ACORU | GUIDE

BUYER'S GUIDE

How to evaluate an APP fraud prevention platform

Five capabilities every fraud prevention platform should deliver, a comparison of common approaches, and 15 vendor evaluation questions.

Contents

01 The industrialization of social engineering 04

02 Three common approaches and their limitations 05

03 Five capabilities to evaluate 06

04 Continuous account intelligence 10

05 Regulatory landscape: what you need to know 12

06 15 questions to ask any provider 13

EXECUTIVE SUMMARY

Why this guide exists

Fraud teams at banks and financial institutions face a structural problem. The tools they rely on were designed for a threat that has already shifted under their feet. Transaction monitoring, online fraud detection tools, and point-of-payment scoring all share the same blind spot: they evaluate sessions, devices, and payments at a point in time. None of them saw what happened before the customer opened the app. By the time any of them fire, the money is gone.

Authorized fraud (scams, APP fraud, social engineering) is the fastest-growing share of fraud losses at many institutions. Regulators in the UK, Europe, and the US are responding with reimbursement mandates and compliance requirements that place financial liability squarely on banks. The question is no longer whether to address authorized fraud. **The question is how to detect it before a transaction is initiated.**

£576.4m
APP fraud losses recorded by UK Finance in 2025

+19%
Increase year on year

248,070
APP fraud cases

Source: UK Finance, Annual Fraud Report 2026.

WHAT THIS GUIDE DELIVERS

- Five capabilities every fraud prevention platform should deliver
- A comparison of common approaches
- 15 vendor evaluation questions you can bring into any procurement conversation

WHO THIS GUIDE IS FOR

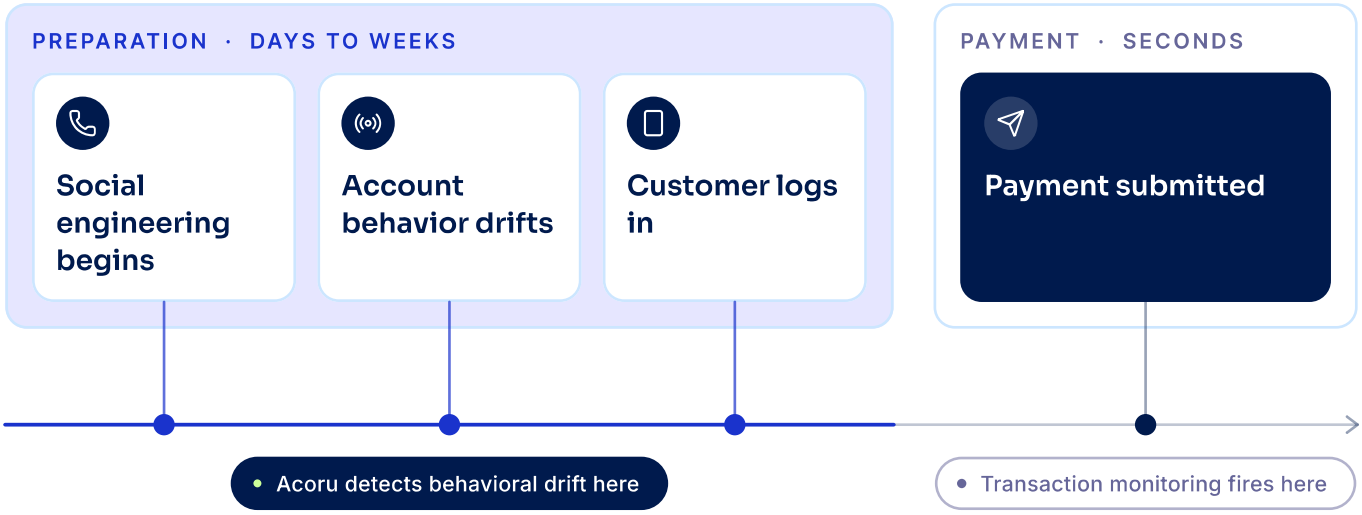
- Heads of Fraud Operations assessing platform investments
- Financial Crime Directors building a business case for the board
- CISOs evaluating data privacy and residency requirements

01 THE PROBLEM

The industrialization of social engineering

Most fraud-prevention infrastructure was built to stop unauthorized fraud: card theft, credential stuffing, and account takeover by external attackers. These systems analyze individual transactions at the time of payment and flag anomalies relative to a baseline.

