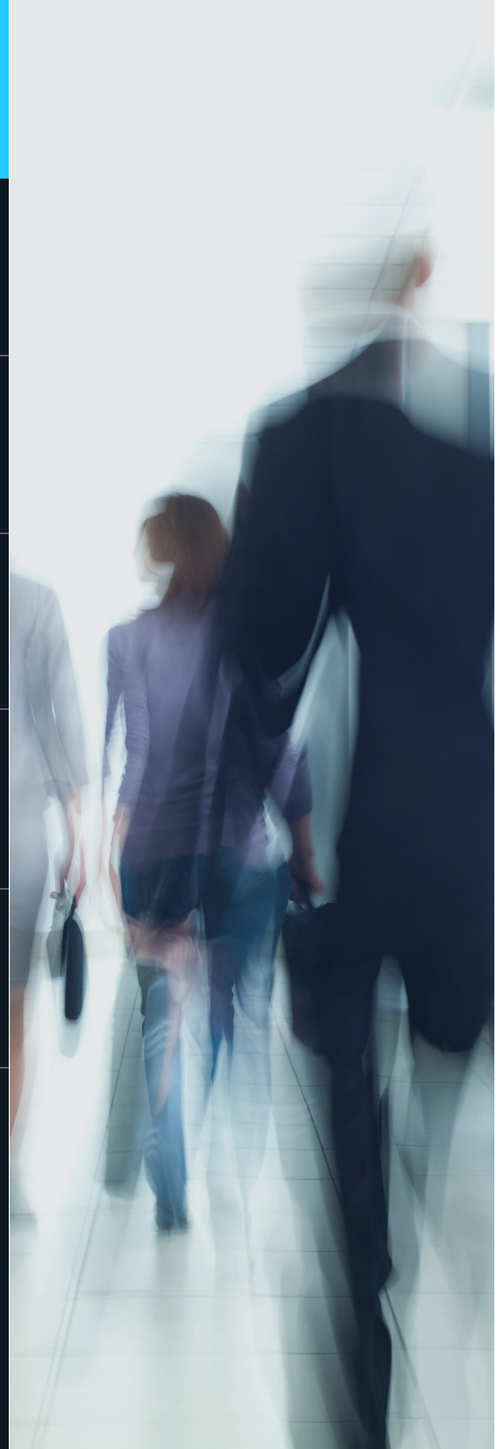
NICE
Actimize

Fight Fraud Fiercely with Mule Defense:

Real-Time Defense.
Transactions Secured.



The Challenge

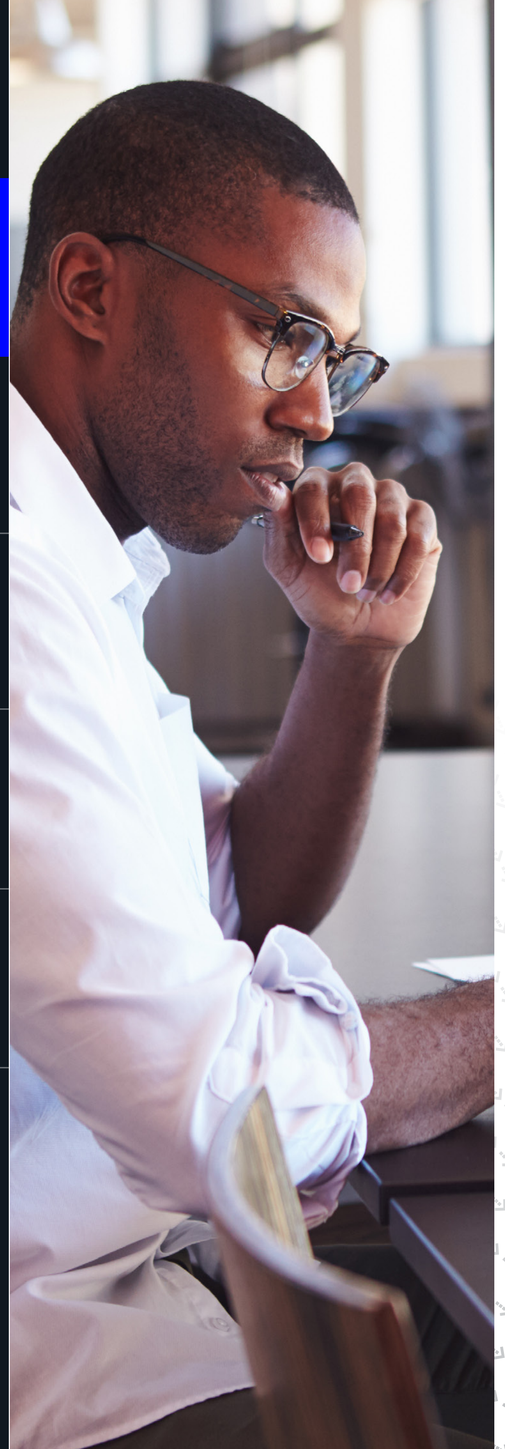
Mule accounts have become an increasingly prevalent element of fraudulent schemes, acting as the primary pathway for moving funds from various sources of fraud, such as scams, check fraud, account takeovers, and authorized push payment (APP) fraud, into the accounts of fraudsters themselves. Startlingly, studies have shown that up to 40% of fraudulent new accounts are mule accounts.

