Elmore

Green Swan Compliance

Authorised Push Payment (APP) Fraud Reimbursement Insurance

Executive Summary

This e-guide examines the rationale behind introducing the new and far-reaching APP reimbursement regulations by the Payment System Regulator (PSR) that will apply to over 1,000 UK firms under Special Directive 20 (SD20), and how the insurance industry can help mitigate potentially far-reaching unintended APP-related industry risks.

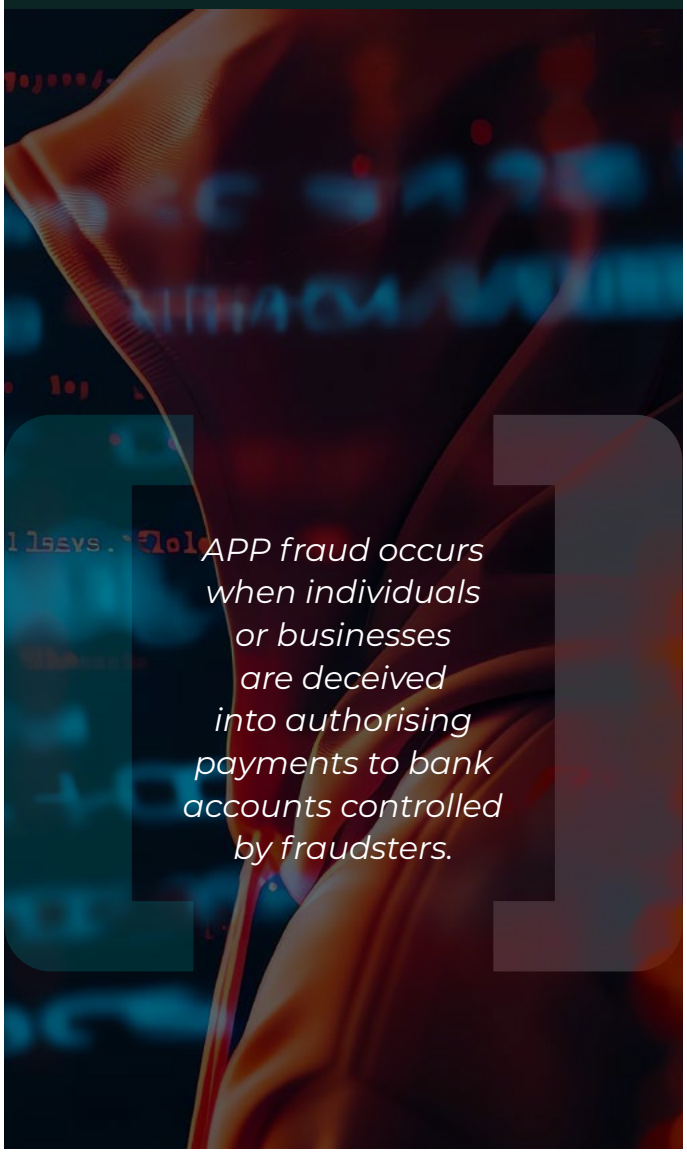
APP fraud reimbursement insurance is now available as part of the risk mitigation measures that firms can use to mitigate what may be severe and unintended industry-wide risks from these new regulations - particularly those firms that now have APP liability when receiving UK Faster Payments and CHAPS.

The new APP rules come into force on the 7th of October 2024 and are a potential minefield for many unprepared Financial Institutions (FI) - particularly small to medium-sized firms. Although this new bold action is designed to help improve fraud prevention, it is highly likely to create significant new risks and have unintended consequences for many UK banks, E-Money Institutions (EMIs), and Authorised Payments Institutions (APIs) as well as their Agents and Distributors.

In partnership with **Elmore Insurance Brokers** APP insurance is now available to qualifying UK banks, Payment Service Providers (PSPs), EMIs and APIs. Our new-to-market, innovative solution takes a proactive approach to insurance, combining our digital patented audit technology, **Regulatory Audits as a Service (RAaaS)** to help mitigate risk and exposure from these new regulations.

