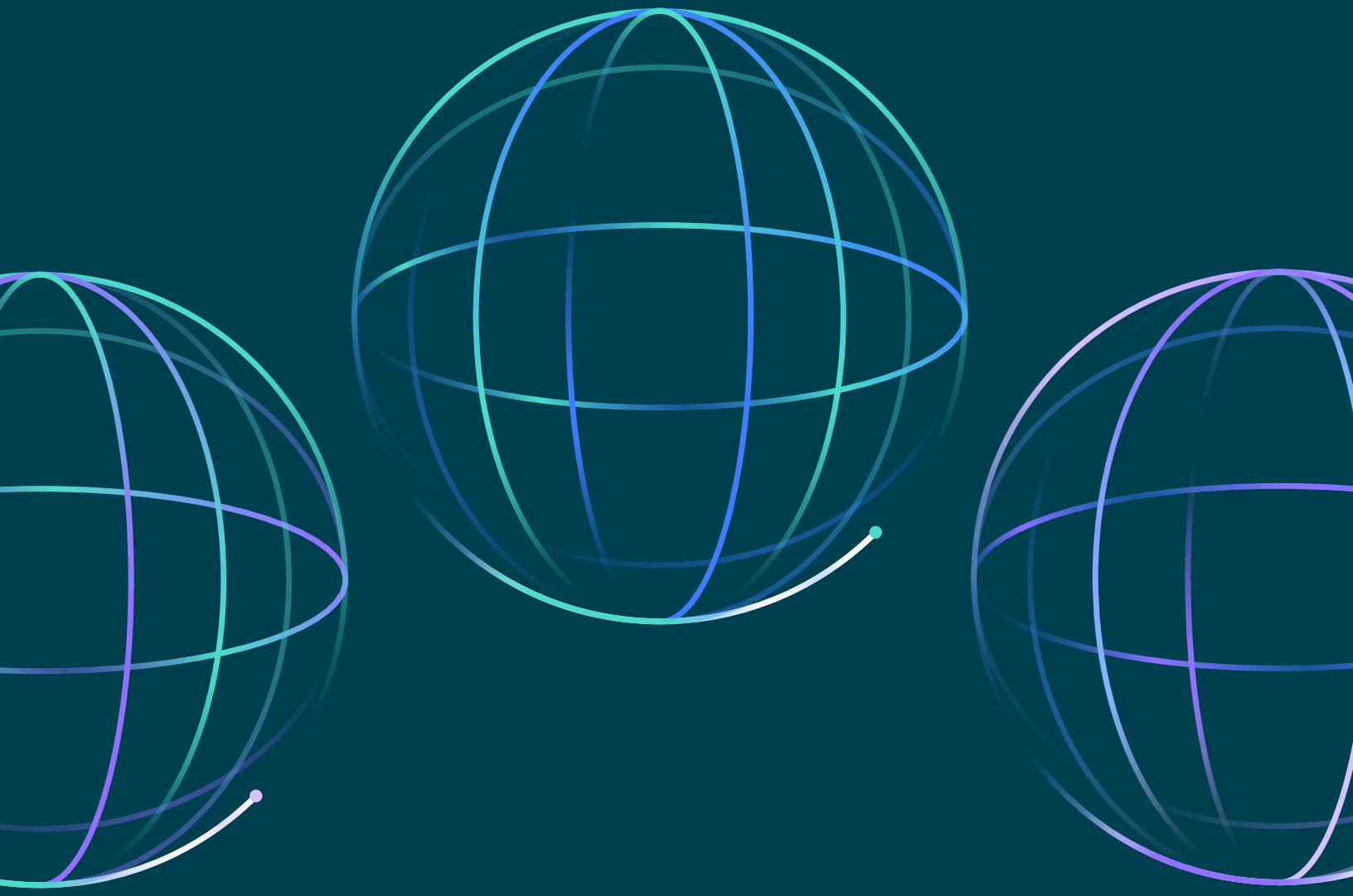
OneSpan

Global authorised push payment scam regulations

Comparing approaches in EU, UK, Singapore, Hong Kong, and Australia



WHITE PAPER - JANUARY 2025

Contents

Introduction

In recent years, authorised push payment (APP) fraud has risen to unprecedented heights. For example, according to UK Finance, £213.7 million was lost to APP fraud in the first half of 2024 in the UK alone. In the Netherlands, bank impersonation scams resulted in losses of more than €28M in 2023.

