NICE
Actimize

eBook

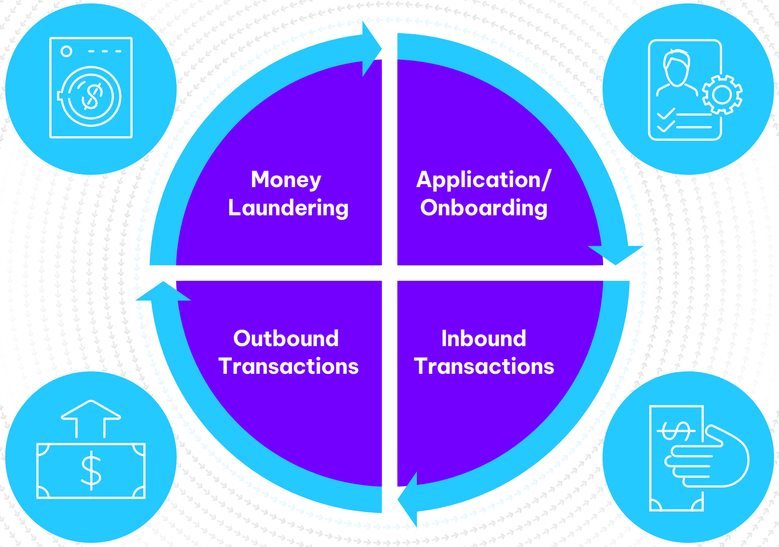
Disrupting Money Mules: The Best Practice Guide for Financial Institutions

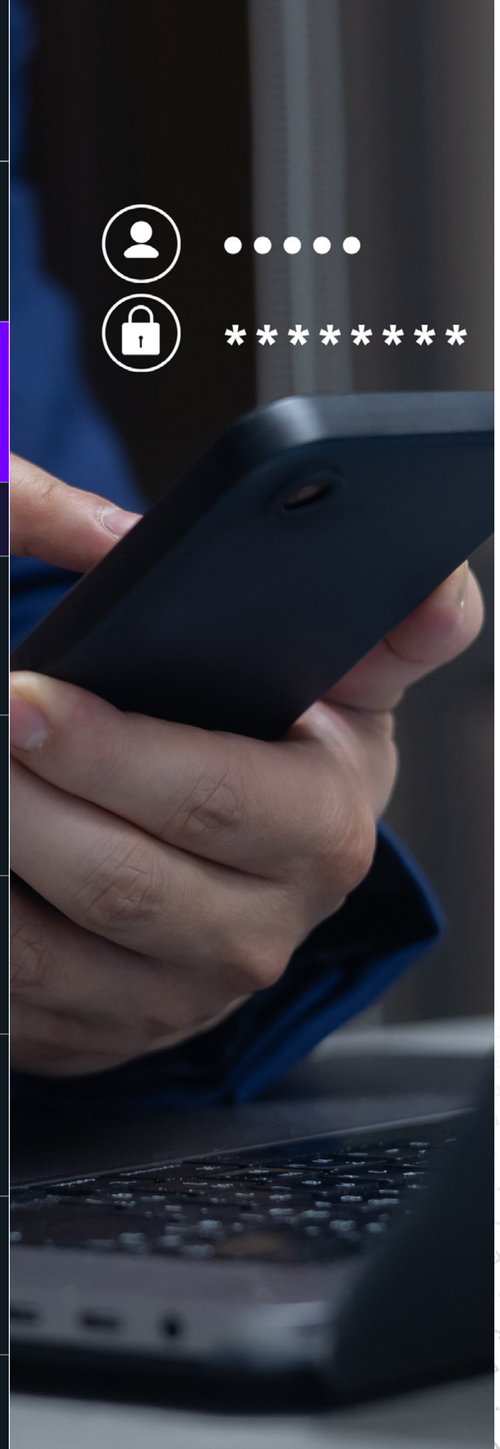
Unmasking Money Mules: A Blind Spot in Financial Crime Programs

Money mules have long been a fixture in financial crime, yet many institutions fail to comprehend the strategic threat they pose. Rather than viewing mules as isolated issues, it's time to recognize that they are a critical component in the broader financial crime ecosystem—spanning both Fraud and AML. In reality, mules likely account for a significant portion of suspicious activity alerts. Not assessing mules as an enterprise-wide risk leads to operational inefficiencies and missed opportunities for early intervention. Reframing mule activity as a cross-institutional risk allows financial institutions (FIs) to streamline investigative efforts while also reducing compliance costs and mitigating broader threats to the integrity of their financial operations.

