ACORU | CASE STUDY

CONTINUOUS ACCOUNT INTELLIGENCE

Closing the transaction monitoring gap at a mid-sized European bank

How the bank used continuous account intelligence to classify first-party and counterparty accounts and surface scams before a transaction is initiated.

01 THE PROBLEM

Where transaction monitoring falls short

Authorized push payment (APP) fraud rarely stands out in transaction monitoring. The customer authorized the payment. Strong Customer Authentication passed. The rules engine saw little unusual, because little unusual happened at the transaction level. The manipulation started days or weeks earlier, in the account, before a transaction was initiated.

Transaction monitoring (TM) was built to evaluate individual transactions. Regulators expect it for anti-money laundering (AML). Most banks extend it to fraud, and it does both jobs well. It was never built to tell whether an account is trending toward victim or mule status.

Even institutions that feed session data into their TM hit the same wall: a scam does not have to produce an anomalous transaction. The signals sit upstream, in account activity and channels the TM never sees.

That is the structural gap. Tuning rules and thresholds won't close it. A different detection model will.

02 THE BANK

One bank's alert problem

A mid-sized European bank ran into that gap directly. Its victim-focused controls ran on a leading incumbent platform and produced high alert volumes, most of them legitimate activity. Mule accounts needed a different lens. The bank ran Acoru alongside the incumbent, classifying Victim and Mule accounts using only its own data, including counterparty accounts held at other institutions, read from the payments its customers send to and receive from them.

UK APP FRAUD LOSSES

19%

Rise in UK APP fraud losses, to £576.4 million

Source: UK Finance, Annual Fraud Report 2026

03 THE REGULATORY STAKES

What reimbursement rules cost banks

That gap has a price. Under PS23/4 (the UK Payment Systems Regulator's mandatory APP fraud reimbursement policy), sending banks reimburse victims up to £85,000 per claim and split the cost 50:50 with the receiving bank. In the US, Nacha's fraud monitoring rules took effect in two phases between March and June 2026.

Sending and receiving banks must now run risk-based processes to identify fraudulent ACH entries, including those authorized under false pretenses. Deloitte puts US APP fraud losses at $8.3 billion in 2024, with $14.9 billion possible by 2028. In both markets, the receiving bank now shares responsibility. Transaction monitoring alone sees the risk late.

£85,000

Maximum reimbursement per claim under PS23/4

50:50

Cost split between the sending and receiving bank

$8.3bn

US APP fraud losses in 2024, with $14.9 billion possible by 2028

Sources: Payment Systems Regulator, PS23/4; Deloitte

04 THE SOLUTION

Classifying every account before the transaction

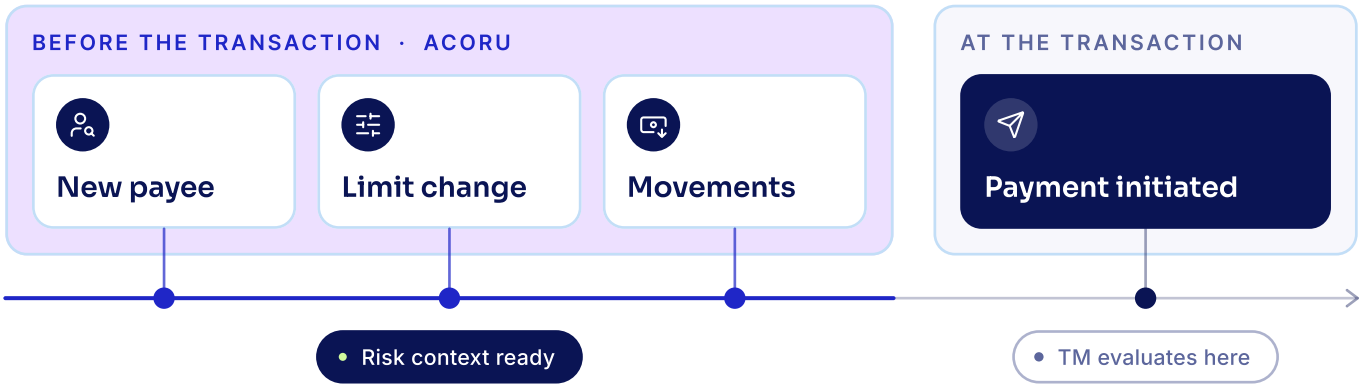
Acoru closes the gap by classifying accounts continuously, before a transaction is initiated. Classification does not wait for a payment. It updates with every account event: logins, profile and limit changes, new payees, incoming and outgoing movements, and call center interactions. Session and device signals add context. Each event can look routine. Together, these pre-fraud signals show an account trending toward Victim or Mule status. Acoru reads them as they arrive, so the risk context is ready before the customer reaches the payment screen.