APP fraud occurs when a fraudster tricks a victim into authorizing a payment to a fraudulent account. This is often done through sophisticated social engineering techniques, such as phishing emails, phone calls, or text messages. The fraudster may impersonate a trusted individual or organization, such as a bank, the police, or a government agency. They may create a sense of urgency, claiming that the victim needs to act quickly to avoid a negative consequence. Once the victim is convinced, they are instructed to transfer money to a specific bank account controlled by the fraudster.

In response, governments globally are intensifying anti-scam measures, introducing new guidelines to banks, telecommunications providers, and other key sectors to improve security controls and mitigate fraud risks for consumers and businesses.

This paper provides an overview of the most important anti-scam regulations around the world, focusing primarily on APP fraud in a digital banking context, but also touching on regulation related to other digital banking scams such as phishing. Our focus is on regulations in the United Kingdom, European Union, Singapore, Hong Kong, and Australia, which lead the world in anti-scam regulation.

This paper provides an overview of the most important anti-scam regulations around the world, focusing primarily on APP fraud in a digital banking context, but also touching on regulation related to other digital banking scams such as phishing.

United Kingdom

The United Kingdom was the first country globally with a coordinated approach against APP fraud, largely driven by the country's payment systems regulator (PSR).

On 28 May 2019, the Contingent Reimbursement Model Code for Authorised Push Payment Scams (CRM), drafted by the APP Scams Steering Group of the PSR, entered into force. The CRM Code was a voluntary code designed to protect consumers from APP scams. Under this code, participating financial institutions committed to implementing various organizational and technical measures to detect and prevent APP scams, and to reimbursing victims of APP scams in certain circumstances.

Some of the most important organizational and technical measures in the CRM Code include:

- **Consumer education.** Firms should take reasonable steps to raise awareness and educate customers about APP scams and the risk of fraudsters using their accounts as mule accounts.

- **Preventing and detecting APP scams**. Financial institutions initiating payments implement transaction monitoring to detect fraudulent payments and behavioural analytics to detect changes in the customer's behaviour, as well as actions such as warning mechanisms, confirmation of payee (see below), and delaying suspicious payments. Financial institutions receiving payments should use transaction data and customer behaviour analytics to identify accounts used to receive funds from APP scams.

- **Reimbursement.** Financial institutions reimburse victims of APP scams, unless they ignored effective warnings, did not take appropriate actions following a clear negative confirmation of payee, or acted with gross negligence.

The CRM Code was a voluntary code, and in 2019 the PSR started replacing it with mandatory measures.

In August 2019, the PSR gave members of the UK's six largest banking groups Specific Direction 10 to implement confirmation of payee (COP) by the end of March 2020. With confirmation of payee, the payment service provider (e.g., bank) of a payer who initiates a credit transfer can request the PSP of the payee to verify whether the name and bank account number of the payee, as provided by the payer, match. If they don't match, the payer's PSP must inform the payer about the discrepancy and the degree of the discrepancy, and this within a few seconds after entry of the payee information by the payer. The payer remains free to decide whether or not to authorise the credit transfer, even if a discrepancy was detected.

Confirmation of payee can be very helpful to address social engineering fraud, as fraudsters sometimes try to convince victims that a certain bank account number belongs to a trusted beneficiary, while in reality if belongs to a money mule. The matching service is not a silver bullet as it relies on the ability of the payer to correctly interpret the notification and take appropriate action, while fraudsters might convince the victim to ignore the notification. But it's certainly a relevant countermeasure.

On 7 October 2024, the PSR's requirements for mandatory APP fraud reimbursement for "faster payments", as specified in Specific Direction 20, come into effect. As of this date, in-scope PSPs will be required to reimburse victims up to a maximum of £85,000 within five working days, and receiving PSPs will be required to share the cost of the fraud loss with the sending PSP under a 50-50 split. The CRM Code was retired on 7 October 2024 with the introduction of the PSR's statutory reimbursement framework.

European Union

On 28 June 2023, the Directorate-General for Financial Services (DG FISMA) of the European Commission published its long-awaited draft proposals for a Directive on Payment Services and Electronic Money Services (PSD3) and a Regulation on Payment Services (PSR), the long-awaited successors of the revised Payment Services Directive (PSD2).

Subsequently, the review process by the European Parliament and Council kicked off. In November 2023, the European Parliament's Economic and Monetary Affairs Committee (ECON) published draft reports on the proposals with recommendations for amendments. On 14 February 2024, ECON voted to adopt both texts. Finally, on 23 April 2024 the European Parliament voted to adopt both texts in plenary, closing the first reading. The legislative process now continues with a review by the European Council and trilogue negotiations between the Commission, Parliament and Council, which are expected to conclude in the first half of 2025.