This is a significant issue not only for the financial institutions (FIs) involved, but also for the good customers who may unwittingly serve as mules or who may be denied new accounts due to stricter rules aimed at preventing such activity. Identification of mule accounts is now the current challenge. FIs must continuously monitor throughout the entire customer life cycle, ensuring that if an account becomes a mule (whether knowingly or unknowingly), the FI in question can identify it and take appropriate action; mules have morphed from just a new account issue. Furthermore, the use of advanced analytics can help to minimize false positives, thereby making it easier for proper new accounts to be created by legitimate customers.

The Challenge

With the current regulatory environment and oversight, it is worth noting that there are considerations for potential shift of liability occurring in the banking industry, with FIs increasingly facing possible accountability for inbound transactions of fraudulent funds, not just outbound transactions. With soon-to-be finalized legislation moving through the U.K.'s Parliament, as well as rule changes for popular peer-to-peer (P2P) applications, banks may need to adapt quickly in order to avoid negative monetary and reputational consequences.

Lastly, it is important to recognize that recent spikes in various forms of fraud, including APP and check fraud as well as scams, have only served to increase the risk of mule accounts. Given the fact that mules are a necessary component of shifting ill-gotten gains to fraudsters' accounts, it is perhaps unsurprising that these two phenomena are positively correlated. This represents a significant challenge for banks, particularly given the rise of pressure from movements such as the Contingent Reimbursement Model in the U.K., through which banks are voluntarily reimbursing victims of APP fraud. As such, it is vital to identify suspicious mule account activity before transactions occur, in order to prevent potential liability from falling on the FI.

