP fraud in May 2022, empowering the Payment Systems Regulator (“PSR”) to mandate victim reimbursement for APP scams. The Financial Service and Market Bill, enacted in

June 2023, formalised this legislative change. The PSR published their first APP Scams Performance report in October 2023, highlighting the inconsistent outcomes for consumers who report an APP scam to their financial institution. The APP legislation aims to adopt a unified approach in the UK context.

On 19 December 2023, the PSR released the APP scams reimbursement policy (PS23/4). This document outlines the final requirements, legal instruments, and supplementary guidance for the policy’s implementation. The policy is set to commence on 7 October 2024, presenting a challenging target date.

PS23/4, published in December 2023, introduced three finalised legal instruments for UK firms:

01 Specific Requirements (SR1)

Mandates the incorporation of PSR’s reimbursement requirements into Faster Payment rules. It establishes a 35-business day timeframe for sending Payment Service Providers (“PSPs”) to decide on reimbursing an APP scam case, with the decision being final. Sending PSPs are liable for full reimbursement if their decision is to not reimburse, and the case is overturned.

02 Specific Direction (SD20)

Requires Faster Payments participants, (PSPs involved directly or indirectly), to comply with reimbursement requirements and rules. Indirect Access Providers (“IAPs”) are exempt from passing on obligations to indirect PSPs, but they must provide the PSR with an annual list of indirect PSPs to whom they provide access to Faster Payments and update it as needed.

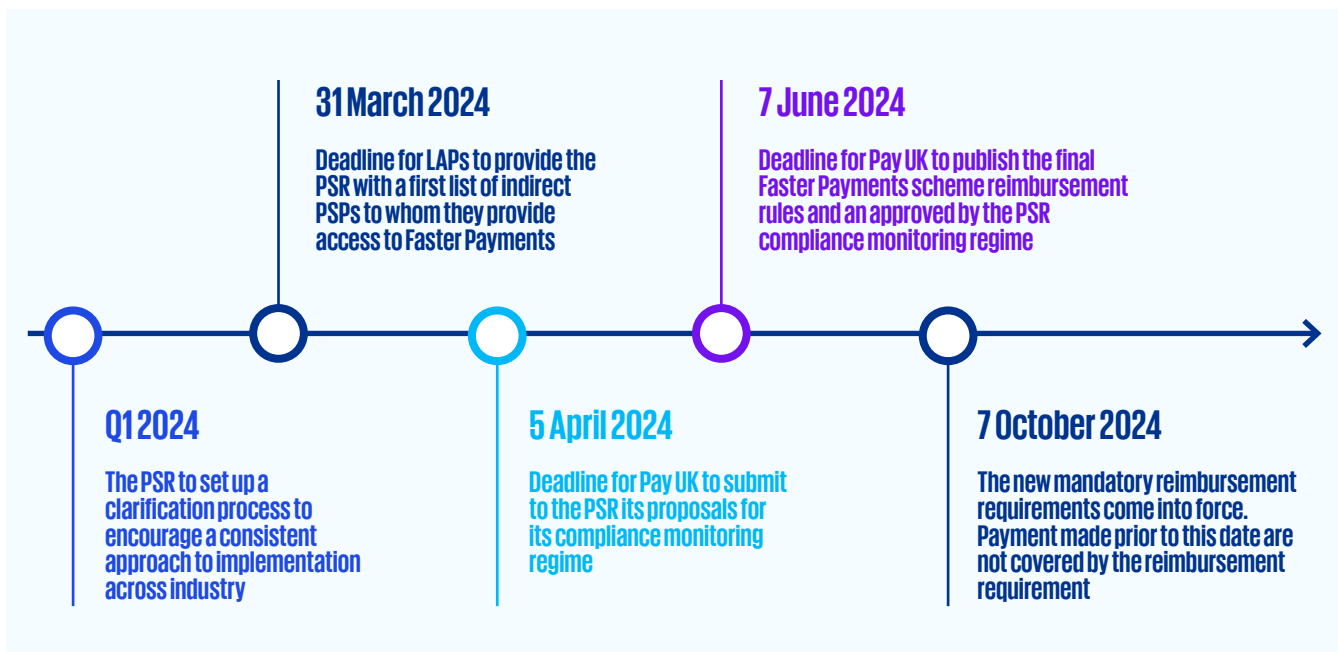
03 Specific Direction (SD19)

Mandates Pay.UK to establish and implement an effective compliance monitoring regime.

