Lynx

AI against Fraud & Financial Crime

White Paper

Money Mules Revealed

Exposing Mule Strategies, Global Impacts, and the Urgent Need for Real-Time Detection

Table of Contents

Uncovering Money Mules: A Comprehensive Guide

Executive Summary

Organized crime groups (OCGs) are exploiting vulnerabilities in financial institutions (FIs) to recruit and onboard money mules to launder billions of dollars each year. Criminals have adapted alongside changing technologies to target FIs and their customers at scale, leveraging social media platforms, Crime-as-a-Service (CaaS), AI-powered tools, and breached identity data to socially engineer victims, create fake identities, and bypass security measures like Identity Verification (IDV) and Know Your Customer (KYC).

Executive Summary

Money mules play an increasingly crucial role in legitimizing OCG profits from digital crimes such as authorized push payment fraud (APPF), identity theft, and phishing, along with proceeds from physical crimes including drug trafficking, smuggling, and human trafficking. Three main types of money mules — Compromised, Recruited, and Fake Mules — highlight how criminals exploit FIs and use mule accounts to launder money.

Global and regional task forces and regulatory bodies are taking steps to address the serious money mule and money laundering problem. These efforts are driving changes in AML and fraud prevention practices that impact money muling.

FIs globally continue to grapple with financial losses and increased operational costs, and some FIs now face regulatory penalties as illicit funds flow through their systems and fuel more criminal activity. The dynamics of money mules are unique in each region and country. For instance, in the UK APPF and money muling are increasingly intertwined and impactful. New regulations around APPF reimbursement are expected to drive more investment in mule detection technologies. In contrast, across Latin America, new digital banks, person-to-person mobile money transfers, and payment services are increasing financial access for underbanked people and businesses but making it easier for OCGs to commit digital crimes and onboard money mules to launder illicit profits. Regulations remain inconsistent across the region.

Regardless of the region or country, **FIs are facing money mule and money laundering risks due to the real-time availability of their digital products and services, but lack real-time solutions.** They are unable to detect if funds customers receive are from illicit sources or identify if a customer is exhibiting muling behavior in real time. Traditional fraud prevention and AML methods which use unsupervised machine learning (ML) are reactive and ineffective against money mules, allowing mules to launder money unchecked and creating a vicious cycle of crime.

Money muling is a real-time problem that requires a real-time solution. FIs need to detect and stop illicit funds and mules in real time to block suspicious activity, prevent illicit funds from leaving their systems, and shut down mule accounts.

Executive Summary

FIs must use supervised ML models that learn from labeled data and retrain daily to avoid drift and performance degradation given ever-evolving criminal tactics, customer behaviors, and emerging technologies. These models detect more money mules while blocking fewer legitimate transactions.

Lynx's Daily Adaptive Models (DAMs) use supervised learning, retrain with the latest transaction data daily, and integrate diverse non-transaction data sources to detect more money mules. Key benefits from DAMs include real-time detection, improved accuracy, reduced operational costs and analyst fatigue, and enhanced regulatory compliance.

Lynx built one Tier 1 banking customer a money mule DAM which achieved a **65% Account Detection Rate (ADR) and a 70% Value Detection Rate (VDR) at a low rate of 10 false positives per 10,000 transactions**— a significant improvement over the bank's previous model— with a response time of less than 100ms.

Reach out to schedule a proof of concept, no PII required. Lynx will analyze your transaction data to demonstrate how many undetected or dormant mule accounts you have and how much money you could save.

Website: lynxtech.com
Email: info@lynxtech.com

> *Financial Institutions (FIs) struggle to keep up with the growing money mule problem.*

Introduction

Organized crime groups (OCGs) around the world are successfully committing authorized push payment fraud (APPF), identity theft, phishing, and other scams. They increasingly utilize money laundering infrastructure to move money through financial systems, legitimizing their illicit profits from these digital crimes and physical crimes such as drug trafficking, smuggling, and human trafficking. A 2024 Nasdaq Verafin report found that an estimated $3.1 trillion in illicit funds flowed through the global financial system in 2023; fraud scams and banking fraud schemes alone accounted for $485.6 billion in losses.

Money mules play a crucial logistical role in money laundering by facilitating the flow of illicit funds. Mules are individuals, or fabricated identities in some cases, who are recruited or coerced into moving illicit funds through their bank accounts to obscure the origin of criminal money. Money muling is a persistent global issue with links to every aspect of organized crime, including cybercrime; in fact, Europol reports that over 90% of money mule transactions are linked to cybercrime.

Financial Institutions (FIs) struggle to keep up with the growing money mule problem, unable to detect and stop money muling as illegal funds flow into and out of mule accounts in real time. As a result, FIs face financial losses, operational costs, and potential regulatory penalties. Customers who lose money in scams often don't recover their funds, with many suffering life-altering losses.