FIGURE 1 · AUTHORIZED FRAUD HAPPENS BEFORE THE PAYMENT



Every legacy control sees a genuine customer. The decisive signals appear days to weeks earlier, in the account.

Authorized fraud operates differently. The customer is the one making the payment. Their credentials are valid. Their device is recognized. Their biometrics match. Their behavior looks normal because it is their behavior. The manipulation happened before they ever logged in: over a phone call, via a text message, or through a fake investment website.

Transaction monitoring sees a legitimate payment and has no reason to intervene. Online fraud detection tools (the behavioral biometrics and device intelligence platforms that banks deploy to catch account takeover) see a clean session and have no reason to intervene. Both were built for a different threat. The receiving side further compounds the exposure. Most fraud platforms only analyze outbound payments.

Every inbound payment arriving at a customer account goes unread: the counterparty behind it, the relationship pattern it reveals, the mule activity it may indicate. The EU Instant Payments Regulation has required Verification of Payee on euro credit transfers since 9 October 2025, and settlement inside 10 seconds. A mule account opened in the right name passes that check, which puts the receiving bank in focus.

PSD3 and the Payment Services Regulation are not yet in force. Once they apply, payment service providers will have to monitor transactions for fraud on both sides and share fraud-related information with each other. Institutions that cannot read inbound payments today will be building that capability under a deadline.

> Authorized push payment fraud losses are climbing across major markets, and the regulatory response is accelerating. Transaction monitoring and online fraud detection tools were not designed to stop it.

This is not a tuning problem. You cannot solve it by adjusting thresholds, adding rules to a transaction-monitoring engine, or deploying improved session analysis. The issue is architectural: systems built to evaluate individual events in isolation, whether transactions or sessions, cannot detect the account-level patterns that precede a scam.

FIGURE 2 · THE FIVE PHASES OF AN APP SCAM



Once a payment clears an instant payment network, the window to recover it is measured in seconds. Detection has to happen in phases 1 to 3.

02 COMPARISON

Three common approaches and their limitations

CAPABILITY	TRANSACTION MONITORING	POINT SOLUTIONS	CONTINUOUS ACCOUNT INTELLIGENCE
Detection timing	At the point of payment	At the point of payment or login	Continuous, before a transaction is initiated
Signal scope	Single transaction data	Session or device data	Cross-channel account lifecycle, behavioral, and contextual data
Authorized fraud detection	Minimal (customer behavior looks normal)	Partial (session anomaly detection)	Strong (account-level pattern recognition across time)
Mule account detection	Post-transaction flagging	Limited or absent	Continuous classification: Regular, Victim, Mule, Laundering, and Honeypot

CAPABILITY	TRANSACTION MONITORING	POINT SOLUTIONS	CONTINUOUS ACCOUNT INTELLIGENCE
Regulatory readiness (PS23/4, Reg E, Nacha)	Reactive reporting	Partial coverage	Pre-transaction information with audit trail
Data control	Vendor-dependent	Vendor-dependent	Institution-controlled (on-premises, private cloud, or hybrid)

The gap is clear. Transaction monitoring was designed for a world in which the attacker controlled the device. Online fraud detection tools were built for the same threat model: catching an unauthorized actor impersonating your customer. They do that job well. Against APP fraud, both categories miss the point entirely. Their session is clean. Their biometrics match. Their device is recognized.

The manipulation happened days or weeks earlier, across channels these tools were never designed to read. Neither approach reconstructs the account-level story that reveals when a customer is being groomed, when a mule network is being assembled, or when a victim is being prepared to authorize a payment they will immediately regret.

03 EVALUATION FRAMEWORK

Five capabilities to evaluate

When assessing fraud prevention platforms, the evaluation should go beyond feature lists. What matters is whether a platform can detect and prevent fraud at the right point in the attack lifecycle: before a transaction is initiated. The following five capabilities define that standard.