In a time of increased online transactions for both personal and business payments, both in Ireland and globally, fraudsters are adapting their methods of deception. It is crucial that firms exhibit their ability to maintain trust with consumers in this environment, taking steps to ensure they are protected against fraud. Taking proactive steps now will enable Irish payment providers to ensure consumers are protected against fraud.

The Central Bank has indicated that as part of its ongoing review of the Consumer Protection Code 2012, it is considering what policy measures it can introduce within the scope of its specific rule-making powers to contribute to the protections of consumers in a digital environment more generally. This move by the Central Bank underscores the importance of these regulatory changes in the UK for Irish firms, recognising that further improvements are needed at an EU level to address APP fraud.

KEY DATES FOR APP VICTIM REIMBURSEMENT LEGISLATION:



The current EU legislative framework does not set out liability for APP fraud, however, a proposal by the European Commission enables the granting of refunds for consumers in two situations:

1. For consumers who suffered losses due to the failure of the payment service provider’s (“PSP”) IBAN / name verification service to detect a mismatch between the name and IBAN details of the payee; and
2. For consumers falling victim of a “spoofing” fraud where they have been contacted by a party impersonating the consumer’s bank, tricking them into acting which subsequently results in their financial loss.

On the 28th of June 2023, The European Commission published the Third Payment Services Directive (PSD3) and a Payment Services Regulation (PSR). PSD3 is seen to improve and enhance consumer protection measures in the payments sector. This Directive looks to tackle new types of fraud, in particular fraud relying on manipulative techniques, like APP fraud. The European Parliament is expected to vote on both texts during the first plenary session in April 2024. The key amendments proposed by ECON include:

- Simplified authorisation process for existing payment and e-money institutions under PSD3. Expansion of customer rights to refunds in APP fraud cases under PSR3.
- Enhanced data security requirements and transparency of charges for customers. It also proposes to extend to regular credit transfers the compulsory IBAN/name checking service which had initially only been proposed for instant payments.
- Given the complexity of negotiations and the approaching European elections, it is estimated that the PSR could take effect in the second half of 2026, with PSD3 taking full effect in early 2027.

The UK’s APP legislation enhances consumer protection, allowing victims to request reimbursement from PSPs. All payment firms share reimbursement costs equally, with a 50:50 split between sending and receiving firms. Consumers benefit from a minimum standard, ensuring most victims are reimbursed within 5 business days, and additional safeguards are provided for vulnerable customers. Non-compliant firms face regulatory investigation.



A TYPICAL APP FRAUD JOURNEY

During an APP scam, fraudsters deceive consumers into making payments, often under the guise of a legitimate body such as a well-known retailer in order to win the consumer’s trust. Such scams rely on voluntary authorisation, often following the below steps:



What does the APP legislation mean for PSPs?

The UK’s Financial Conduct Authority (“FCA”), defines a vulnerable customer as “somebody who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.” The FCA outlines four categories of vulnerability in its determination, namely, health, life events, resilience and capacity.

Under the new legislation, reimbursement will be extended to various participants:

- Consumers (those acting for purposes other than trade, business, or profession)
- Micro-enterprise (with less than 10 employees and annual turnover and/or annual balance sheet less than £2m)
- Charities (with annual income less than £10m)

Exceptions arise when victims are complicit in the fraud or have demonstrated gross negligence. Sending PSPs can extend reimbursement windows when additional information is necessary for claim assessment, and they have the flexibility to implement a maximum reimbursement level, apply a claim excess, and set time limits, with a minimum of 13 months.

The legislation promotes additional supports for vulnerable customers, especially in the context of assessing whether gross negligence was a contributing factor to the loss. This signals the continuing move to protect such customers, requiring a heightened awareness by financial institutions of consumers’ personal circumstances.