Due to the complex nature of APP fraud, getting insurance and keeping APP insurance coverage requires forward planning by firms that they need to start now, as well as a disciplined approach to compliance auditing and controls to ensure that the maximum amount of insurance is available for the premium paid. This guide also explains the process that has been developed with the insurance industry to make the application process and the audit verification and monitoring process as digital as possible for all concerned.

Table of Contents



1.0 Background to APP fraud

1.1. APP fraud occurs when individuals or businesses are deceived into authorising payments to bank accounts controlled by fraudsters. This type of fraud often involves impersonation scams, invoice fraud, investment scams, etc.

1.2. According to UK Finance, APP fraud losses in the UK reached £459m in 2023.

1.3. Today, most of the major banks in the UK are already part of the Contingent Reimbursement Model to reimburse vulnerable customers' loss due to APP fraud.

1.4. Coming into effect 7th October 2024, the new APP fraud reimbursement regulation mandates that PSPs must reimburse victims of APP fraud over the Faster Payment System (FPS) including banks, e-money institutions and some authorised payments institutions.

1.5. Payments of up to £415,000 are covered, and reimbursements must be made within five business days of the fraudulent payment report being received.

1.6. Sending PSPs can deny APP fraud claims submitted more than 13 months after the final payment to the fraudster (although the customer could still take its claim to the FOS if the PSP opts to deny the claim).

1.7. While the sending PSPs will make the initial reimbursement payment (apply a claim excess of £100), the receiving PSP will be liable to pay the sending PSPs 50% of the reimbursed amount.

1.8. The reimbursement obligation will apply to consumers, micro-enterprises and charities.

1.9. The PSP will have to reimburse the customer, if vulnerable, regardless of whether the customer acted with gross negligence and without applying any excess.

1.10. These new requirements create a significant financial risk for most of the smaller banks, EMIs and payment firms, further exacerbated for EMIs (Banking as a Service fintechs) who operate with a network of Agents and Distributors acting on their behalf.

1.11 The **PSR** has consulted the industry for some time on these new regulations and requests for them to be delayed or amended have been rejected. It is unlikely that the new government will do a U-Turn on these regulations and as a result the industry needs to focus quickly on implementation and risk reduction measures.

2.0. Main types of APP fraud

2.1. Impersonation Fraud

a. Impersonation of Banks or Officials

Fraudsters pose as bank representatives, police officers, FCA, FOS or other officials to convince victims that their money is at risk and needs to be transferred to a 'safe' account.

b. Impersonation of Family Members or Friends

Scammers impersonate friends or family members in distress, asking for urgent financial help.

2.2. Invoice or Mandate Fraud

Fraudsters intercept legitimate invoices or create fake ones, tricking businesses or individuals into paying the fraudster's account instead of the legitimate payee's account. This often involves changing the bank account details on an invoice.

2.3. Purchase Fraud

Victims are deceived into paying in advance for goods or services (like online shopping or holiday rentals) that do not exist or are never delivered.

2.4. Investment Fraud

Scammers offer fake investment opportunities promising high returns. These can include schemes involving stocks, bonds, cryptocurrencies, or property.

2.5. Romance Fraud

Fraudsters build online relationships with victims, gaining their trust over time before fabricating a financial emergency and requesting money.

2.6. CEO or Business Email Compromise (BEC) Fraud

Scammers impersonate senior executives or business contacts through email, instructing employees to make urgent payments to the fraudster's account.

2.7. Advance Fee Fraud

Victims are asked to pay an upfront fee for a service or product that never materialises, such as loans, lottery winnings, or inheritances.

2.8. Rental Fraud

Fraudsters advertise properties for rent that they do not own or that do not exist. Victims pay deposits or rent in advance and find out later that they have been scammed.

2.9. Refund Fraud

Scammers claim to be from a company that owes the victim a refund. They trick the victim into 'accidentally' sending too much money and then request the excess amount to be returned.