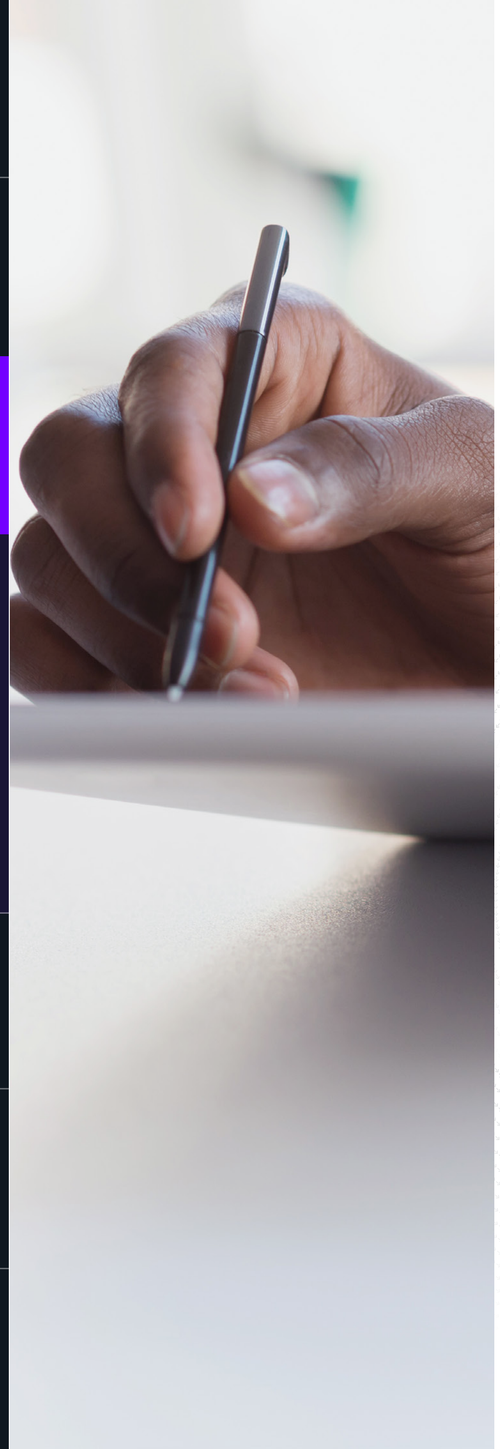


The Solution

IFM-X: Mule Defense not only identifies mule accounts via case-specific models, network analytics, and point-solution enrichment, the solution also provides out-of-the-box strategies for interdiction. This detection and interdiction apply for both new and mature accounts, and continuously monitors throughout the customer life cycle to catch any emergent threats and mule rings.

Money mules have emerged as a major fraud problem in addition to being an anti-money laundering (AML) concern. Rather than simply responding to the shift in liability on a tactical basis, a comprehensive and strategic approach is necessary to address the issue of money mules. It's important to recognize that mule accounts can not only cause financial losses, but also pose a serious threat to the brand reputation of FIs.

Mule Defense is a crucial component of the IFM-X Enterprise Fraud management system. Unlike other point solutions that may be limited by a singular vantage point, Mule Defense can integrate with a network of best-in-class third-party providers to triangulate points of view for risk analysis. With cutting-edge data and advanced analytics at its disposal, Mule Defense can swiftly identify and intercept mule accounts throughout the customer life cycle, ensuring that fraudulent activities are promptly halted, and the FI's reputation remains untarnished.