The current draft of the PSR from the European Parliament proposes anti-fraud measures focusing specifically on APP fraud. The prevention measures specifically targeting APP fraud include the following:

IBAN/name matching service

Article 50 of the PSR mandates PSPs to implement an IBAN name matching service, which is the same as COP described above. The service must be provided free of charge. The IBAN/name matching service builds on a proposal by the European Commission present in the legislative proposal on instant payments from 26 October 2022. This proposal applies only to instant credit transfers and only in euro. The new proposal in the PSR is more general and applies to all credit transfers (instant or not, euro or other currency).

Liability for fraud

Article 59 discusses liability for impersonation fraud where the victim is manipulated by a fraudster who pretends to be an employee of the victim's PSP or any other entity (e.g., the police). In the European Commission's original proposal from June 2023, impersonation fraud only covered fraud cases where the fraudster impersonates the victim's PSP, and not other types of entities. Hence, the scope of impersonation fraud has significantly expanded. This expansion is a welcome change for consumers, as in many APP cases the fraudster impersonates an entity different from the PSP. This will most likely be a major topic in the upcoming trilogue negotiations among the Commission, Parliament, and Council.

The PSP is liable for impersonation fraud if the fraudster, who pretends to be an employee of a certain entity, manipulates the victim using the name, email address, or telephone number of that entity and that manipulation gives rise to fraudulent payments authorised by the victim under the condition that the victim reported the fraud to the police and notified their PSP. In such a scenario, the victim's PSP has to refund the victim the full amount of the fraudulent authorised payment transaction.

The PSP is not liable if the victim acted fraudulently or with gross negligence. However, the burden to prove that the victim acted fraudulently or with gross negligence resides with the victim's PSP.

In addition, the PSP could transfer liability to the electronic communications provider used by the fraudster to communicate with the victim, if the PSP informs this provider about the fraud case and if this provider does not remove fraudulent content related to the fraud case. The PSR defines an electronic communications provider as a company subject to the European Electronic Communications Code (ECCC) or the European Digital Services Act. These companies are traditional telecommunications providers, such as mobile network operators, fixed-line operators, and Internet service providers, as well as social media platforms, messaging apps, online marketplaces, content sharing platforms, online travel and accommodation platforms, etc.

PSPs in many European countries have long argued that they should not be solely liable for impersonation fraud as the fraud very often originates outside banking or payment applications. The Parliament has listened to this concern

and its draft proposal puts more responsibility on electronic communications providers, similar to the UK, Singapore, and Australia. Nevertheless it is still the PSP that needs to refund the victim, after which the PSP can try to obtain a refund from the electronic communications provider. This may still put significant burden on PSPs to obtain a refund.

Electronic communications service providers are also required to educate and alert their customers about new forms of scams, explain which precautions they can take to avoid falling victim, and inform them how they can report fraudulent content.

Finally, the draft proposal of the European Parliament states that all providers involved in the fraud chain have to put organisational and technical measures in place to prevent and mitigate payment fraud. It is not specified which measures are meant. This will most likely be developed further in the Regulatory Technical Standards (RTS) accompanying the PSR.

Transaction monitoring

Article 83 of the PSR basically contains the same requirements related to transaction monitoring as those present in the RTS on SCA for PSD2. It requires PSPs to have transaction monitoring mechanisms in place to support the implementation of SCA and its exemptions, and to detect and prevent potentially fraudulent payment transactions. The latest review of the European Parliament states that, when transaction monitoring mechanisms provide strong evidence for suspecting a fraudulent transaction, payment service providers have the right to block the execution of the payment.

Fraud data sharing

To improve the protection of payers against fraud in credit transfers, PSPs should be able to perform transaction monitoring based on information as comprehensive and up to date as possible. This includes collectively using information such as IBANs of payees, manipulation techniques, and other circumstances associated with fraudulent credit transfers identified by PSPs. Article 83 therefore provides a legal basis for PSPs to share fraud-related information between themselves in respect of GDPR.

More specifically, PSPs have to exchange identifiers (e.g., names, personal identification numbers, organisation numbers) and other transaction information with other PSPs about payees who are believed to be recipients of a fraudulent payment, when the PSP has sufficient evidence to assume that there was a fraudulent payment transaction. It can be assumed that sufficient evidence is available when at least two customers of the same PSP have informed them that a unique identifier of a payee was used to make a fraudulent credit transfer.

User Education

Article 84 introduces an obligation for PSPs to carry out education actions to increase awareness of payments fraud among their customers and staff. Specifically, PSPs must give their customers clear indications on how to identify fraudulent attempts and how to avoid falling victim of fraudulent actions targeting them. Payment service providers have to inform their customers of where they can report fraudulent actions and obtain fraud-related information.