2.10. Cryptocurrency Fraud

Victims are deceived into sending cryptocurrency to fraudsters under the pretence of investments, purchases, or other opportunities.

2.11. Fake Charities

Fraudsters pose as charities or use the cover of a charitable cause to solicit donations that go directly into their accounts.

2.12. Employment Fraud

Victims are offered jobs and asked to pay for training materials, background checks, or other fees, but the job does not exist.

2.13. Ticket Fraud

Scammers sell fake tickets for concerts, sports events, or other activities. Victims pay for tickets that either do not exist or are not valid.

Note: New types of fraud are likely to emerge after 7th October 2024.

3.0. Payment Systems Regulator – Specific Direction 20 (SD20)

3.1. The PSR has issued guidance on the new fraud reimbursement rules, set by the operator of Faster Payments, Pay.UK, under **Specific Direction 20 (SD20)**. This requires PSPs to follow certain rules for reimbursing victims of authorised push payment (APP) fraud. All firms are responsible for determining their legal obligations and all firms that participate in FPS and provide relevant accounts must comply with SD20 and the FPS reimbursement rules unless they can demonstrate otherwise.

3.2. The following definitions are all covered under SD20:

3.2.1. Account controlled by the consumer means a relevant account that a consumer can access and make payments from. It is not sufficient for it to be in the consumer's name.

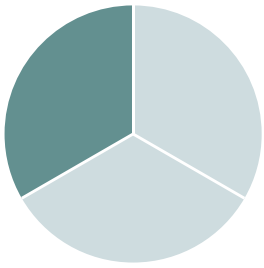
3.2.2. Authorised push payment (APP) means a consumer payment initiated by the sending PSP in accordance with an authorisation given by its consumer.

3.2.3. APP scam (authorised push payment scam) means where a person uses a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade a consumer into transferring funds from the consumer's relevant account to a relevant account not controlled by the consumer, where:

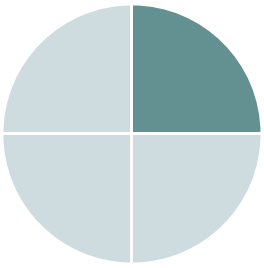
i) the recipient is not who the consumer intended to pay, or

ii) the payment is not for the purpose the consumer intended

For the avoidance of doubt, if the consumer is party to the fraud or dishonesty, this is not an APP scam for the purpose of the FPS reimbursement requirement, or the FPS reimbursement rules.

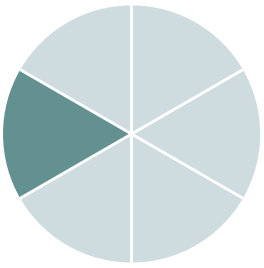


1 in 3 consumers have fallen victim to an APP scam

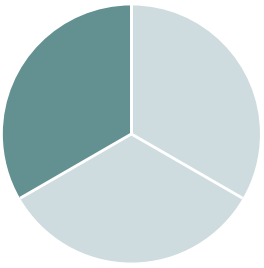


25% of APP fraud cases are identified by the victim's bank

4 in 5 APP scam victims are reimbursed



15% of APP scam victims leave their bank



1 in 3 victims report that their mental health has suffered

3.2.4. Authorisation for the purpose of SD20, in the context of a payment means that the payer has given their explicit consent to:

i) the execution of the payment transaction, or

ii) the execution of a series of payment transactions of which that payment transaction forms part

3.2.5. Consumer for the purposes of SD20, refers to service users of PSPs. These are individuals, micro-enterprises (an enterprise that employs fewer than ten persons and that has either an annual turnover or annual balance sheet total that does not exceed €2 million) or charities (a body whose annual income is less than £1 million per year and is a charity as defined by the Charities Act 2011, Charities and Trustee Investment (Scotland) Act 2005 or the Charities Act (Northern Ireland) 2008).

3.2.6. Directed PSP means a PSP participating in the Faster Payments scheme to which SD20 applies.

3.2.7. Faster Payments Scheme or FPS means the Faster Payments scheme, a regulated payment system designated by Order from the Treasury on 1 April 2015.

