NICE Actimize

Case Study

Global FI prevents $1.7 million of attempted fraud monthly

The Customer

A top five financial institution offering consumer banking and lending, commercial banking, corporate and investment banking, and wealth management. The firm leveraged peer-to-peer (P2P) payments to spur growth and market share.

The Outcome

85%

Increased fraud detection to an 85% Value Detection Rate (VDR) while reducing false positives.

50%

Streamlined alert workflows, leading to 50% faster alert resolution times for those alerts that still required fraud analyst intervention.

$1.7m
monthly

Additional $1.7 million of attempted fraud prevented monthly.

The Challenge

The rise in adoption of P2P payment rails, increasing customer expectations for frictionless (CX), and constraints on time available to review and action alerts—all of this puts substantial pressure on fraud operations teams. The speed of these transactions presents a need for smarter automation and more accurate, faster decision-making within fraud operations.

On top of that pressure, this FI was concerned about customer experience (CX) and ensuring regulatory compliance. Customers defrauded through P2P payment applications might question a firm's ability to protect accounts and take their business elsewhere. In parallel, with the shift of liability, the FI was concerned that authorized push payment (APP) fraud manifesting in P2P payments would result in further losses.

Fraudsters were targeting P2P payments because:

- They could cash out quickly with anyone, anywhere.
- Unlike cross-border or inter-bank transfers that require multiple verifications, P2P payments were not subject to the same controls.
- Frauds over instant payments are difficult for consumers to address.

Fraudster used instant payments as the means of cash out for:

Account takeover (ATO) or 'unauthorized' fraud, where the user who instructs the bank to make a payment does not have the authority to transact on that account.

A fraudster obtaining credentials illicitly will log into a consumer's account, then use a payment application to steal funds.

Authorized Push Payment (APP) scams or 'authorized' fraud, involves the fraudsters using payment applications to cash out. In this fraud scheme, the authorized account holder is manipulated into approving a payment under false pretenses. Ultimate liability for these transactions can fall on the consumer's bank, which affects revenue. 'Liability shift' to the bank doesn't always occur, which creates a negative consumer experience that can cause customer attrition, impact revenue, and invite regulatory oversight due to consumer complaints.

NICE Actimize

The Solution

NICE Actimize examined the financial institution's fraud strategies with internal stakeholders. A major focus was weighing their risk appetite versus the customer experience. The business goal was to create a data-informed approach, while balancing fraud prevention processes.

NICE Actimize was able to secure its instant payment channels with:

- Continuous model optimization to prevent degradation, preserve rates of detection, and prevent of fraud.
- Risk signal orchestration support using advanced analytics to identify behavioral patterns, enabling the firm to further detect and prevent fraud involving P2P payments.
- NICE Actimize successfully achieved high detection rates while maintaining low false positives, reducing financial losses for the FI while improving customer experiences.

If you want to learn more about how to improve fraud detection, contact us.

Get started now