In the latest draft proposal of the European Parliament, this article additionally requires European Member States to allocate substantial means to investing in education on payment-related fraud, for example via media campaigns or lessons at schools. Payment service providers and electronic communications service providers have to cooperate free of charge with the Member States in those educational activities.

Singapore

On 24 October 2024, the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) jointly published the Guidelines on Shared Responsibility Framework (SRF), which will become effective as of 16 December 2024. This followed a consultation period which ran from October until December 2023. MAS regulates the financial services industry in Singapore, while IMDA oversees telecommunications providers.

The Guidelines set out the roles and accountabilities of consumers, responsible financial institutions and responsible telecommunications companies under the Shared Responsibility Framework (SRF). The Guidelines clarify the allocation of responsibility for losses arising from phishing scams specifically, and the operational workflow for consumers to report such scams. Since only phishing scams are included in the scope of the SRF, its scope is relatively limited compared to other countries and regions.

In particular, the SRP requires financial institutions to provide:

- Real-time notifications to customers about the activation of a security token, logins from a new device, and high-risk activities.
- Real-time notifications to customers about outgoing transactions.
- A reporting channel allowing customers to block suspicious transactions.
- A self-service feature allowing customers to block access to their account, also referred to as the kill switch.
- Real-time transaction monitoring to detect fraudulent transactions and blocking of fraudulent transactions that would result in losses above a certain threshold, as well as transactions following the fraudulent transaction.

Telecommunications providers also need to provide the following:

- They must only allow SMS messages with alphanumeric sender IDs from authorized aggregators, licensed by IMDA. SMS messages with an alphanumeric sender ID originating from unauthorized aggregators should be blocked.
- They have to implement an anti-scam filter to block SMS messages containing malicious URLs.

In terms of liability for scams, the SRP implements a waterfall approach: the financial institution involved in a phishing scam bears the losses of the scam if they failed to comply with their duties. If the financial institution complied with its duties, but the telecommunications provider did not, then liability shifts to the telecommunications provider. Finally, the customer bears the losses if both the financial institution and telecommunications providers complied with their duties.

In addition to the SPF, the Singaporean government recently introduced the Protection from Scams Bill into parliament. This Bill, which was introduced on 11 November 2024 after a public consultation period that ran in September 2024, grants police forces the right to issue Restriction Orders (ROs) to banks to restrict an individual's banking transactions, if there is reasonable belief that the individual will make money transfers to scammers. As such, police forces can better protect targets of ongoing scams who refuse to believe that they are being scammed. The Ministry of Home Affairs (MHA) said the RO will be issued only as a last resort, after other options to convince the scam victim have been exhausted.

Hong Kong

In September 2024, the Hong Kong Monetary Authority (HKMA) announced that it will launch an industry consultation about a responsibility framework regarding digital scams. The framework is expected to focus on APP fraud, and exclude other types of fraud, such as fraud based on phishing attacks.

Australia

In November 2023, the Australian Banking Association (ABA), which groups community-owned banks, building societies, credit unions, and commercial banks, launched the Scam-Safe Accord. In this accord, the banking sector committed to certain actions to protect Australian citizens against online scams. In particular, the following initiatives have been agreed upon:

- Deployment of a confirmation of payee (COP) system, allowing banks to detect discrepancies between the name and the bank account number of the beneficiary in a credit transfer. Fraudsters often try to trick victims to transfer money to a certain bank account number, believing it belongs to a trustworthy beneficiary while in reality it belongs to the fraudster or an accomplice. This system is planned to be rolled out in 2024 and 2025.
- By the end of 2024, banks will verify the identity of customers opening a new bank account using biometric technology (i.e., face scan, fingerprint scan, or behavioural biometrics).
- If a customer intends to transfer money to a new beneficiary or wishes to raise credit transfer thresholds, banks will ask more questions, issue warnings, or implement delays. This will be deployed by the end of 2024.
- Sharing scam intelligence between banks via the Australian Financial Crime Exchange (AFCX) and Fraud Reporting Exchange (FCX). For example, banks will share bank account numbers known to belong to money mules, so that banks can block credit transfers to these accounts.
- Limiting payments to high-risk channels, such as cryptocurrencies and other "getaways vehicles" to move money out of Australia.

The Australian telecommunications sector also did not stand still in its fight against scams, especially since Scamwatch, an Australian government website providing information about scams, reported SMS and phone calls as one of the main tools to perpetrate online scams. In July 2022 the Australian Communications and Media Authority (ACMA) registered the industry code "Reducing Scam Calls and Scam SMS", also referred to as the "Scam Code". It essentially requires Australian network carriers to block calls and SMS messages that could be fraudulent, for example because an SMS message is sent using a sender ID that the sender is not entitled to use.