FIs need a real-time solution to address this real-time money mule problem. They must intercept money mules before illicit funds leave their systems, reducing criminal funding and slowing down OCGs, thus preventing further criminal activity.

This white paper explores the complexities of the money mule problem and presents a path forward to halt muling activities. It discusses how mules are recruited and created, how they operate within the criminal cycle, the regulatory landscape surrounding money laundering globally, and the necessity of leveraging advanced supervised machine learning (ML) technology to stop mules and illicit money flows in real time.

Money Mules 101

Criminal operations are only successful if they generate profits. These profits must be cleaned and laundered to obscure their illicit origins.

Once OCGs obtain illegal funds, they must launder the money to make it appear as if it has been legitimately obtained. Here is how the process works.

OCGs Generate Money Through Criminal Activities

OCGs may:

- Steal or skim credit and debit cards (unauthorized fraud).
- Manipulate or socially engineer victims into sending them funds (scams and APPF).
- Coerce victims into sharing login credentials and identity documents, taking over the victims' financial accounts and stealing funds (account takeover (ATO) and identity theft leading to unauthorized fraud).
- Threaten to harm victims or their loved ones if they fail to pay (extortion).
- Cultivate, manufacture, distribute, and sell illegal substances (drug trafficking).
- Coerce or force individuals into human trafficking, child slavery, or prostitution.
- Utilize digital platforms to facilitate the sale of resources from illegal mining and deforestation in LATAM, laundering these proceeds through online marketplaces and complex financial networks.

OCGs then route the illegally obtained money through banking systems in order to clean it (money laundering). This is where money mules become crucial in the process.

Money Mules Launder Illicit Funds

Money mules are logistical intermediaries in the criminal cycle that launder money. Money mule accounts receive and transfer illegally obtained funds on behalf of criminals. Muling disguises the illicit origin of funds, making it difficult for FIs and law enforcement agencies to trace the criminal money trail, ultimately legitimizing OCG profits. These profits are then reinvested to facilitate further crimes including fraud, human trafficking and exploitation, and terrorist activities.

Money mules can be categorized into three main types, as shown in ***Figure 1:*** Compromised Mules, Recruited Mules, and Fake Mules. These categories highlight various methods by which criminals exploit accounts for money laundering purposes.

Compromised Mules	Recruited Mules	Fake Mules
Criminals gain unauthorized access to legitimate bank accounts and use them for muling.	Individuals are recruited to actively or passively enable muling within their accounts. They may or may not be aware of the illegal nature of the activities they perform or allow.	Criminals create fictitious identities with synthetic data to open bank accounts and use them for muling.

Figure 1

Compromised Mules

Compromised Mules, also known as third-party fraud, involves a legitimate bank account that has been compromised (accessed by criminals without the account holder's authorization). Criminals gain unauthorized access to the victim's account through phishing, identity theft, one-time password (OTP) theft, ATO, or other methods. If there are funds within the account, criminals may withdraw them before using the compromised account to launder stolen funds.

Recruited Mules

Recruited money mules, also known as first-party fraud, involves individuals who are solicited to perform money muling using their bank accounts. These individuals may actively participate in muling activities or may passively give their account access to others. They may or may not be fully aware of the illegal nature of these activities.

Active and Unaware Mules

One common example of an active yet unaware recruited mule is a person who responds to an online job advertisement that promises high earnings for minimal work. These individuals find out that the "job" involves receiving and sending funds through their bank account, unaware that they are laundering illegal funds for a criminal organization.

Passive Mules

One prevalent example of a passive recruited mule is when university students in the UK are targeted and recruited over social media or face-to-face interactions, with the promise of making an easy few hundred pounds. Students share access to their bank accounts and cards for a brief period like a weekend - no questions asked. Criminals then use their accounts for muling before returning access. In return, the students

receive a one-time payment, often without the students realizing the criminal implications. It's also important to note that university students tend to have low balances and are more likely to accept such offers - a fact that criminals capitalize on. OCGs aggressively recruit students using this method; in fact, 65% of all mules in the UK are 30 years old or younger.

Another notable example of passive recruited muling occurs in Singapore, where citizens are recruited to sell access to their Singpass (a government-sponsored digital ID). Criminals purchase the identities to open or take over financial accounts for money muling, enabling illicit activities regardless of the individual's awareness.