01 Continuously monitor accounts

The platform should continuously monitor accounts, not just at the time of a transaction or login. Account behavior changes over days, weeks, and months before a scam payment occurs. A customer who has never received a large inbound transfer suddenly receives one from an unknown source and then initiates an outbound payment to a new payee within hours: that pattern is invisible to transaction monitoring and session-level fraud tools, which see only the login and the payment. It is obvious to an account-level system that has been watching.

ASK

Does the platform monitor account behavior between transactions, or only at the point of payment?

02 Pre-transaction fraud controls

Detection after the fact is monitoring. Prevention requires acting before a transaction enters the payment rails. The platform should be able to trigger interventions (alerts, beneficiary review, customer outreach, dynamic in-app messaging) during the payment preparation phase, before a transaction is initiated. Once a payment clears an instant payment network, the window to recover it is measured in seconds, not hours. The only reliable defense is stopping it before submission.

ASK

At what point in the payment lifecycle does the platform intervene? Before submission, at submission, or after settlement?

03 Cross-channel signal correlation

Scams do not begin in the banking app. They begin with a phone call, a text message, a social media ad, or a search engine result. The manipulation moves across channels before it reaches the payment screen. A fraud platform that only ingests digital banking data is looking at the last frame of a movie and trying to guess the plot.

The platform should correlate signals from digital banking, call center interactions, payment systems, device data, and, where available, external intelligence feeds. The goal is not more data for its own sake. The goal is context: understanding what happened before the customer opened the app.

ASK

What data sources does the platform ingest, and can it correlate signals across channels in real time?

04 Account classification and mule detection

The platform should classify every account into a current risk state and keep that state updated. A five-state model covers the ground: Regular (no current risk indicators), Victim (at risk of being deceived or already manipulated), Mule (Complicit, Witting, or Unwitting), Laundering (accounts that move or mix illicit funds), and Honeypot (decoy accounts deliberately exposed to gather intelligence on attackers). For most institutions, the practical priorities are Victim protection and Mule detection: stopping customers from being deceived and identifying accounts used to receive and move stolen funds.

FIGURE 3 · NOT EVERY MULE LOOKS THE SAME



Mule is one of five account states: Regular, Victim, Mule, Laundering, and Honeypot.

Mule detection is where most fraud platforms fail entirely. Mule accounts are the infrastructure of scam networks. Without the ability to identify recruitment patterns, activation signals, and cash-out behavior, you are fighting scams one victim at a time while the network that enables them operates freely across your customer base.

The platform should continuously classify accounts and update those classifications as new data arrives, rather than just flag individual transactions as suspicious.

ASK

Does the platform classify accounts across all risk states (regular, victim, mule, laundering) on an ongoing basis, or only flag individual transactions?

05 Explainability and regulatory compliance

Regulators in every major market are tightening requirements around fraud prevention. PS23/4, the UK Payment Systems Regulator's mandatory APP fraud reimbursement policy, requires payment service providers to refund victims up to £85,000 per claim, with the cost split 50:50 between the sending and receiving providers. In the EU, PSD3 and the Payment Services Regulation will add customer protection obligations once they apply. In the US, Nacha's 2026 credit-push fraud monitoring rules require receiving institutions to monitor for fraudulent credits, with Phase 1 effective 20 March 2026 and Phase 2 from 19 June 2026.

A fraud prevention platform must produce decisions that are explainable to regulators, auditors, and customers. Black-box scores are a compliance risk. Every fraud decision should trace back to observable account behavior: what changed, when it changed, and why the system flagged it.

ASK

Can the platform produce explainable, auditable fraud decisions grounded in observable account behavior?

THE REGULATORY REALITY

A platform that cannot demonstrate it acted before a transaction was initiated, and that lacks an auditable decision trail, creates regulatory exposure. This is the operational reality driving investment decisions in fraud platforms today.

04 THE ACORU APPROACH

Continuous account intelligence

The Acoru Continuous Account Intelligence Platform monitors, classifies, and protects accounts before a transaction is initiated, across every channel a bank operates.

How Acoru maps to the five capabilities

01 **Continuous account monitoring.** Detects preparation-phase anomalies days or weeks before a scam payment is attempted.

02 **Pre-transaction fraud controls.** Alerts, beneficiary review, and dynamic intervention fire before a transaction is initiated.