A Multi-Pronged Strategy for Disrupting the Mule Lifecycle

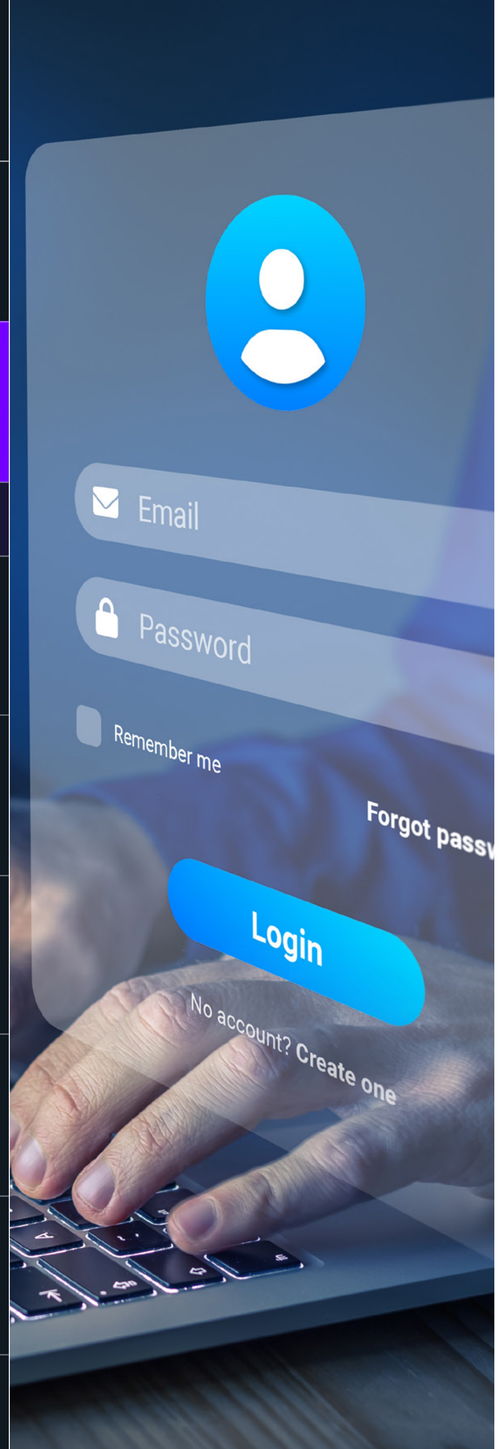
Money mules represent a complex, multifaceted challenge. Whether as the immediate recipient of funds from a scam or other illicit activity, or the downstream launderer of funds on behalf of organized crime, mules serve as essential conduits for illicit money movement, touching every part of the financial crime landscape. Account holders can range from individuals who are naive or have hit financial hardship, to those acting under duress or knowingly complicit in illicit activity. Sophisticated corporate structures are often used to facilitate high-value laundering and payment diversion schemes, fronted by mules. Mules are often embedded deep within transaction chains—appearing not just at the point of entry, but at subsequent movements of illicit funds—making them harder to detect and disrupt. Effectively addressing this issue requires a multi-pronged strategy that goes beyond frontline detection to encompass a deeper understanding of the mule lifecycle and their roles in the broader financial crime ecosystem.





Account Opening and Onboarding

The account opening phase represents a critical point of vulnerability and opportunity for FIs in the fight against money mules. If a mule account is successfully onboarded, it becomes an entry point for the movement of illicit funds, often slipping under the radar for months. Mules at onboarding can consist of individuals or corporate entities. Some individuals may act under coercion or duress, while others are drawn in through social engineering or recruited by criminal organizations. Still others may attempt to open corporate accounts that appear legitimate on the surface, concealing their underlying criminal intent. Common warning signs can include inconsistent identity data, newly formed businesses with limited trading history and repeated use of shared contact details. Intervening at this stage can prevent downstream risk exposure, reduce the alert burden and significantly strengthen financial crime defenses.