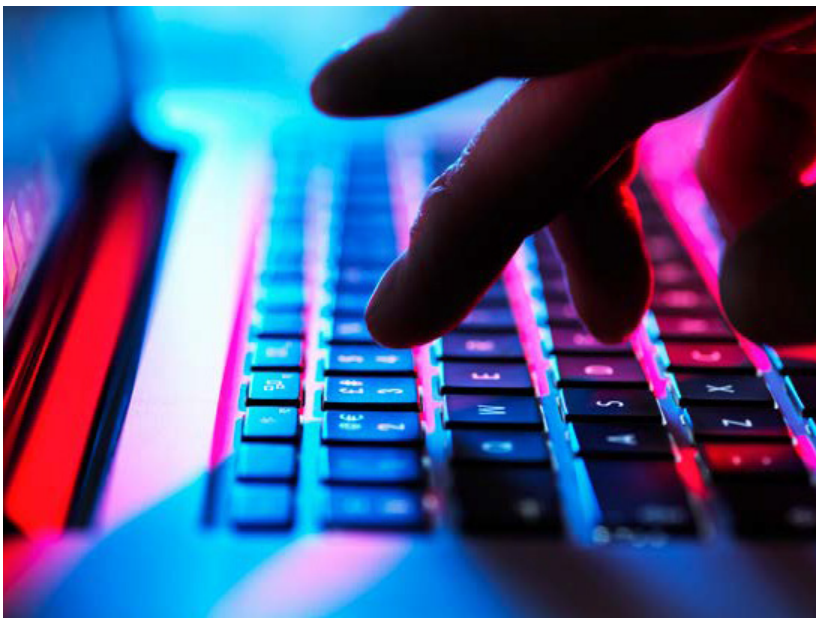
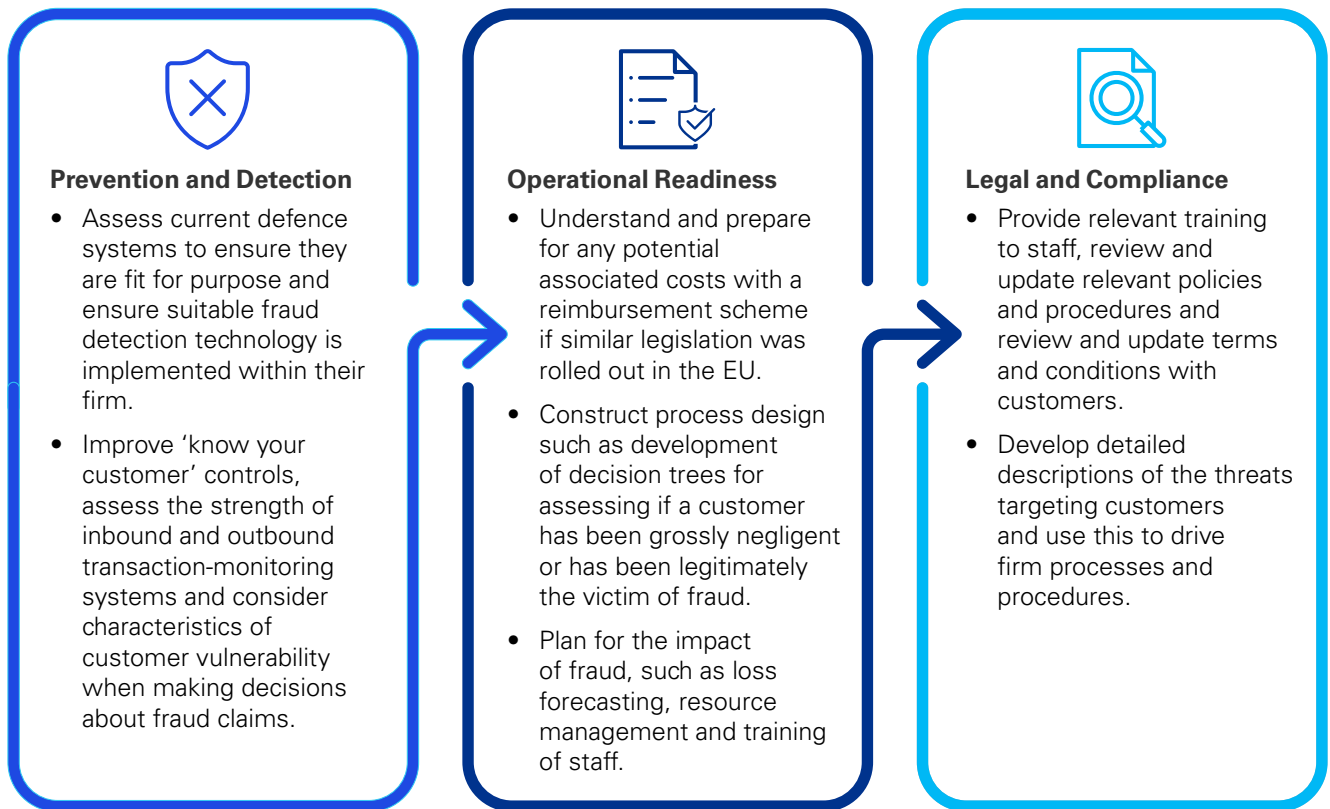
With the ongoing consultation of the Consumer Protection Code and an updated and modernised Code on the way, it is likely that similar legislation may be introduced in Ireland. PSPs in Ireland can look to the UK to build a framework which can proactively address similar regulation should it be introduced here in the coming years.



