NICE Actimize

Brochure

IFM-X: The Authority in Payments Fraud, Scams and APP Risk Mitigation

Typology-Specific, Multi-Model Execution Stops Authorized Push Payment Fraud and Scams

As consumers have adopted faster payment rails into their financial habits, so too have fraudsters: as the saying goes, faster payments = faster fraud. Scams and social engineering attacks are leading to rampant authorized payments fraud. The impact has caused government agencies to step in.

An example is the U.K. Payment Systems Regulator (PSR) who has proposed shift in liability to include mandated reimbursement of authorized push payment (APP) fraud victims shared between both sending and receiving financial institutions (FIs). How can FIs keep up with this proliferation of authorized fraud, protect their customers, and themselves? The answer is using the right technology.

NICE Actimize's IFM-X blocks APP fraud. By incorporating a typology-specific approach for scams and APP fraud, FIs are able to compare data points simultaneously against multiple models to identify the specific scam typology occurring. These cases can be automatically decisioned, or where required, routed to fraud analysts who can get fast resolution by leveraging an information-rich user interface when reviewing prioritized alerts. This leads to better management of Total Cost of Fraud:

- Improved customer experience (CX) and decreased false positives
- Reduced fraud losses
- Optimized operational execution and reduced operating expenses
- Increased ROI
- Surpassed compliance requirements

FIs need proactively fight to prevent customers from becoming victims of scams. Using a combination of multidimensional profiles, expert features that are typology-specific, and multi-model scores, IFM-X stops APP fraud and scam transactions. This will prevent fraud losses, safeguard the FI's reputation, and protect customers.

→ Learn More

Challenge:

A payment is made by the actual customer logging in from a verified location or trusted device. It's difficult to differentiate from the customer's genuine behavior, needing non-traditional data and sophisticated analytics.

Resolution:

Data enrichment drives additional insights for accounts, including collective intelligence for known scam risks and multidimensional profiles consisting of behavioral biometrics, historical consumer profile activity, and money movement data. Aggregation of multiple data enables detection and prevention tailored to scams and APP activity.

Challenge:

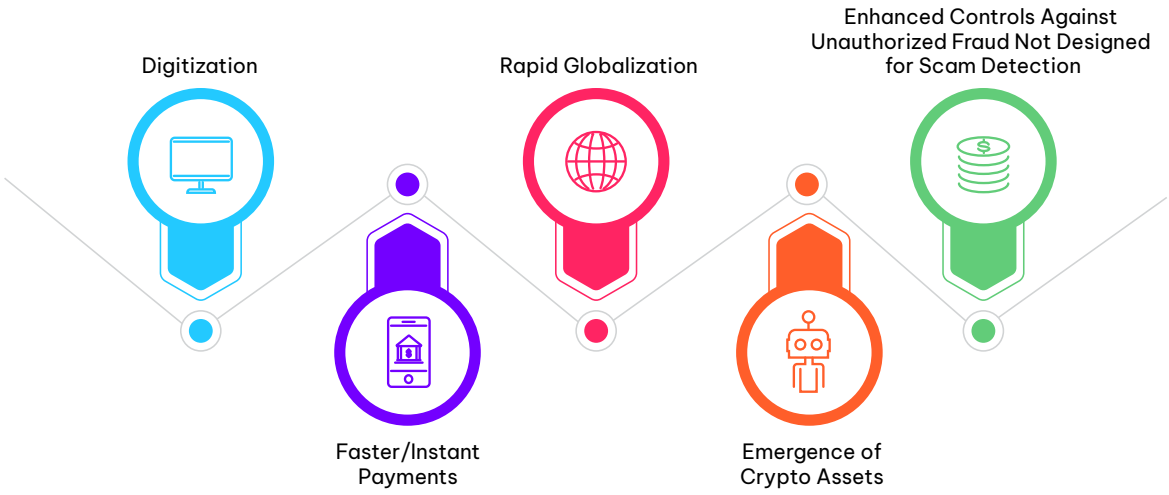
There are several different scams and typologies to monitor. The current transaction-centric, one size fits all, approach just isn't enough. FIs need dedicated alerting and related workflow management that drives operational efficiency, accuracy, and better protection for customers and their funds.