How to Take Action: Practical Steps for Early Intervention

Understand and train employees on red flag mule indicators, which may include:

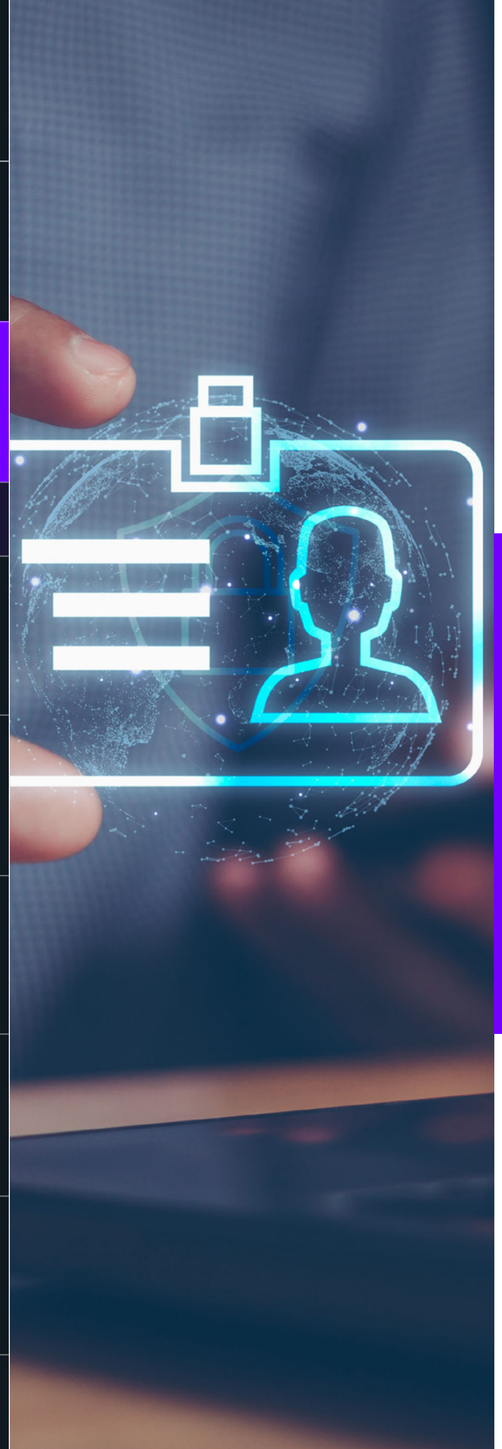
- Inconsistent personal information provided
- Unusual behavior from the customer, such as reluctance to provide information or pressuring to open accounts quickly
- Multiple accounts opened from the same device or IP address
- Vulnerable customer or customer unable to answer basic KYC questions

For prospective customers who exhibit traits of mules, especially when it comes to corporate entities, consider Enhanced Due Diligence to determine:

- How recently was the company established?
- What is the ownership structure?
- What is the intended activity?
- What is the history of the applicant within your organization?

Validate and verify applicant information and documents against trusted internal and external data sources

Investigate repeated use of the same contact information (emails, phone numbers, addresses) across multiple applications or existing customers



Driving outcomes through technology

Advancements in AI and analytics can accelerate the identification of mules during the onboarding process. It is critical that the right information is gathered and verified, and that the customer profile is analyzed for mule red flag indicators, which includes analyzing peer and historic information to drive greater accuracy.

Technology considerations to aid in mule detection at onboarding include:

- AI-powered risk profiling to detect customer risk anomalies or suspicious indicators in real time
- Device fingerprinting and behavioral biometrics to assess identity authenticity
- Corporate registry and universal beneficial ownership (UBO) screening, as well as document validation and verification
- Geolocation, device and IP analysis to identify remote access or fraudulent attempts to open an account

Inbound Transactions

Inbound transactions often provide the first tangible evidence of mule involvement—serving as the initial point where illicit funds enter the financial system. At this stage, inbound funds can originate from new mules or conversion of legitimate accounts into mule accounts, an important distinction from onboarding. Some mules deliberately open accounts with the intent of using them for illicit purposes, while others may have initially opened legitimate accounts that remained active for years before being repurposed for mule activity. In this case, individuals may be coerced, forced or willingly allow their accounts to be utilized as mule accounts. Common indicators are vulnerable people, especially those who have fallen on hard times financially. Students and young people are a common group targeted by organized crime.

