Authorized Payment Protection

Empowering account-to-account payment processors, banks and, peer-to-peer platforms to conduct real-time risk evaluations at point of payment, to combat Authorized Push Payment fraud

equifax.co.uk/business

Combatting Authorized Push Payment fraud: A growing financial and regulatory burden

The shift towards real-time payments has driven innovation but has also led to a significant increase in **authorized push payment fraud**.

This sophisticated form of scam occurs when fraudsters deceive and socially engineer customers into willingly authorising an account-to-account (A2A) transfer to an account under false pretences.

Unlike traditional fraud, the payment is authorised by the customer, making instant settlement a major challenge for detection and recovery. The ease and speed of these payments, coupled with the ability of criminals to use tools like generative AI to create convincing scams, make authorized push payment fraud **increasingly pervasive and difficult to counteract.**

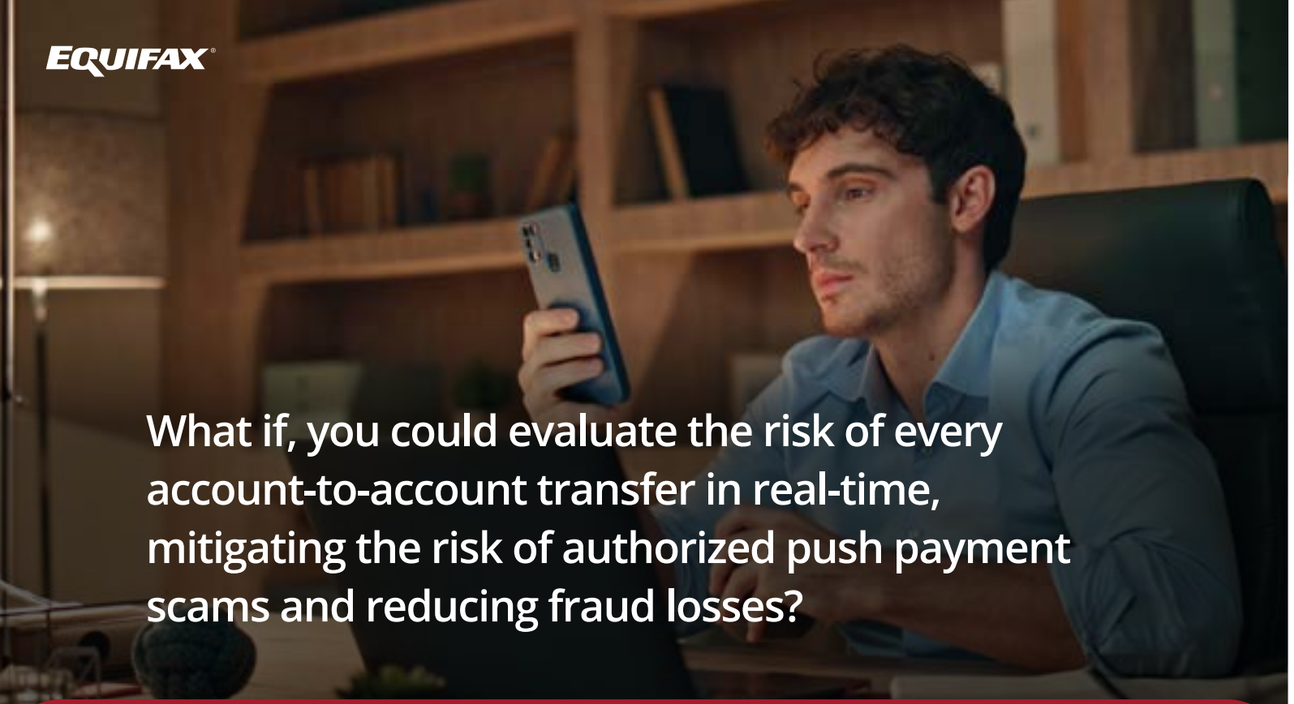
The financial and regulatory stakes are escalating. In the first half of 2025, **£257 million** was lost to Authorized Push Payment fraud in the UK, a **12% increase** from the previous year, with only **62% of stolen funds** being returned to victims[1].

Globally, authorized push payment fraud is reaching alarming levels, and is predicted to reach $331 billion worldwide by 2027[2].

Authorized push payment fraud now represents 40% of all fraud losses in the UK[1] and regulations mandate that the sending bank or Payment Service Providers (PSPs) reimburse customers for most authorized push payment fraud cases within five working days, up to £85,000 per claim, with a 50/50 liability split between sending and receiving PSPs.