Resolution:

Typology-specific fraud detection models identify and adapt to different scams that then enable more efficient workflows, routing cases to experts trained in that particular scam typology. With pre-packaged rules, alerts, and workflow management, resolution is quick, easy, and able to keep up with changing fraud patterns.

→ Learn More

Authorized Payment Fraud: Key Drivers



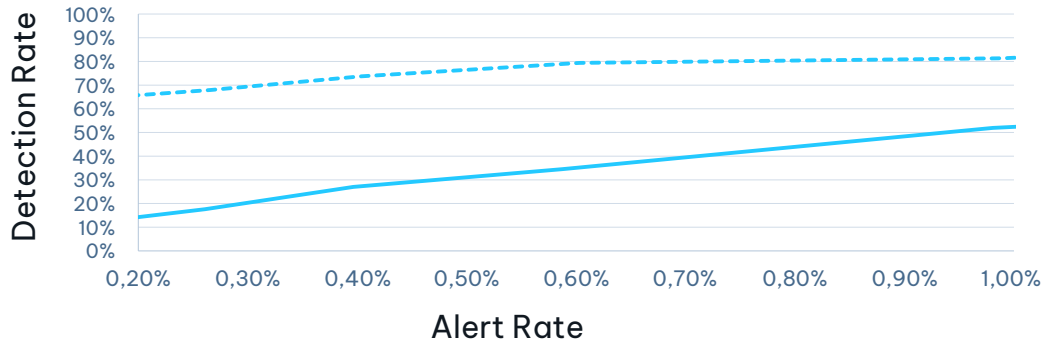
Case Study

In a recent project with a Top Tier European Financial Institution, the FI faced a challenge with detecting and stopping APP Frauds; they were losing an average of £750 per transaction on external domestic transfers due to social engineering attacks.

To address this challenge, NICE Actimize created a model incorporating 52 expert features that identified 2,000 cases of fraud per month, stopping a cumulative £1.5 million in fraud. Combined with the new typology-specific approach, routing cases based on risk scores to teams specializing in specific fraud typologies, the multi-execution model was able to detect more account takeover and social engineering frauds, increasing their fraud detection rate by 270% compared to legacy, transaction-based models. (This financial institution did not have a scams strategy, and out of the gate saw a 270% uplift.)

Top 10 Banks in Europe

Artificial Intelligence Defends Against Social Engineering Fraud



At 1,000 alerts per day, improved fraud detection rate by

270%

Two models

running concurrently for every transaction, including account takeover and social engineering

For domestic transfers,

2,000 fraud cases

identified per month with a value of £750 per case, cumulative value of £1.5 Million avoidance per month

→ Learn More

Solution Strengths to Stay Ahead of the Competition

Data Coverage and Enrichment

Data enrichment on phone signals, payee intelligence, digital channel behavioral analysis, and more to drive additional insights

Scam Specific Analytics and Risk Scores

Data driven expert features and AI models to increase detection rates and reduce false positives, with 20 models running simultaneously

Multi-Dimensional Profiles

Better insight into customer behavior by profiling data on beneficiaries, channel, and transactions in parallel

Collective Intelligence and Insights

Unique insights from cross-FI data that, in turn, is used in enhancing detection of scams/APP fraud

Pre-packaged, typology-specific rule sets

Ability to tailor scam-specific rules to author powerful Day One fraud strategies and adaptability to changing fraud patterns

Scam specific alerts and workflow support

Scam-specific alerts to help route them to analysts who are trained on specific typologies

With IFM-X from NICE Actimize, FIs don't have to worry about upcoming shifts in liability. Multidimensional profiles and typology-centric resolution protect both the FI and its customers. Using multi-model execution and routing with smart workflows specific to scam typologies, fraud operations teams work smarter and more efficiently. Most importantly, only legitimate payments are conducted by the customers, and frauds are stopped.

→ Learn More

NICE Actimize

Know more. Risk less.

info@niceactimize.com
niceactimize.com/blog
@NICE_actimize
/company/actimize
NICEactimize

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

niceactimize.com