The Serious Implications of Being a Money Mule

In all cases of recruited mules, the implications for mules are significant, even when unaware that they are laundering funds or enabling money laundering. Suppose a bank detects muling activity associated with an account. In that case, it signals potential fraud, leading to flags and shutting down the individual's accounts and any associated financial products, preventing them from accessing their accounts, student loans, and mortgages. The bank will report the activity to law enforcement, possibly resulting in criminal penalties. Former mules can suffer from lost employment opportunities, low credit scores, and a persistent lack of access to financial products and services for extended periods of time.

Fake Mules

Fake money mules, also known as new account fraud, involves the creation of fictitious identities that criminals create with synthetic data to open bank accounts for money muling purposes.

Synthetic Identities

Criminals generate synthetic identities by combining stolen and fabricated data. They might use stolen national identification numbers to create new identity records, embedding legitimate-seeming data such as names and addresses, then manipulating visual identification using automated tools

to fashion convincing fake identity documents. Criminals might set up an online history with fake social media profiles and email accounts to further the illusion of legitimacy.

Gaps in IDV and KYC

Criminals exploit weaknesses in Identity Verification (IDV) and Know Your Customer (KYC) processes in financial institutions and use synthetic identities to open bank accounts for money muling.

Some gaps arise due to IDV vulnerabilities. Consider that IDV fundamentally checks if the identity data the customer inputs during account onboarding, including visual data from facial recognition, matches the data on their identity documents. However, existing IDV often does not utilize, for instance, Public Key Infrastructure (PKI) technology to check Radio Frequency Identification (RFID) chips in identity documents that confirm the validity of data on the document. In other cases, the onboarding application that initialized the camera for the facial recognition check may be insecure and vulnerable to a real-time injection or overlay attack. Additionally, criminals can create fake histories for new email accounts in IDV processes that rely on "scoring" email legitimacy. In all of these cases, the lack of integration between IDV and KYC procedures allows criminals to leverage these weaknesses to create and manage mule accounts without detection.

Decoupled Systems

Another key reason criminals succeed in using synthetic identities is when IDV is decoupled from KYC, as in many FIs. Onboarding data may not be coupled with application data, which in turn may not be coupled with login and transactional data. This decoupling prevents FIs from reconciling identities with customer behaviors and allows criminal groups to successfully create bank accounts with synthetic identities and then operate mule accounts without detection.

For instance, FIs may not realize that an identity is synthetically created in the first place or that an automated attack was used to onboard the account (IDV). Then, due to the separation of IDV and KYC, they aren't aware when a separate criminal from a different location has logged in to the account to perform money muling and transfer the funds (KYC), or if a criminal group is using bot-like services to automate muling activity. This separation can enable criminals to use synthetic identities to open bank accounts and manage mule operations seamlessly, as monitoring systems fail to reconcile disparate data sources.

The State of Money Muling Globally

There is considerable variance worldwide in how organized crime groups (OCGs) leverage money mules, how regulators implement AML regulations and guidelines, and how FIs implement or fail to utilize technology to detect money mules. This section provides a snapshot of the global mule problem and regulatory environment. It also examines two regions — the UK and Latin America (LATAM) — to highlight the unique context in which money mules operate and how FIs and regulators are working to detect and stop mules.

AML Regulations and Money Muling Risks Around the World

Global regulatory efforts, such as those by the Financial Action Task Force (FATF) and regional efforts like the EU's Anti-Money Laundering Directives and the Financial Action Task Force of Latin America (GAFILAT), are driving changes in AML practices that impact money muling. Countries that are part of these groups develop laws and regulations to meet agreed-upon requirements and recommendations. Subsequently, FIs in these countries must comply by enhancing their AML practices and investing in more effective AML and fraud prevention technologies, which help curb money muling.

In addition, sanctions play a crucial role in stopping mules. Global and regional bodies, such as the UN and EU, and individual countries issue financial sanctions against various individuals and organizations associated with terrorism, human rights violations, and money laundering activities. In-scope FIs must screen customers, organizations, and transactions against sanctions lists to prevent illicit activities. This helps reduce the risk of enabling money laundering and muling, terrorist financing, fraud, and other crimes.

Each country and region has a unique AML regulatory posture and money laundering risks. ***Figure 2*** below provides a sample of key AML regulations, financial sanctions lists, and AML Index risk scores from the Basel AML Index 2023 to highlight regional variations.