3.2.8. FPS APP scam claim means one or more FPS APP scam payments made as part of an APP scam and made to the victim's PSP.

3.2.9. FPS APP scam payment for the purposes of this direction, means an APP, authorised by a victim as part of an APP scam, that has all the following features:

i) It is executed through the Faster Payments scheme.

ii) It is authorised by a PSP's consumer.

iii) It is executed by that PSP in the UK.

iv) The payment is received in a relevant account in the UK that is not controlled by the consumer.

v) The payment is not to the recipient the consumer intended or is not for the purpose the consumer intended.

3.2.10. FPS reimbursement requirement means the obligation conferred on directed PSPs under paragraph 3.1 of SD20.

3.2.11. FPS reimbursement rules means any rules created as a result of Specific Requirement 1 (Faster Payments APP scam reimbursement rules) imposed on the Faster Payments scheme operator to create and implement rules on PSPs reimbursing their consumers when they fall victim to APP scams.

3.2.12. Indirect access provider means a PSP with access to the Faster Payments Scheme that has an agreement or arrangements with another person for the purpose of enabling that other person (the 'indirect PSP customer') to provide services for the purposes of enabling the transfer of funds using the Faster Payments scheme or to become a PSP in relation to the Faster Payments Scheme.

3.2.13. Member of the Faster Payments Scheme means a directly connected settling or directly connected non-settling participant.

3.2.14. Operator has the same meaning as under section 42(3) of Financial Services Banking Reform Act 2013 (FSBRA) in relation to the Faster Payments Scheme. The term Faster Payments Scheme operator is to be understood accordingly.

i) Participant has the same meaning as under section 42(2) of FSBRA.

ii) Payment System has the same meaning as under section 41(1) of FSBRA.

iii) Payment Systems Regulator (PSR) is the body corporate established under section 40 of FSBRA.

3.2.14. Payment service provider (PSP) has the same meaning as under section 42(5) of FSBRA.

3.2.15. Reimbursable FPS APP scam payment means an FPS APP scam payment where the consumer standard of caution exception does not apply, the victim is not party to the fraud or claiming fraudulently or dishonestly to have been defrauded and the claim was made within the time limit set out in the reimbursement rules.

3.2.16. Relevant account means an account that is provided to a service user, is held in the UK and can send or receive payments using the Faster Payments Scheme, but excludes accounts provided by credit unions, municipal banks and national savings banks.

3.2.17. Sending PSP means a PSP that provides a relevant account for a consumer, from which one or more FPS APP scam payments were made.

3.2.18. Service user means a person who uses a service provided by a payment system and is not a participant in that payment system.

3.2.19. Victim means a consumer who has made one or more FPS APP scam payments.

3.3. The full SD20 Reimbursement Requirements document can be viewed **here**.

4.0. What does this mean for PSPs?

4.1. All PSPs must implement robust fraud detection and prevention measures, including advanced cybersecurity protocols and educate their customers to recognise and avoid scams.

4.2. They must also make sure that they communicate clearly with their customers about the reimbursement process and what customers need to do if they fall victim to fraud.

4.3. EMI principals and agency banking providers will be exposed via their agent and distributor network; enhanced oversight and controls are paramount.

4.4. Most importantly, planning to cover the cost of reimbursing fraud victims is crucial. However, it is these mandatory payouts which expose the PSPs financially, and for the smaller organisations in particular, could have devastating consequences.

5.0. APP fraud reimbursement insurance

5.1. The Intended outcome of the new APP regulations is to reduce APP fraud by providing direct financial incentives for Financial Institutions (FI) to improve the number, quality and sophistication of not only their own direct APP control, but also those of other FIs in the payments chain with the 50% flow down provision. There are likely to be a number of unintended and serious consequences for FIs.

5.2. Getting APP insurance is one risk reduction measure that you can apply to your risk-based approach. The nature of your business, the way you treat and track vulnerable customers, the quality of your systems, people and processes and the sophistication of your controls, will all impact your ability to prove that there was no gross negligence should your business have to refund an APP transaction, and that a customer was not 'vulnerable' at that time.

