



Authorised Push Payment (APP) fraud prevention and Mule Detection

For Safer Payments in Banking

SECTION 01

Executive Thesis.

Real-time payments and mandatory reimbursement have moved APP fraud and mule activity upstream — European banks now need consumer trust intelligence at three decision points: **payment authorisation, account opening and ongoing monitoring, and reimbursement decisioning.**

SECTION 02

Key Findings.

01

Authorised Push Payment (APP) fraud is not an isolated fraud problem.

APP fraud sits inside a wider ecosystem of trust-based fraud — friendly fraud, chargeback misuse, refund and INR claims, mule activation. Purchase scams are structurally identical to the first-party fraud dominating merchant payments. Banks can leverage merchant-side trust intelligence to make APP defence proactive rather than reactive.

03

Mule accounts active across the banking network are the infrastructure that enables APP fraud proceeds to move.

Every APP fraud requires a receiving account. Mule accounts are the infrastructure that moves the proceeds. Most current scam detection stops the victim from sending — it does not disrupt the receiving infrastructure, which remains live for the next victim.

02

Banks can see their account holders, but have limited visibility of the other half of the transaction.

An issuing bank sees its own customer; it cannot see the receiving account. The fraud succeeds in the gap — a payment that looks unremarkable from one side, an account that looks clean from the other. Strong Customer Authentication cannot stop fraud the legitimate customer has authorised.

04

Mule accounts are activated by circumstance, and evade fraud detection focused on thin-file accounts.

Mule accounts are not synthetic identities. They are real accounts activated in-life by recruitment, coercion or financial pressure — long after onboarding controls have cleared them. Onboarding controls built for thin-file risk cannot see this. The weakest point in mule defence has shifted from onboarding to in-life.

05

Trust signals applied before authorisation prevent losses; the same signals at dispute make reimbursement decisions defensible.

Once funds clear a real-time payment rail, recovery is the exception. The trust intelligence that prevents APP fraud upstream — vulnerability, scam typology, intervention history, receiving-account behaviour — captured at the moment of dispute becomes the defensible evidence for reimbursement.

SECTION 03

Why This Matters to Banks.

For European banks, APP fraud is now a **P&L, compliance and customer-experience problem at once**. Mandatory reimbursement is live under the UK PSR; SEPA Instant has made post-hoc remediation impossible. Exposure compounds across all three decision points.

EVIDENCE · METRICS

€167_m · £144.4_m

Investment scams drove the largest UK APP losses by value in 2024 (+34% YoY).

FINDING 1 · SOURCE ¹

€2.2_{bn}

EEA credit-transfer fraud in 2024 (+16% YoY); 85% of losses borne by payment service users tricked into initiating fraudulent transactions.

FINDING 2 · SOURCE ²

10,759 · 226,957

Europol EMMA 2025 identified 10,759 mule accounts across 26 European countries; UK banks closed 226,957 mules in 2024 (+23% YoY).

FINDING 3 · SOURCES ³, ¹

SECTION 04

Adoption & Regulation.

ADOPTION PATTERNS OBSERVED

European banks are exploring how learnings from the merchant payments landscape — chargeback abuse, refund fraud, first-party dispute behaviour — can be applied to APP fraud prevention and mule detection.

REGULATORY / INDUSTRY DIRECTION

- **UK PSR mandatory APP reimbursement:** live since October 2024. ⁴
- **SEPA Instant Payments:** receive obligation in force January 2025; send + Verification of Payee from October 2025 across the euro-area. ⁵

SECTION 05

Common Blockers.

SECURITY

Centralised data pooling concentrates risk.

DATA

GDPR, consent and EEA residency rule out raw data sharing; federated architectures keep raw data inside each environment.

INTEGRATION

<250ms pre-auth latency; standardised protocols needed; no data egress.

GOVERNANCE

Banking data must not be exposed or moved beyond the perimeter.

SECTION 06

What Is Not Working Today.

01

Retrospective detection downstream of payment authorisation is documentation, not prevention.

02

Scam intervention on the sending side reduces direct losses but leaves the receiving mule infrastructure intact and available for the next victim.

SECTION 07

What Banks Should Prioritise in the Next 30–90 Days.

01 **Audit your decision latency at pre-authorisation.**

What share of APP fraud cases is identified before payment authorisation versus after settlement? Mostly post-settlement means the architecture is processing claims, not preventing losses.

02 **Establish your visibility of receiving-side accounts.**

For most issuing banks this visibility is limited or non-existent — the receiving account looks clean because no signal flows from the bank that holds it. Understanding the gap is the starting point for change.

03 **Audit the evidence base for your reimbursement decisions.**

For your last 100 decisions, how much of the evidence base (vulnerability, scam typology, intervention history, receiving-account behaviour) was available at the moment versus reconstructed afterwards? Reconstructed evidence is slower and harder to defend.

Each audit reveals a symptom of the same root cause: **the behavioural signal that would change each decision lives outside the institution's data perimeter.**

Closing the gap requires cross-ecosystem trust intelligence across merchant payment rails and banking rails, without centralising raw data.

SECTION 08

About Trudenty.

Trudenty operates the **Trust Network** — infrastructure for federated trust intelligence that delivers consumer trust signals across issuers, acquirers and merchants into pre-authorisation, account opening and ongoing monitoring, and reimbursement decisioning — without centralising raw data.

trudenty.com

AUTHORS

Lerato Matsio, CEO · **Colin McCloskey**, Head of Fraud Risk Intelligence

For more of our perspectives, visit our [Insights Hub](#).

SOURCES

Sources.

-
- 01** **UK Finance**, Annual Fraud Report 2025 (28 May 2025) — covers full-year 2024.
-
- 02** **European Banking Authority and European Central Bank**, Joint Report on Payment Fraud (15 December 2025).
-
- 03** **Europol**, European Money Mule Action (EMMA) 2025.
-
- 04** **Payment Systems Regulator (UK)**, PS25/5 — APP Scams Reimbursement Consolidated Policy Statement (May 2025).
-
- 05** **European Union**, Regulation (EU) 2024/886 — Instant Payments Regulation.
-