Country/Region	Key AML Regulations and Financial Sanctions Lists	AML Index risk score 1 (low) to 10 (high)	Additional notes
Global	FATF recommendations UN Security Council Sanctions List	5.31	
LATAM	Financial Action Task Force (FATF) of Latin America (GAFILAT) Recommendations	5.4* (*Includes LATAM and the Caribbean)	
European Union	6th Anti-Money Laundering Directive EU Financial Sanctions	3.96* (*Includes the EU and Western Europe)	EU member states' AML regulations are largely driven by the EU's AMLDs.
Belgium	Anti-Money Laundering (AML) Law	4.13	
Brazil	Law 9.613 (Anti-Money Laundering Law)	N/A (not included in report)	
Czech Republic	Act No. 253/2008 Coll.	3.82	
Finland	Act on Preventing Money Laundering and Terrorist Financing	2.96	
Greece	Law 4557/30.07.2018	3.7	
Hungary	Act LIII of 2017	4.94	
Italy	Legislative Decree 231/2007	4.56	
Luxembourg	Law of 12 November 2004	3.67	
Netherlands	Anti-Money Laundering and Anti-Terrorist Financing Act	4.15	
Norway	Anti-Money Laundering Act	3.45	
Poland	Polish AML Act	4.46	
Portugal	Law No 83/2017 of 18 August	4.08	
Romania	Law no. 129/2019	4.9	
Spain	Royal Decree-Law 7/2021	3.96	
Sweden	Money Laundering and Terrorist Financing (Prevention) Act	3.2	
Switzerland	Anti-Money Laundering Act (AMLA)	4.05	
United Kingdom	The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 PS23/4: APP scams reimbursement Sanctions List from the UK Sanctions and Anti-Money Laundering Act 2018	3.66	
United States	Bank Secrecy Act PATRIOT Act Anti-Money Laundering Act of 2020 OFAC Sanctions Lists	4.3	Legislators in the US recently introduced the Protecting Consumers from Payment Scams Act to protect consumers from payment fraud, with provisions for shared reimbursement liability among sending and receiving FIs.

Figure 2

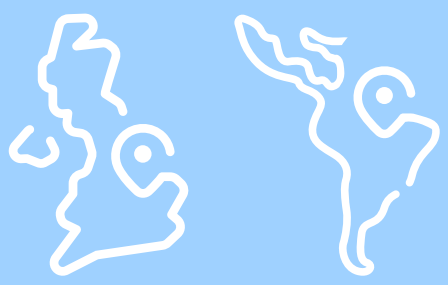
Regional Money Mule Case Studies:

The UK and LATAM

This section presents regional case studies of the UK and LATAM to provide concrete examples of how money mules can operate in different contexts and how regulators and financial institutions (FIs) are responding to the problem.

Case Studies

The UK and LATAM



Case Study:
Money Mules in the UK

Money muling is a growing problem in the UK. The National Crime Agency estimates that £10 billion of illegal money is laundered each year in the UK and CIFAS found that over 37,000 bank accounts demonstrated money muling behavior in 2023. Some estimates project that nearly 40% of all dirty money globally is laundered through London and UK crown dependencies and territories.

Organized Crime Groups (OCGs) use these mule accounts to launder proceeds from crimes including drug trafficking, human trafficking, and financial crimes such as Authorized Push Payment Fraud (APPF), a particularly impactful type of fraud in the UK. The Payment Systems Regulator's (PSR) latest data shows that in 2023, UK victims reported 252,626 APPF cases costing almost £341 million.

Contributing factors

Several factors enable money muling in the UK. Advanced real-time payment systems such as the Faster Payments Service (FPS) and the Clearing House Automated Payment System (CHAPS) bring numerous benefits to consumers and businesses but also facilitate the rapid and irrevocable transfer of illicit money, making it difficult to detect. In addition, nimble Fintechs frequently create new digital products and services with lower-friction digital account onboarding, transfers, payments, and investing. These FIs may have weaker security controls than more established banks, given their limited resources, creating security gaps that criminals exploit.

Even though the UK has regulations mandating IDV controls, many UK-based FIs still struggle to implement foundational static AML practices like screening and KYC and lack robust IDV during onboarding, increasing the risk of unauthorized account use and fake mules. Further, most UK-

based FIs lack the ability to detect mules and illicit funds flowing into customer accounts in real time.

The UK also grapples with high levels of cybercrime. Sophisticated OCGs exploit social media and Cybercrime-as-a-Service (CaaS) platforms, targeting victims, committing fraud and other crimes, and recruiting unsuspecting individuals as money mules. Criminals have quickly adopted new AI technologies to generate deepfakes and synthetic identities that bypass IDV, facilitating the mass-onboarding of mule accounts.

Regulatory Environment

The UK's regulatory bodies have stepped in to protect consumers in response to rising fraud and money laundering rates. The most notable recent development is the PSR's new APPF reimbursement rules for FIs using FPS.

