Managing Disputed Transfers: Authorized Push Payment Fraud vs. Customer Abuse

Executive Summary

Authorized Push Payment (APP) fraud represents a critical challenge for financial crime operations, as payments are often technically valid and authenticated by the customer, yet criminally manipulated. In 2025, UK Finance reported £576.4 million in APP fraud losses, a 19% increase in value from the previous year.The implementation of the Payment Systems Regulator (PSR) mandatory reimbursement framework on October 7, 2024, has shifted the operational landscape. While 89% of reimbursable losses are being returned to victims, firms must now balance robust consumer protection with the rising risk of first-party fraud—where customers knowingly participate in a payment and later claim a scam occurred. Effective management requires a shift from viewing authentication as "consent" to a deep, evidence-led reconstruction of customer intent, vulnerability, and the criminal operating model.

The Rising Complexity of APP Fraud

APP fraud has evolved significantly, shifting from "malicious redirection" (changing legitimate account details) to "malicious payee" scams. In these cases, the customer deliberately pays the intended recipient, but the underlying purpose—such as an investment, purchase, or romance—is fraudulent.

Market Data and Trends (2025)

- **Total Losses:** £576.4 million across 248,070 cases.
- **Growth:** A 19% increase in value and a 7% increase in cases compared to 2024.
- **Reporting Volume:** The PSR recorded approximately 352,000 reported claims in the 15 months ending December 31, 2025.
- **Reimbursement Success:** 82% of claims were closed within five business days, and 98% within 35 business days.

The Mandatory Reimbursement Framework

The regulatory environment for in-scope Faster Payments and CHAPS APP scams is defined by strict timelines and financial liabilities:

- **Mandatory Reimbursement Cap:** £85,000 per claim.
- **Liability Split:** Receiving Payment Service Providers (PSPs) generally contribute 50% of the reimbursed amount.
- **Timeline:** Sending PSPs usually have five business days to decide a claim, with a maximum window of 35 business days.
- **Exclusions:** Mandatory reimbursement does not apply if the consumer acted fraudulently ("first-party fraud") or with gross negligence (the "consumer standard of caution").

Technical Authentication vs. Informed Intent

A critical operational pitfall is treating successful Strong Customer Authentication (SCA) as proof that no scam occurred. APP fraud is defined by manipulation, not the absence of participation.| Concept | Definition in APP Context || ------ | ------ || **Authentication** | Confirms the instruction traveled through the expected channel (device, biometric, passcode). || **Authorisation** | The technical approval of the transaction by the customer. || **Informed Intent** | What the customer understood about the recipient and the purpose of the payment at the time of transfer. |

The Impact of Deception

In bank-impersonation, investment, or romance scams, victims may consciously approve transactions while being under total fraudulent influence. For example, a victim may believe they are moving money to a "safe account" to protect their savings. Therefore, authentication logs must be viewed as just one component of a broader evidential picture.

Distinguishing Victimization from First-Party Abuse

Firms must differentiate between genuine victims and customers attempting to exploit reimbursement mechanisms.

Red Flags for First-Party Fraud

- Undisclosed pre-existing relationships with the beneficiary.
- Selective disputes of repeated payments.
- "Circular" funds movement returning to the customer or connected parties.
- Device or network links between the payer and the receiver.
- Fabricated documents or material contradictions in the customer's story.

The Problem of Civil Disputes

Civil disputes involving disagreements with legitimate suppliers (e.g., non-delivery of goods) are out of scope for APP reimbursement. Investigations must evaluate the supplier's trading status and whether there was an actual intent to deceive versus a simple breach of contract.

Operational Excellence: The Five-Layer Investigation

To reach defensible decisions, FinCrime operations should employ a multi-layered investigative approach:

1. **Transaction Reconstruction:** Building a timeline of internal movements, beneficiary creation, interventions, and subsequent fund flows.
2. **Channel and Device Evidence:** Analyzing IP addresses, geolocation, session age, and remote-access indicators to distinguish APP from account takeover (ATO).
3. **Structured Customer Interviewing:** Using neutral, trauma-sensitive questioning to establish how trust was built and what representations were made.
4. **Receiving-Side Intelligence:** Collaborating with the receiving bank to identify mule accounts, cash-out routes, and shared device identifiers.
5. **Vulnerability Assessment:** Evaluating how health, cognitive impairment, or financial distress affected the customer’s ability to resist manipulation. The

consumer-standard-of-caution exception cannot be applied if the customer was vulnerable to that specific scam.

Adjudication Framework and Defensive Analytics

A resilient adjudication framework separates the investigation into four distinct questions:

1. Was the payment technically authorized or unauthorized?
2. Does the event meet the definition of an APP scam, or is it a civil dispute?
3. Is there evidence the customer knowingly participated in fraud?
4. Does any lawful reimbursement exception (like gross negligence) apply?

The Role of Analytics

- **Pre-payment Models:** Analyze unusual beneficiaries and deviation from normal customer behavior to trigger dynamic, typology-specific interventions.
- **Post-claim Analytics:** Use network analysis to identify clusters of claims connected to common receiving infrastructure or "mule" networks.
- **Natural-Language Tools:** Help structure call notes and identify inconsistencies between a customer's timeline and system events.

Strategic Implications for Financial Crime Leaders

Managing disputed transfers is a cross-functional responsibility involving AML, fraud prevention, legal, and customer vulnerability teams. Success is not measured by the volume of approvals or rejections, but by the accuracy and defensibility of the decisions.**Key Strategic Recommendations:**

- **Avoid Assumption of Intent:** Do not equate technical action with informed consent.
- **Establish Evidential Thresholds:** Allegations of first-party fraud should require high burdens of proof and independent review.
- **Continuous Feedback:** Use intelligence from confirmed scams to update preventive controls and typology-specific warnings.
- **Focus on Vulnerability:** Integrate vulnerability assessments into the core of the investigation rather than treating them as an administrative addition.