If illicit funds go unchallenged at this stage, they are likely to be laundered or redirected quickly through downstream channels. Mules at this stage may receive multiple low-value transfers from unrelated accounts, or large deposits followed by rapid outbound movement. This initial movement of funds can easily go unnoticed without intelligent monitoring and contextual understanding. Identifying and acting on suspicious inbound patterns helps break the flow of illicit money before it is forwarded on and eventually out of the jurisdiction.

Proactive Steps to Identify Suspicious Inbound Behavior

Utilize the information gathered at onboarding, along with any historic information on the customer and their activity, to determine normal vs. abnormal activity

Compare the customer activity against their peers for anomalies

Monitor the account for unusual transaction patterns such as:

- unexpected or unusually large deposits
- frequent credits from disparate or unconnected originators
- movement of funds with no clear rationale

Analyze the customer's interactions to determine how they are accessing the account, what authentication was used and if the devices are in line with expected customer activity

Assess the customer transactions against reported fraud complaints or historic fraud attempts to identify potential associations

How technology can enable solutions

Agile and AI-powered technology plays a vital role in enhancing inbound transaction intelligence, crucial for detecting mule activity at its entry point into the financial system. Identifying suspicious behaviors and interactions, as well as unusual deposits or originators, is pivotal to stopping the movement of funds before they can be redirected or laundered.

Technology that enhances inbound transaction monitoring includes:

- Real-time monitoring of incoming transactions to determine mule activity
- AI-powered anomaly detection tailored for inbound financial patterns
- Link analysis to uncover connected accounts or mule networks
- Dynamic behavioral profiling to understand typical vs. atypical inflow patterns
- Inbound transaction scoring engines that incorporate sender and flow risk

Outbound Transactions

The outbound transaction stage offers one of the most visible indicators of mule activity, particularly when funds are quickly paid out of the account after being received. This is the convergence point between fraud and AML, and where many organizations fail to integrate their monitoring systems. Failing to detect mules here results in the FI being the global financial gateway for organized crime in the distribution of illicit funds, exposing them to fraud losses and regulatory scrutiny. Mule accounts often exhibit suspicious behaviors, such as rapid transfers through the mule accounts, burst payments from unrelated originators or disbursed across unrelated beneficiaries, or payments broken into small amounts to avoid thresholds. These signals may indicate layering or movement on behalf of fraudsters or criminal networks. Detecting and having the ability to stop outbound transactions originating from mule accounts is key to stopping the money flow at its source and mitigating the risk of organizations being used by organized crime.