5.3. Many factors will impact your ability to get APP Reimbursement Insurance and the pricing of this insurance will be based on a mandatory Remote Access as a Service (RAaaS) Compliance Audit (point 7), so we can clearly understand the mitigation controls you currently have in place and your exposure level.

5.4. The insurance policy will only cover the high spikes not your run rate fraud.

5.5. Eligible Participants: All participants within the Faster Payments Service (FPS) can obtain insurance, including:

i) EMI principals

ii) Banks offering agency banking

II) Individual agents and distributors

5.6. This insurance ensures that PSPs can comply with regulations while maintaining financial stability.

5.7. Risk Assessment: The insurance risk is high due to the prevalence of APP fraud. Effective fraud prevention measures are crucial for reducing exposure.

5.8. Robust measures include:

i) Confirmation of Payee

ii) Enhanced customer onboarding such as CIFAS checks

III) Strong cybersecurity protocols: including SCA and authorisation methods

iv) Customer education and communication be vigilant and prevent gross negligence

v) Robust anti-fraud verification process: Including high risk payment verification and cool-off periods for large payments

5.9. Insurable PSPs:

i) Banks and Financial Institutions with established fraud monitoring systems and secure transactional environments (mentioned above)

ii Fintechs: particularly in need of reimbursement to cover the cost of reimbursement loss, specifically for any fraud spikes.

6.0. APP fraud Regulatory Audit as a Service (RAaaS)

6.1. The APP RAaaS will review the risk mitigation and compliance controls that you have in place and it is intended, primarily, to provide the data to the underwriters to allow them to provide a risk based decision for your insurance policy - it is not intended to provide you with a consulting recommendations report for reducing this risk*.

Risk Mitigation measures for reducing APP fraud include, but not limited to:

6.1.1. Compliance

i) Culture of compliance in your FI.

ii) Adherence to the FCA 12 principles – especially consumer duty.

iii) Good quality and well-documented policies, procedures, and processes are implemented and followed in practice.

iv) Quality HR processes, team training and education.

v) Warnings and UKFP 'cooling off periods for suspicious transaction' (and how they have been implemented and whether they are sufficient to support gross negligence).

vi) The quality and nature of your past compliance audits and those of your suppliers (including banking partners and client money banking partners where relevant).

6.1.2. APP Mitigation Processes

i) The nature of your business and its risk profile to APP fraud typologies.

ii) Effective use of real-time APP fraud detection technology.

ii) Effective KYC/KYB and regular refreshes.

iv) Confirmation of Payee implementation.

v) CIFAS membership and effective use of this system and fast collaboration with other FI and CIFAS members.

vi) Fraud team size, quality, structure, tools, data, SLAs, 24x7 operations and empowerment.

vii) GIMLET membership (not open to all FIs).

viii) The nature and quality of your past fraud data including FOS complaints and general complaints.

ix) Other terms and conditions on your contracts and supply chain partners that related to APP controls and risk mitigation.

6.1.3. Consumers

i) Consumer education and warnings.

ii) Vulnerable customers – tracking them in your CRM and the application of FCA regulations as they relate to APP.

iii) Methods of communications with customers and your FI ability to demonstrate these in contested and legal situations.

6.1.4. Payment Procedures

i) Payment limits (sending and receiving), especially those relating to new payees and new receiving accounts and their cumulative values.

ii) Processes and procedures for tracking high-risk business (including crypto, FX, NFT and non-FIAT products) as well as those goods and services purchased online.

iii) Policies and procedures for refunding and paying APP reimbursement to customers and to receiving FIs, with and without consumer challenge and/or legal challenge.

6.1.5. Protection

i) The level of your APP insurance to cover fraud spikes.

ii) The level of insurance for wind down cover in the event that your FI were to hit a wind down trigger from APP fraud reimbursement.