Counterparty accounts are classified the same way, including accounts held at other institutions.

When a customer selects a payee and enters an amount, risk context on the first-party and counterparty accounts is already calculated. Mule accounts, proceeds-collection accounts, and other high-risk counterparties can be identified using only the bank's own data. Consortium Manager, Acoru's optional intelligence-sharing add-on, can extend that view but is not required. Classification covers incoming and outgoing transactions alike.

That two-way picture changes what the TM system receives. By the time a transaction reaches the rules engine, the system has already documented risk context for the first-party and counterparty accounts. The bank can route higher-confidence cases straight to investigators and let lower-risk transactions clear with less friction.

FIGURE 1 · THE SIGNALS SIT UPSTREAM OF THE TRANSACTION



> Most scams leave little for TM to catch at the transaction level. Continuous account intelligence gives the bank risk context before a transaction is initiated.

05 OPERATIONAL PAYOFF

What fraud teams can act on

With Victim and Mule classifications already in place for first-party and counterparty accounts, fraud teams can act on them:

Block mule transfers
Stop a transfer to a Mule-classified counterparty account before it is initiated, using classification built entirely from the bank's own data.

Prioritize the queue
Prioritize the investigator queue by account risk, so high-confidence cases reach investigators first.

Focus TM review
Low-risk classifications let the bank prioritize full TM review for the transactions that need it, so analysts spend less time on legitimate activity.

Escalate with evidence
Escalate a payment from a Victim-classified account with the evidence attached: the specific account events and signals that drove the classification. The bank can then choose a response that fits the risk, such as a targeted warning, a hold, or a call-back.

Screen incoming payments
When the bank is the receiving institution, its own accounts are already classified, so Mule accounts can be identified before illicit funds arrive. That reduces the receiving bank's reimbursement exposure under PS23/4 and supports its receiving-side obligations under Nacha's fraud monitoring rules.

Decisions and reason codes flow into the bank's existing TM and case management workflows, with no rip and replace.

RESULT

Acoru raised fewer than a quarter of the incumbent platform's alerts on the same transfers, with no reduction in confirmed fraud detected.

Acoru data, mid-sized European bank

06 OUTCOMES

What changed for the bank

The results are measurable. About 75% of the accounts in mule rings the bank later confirmed were flagged before they moved any money. Starting from a single case, the bank uncovered more than 15x the money it had confirmed moving through one ring. And because the risk context exists before a transaction is initiated, each intervention comes with its evidence: decision logic, reason codes, and the account events behind them, documented at the moment of action.

For the TM system, the effect is additive. Acoru ran alongside the incumbent platform, covering the window before a transaction is initiated, which transaction monitoring was never built to see. TM keeps its job and receives each transaction with the account's risk context already attached.

~75%

of accounts in later-confirmed mule rings flagged before they moved any money

15x+

the money the bank had confirmed moving through one ring, uncovered from a single case

< ¼

of the incumbent platform's alerts on the same transfers

Source: Acoru data, mid-sized European bank

> That is the difference between managing scam losses and preventing them.

“

Better data, and better analytics, are the best shield a payment firm can invest in to mitigate their exposure to APP scams.

Chris Hemsley, Managing Director, Payment Systems Regulator | Fraud Leaders' Summit, February 2024

To see how continuous account intelligence works alongside your transaction monitoring, visit acoru.com.

Visit acoru.com

Classify accounts. Trace mules. Stop scams.

ACORU

Copyright © 2026 Acoru. All rights reserved. This document may not be copied, distributed, displayed or performed for commercial or non-commercial purposes. No derivative works are permitted. The material must not be used for commercial purposes without prior written permission from Acoru. For further legal information, visit acoru.com.