Last but not least, in September 2024 the Australian government introduced the Scam Prevention Framework (SPF) for public consultation. The SPF, which amends the Competition and Consumer Act from 2010 and which was presented to Parliament on 7 November 2024, requires businesses in certain industries to protect their customers against online scams. The SPF seeks to build upon and consolidate various sectoral initiatives, such as the above-mentioned Scam-Safe Accord and Scam Code, within a responsive and adaptable framework.

Under the SPF, the Australian government may make a code for a certain regulated sector, known as an "SPF Code". An SPF Code will contain sector-specific requirements for regulated entities. The following sectors are identified as sectors that could be included within the SPF:

- Banking and insurance
- Telecommunications services
- Digital platform service providers, including social media providers, paid search engine advertising, and direct messaging services
- Broadcasting service providers

Regulated entities need to comply with the six principles of the SPF:

- **Governance.** Regulated entities need to document and implement policies, procedures, metrics, and targets to combat scams, and publish information about how they protect citizens against scams.
- **Prevent.** Entities need to take reasonable steps to prevent scams relating to their services. Examples of reasonable steps are identifying consumers who have a higher risk of being targeted by scams, providing warnings to at-risk consumers, and providing information to assist them in identifying scams and steps they can take to minimize the impact of scams.

- **Detect.** Entities have to take reasonable steps to detect scams as they are happening or after they have happened, regardless of whether any loss has already been incurred. This includes identifying citizens that have been or could have been impacted by a scam.
- **Report.** Entities need to report information about scams to the appropriate regulator. Examples are bank account details that scammers instruct victims to transfer funds to, and phone numbers used by scammers to get in touch with victims.
- **Disrupt.** Entities have to take reasonable action to disrupt (suspected) scams relating to their service. Examples are blocking credit transfers, removing scam advertisements, and blocking SMS messages.
- **Respond.** Entities must maintain an accessible mechanism allowing citizens to report actual or possible scams, and an internal dispute resolution procedure to address complaints from citizens about scams.

Non-compliance with SPF can result in fines up to AU$50 million or 30% of turnover, and victims may seek reimbursement if proper controls are not in place.

Conclusion

The regulations of the United Kingdom, European Union, Singapore, and Australia all focus on tackling digital scams. Their approaches have many similarities but each has unique elements.

First of all, the latest regulatory initiatives in the UK, EU, and Australia focus on tackling APP fraud, while Singapore focuses only on phishing scams. With the significant increase of APP fraud globally, Singapore could enhance consumer protection by including social engineering scams and scams originating outside Singapore into the SPF.

The EU, Singapore, and Australia follow a cross-sector approach, involving not only Payment Service Providers, but also telecommunications providers. In the EU and Australia, the scope is further enlarged to digital platform service providers. The UK, on the other hand, focuses primarily on payment service providers, with limited involvement of other sectors. A cross-sector approach might be more effective at tackling APP fraud, and also distribute the liability of APP fraud more evenly.

Mandatory reimbursement of fraud victims is present in the regulations in the UK, EU, and Singapore, but is absent in Australia. Australia does not mandate formal victim compensation, but it emphasizes real-time intelligence sharing and scam disruption in order to prevent APP scams.

In terms of technical countermeasures, confirmation of payee is the main mechanism to prevent APP fraud in the UK, EU, and Australia. However only the UK focuses on behavioural analytics, which is useful to detect APP scams at the sending and receiving PSP, and transaction monitoring for incoming transactions, which is a meaningful approach to detect money mule accounts at the receiving PSP.

In the coming years it will be interesting to see which regulatory approach will be the most successful at tackling APP scams and whether the measures suffice to keep up with increasingly sophisticated scams. It can also be hoped that other countries and regions take similar regulatory steps to protect consumers and businesses.

About the author

Frederik Mennes is Director of Product Management & Business Strategy at OneSpan. In this role, he is responsible for defining and implementing OneSpan's business strategy for specific industry verticals, and to determine how OneSpan responds to security and regulatory market trends. Previously, Frederik led OneSpan's Security Competence Center, where he was responsible for the security aspects of OneSpan's products and infrastructure. He has an in-depth knowledge of authentication, identity management, and security technology in general.

For more information or to discuss regulatory developments and compliance in more detail for your business, contact the author at frederik.mennes@onespan.com.

About OneSpan

OneSpan helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at
OneSpan.com

Contact us at
OneSpan.com/contact-us

OneSpan