Starting on October 7, 2024, the rules require APPF reimbursement liability to be split 50/50 between sending and receiving FIs. Financial institutions must reimburse APPF fraud up to £85,000 per claim, with no minimum amount, and must refund most APPF victims within five business days. Pay.UK, the operator and standards body for the UK's interbank retail payment systems, oversees regulatory monitoring and enforcement, requiring FIs to report transaction data to Pay.UK monthly.
The PSR's reimbursement rules mark a significant step towards protecting consumers and limiting APPF and are at the forefront of efforts to stop money muling. Both sending and receiving FIs are held responsible for the costs of APPF and are incentivized to detect inbound payments associated with fraud, the money mule accounts these payments are sent to, and outgoing fraudulent payments. The high reimbursement maximum of £85,000 encourages increased investments in robust fraud and money mule detection and prevention systems. This new regulation has the potential to stop more financial crimes, enhance consumer reimbursements and protections, and reduce criminal funds in the UK's financial ecosystem. These new rules are expected to influence regulatory changes globally, with jurisdictions from the EU to Asia to the Americas paying close attention to how the regulations impact financial crime.

Case Study:
Money Mules in Latin America

The Magnitude and Root Causes of Latin America's Mule Problem

In LATAM, Organized Crime Groups (OCGs) perpetrate crimes like drug trafficking, extortion, human trafficking, and smuggling, generating significant illicit profits which they then launder. A 2021 report from the Economic Commission for Latin America and the Caribbean estimated that tax evasion and illicit financial flows are around $325 billion per year in the region.

In LATAM, criminals benefit from significant data breaches and rapidly shifting digital banking products. Pervasive identity data breaches have impacted millions in countries across Latin America including Costa Rica, Argentina, Mexico, and Colombia, with major cyberattacks directly targeting government institutions and databases. For instance, in early 2024, cyber researchers discovered an exposed database containing personal information including names, dates of birth, and taxpayer identification numbers for over 220 million Brazilians — potentially the entire population of the country. Peru has also seen numerous high-profile identity data breaches impacting millions, in healthcare, telecommunications, and the national registry. These breaches give criminals ample opportunities to purchase stolen data, commit identity theft, launch targeted scams, create synthetic identities, and recruit money mules. In the region, mules are often referred to as "dwarf" accounts or "Orange accounts".

Latin America's unique digital banking products and markets are pivotal in the money mule problem. New digital banks and person-to-person mobile money transfer and payment services increase financial access

for underbanked people and businesses. Anyone can create bank and payment accounts using just a phone number, often with little to no IDV, even from prepaid devices like “burner” phones. The widespread adoption of cryptocurrencies in Argentina, Brazil, Colombia, El Salvador, and Mexico, coupled with inconsistent and weak regulations, has further spurred crypto-fueled money laundering, extortion, and fraud,

While new financial products and technologies have certainly improved financial access, OCGs increasingly exploit the low-friction ecosystem to create accounts and commit APPF and other scams, extortion, and money laundering.

Current AML regulations and effectiveness vary significantly across the region. According to the Basel AML Index 2023 report, in aggregate, Latin America’s AML and anti-terrorism frameworks and laws approach global averages, but money laundering investigations and prosecutions remain generally ineffective. If FIs and regulators fail to enact serious changes, the money mule problem can and likely will worsen.

A Common Muling Scenario in LATAM

Here’s one typical method LATAM OCGs use to target FIs and their customers for financial gain. A criminal, often in prison, uses a prepaid burner phone to set up a digital banking account. They then target and socially engineer victims by impersonating a loved one or authority figure, committing fraud, or by threatening harm, committing extortion. The victim sends funds to the criminal’s account.

The then criminal works with a money mule outside of the prison who withdraws the funds from the account at an ATM. The mule cleans the funds through a series of transfers between money mule accounts, which, like the fraudulent account, are all easily established using prepaid devices. This chain of crimes is typically orchestrated by an OCG that recruits numerous criminals and mules to scale its operations, ultimately funding additional criminal activities.

Reactive Solutions Don't Address the Real-Time Money Mule Problem

Currently, FIs struggle to identify and prevent illicit money from flowing through their systems in real time, unable to detect when funds customers receive are from illicit sources or identify when a customer account is exhibiting muling behavior.