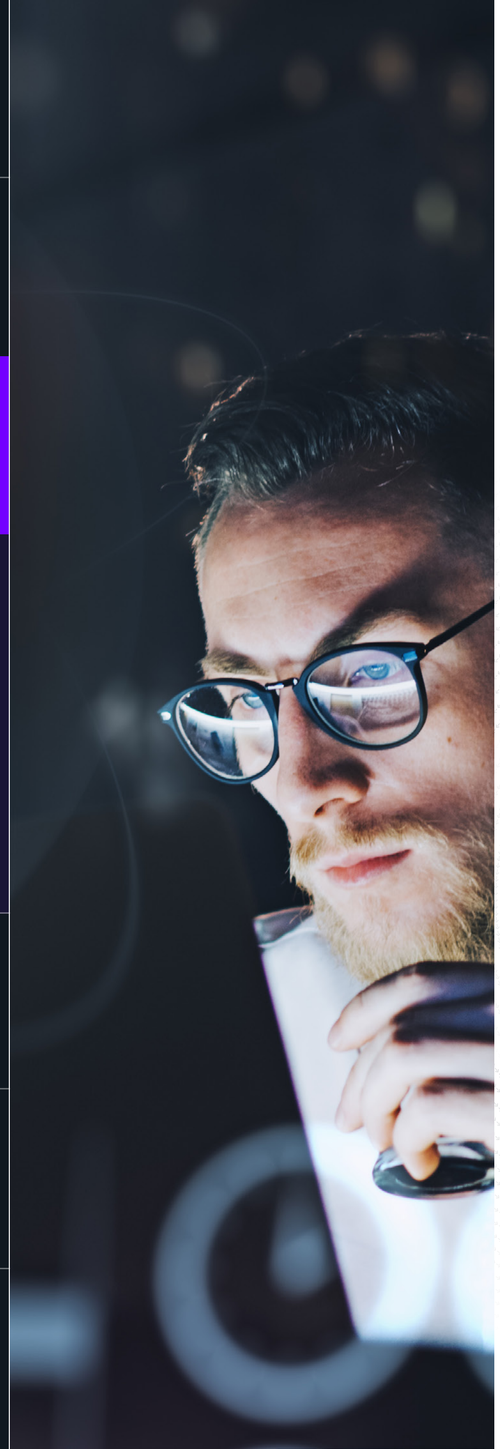
Problem 1
Application & Account Opening

40% of new fraudulent accounts are used for mule activity.[1] Without purpose-built models that can detect and prevent identity fraud and mules, FIs risk both allowing mule accounts to slip by as well as falsely punishing legitimate new accounts from being created.

Resolution

AI-enabled identity profiling models detect stolen and synthetic identity fraud and mule accounts. This allows FIs to stop new mule accounts, thus preventing a double loss—the fraud loss and the loss of the new account underwriting, and additional acquisition costs.

[1] NICE Actimize: 2023 Fraud Insights Report (2023)

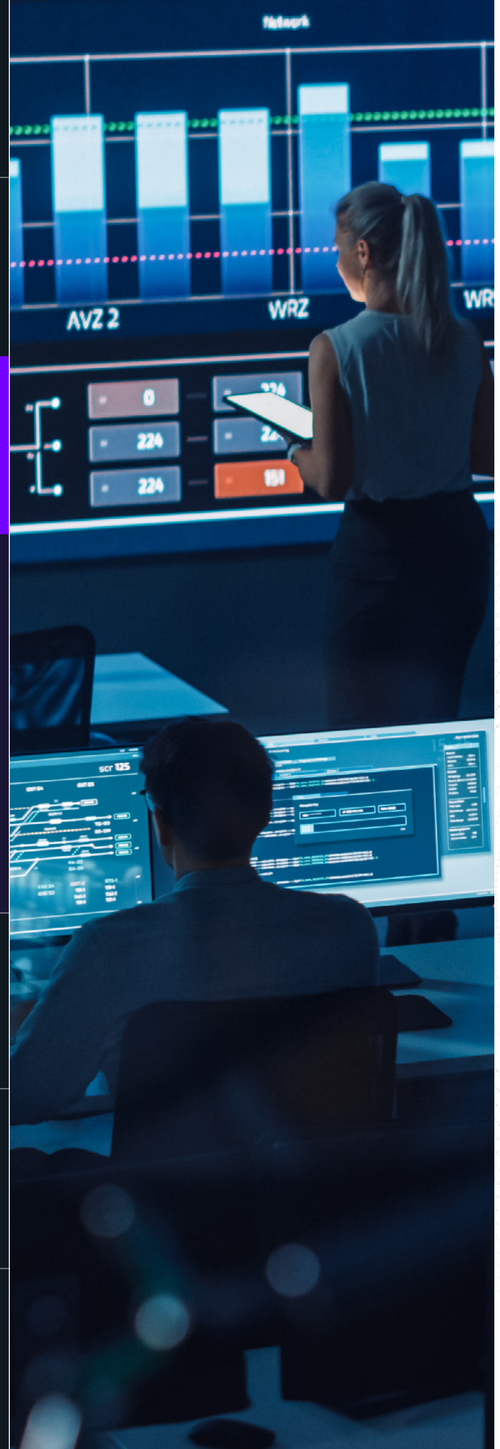


Problem 2
Account Monitoring

In addition to identifying mule accounts during the application and account opening stages, it is imperative for FIs to stop mules across the account's life cycle. Whether an account becomes a mule account wittingly or unwittingly, it can lead to financial losses and/or reputational damage for the FI.

Resolution

Patent pending AI-powered behavioral analytics monitor the account throughout the customer life cycle and identify mules across both early and mature accounts.