To combat this, banks and PSPs can delay payments if fraud is suspected, provided adequate warnings are given. The Payment Systems Regulator (PSR) now requires warnings to clearly assess the probability of an authorized push payment scam, for example "This specific destination account is linked to high-risk activity".

This necessitates real-time, robust monitoring systems and highly granular risk scoring for every transaction.



What if, you could evaluate the risk of every account-to-account transfer in real-time, mitigating the risk of authorized push payment scams and reducing fraud losses?

Authorized Payment Protection, is a purpose-built solution designed for real-time authorized push payment fraud prevention, giving you the dedicated capability you need to comply with new rules, prevent losses, and protect your customers.

At its core, is real-time transaction monitoring of A2A transfers, which forms an essential safeguard. Our solution gives you the option of analysing key attributes of the destination account to provide a risk assessment, helping ensure consumers are not being scammed.

This approach is essential for staying ahead of threats, especially as generative AI makes it easier for fraudsters to create convincing scams at scale.

Authorized Payment Protection is delivered via our advanced platform and leverages Equifax's data network and fraud consortium.

When one of your customers makes an A2A payment, our solution instantly analyses hundreds of data points, such as the device being used, its location, and the transaction history.

This allows you to detect and prevent fraudulent transactions, protecting both your business and your customers from financial loss.

Key benefits

The following quantifiable benefits demonstrate the value of Authorized Payment Protection to your business:

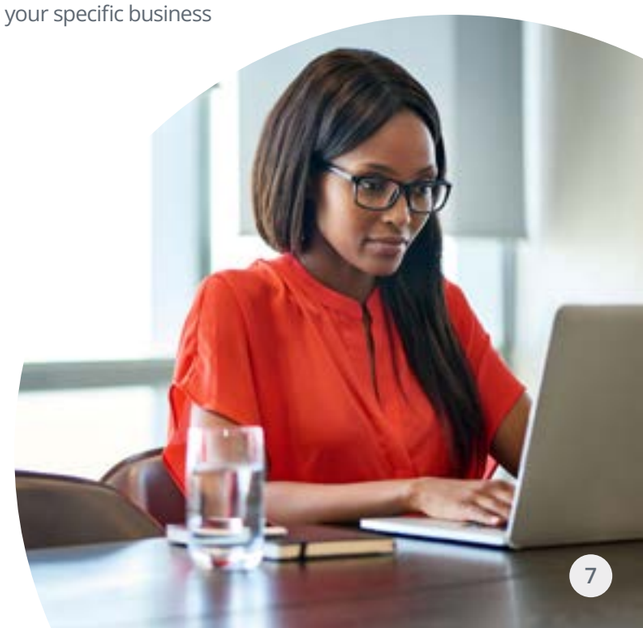
Minimise losses from authorized push payment fraud by proactively identifying and preventing fraudulent transactions before processing. This is achieved through a specialized fraud network that focuses on destination account risks, helping to detect and disrupt the use of money mule accounts.

Help preserve consumer trust and your reputation by safeguarding your customers from sophisticated scams and financial loss.

Protect your business from fines and regulatory losses by adopting robust fraud monitoring required to meet mandatory reimbursement standards.

Maintain operational efficiency by ensuring legitimate payments go through smoothly while flagging risks for minor friction review, instead of outright denial.

Gain full, granular control: Manage risk thresholds, allowing you to tailor protection to your specific business and customer needs.



How it works

Authorized Payment Protection is embedded into your real-time payment systems to enable you to evaluate the risk of each A2A transaction instantly. It screens both the origin and destination accounts to provide a full risk assessment.

Payee initiates transfer

When a customer initiates an **A2A payment**, transaction details are immediately shared to the platform via a dedicated Risk API, ensuring rapid and secure data exchange for instantaneous evaluation.

Real-time risk evaluation

Our real-time transaction monitoring immediately analyses the **transaction** and hundreds of **data points**, including the **device** being used, its **location**, and the **transaction history**.
When destination accounts are integrated with our tool, our proprietary AI-powered model assesses key attributes like linked **transaction velocities**, **account history**, and **known fraud**, leveraging our fraud consortium for critical insights.

Risk score calculated

A **highly granular risk scoring** is provided for every transaction and a recommended action. A low score suggests normal processing, while a high score recommends blocking the transaction.

Custom policy application

Your team applies **customisable business policies** to approve, deny, or apply minor friction for manual review based on the risk score. This ensures good customers enjoy a seamless experience while preventing the riskiest payments.

Approve | **Decline** | **Review**

Feedback loop

A crucial feedback loop continuously refines the **model's accuracy**.