Figure 3 visualizes the basic money muling scenario in most FIs today. When an originating account sends funds into a customer's account, the FI needs to identify if the originating account is an illicit source of funds but does not have a real-time tool that can quickly or accurately do so. If the funding source is illicit and the customer account is being used for

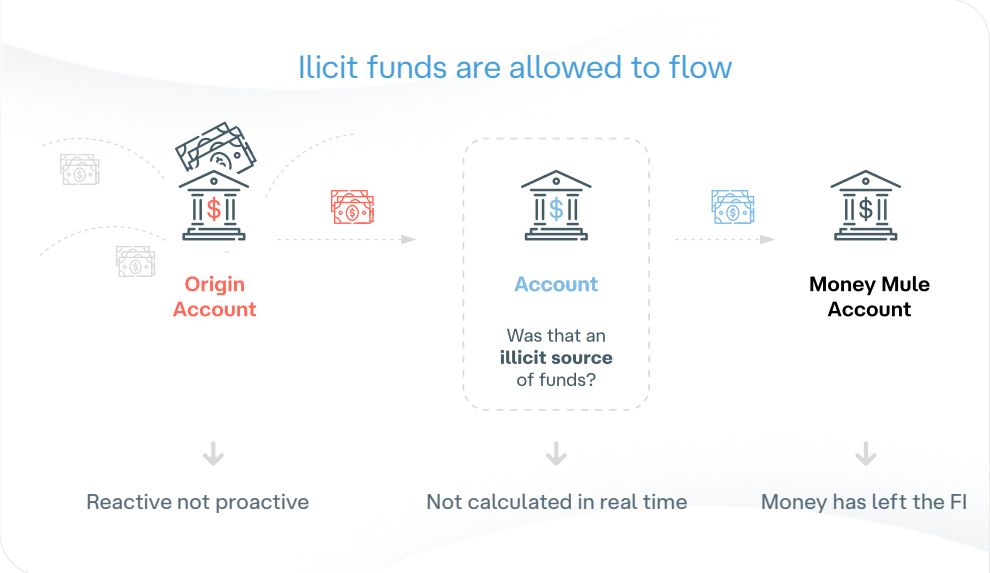


Figure 3

money muling, the illicit funds quickly move from the customer's account to another mule account outside of the FI. Illicit funds flow through the FI unabated.

This scenario continues because current solutions remain reactive and are not designed to stop real-time money muling. **Solving this real-time problem requires real-time solutions.**

Outdated Fraud Prevention and AML Approaches Falls Short

When FIs and AML teams monitor transactions, they tend to use unsupervised machine learning (ML) models to identify and flag unusual long-term account activity associated with money laundering. The goal is not to stop money laundering as it happens; but rather, to learn about the criminal activity network and sharing suspicious activity reports with law enforcement as soon as possible for wider takedown efforts. In this framework, teams aim to avoid alerting criminals by observing criminal activity and gathering intelligence on broader criminal networks instead of immediately halting money laundering.

This reactive approach no longer works. Unsupervised ML models generate many false positives, as the unusual activity they detect doesn't always equate to money muling. In addition, these models are unable to accurately identify money mule accounts in real time.

FIs now face money laundering risks based on the real-time availability of their products and services: nearly anyone can set up a bank account online in just minutes and financial tools and products are more accessible than ever. Fintechs constantly introduce new products, services,

> *Solving this **real-time problem** requires **real-time solutions.***

payments, and transaction types. Real-time payment rails are widespread and enable instant, irrevocable payments, making fraud and muling easier to commit and harder to stop.

Criminals have adapted alongside changing technologies to target vulnerable FIs and their customers at scale:

- OCGs use social media platforms to gather identity information, target victims, recruit money mules, and construct fake identities.
- Attackers capitalize on widespread data breaches and Crime-as-a-Service (CaaS), purchasing exposed identity data, user credentials, and illicit AI-powered tools that automate social engineering scams.
- Criminals sniff out weaknesses in digital-only onboarding processes and exploit vulnerable IDV to launch identity and account takeover (ATO) attacks, creating money mule accounts to launder money.
- Criminals rapidly invoke breached data using CaaS technologies, applying for banking products, generating fake documents, and slipping through onboarding undetected.
- Well-funded OCGs profit and reinvest in broader cycles of crime.

FIs Struggle and OCGs Benefit

In the current environment, FIs often miss entire attack sequences as criminals quickly onboard numerous money mule accounts, launder money through them, and close them without detection. Unsupervised ML solutions perform far worse than supervised models and are not able to accurately detect this money laundering and muling behavior. FIs are burdened with significant financial losses, and heightened operational costs, and analysts experience alert fatigue due to disparate data and high false positives. The ongoing demand for stronger regulations, such as the UK's APPF reimbursement rules, adds to the challenges, requiring significant resources and procedural changes among fraud and compliance teams.

The inability to stop money mules in real-time enables illicit funds to flow unabatedly, ultimately supporting more crimes and money laundering, creating a vicious cycle that demands urgent change.

Stopping Money Mules with Real-Time Supervised Machine Learning

FIs need real-time detection capabilities to address the real-time money mule problem. They must be able to detect and stop illicit funds and mules in real time, blocking suspicious activity before it leaves their systems, shutting down mule accounts, and catching attempts to onboard mules. These capabilities need to extend throughout the FI, from in-person bank branches and ATMs to digital banking, mobile applications, and phone banking.