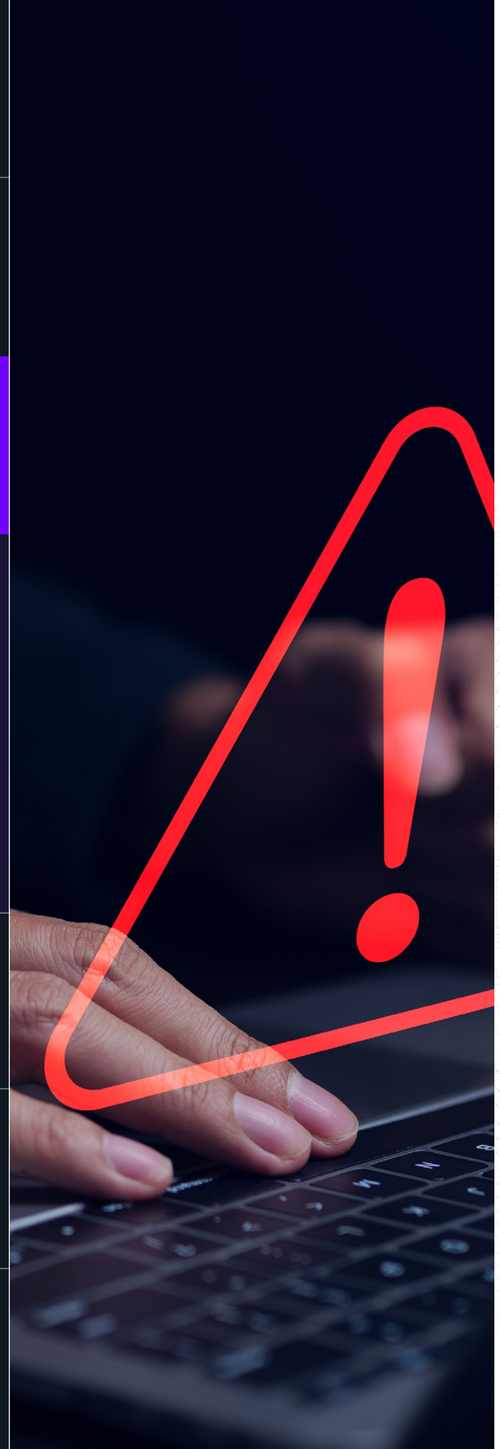


Problem 3
Inbound Transactions

Monitoring and detecting high risk for outbound payments has been the cornerstone of fraud prevention systems. With increased focus from lawmakers and regulatory groups, who are in support of a shift in liability for receiving banks, there is a need to monitor inbound transactions in real-time.

Resolution

Purpose built predictive features detect the risk associated with inbound payments in real-time, allowing banks to withhold funds, place accounts under surveillance, and reduce fraud losses-making it harder for money mules to pass through fraudulent funds.



Problem 4
Network Crime

Besides identifying individual mule accounts, it is imperative that FIs can both identify mule rings that may be plaguing their accounts as well as stop this mule activity.

Resolution

IFM-X Money Mule Defense provides advanced network analytics and packaged network narratives that can identify and stop mule rings, as well as prevent mule accounts from causing damage – either reputational or monetary. The solution achieves this by utilizing multi-model, cross-channel analytics rather than focusing on individual channels.

NICE Actimize

Case Study

In a recent project with a top-tier U.S. FI, the firm faced a challenge with detecting and stopping new account frauds, including mule accounts. They were experiencing a loss of $80 million annually through this typology. The transaction monitoring models they employed only detected $10 million of the total fraud losses, roughly 13%. However, with the new typology-based multi-model execution, not only were they able to increase the detection rate to 58%, but they also caught $48 million in fraudulent transactions as well.