03 **Cross-channel signal correlation.** Ingests digital banking, call center, payment, and device data. Inbound and outbound.

04 **Account classification.** Every account is continuously classified: Regular, Victim, Mule, Laundering, or Honeypot.

05 **Explainability and compliance.** Every decision traces to observable account behavior, with a signed audit trail on every event, score, policy, and model execution.

Generative AI capabilities

The Platform includes three generative AI components designed to reduce analyst workload and accelerate fraud response:

AI Assistant

Answers plain-language risk queries, summarizes investigations, and assists with rules and reporting. Every response traces to the behavioral sequence behind the classification.

AI Workforce

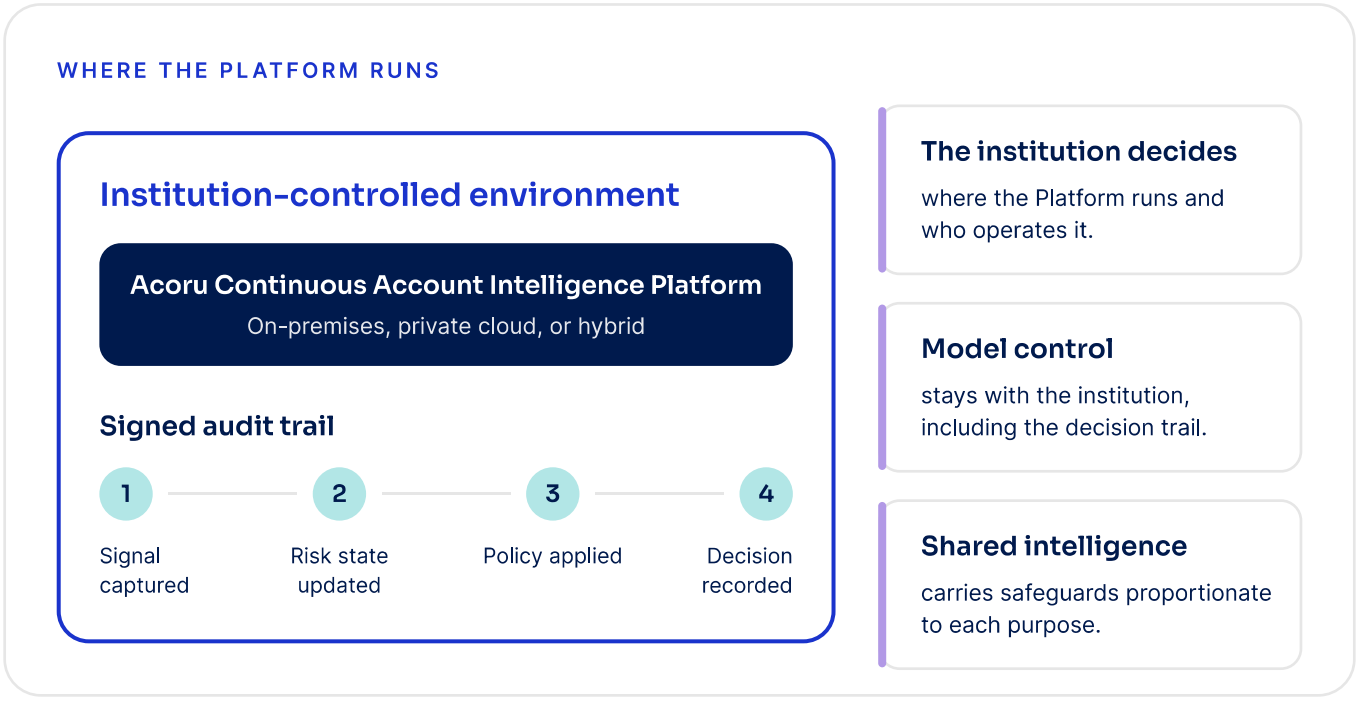
Executes multi-step fraud workflows inside institution-defined boundaries, from case triage to suspicious activity report (SAR) preparation, freeing analysts to focus on complex investigations.

Large Account Model (LAM)

Reads an account's full lifecycle as one continuous sequence, the way a language model reads a paragraph. That sequence is what surfaces behavioral shifts a point-in-time model cannot see.