This is only possible with advanced ML models that operate in real time. Calculating the financial behavior of an account that has received money, sent money, or is receiving money inside and out of the financial institution. Human-created rules alone cannot manage this complex task. Financial products and payment types constantly change alongside consumer behaviors and criminal attack methods. Humans can't comprehend the complex and ever-changing relationships between the tens of thousands of data points that are present in digital transactions, much less manually writing and updating enough rules to effectively stop money mules without blocking legitimate customer behaviors. Advanced ML algorithms and techniques are essential to process the complex money mule problem and accurately detect and stop muling.

Traditionally, AML tools have relied on unsupervised ML models that perform inadequately, failing to detect enough mules and inundating analysts with false positives. FIs need to use supervised ML models trained with labeled data, given the thousands of data points involved in a single transaction. These models perform more accurately and detect more money mules and illicit funding sources while reducing false positives.

These ML models must also quickly adapt and retrain to avoid drift and performance degradation given the fast-changing criminal tactics, customer behaviors, and emerging products and technologies. Static models that retrain infrequently perform worse over time, detecting fewer mule accounts and behaviors.* These models must train with more than just transactional data, as account data, onboarding data, and non-monetary transactions are all crucial to understanding and detecting money mules.

Explore Machine Learning Insights

For a detailed discussion of Machine Learning and the model construction process, read Lynx's comprehensive white paper, "Detecting Fraud in Payment Systems with Supervised Machine Learning."

Lynx Uses Daily Adaptive Models to Detect and Stop Money Mules

Effective detection of money muling activities relies on the use of daily adaptive machine learning models (DAM). Developed from our expertise, these models continuously update through retraining with new data, enabling financial institutions (FIs) to swiftly adapt to the latest criminal methodologies and trends in financial fraud. This adaptive approach is crucial for maintaining detection accuracy amid constant innovations in financial products and evolving customer behaviors.

Figure 4 demonstrates the process by which Lynx's real-time solution identifies money mule accounts. By integrating diverse data sources, such as customer account activities and transaction histories, these models refine their understanding of patterns associated with money mule activities. This allows for real-time risk scoring, distinguishing between suspicious and legitimate transactions, and stopping mules in their tracks to prevent illicit funds from leaving the FI without blocking customers' legitimate transactions. After all, just because a customer's behavior is unusual, it doesn't mean it's money muling.

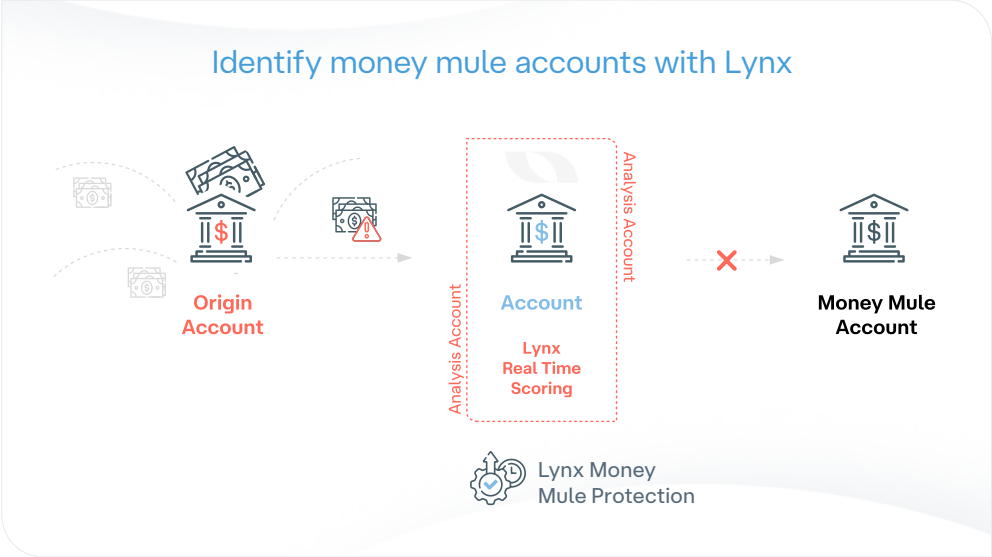


Figure 4

The dynamic capabilities of these models allow them to rapidly process new information and swiftly adapt to evolving tactics used by organized crime groups. By evaluating transaction data in real time, they provide timely insights that prevent illicit funds from exiting financial systems and support proactive fraud prevention.