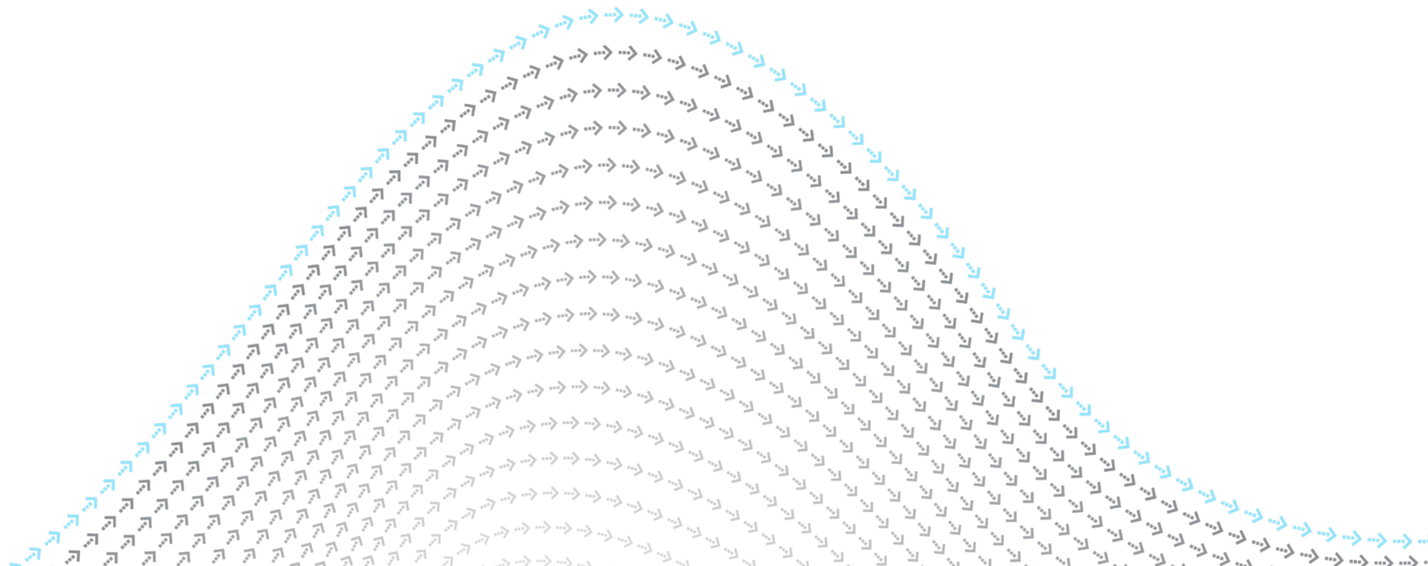
What FIs Should Do to Mitigate Outbound Risks

Monitor for red flags associated with mule activity, such as:

- rapid or structured outbound transactions that follow immediately after deposits
- burst payments disbursed across multiple beneficiaries
- unusual transactions that deviate from expected customer activity

Assess customers against third-party data such as adverse media, fraud watchlists or corporate registry information (where applicable)

Analyze the customer's interactions to determine how they are accessing the account, what authentication was used and if the devices are in line with expected customer activity

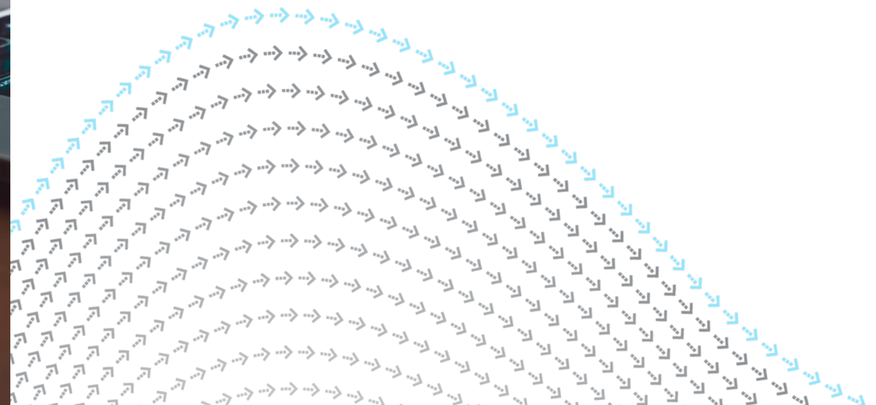


Leveraging technology for impact

Real-time and dynamic monitoring tools are integral when it comes to preventing the continued movement of funds between mule accounts. It is important that FIs set the right transaction triggers for further analysis and that they are constantly assessing both their customers' information as well as their behaviors for potential mule activity.

Tools and technology that strengthen outbound transaction monitoring include:

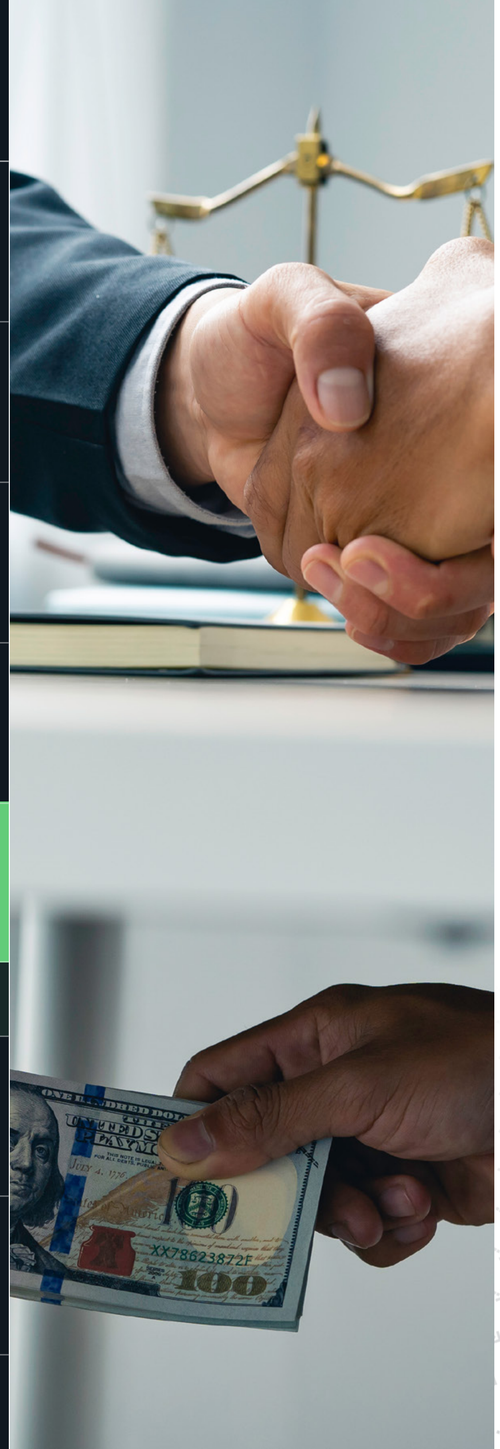
- Machine learning-based transaction monitoring models that detect anomalous behavior
- Velocity checks to flag high-frequency outbound transactions
- Real-time deviation detection from established customer profiles
- Risk-based destination scoring using geographic and network data



Money Laundering

In the final stage of the mule lifecycle, accounts are often deeply embedded in laundering operations, working across networks to layer and integrate illicit funds. This is where complexity and risk become most pronounced. At this stage, mules often transact with other mules; they are rarely aware of each other's existence, with transaction instructions originating from the criminal handler who coordinates the mule network. These networks are global and often span tens or hundreds of hops before the funds are deposited into an account controlled directly by the organized crime gang, or withdrawn to purchase assets on behalf of the criminal controllers. Unbeknownst to many FIs, several hops likely occur between mule accounts within the same FI.

Missed detection here not only enables money laundering to persist, but also increases regulatory exposure and complicates future investigative efforts. Typical behaviors include multi-hop transfers, circular fund movements and the use of shell companies to obscure the true origin and destination of money. These sophisticated tactics require institutions to go beyond surface-level monitoring and leverage advanced analytics to reveal hidden relationships and transaction patterns.



Steps to Uncover and Disrupt Embedded Laundering Activity

Implement monitoring systems to flag certain behaviors that would not be deemed typical, like fund flow-through, burst payments, structuring and unusual transactions compared to the customers' history or peers