Data privacy and residency

Acoru runs on-premises, in a private cloud, or in a hybrid environment, single- or multi-tenant. The institution decides where Acoru runs and who operates the infrastructure. For regulated financial institutions, this is not a feature preference. It is a compliance requirement.



05 REGULATORY LANDSCAPE

What you need to know

Fraud prevention is no longer optional. Regulators and scheme operators across major markets are shifting liability to financial institutions and requiring proactive intervention capabilities. Any platform investment should account for the following requirements:

REQUIREMENT	WHAT IT REQUIRES	IMPACT ON PLATFORM SELECTION
UK **PS23/4 APP fraud reimbursement**	Payment service providers must refund APP fraud victims up to £85,000 per claim; costs are split 50:50 between sending and receiving providers.	**Platforms must demonstrate pre-transaction intervention to reduce reimbursement exposure.**
EU **PSD3 and the Payment Services Regulation**	Not yet in force. Once they apply, payment service providers will have to monitor transactions for fraud on both sides, share fraud-related information with each other, and refund consumers deceived by someone impersonating their own bank.	**Platforms must produce explainable decisions and support regulatory reporting.**
US **Nacha credit-push fraud monitoring rules**	Risk-based monitoring to identify ACH credit entries initiated due to fraud, including transactions authorized under false pretenses. Phase 1 effective 20 March 2026; Phase 2 from 19 June 2026.	**Mule account detection becomes an operating-rule requirement, not just a fraud prevention capability.**
US **Regulation E**	Consumer protection for electronic fund transfers; expanding interpretation of bank liability.	**Platforms must document the timing of interventions and the rationale for decisions.**
EU **EU Instant Payments Regulation**	Verification of Payee required on euro credit transfers since 9 October 2025, with settlement inside 10 seconds. A mule account opened in the right name passes the check.	**Inbound payment analysis matters. Platforms that only monitor outbound payments cannot classify the receiving account.**

06 VENDOR EVALUATION

15 questions to ask any provider

Use these questions in any vendor conversation or RFP process. They are designed to surface the capabilities that matter most for authorized fraud prevention and regulatory compliance.

Detection and prevention

01 At what point in the payment lifecycle does your platform detect and intervene: before transaction submission, at submission, or after settlement?

02 Does your platform monitor account behavior continuously, or only during active sessions and transactions?

03 How does your platform detect authorized fraud where the customer's credentials, device, and behavior all appear legitimate?

Data and signal coverage

04 What data sources does the platform ingest (digital banking, call center, payment systems, device, external intelligence)?

05 Can the platform correlate signals across channels in real time to reconstruct pre-transaction context?

06 Does your platform analyze inbound payments as well as outbound? How does it classify accounts receiving funds before a payment posts?

Mule detection

07 How does your platform identify mule accounts: at the individual-transaction level or through network-level pattern analysis?

08 Can the platform detect mule recruitment, activation, and cash-out patterns across the customer base?

Explainability and compliance

09 Can every fraud decision be traced back to specific, observable account behavior?

10 How does your platform support PS23/4 reimbursement requirements, EU obligations, or Nacha credit monitoring rules?

11 What audit trail does the platform produce for regulatory examinations?

Deployment and data residency

12 Where is customer data stored and processed? Can the platform be deployed on-premises, in a private cloud, or in a hybrid environment?

13 Who controls the fraud models and the data used to train them?

Operational impact

14 What measurable outcomes can you demonstrate: reduced scam losses, reduced false positives, and improved analyst efficiency?

15 What is the total cost of ownership, including integration, ongoing model tuning, and analyst training?

NEXT STEPS

Where to go from here

Fraud prevention has become an operational and regulatory requirement, not just a technology investment. Customer trust, financial exposure, and institutional reputation all depend on what happens before a transaction is initiated.

The five capabilities outlined in this guide (continuous account monitoring, pre-transaction controls, cross-channel signal correlation, account classification, and explainability) represent the minimum standard for institutions serious about stopping authorized fraud before it happens.

Acoru offers a structured assessment of your current fraud-prevention posture, a walkthrough of continuous account intelligence in practice, and a clear view of the expected outcomes for your institution.

Request a consultation

Contact us at acoru.com

Visit acoru.com

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.