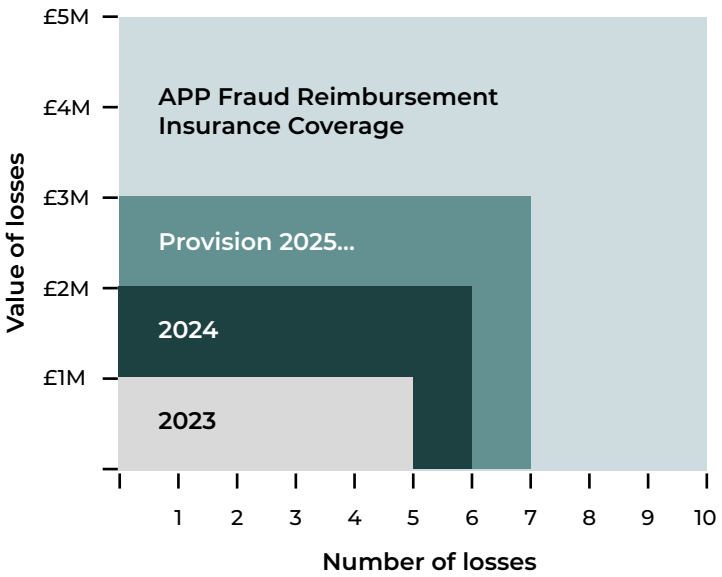
iii) Cyber insurance and other insurance policies that may offer additional cover to your APP insurance policy.

6.2. APP Fraud Reimbursement Insurance

Products will be tailored to your individual requirements with the application and supervision process supported by Green Swan's digital compliance services.
*Please contact Green Swan Compliance separately should you require bespoke advice or support - **contact us**

6.3. APP Fraud Reimbursement Insurance Overview

Insurers will provide coverage for losses in excess of your provisioned APP loss rate. There will be a rate range from conservative to aggressive depending on the proximity of coverage to provisioned losses.



7.0. APP Insurance Application and Risk Monitoring Process

7.1. The following standard steps may be adapted to individual firms' requirements and should be regarded as indicative:

1. Request an initial meeting (mutual NDA applies) with Green Swan Compliance and Elmore Insurance Brokers.
2. Initial meeting normally via video call or face-to-face at the Lloyd's building.
3. Completion of the initial insurance form questionnaire for a draft quotation for a SD20 firm.
4. Additional information requests from underwriters.
5. Indicative insurance quote and legal terms presented to SD20 firm.
6. SD20 firm commissions APP insurance audit with Green Swan.
7. Completed APP insurance application form and APP audit report presented to underwriters for final quotation and policy confirmation.
8. Insurance documents signed and premium paid for by SD20 firm.
9. Weekly/monthly submission of loss data, and any additional audit updates as agreed in policy terms.
10. Risk updates and digital APP audits by Green Swan Compliance to provide updated risk profiling and assessment of controls to underwriters during the term of the insurance cover, as agreed in the policy Terms and Conditions.

Further Reading:
The PSR has also produced detailed guidance on APP fraud, including FAQs and information on related topics, which you can access **here**

Elmore

Green Swan Compliance

ELMORE

Elmore is a specialist risk and insurance intermediary offering advisory, broking, and claims management services to businesses from start-up to enterprise.

We provide professional advice and support at every stage of an insurance transaction. We simplify buying processes and make insuring new risks accessible to businesses of all sizes.

Telephone: +44 (0)207 118 1839
Website: elmorebrokers.com
Email: info@elmorebrokers.com

Simon Gilbert - Managing Director
simon.gilbert@elmorebrokers.com

GREEN SWAN COMPLIANCE

Green Swan Compliance are a team of experienced EMI practitioners with first-hand experience in launching new EMI businesses and day2day EMI operations from start-ups to global enterprises.

We are well-versed in the challenges of operating as an EMI principle with Agents and Distributors, and the practical limitations of being an Agent.

Website: greenswancompliance.com
Email: hello@greenswancompliance.com

Leven Li - Director/Co-Founder
leven@greenswancompliance.com