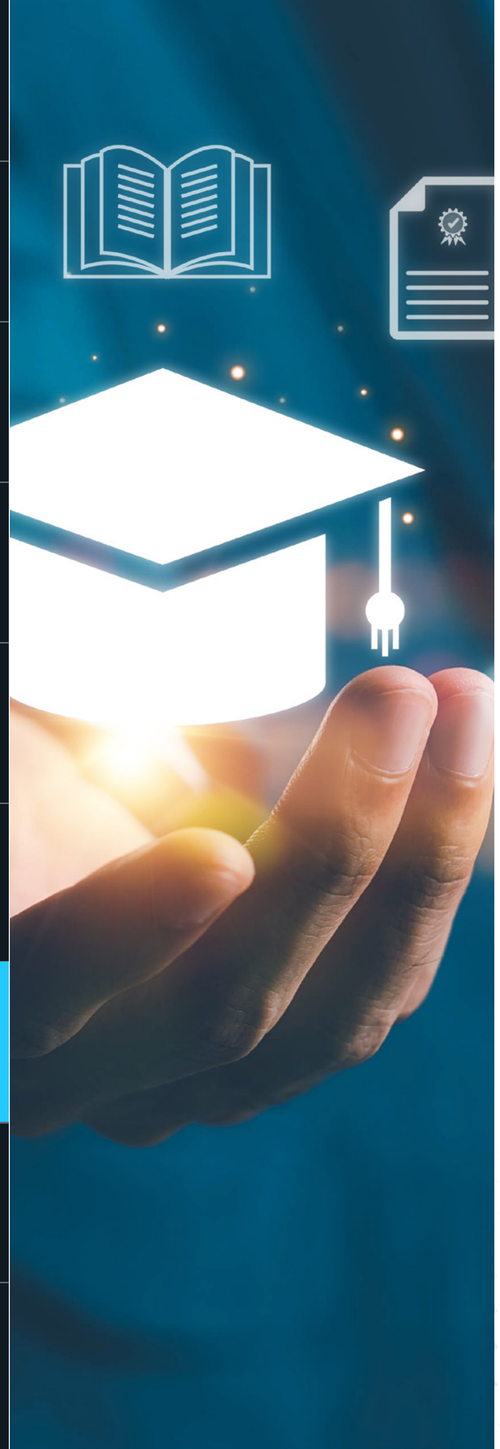
For corporate customers, use KYC or third-party data to identify activity deviations and understand concerns like business nature, company age and reported turnover

Consider utilizing technology such as community analytics to detect networks of mules operating within your organization

Technology Solutions That Power Deeper Laundering Detection

At this stage of the mule lifecycle, the network's primary purpose is to layer the illicit funds, circulating them through FIs and across borders, distancing the funds from the crime, making them available for use by the criminal organizations. AI-driven technology expands and accelerates the detection of anomalies, red flags and connected entities, while providing a unified platform to conduct the necessary investigation for quick and efficient resolutions.

- Entity resolution consolidates customer and counterparty profiles, linking related profiles to identify mule networks
- Community analytics uses graph technology to detect clusters of suspicious networks linked to mule accounts
- Transaction monitoring identifies red flags like fund flow-through, burst activity, fund circulation and transaction value/volume deviations
- Anomaly detection uses unsupervised machine learning to identify subtle, suspicious deviations in customer behavior and transactions that traditional rules-based systems might miss
- Data intelligence tools enrich customer and counterparty profiles for greater clarity on the customer's normal vs. abnormal activity
- An advanced case management platform centralizes alerts to visualize suspicious activity and aid investigation decisioning through tools like agentic AI



The Importance of Educating your Team & Consumers about Mules

A critical but often overlooked aspect of combating money mule activity is education—both for the public and for those within FIs. Many individuals become mules through recruitment, sometimes unaware of the gravity of their actions or the potential repercussions, such as arrest, prosecution or long-term financial consequences. They are usually lured by promises of easy money, manipulated through scams, coerced or threatened into assisting organized crime in moving illicit funds.

Raising public awareness about the risks and legal ramifications of acting as a mule is essential to prevention. At the same time, frontline bank staff must be equipped with the knowledge and training to spot potential mule behavior during face-to-face, telephone or digital interactions with customers —such as unusual account activity, explanations or signs of third-party coercion. By embedding education into both community outreach and internal operations, FIs can play a pivotal role in disrupting the mule pipeline before it begins.

Building a Unified Front: Strengthening Your Defense Against Money Mules

Bringing together proactive detection, strategic intervention, advanced technology and education creates a comprehensive defense against the pervasive threat of money mules. By addressing mule activity at every stage of the lifecycle— and recognizing its interconnected role across fraud and AML— FIs can reduce risk, improve efficiency and protect both their customers and reputations. A unified, intelligence-led approach not only strengthens operational resilience but also ensures a more coordinated and cost-effective response to financial crime.

To learn more about how NICE Actimize can help your organization build a stronger, end-to-end defense against mule activity, contact us today

Get In Touch →

About NICE Actimize

As a global leader in artificial intelligence, platform services, and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime, and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks. Learn more at www.niceactimize.com.

© Copyright 2025 Actimize Inc. All rights reserved.