FIRM READINESS

With €1.8 billion worth of fraud reported in the EU in 2022, a 7% increase from 2021 (according to OLAF, the EU’s anti-fraud watchdog) firms need to act now to adapt an enhanced focus on protecting consumers from APP fraud. The introduction of this legislation in the UK confirms a heightened concern regarding this issue among regulators.

Firms should take steps now in advance of similar regulation being introduced in Ireland to prevent additional losses and protect consumer.



Yvonne Kelleher
 Managing Director
 Risk Consulting
 KPMG in Ireland

“Consider constructing process design such as development of decision trees for assessing if a customer has been grossly negligent or has been legitimately the victim of fraud”

HOW CAN KPMG HELP?



We can help review your Risk Assessment Framework, with a focus on APP scams and financial crime, and the impact this has on your customer base. We will also develop treatment policies for all categories of vulnerability to ensure that the needs of all customers are met. We have a vast amount of experience implementing risk frameworks, working on areas such as culture, conduct and business behaviours in recent times.



Our payment experts alongside our risk and regulatory experts can assist you and your firm to navigate through the new legislation and assess what are the practical implications for your firm and customers.



KPMG have a clear understanding of industry standards for consumer protection within the financial services sector (e.g., Consumer Protection Codes). This knowledge is rooted in our first-hand experience of working alongside industry peers and regulators on such matters over the last 15 years. Our work to date includes new regulatory implementation, running of conduct risk programmes and the establishment of vulnerable customer frameworks. Our team also has experience working on consumer protection programmes in the UK, Australia and within Europe.



KPMG can help you develop and execute a technology strategy and operation model that supports the utilisation and development of existing and future data for an effective APP fraud detection programme. We can help you employ technology to aid customer identification and verification, customer due diligence and customer risk assessment, for a more effective mitigation of risk.



KPMG has the capability to tap into the expertise of an array of subject matter experts with backgrounds in legal, technology, and data analytics to assist firms in crafting and executing the essential framework for complying with potential APP fraud regulations.



Contact us



Gillian Kelly
Partner & Head of Conduct
Risk Services
KPMG in Ireland
t: +353 87 744 1120
e: gillian.kelly@kpmg.ie



Niamh Lambe
Managing Director
Head of Financial Crime
KPMG in Ireland
m: + 353 87 0504388
e: niamh.lambe@kpmg.ie



Yvonne Kelleher
Managing Director
Risk Consulting
KPMG in Ireland
t: +353 87 050 4349
e: yvonne.kelleher@kpmg.ie



Rosalind Norton
Director
Risk Consulting
KPMG in Ireland
t: +353 87 111 5982
e: rosalind.norton@kpmg.ie



Tony Smith
Associate Director
Management Consulting
KPMG in Ireland
t: +353 87 111 5917
e: tony.smith@kpmg.ie



Luke Ryan
Manager
Risk Consulting
KPMG in Ireland
t: +353 86 103 9997
e: luke.ryan@kpmg.ie



© 2024 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: February 2024. (10143)