Key features

Our Authorized Payment Protection solution is comprised of core components:

Comprehensive view of accounts

Addresses push payment fraud from both origination and destination accounts, using device biometric data and a global fraud network for real-time risk signals.

Fraud consortium

Leverages an extensive network with mandatory fraud reporting feedback to immediately detect and stop known scams across multiple institutions and borders.

Policy management

A robust policy engine for real-time creation and deployment of rules, enabling you to tailor, approve, review, and deny outcomes to your business's specific risk tolerance.

Event analysis and case management

Our user interface provides an in-depth view of risks associated with an A2A transaction for investigation and allows for optional application of minor friction for review without outright denial.

Reporting and analytics

Custom reports can be created on demand using data available in the platform to track performance and trends.

Implementation

Simple Integration

Integration is typically handled through a consolidated API schema for a single platform delivery that enables simplistic integration and scalability, or through a user interface for event analysis and case management.

Customer Lifecycle Fit

Authorized Payment Protection can be embedded into your real-time payment systems. This placement allows you to evaluate the risk of a transaction before it is completed, making it a powerful, pre-emptive tool in your fraud prevention operational model.

Why Equifax?

Choosing Equifax means gaining a partner with a unique and powerful advantage in the fight against fraud.

Purpose-built solution

Our solution has been purpose-built to combat authorized push payment fraud, offering superior protection against evolving scams, unlike generic solutions or those focused solely on account takeover.

Global risk demands a global solution

We leverage decades of robust data collected across numerous industries worldwide to provide tried and tested protection against various global threats.

Broader data sets

We're not focused solely on behavioral biometrics. Equifax has broad data sets that generate a comprehensive view of both parties in an A2A transaction.

Simplified protection via a single platform

We can help you simplify the management of all fraud prevention via a single platform, from real-time alerts to case investigation and reporting, enhancing your operational efficiency.

Addressing inherent issues of A2A payments

The authorized nature of the A2A payments, the speed of transactions, limited visibility of destination accounts, and the evolving tactics of social engineering means financial institutions and PSPs are facing significant challenges in detection and prevention of fraud. We delve into each of these critical issues below:

The payment is authorized

The problem

Unlike other fraud types, authorized push payment fraud involves victims willingly transferring funds, making it difficult for traditional bank systems to detect, as all technical security checks are passed masking the underlying criminal intent.

The challenge for banks/PSPs

Existing fraud systems are designed to look for indicators of unauthorised activity (e.g., suspicious IP addresses, unusual devices, or high-velocity transactions).

How Equifax can help

We provide real-time, destination account analysis, identifying subtle patterns in the receiving account's behavior that traditional systems may miss, even when the payment is authorized by the customer.

The speed of real-time payments

The problem

The instantaneous nature of real-time payment systems means funds are quickly moved, leaving little time to intervene once a scam is realised.

The challenge for banks/PSPs

By the time a customer realises they've been scammed (or existing systems flag the payment as suspicious), the money has already been withdrawn or moved on using "mule accounts". This leaves little time to intervene to freeze the funds.

How Equifax can help

Our solution is embedded directly into the real-time payment flow, allowing for intervention before the final authorization, thus freezing funds before they are lost.

Limited visibility of the destination account

The problem

A bank or PSP primarily focuses on its own customer (the sender). They have limited visibility into the risk profile of the receiving account at another bank.

The challenge for banks/PSPs

Whilst unusual customer behaviour can sometimes be detected using existing systems, it's not easy to determine if the destination account is a newly opened mule account, an account that has received suspicious transfers from other fraud victims, or if the account details are already blacklisted across the industry.

How Equifax can help

We leverage a fraud network and consortium data to instantly assess the risk of the receiving account, providing the missing cross-industry view.

Evolving social engineering tactics

The problem

Fraudsters constantly evolve their methods, using sophisticated social engineering and AI to manipulate customers into deliberately circumventing security warnings.

The challenge for banks/PSPs

No amount of technical security can completely safeguard against a determined and persuasive criminal manipulating a customer into deliberately circumventing security warnings.

How Equifax can help

Our solution's real-time risk assessment and destination account intelligence provide a robust layer of defence by flagging high-risk transactions, even when a customer has been manipulated. This allows for intervention or enhanced warnings to be presented to the customer.

EQUIFAX®

Take the next step

Book a free consultation with one of our fraud experts today.

Discover how we can help you mitigate your specific authorized push payment fraud risks and secure your real-time payment systems.

Speak to our experts

contactus@equifax.com | equifax.co.uk/business

Sources
[1]UK Finance Half Year Fraud Report H1 2025
[2]LSEG Risk Intelligence 2025