NICE Actimize

Case Study

Tier 1 North American Bank Shifts from Fraud Response to Proactive Prevention with Actimize Insights Network

The Customer

A leading Tier-1 North American bank, with a nationwide presence and diverse customer base spanning retail, commercial and institutional segments, engaged NICE Actimize to strengthen its wire payment fraud prevention capabilities. With scam losses rising and fraudsters increasingly targeting new payee scenarios, the bank sought a solution to gain visibility into risky beneficiaries before funds were sent.

The Challenge

The bank's existing wire fraud detection relied solely on internal data and history with counterparties. In the case of new beneficiaries, those the bank had never transacted with before, there was no behavioral history to draw upon. This created a blind spot at one of the most vulnerable points in the payment journey.

Fraud analytics teams recognized that many scams, particularly Business Email Compromise (BEC) and Authorized Push Payment (APP) fraud, exploit these gaps. The lack of cross-institutional intelligence meant risky payees already known to other financial institutions (FIs) could still receive payments from this bank.

Key Challenges

- No external intelligence on beneficiaries new to the bank
- Inability to detect payees already flagged as risky by other FIs
- High fraud exposure in new payee wire transactions despite low transaction volume share

The Solution

NICE Actimize leveraged the Actimize Insights Network to equip the bank with real-time risk indicators for wire payees. Supported by anonymized and privacy-compliant data contributions from a network of FIs, this capability enhanced the bank's visibility into counterparty risks across the broader financial landscape.

Key Capabilities

- **Real-Time Risk Signal Delivery:** Responses within 200 milliseconds at payment initiation or payee onboarding, enabling immediate decisioning such as accept, block, challenge or delay
- **Network Intelligence on High-Risk Payees:** Identification of payees tagged in confirmed fraud by at least two other participating institutions, providing early warning signals of high-risk new payees
- **Seamless Integration:** Real-time risk signals embedded across rules, models and analytics within existing fraud strategies

The Results

13.4%

increase in fraud detection rate

$6.3M

in payments to high-risk payees were challenged or stopped

71 day

reduction in processing times for flagging risky payees

~$441,000

in prevented fraud losses

In one month, the bank processed thousands of domestic and international wire transactions, during which attempted fraud exceeded $3 million in value.

Using only internal data and fraud models, the bank would have achieved a fraud detection rate of 71.6%, preventing approximately $2.24 million in losses. Yet $883,000 in fraud would have gone undetected, with most of those transactions involving new payees with no prior history at the bank. However, many of these new payees were already identified as risks by other institutions.

The Actimize Insights Network had insights about **88% of the bank's** potentially fraudulent counterparties, on average, **71 days earlier** than the bank's internal detection system. With real-time network risk indicators, the FI prevented up to 50% of losses that its internal detection systems would have missed — approximately $441,000.Additionally, by leveraging network intelligence, more than $6.3 million in payments to new but already known high-risk payees were challenged or stopped before release. Without access to this external intelligence, these early warning opportunities would have been missed, and high-risk payees would have successfully received funds.

With the Actimize Insights Network, the bank's fraud detection rate increased from **71.6% to over 85%, significantly reducing its exposure to high-risk transactions.**

Summary

By using risk signals from the Actimize Insights Network, the Tier-1 North American bank shifted to a proactive wire payment-detection strategy. Cross-institutional intelligence closed a critical detection gap, especially in new payee scenarios, most frequently exploited by scammers.

With earlier alerts, faster detection and actionable intelligence, the bank can protect customers more effectively and save hundreds of thousands of dollars in fraud losses each quarter, while maintaining full compliance with data privacy standards.

Get started now