NICE Actimize

Case Study

Top-Tier U.S. Wealth Management Institution Achieves 35% Uplift in Scam Detection on Web-Based Wire Transfers

The Customer

A leading U.S. wealth management and brokerage institution with an integrated banking arm serves affluent and high-net-worth (HNW) clients, managing trillions in client assets. Its digital banking platform processes a significant volume of high-value web-based wire transfers.

The Challenge

Scams now account for 52% of all attempted banking fraud, according to the NICE Actimize 2026 Fraud Insights Report. Unlike unauthorized fraud, where a criminal bypasses a customer's controls to initiate a transaction, scams work by deceiving the customer into authorizing the payment themselves. That distinction fundamentally changes what a fraud detection model needs to look for.

For this institution, the challenge was structural. The FI had previously developed a wire fraud detection model, which was purpose-built, well-tuned and effective at identifying transactions that deviated from a customer's established behavioral baseline. That model was doing what it was designed to do. The problem was that scam transactions, by their nature, rarely trigger anomaly-based detection signals.

The consequences were measurable. Under the general wire fraud model, the institution's scam-specific Value Detection Rate stood at approximately 40%. What the institution needed was a model trained to recognize the specific behavioral signature of a scam.

The Outcome

35%
increase

in value detected per scam alert — meaning each investigation action taken by the fraud team was directed at higher-value scam activity

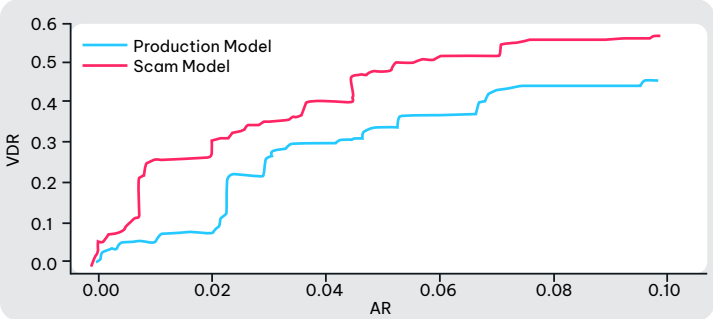
20%
increase

in the Scam Value Detection Rate (VDR) — a higher proportion of scam losses now intercepted before funds leave the institution

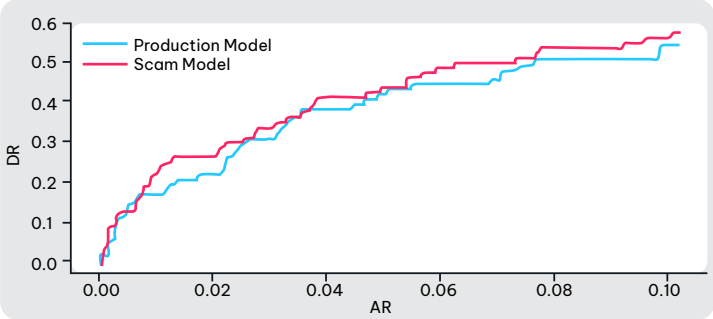
18%
increase

in the number of scams detected — broader coverage across scam typologies, including cases that the general model consistently missed

Value Detection Rate vs. Alert Rate



Volume Detection Rate vs. Alert Rate



The scam-specific model delivered a material improvement across every measure of detection performance, outperforming the general fraud model on the scam transaction population across the full operating range.

Taken together, these results show that detection improvement and operational efficiency are not in tension. The scam model caught more cases, including higher-value ones, and did so without requiring the institution to overhaul its existing detection infrastructure.

The Solution

After reviewing these behavioral patterns, the NICE Actimize analytics team developed features and trained a dedicated model to detect authorized payment fraud. A generic transaction fraud model, even one that incorporates multiple detection signals, would not weigh these features heavily enough to reliably detect authorized payment fraud. Among the most intuitive signals was the time elapsed between payee setup and first payment, a behavioral marker that legitimate transfers rarely exhibit, but scam-induced transactions frequently do.

To further strengthen detection, the NICE Actimize analytics team applied payee risk intelligence from the Actimize Insights Network, a service that aggregates cross-institutional fraud signals. This intelligence served a dual purpose. Features derived from fraud incidence rates at the receiving bank level flagged banks with a disproportionate concentration of confirmed fraud cases across the network, adding a risk signal that no single institution's internal data could generate. At the same time, features such as account tenure on the network, last activity date and average transaction amount reduced friction for new payees already known and trusted across the network. The result was sharper detection at the high-risk end and fewer unnecessary challenges at the low-risk end.

The Solution

Alert-Strategy

The alert-strategy optimization layer combined the outputs of both the scam model and the existing general fraud model into a unified decisioning framework.

Deploying an authorized payment fraud model alongside an existing wire fraud model raised two questions: Would it generate additional alerts? If not, how would the two model scores be combined into a single transaction decision?

Actimize fraud detection solutions address this challenge by using the platform's Multi-Model Execution (MME) framework. Beyond providing the execution framework for executing multiple models concurrently to preserve SLA compliance, MME provides fraud strategy teams with direct control over how scores from multiple models interact to produce a single, governed risk output per transaction.

For this institution, that meant a transaction that the general wire fraud model scored as low risk could be elevated by a high authorized payment fraud score. The FI's fraud strategy team retained full control over that logic and could adjust it without modifying the underlying models or disrupting the existing alert workflow.

Summary

Scams are a distinct fraud problem that require a distinct analytical response. A general fraud model, however well-built, is optimized to detect anomaly, and scam transactions are designed to look normal. For this institution, closing that gap required a dedicated authorized payment fraud model, enriched by cross-institutional payee intelligence from the Actimize Insights Network and governed by a decisioning framework that kept detection broad without expanding operational burden.

The lesson is straightforward. Scam detection improves when the model is built for scams. NICE Actimize delivered that capability through purpose-built analytics, collective intelligence and a multi-model framework that gave the institution's fraud strategy team control over how it all came together.