Defending against APP Fraud

Cases of authorised push payment (APP) across the whole financial service sector rose 12% last year, according to industry body UK Finance. Kym Routledge, BCB Group's Global Head of Compliance, explains the latest regulations on APP fraud, how BCB is working to protect clients and what clients themselves can do to minimise the risks.

What is Authorised Push Payment (APP) fraud?

Authorised Push Payment (APP) fraud is when a victim is **tricked or deceived into authorising a payment** from their own bank account directly to a fraudster's account. Unlike unauthorised fraud (where a payment is made without the account holder's permission, such as a stolen card), in APP fraud, the victim intends to make the payment and authorises it themselves, but they are deceived as to the true recipient or the purpose of the payment.

Common types of APP fraud include:

Impersonation Scams: Fraudsters pretend to be a trusted entity such as a bank, police, HMRC, a utility company, or even a friend/family member, persuading the victim to transfer money.

Invoice Scams/Supplier Impersonation: Businesses are tricked into paying fraudsters sending fake invoices or altered bank details from what looks like a legitimate supplier.

Purchase Scams: Victims pay for goods or services that never materialise or are significantly different from what was advertised.

Investment Scams: Victims are persuaded to "invest" money in fake schemes with promises of high returns.

Romance Scams: Fraudsters build relationships with victims online and then ask for money for fabricated emergencies or investments.

Employment Scams: Fraudsters pose as recruiters or employers, tricking job seekers into making upfront payments for fake equipment, training, or background checks, or into "refunding" overpayments from fraudulent cheques.

BCB GROUP

How to protect yourself from APP Fraud?

As an account holder in charge of all payments from your account, you are the first and best line of defence against APP fraud. Never authorise a payment to a new payee without double-checking (or triple-checking) their identity.

A key tool for these checks is Confirmation of Payee (CoP), in which the account details provided by a payee are cross-checked with the name on the account. As the person controlling the funds, the first responsibility naturally lies with the account holder, but BCB can provide help in making these checks.

How is BCB Group helping to reduce the risk of APP fraud?

Robust due diligence
BCB Group's rigorous onboarding process includes client due diligence and enhanced due diligence of new clients. In the case of commercial partners such as exchanges, this involved stringent standards for their own fraud controls. Because all our clients are onboarded in this way, clients can make payments to another BCB customer account through our proprietary BLINC system with complete confidence.

Proactive fraud prevention
BCB operates an internal system for monitoring transactions, including AI systems to detect suspicious patterns in payments processed for its clients that may be indicative of APP fraud. This helps identify and flag potentially fraudulent transactions before they complete. We also operate sophisticated controls to identify and potentially delay suspicious outgoing payments originating from BCB's clients, providing an additional layer Wof defence against APP fraud.

Working with industry partners
BCB's position as a global payment services provider involves a wide network of business partners from technology companies to payment rails providers and global banks. We are constantly extending our collaboration with those partners to share information on APP fraud and work together to defend our customers.

BCB GROUP

The Payment Systems Reimbursement Regime

Because APP fraud involves an authorised payment, it has historically been difficult to prove and to recover funds lost to APP fraudsters. In a bid to crack down on fraudsters and protect consumers, the Payment Systems Regulator (PSR) (now part of the Financial Conduct Authority) introduced new rules in 2024 stating how payment service providers such as BCB Group should handle APP cases, and how to determine when a reimbursement should be paid. This new regime aims to significantly increase the rate of reimbursement for APP fraud victims.

Who can claim for reimbursement?
The scheme covers retail consumers, micro-enterprises (those that employ less than 10 people and have a balance sheet of less than £10 million) and small charities (with annual incomes under 1 million).

Who pays?
The cost of reimbursement is split 50:50 between the sending PSP (the victim's bank/PSP) and the receiving PSP (the fraudster's bank/PSP).

What types of payments are covered?
The main payment rails covered by the reimbursement regime are the Faster Payments System (FPS) and retail CHAPS payments made in the UK, in pounds sterling.
How much money can be reimbursed?
Victims can recover up to £85,000 per claim. Sending PSPs may in some circumstances apply an optional excess of up to £100 per claim, this would be explained to the victim when they raise the fraud claim.

How soon do I need to report an APP fraud if I want to claim reimbursement?
Victims have up to 13 months from the date of the last fraudulent payment to report the fraud to their PSP.

What information do I need to provide to make a claim?
The details needed will vary from case to case, but the PSR rules require victims to cooperate with their PSP's reasonable requests for information to assess the claim. Naturally, victims are not entitled to reimbursement if they have themselves acted fraudulently or with 'gross negligence'.

BCB Group has established an efficient internal process for receiving, investigating and processing APP fraud reimbursement claims where we are the sending or receiving payment service provider.

BCB GROUP