$80 Million Total Fraud Loss Annually*

Transaction Monitoring Models:
13% - $10 Million in Fraud Losses Detected

Mule Defense Solution (Multi-Model Execution):
58% - $48 Million in Fraud Transactions Detected

* For New Accounts Only (≤ 180 days old)

Top Tier US Financial Institution

Monitoring Incoming Transaction Risk with Typology-Centric Fraud Detection

NICE Actimize

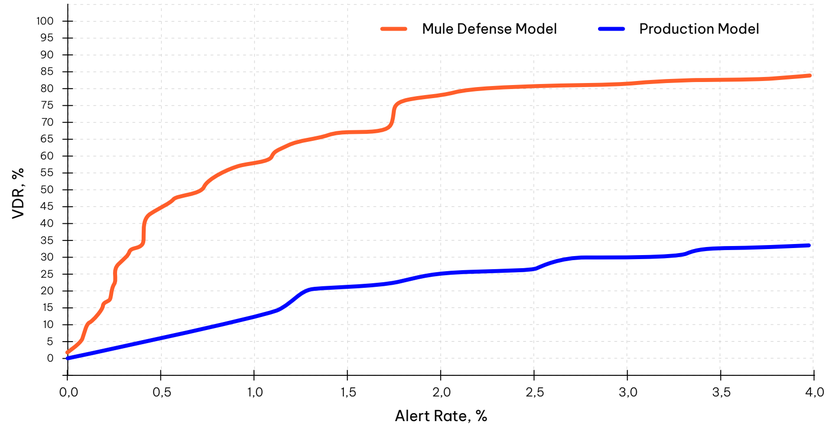
Case Study

The Challenge

- Interdict on incoming transactions and detect suspicious mule behavior
- Previously used a combination of transaction risk models and rules to detect risk
- Large number of frauds were occurring within 30 days of account opening
- High alert volume and a false positive ratio of 89:1

The Solution

- Deployed mule typology-driven detection models that analyze cross-channel activity
- Purpose-built expert features that review sequence of activities
- Segmented profiles and advanced behavioral techniques to determine risk in new accounts



The Outcome - Over One Year

$48M
Total Fraud Prevented

58%
Value Detection Rate (VDR)

45%
Higher VDR than Production Model

Business Value

Data and Coverage

The IFM-X Mule Defense solution monitors mule activity throughout the customer life cycle. This allows for early identification of accounts that could unwittingly become mules and prevents false positives for good new accounts, preserving customer relations and stopping mule transactions and potential monetary loss.

Analytics

Network analytics and advanced modeling methodologies delve deep into the inner workings of mule rings, exposing the illegal activities hidden within the FI's account bases. And with the addition of 3rd-party data that empowers the ability to enrich and augment network information, NICE Actimize's solution delivers a comprehensive, 360-degree view of money mule activity.

Strategy and Operations

The solution provides packaged fraud strategies and context to detect and prevent money mule activities, including uncovering mule rings. The expert features powered by AI/ML are ready to go on day 1, preserving the FI's reputation and keeping regulators at bay.

Wrap-Up

Traditional payments monitoring systems often do not detect money mules' movements as they secure illicit funds from FIs. To address this problem, NICE Actimize has developed a cloud-optimized Mule Defense solution designed to detect, investigate and prevent mule account activity occurring throughout the entire customer life cycle for both existing customers and new accounts. This solution includes the identification of money mules that may either unwittingly be involved in fraudulent transactions or are directly complicit in irregular money movements.

NICE Actimize's Mule Defense solution utilizes deep learning models and purpose-built expert features to detect mule activities across multiple event types and channels in real-time. Connecting the risk elements of mules, the solution identifies compromised accounts and payors by leveraging the power of NICE Actimize's market leading enterprise fraud management platform IFM-X, and vital data from third-party enrichment sources. NICE Actimize also employs a Multi-Model Execution (MME) strategy that use a diverse set of models, techniques, and algorithms to identify and prevent fraud. This allows organizations to quickly adjust their strategy to stay ahead of the most sophisticated fraud schemes. MME offers a multi-dimensional approach to risk assessment, leveraging advanced analytics and machine learning algorithms to gain insights into both authorized and unauthorized fraud and mule activity. By analyzing risk from multiple angles, MME provides a comprehensive view of potential risks.

Using the power of AI and NICE Actimize's collective intelligence across the industry, the solution's model for detecting money mules is continually optimized and enhanced to identify anomalous behaviors and suspicious transactions indicative of money mule activities.

NICE Actimize's Mule Defense solution also leverages the ActOne case management network analytics capability for a holistic view of risk and enhanced ability to uncover entire mule rings.