A case study highlights the impact of these adaptive models: A Tier 1 bank implemented our daily adaptive models to tackle a significant annual money mule problem, resulting in remarkable detection improvements. The model achieved a 65% money mule Account Detection Rate (ADR) and a 70% money mule Value Detection Rate (VDR) at a low rate of 10 false positives per 10,000 transactions, significantly surpassing the bank's prior machine learning model performance. Additionally, the system operates with an impressive response time of less than 100ms.

Moreover, employing supervised learning techniques in these models enhances their accuracy by using labeled datasets to identify suspicious activities, significantly reducing false positives compared to traditional approaches. This advancement aids in reducing the analyst workload and improving compliance operations.

Lynx uses Daily Adaptive Models that retrain each day to adapt to the latest money mule methods, criminal techniques, new financial products and services, and evolving customer behaviors:

Lynx's Daily Adaptive Models are customized for each FI based on their unique mule problems. The models utilize feeder data from onboarding and customer accounts to target money mules with unparalleled accuracy; since any customer account can become a mule account either knowingly or unknowingly at any point in time, this is a crucial capability, as transaction data only tells part of the money muling story. The models also integrate with each FI's custom rules to provide additional safeguards.

Lynx Flex allows FIs to configure API and intelligence feeds through a no-code user interface, providing data extensibility that propagates to models, rules, and reports. Lynx Insights offers alerts and dashboards for a 360-degree view of customers, accounts, alerts, and money mules. Additionally, Lynx's money mule models can function as a standalone scoring module to provide real-time scores for incoming transfers or as part of the broader Fraud Prevention solution, which includes rules, dashboards, alerts, workflows, and more.

Uncovering Financial Institutions Globally

Around the world, the deployment of such models has become integral in bolstering financial system protections and ensuring compliance with regulatory standards. These adaptive systems help institutions minimize financial losses from muling, alleviate analyst fatigue due to high alert volumes, and optimize investigatory resources, thereby reducing operational costs.

By adopting these advanced detection solutions, institutions can significantly enhance their capacity to address evolving fraud tactics. As regulators press for more rigorous controls and reporting, Daily Adaptive Models offer effective and efficient tools to meet these demands and maintain financial integrity.

A Call to Action for the Financial Industry

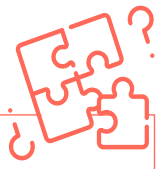
As financial crime continues to evolve, now is the time for institutions to take proactive steps in safeguarding their operations and customers. The threat of money mules not only jeopardizes financial assets but also erodes the trust that consumers place in their financial institutions.

By leveraging innovative solutions like Daily Adaptive Models, FIs can strengthen their defenses against the increasingly sophisticated tactics employed by organized crime groups. The adoption of these advanced detection systems is not just an option; it is an imperative for institutions committed to protecting their customers and maintaining regulatory compliance.

Let us lead the charge in fostering a robust financial ecosystem that prioritizes security and integrity. Together, we can build a future where financial transactions are safeguarded, criminals are thwarted, and trust is restored in the financial system. The time to act is now: Embrace the technologies and strategies that will empower you to stay ahead in the battle against fraud.

Key Takeaways

The Problem



Money Mules Launder Funds Through Financial Institutions on a Massive Scale

- Organized crime groups (OCGs) exploit vulnerabilities in financial institutions (FIs) to recruit and onboard money mules, laundering billions of dollars in criminal funds each year.
- Money muling is a real-time problem for FIs due to the high availability of digital financial products and services.
- It's critical to detect and stop illicit funds and mules in real time by:
  - Blocking suspicious transactions before they leave your systems
  - Shutting down existing mule accounts
  - Catching attempts to onboard mules
- Current approaches using Unsupervised machine learning (ML) generate too many false positives and don't accurately detect money mules in real time.

The Solution

Advanced Real-Time Machine Learning

- Supervised ML models outperform Unsupervised models, detecting more money mules while blocking fewer legitimate transactions, all in real time.
- ML models must retrain daily to remain accurate as criminal tactics, customer behaviors, payment types, and technologies constantly evolve.

Why Lynx Money Mule Detection?

- Lynx's Daily Adaptive Models (DAMs) use supervised learning, retrain with the latest transaction data each day, and integrate onboarding and account data to detect more money mules.
- Key benefits include:
  - Real-time detection
  - Improved accuracy to detect and stop more money mules
  - Reduced operational costs and analyst fatigue
  - Enhanced regulatory compliance
- A leading Tier 1 bank partnered with Lynx to significantly improve their money mule detection capabilities, achieving:
  - 65% Account Detection Rate (ADR)
  - 70% Value Detection Rate (VDR)
  - Just 10 false positives per 10,000 transactions
  - Response time of less than 100ms

Try a POC: find out how many undetected or dormant mule accounts you have and how much money you could save- no PII required.

Get in Touch

Website: lynxtech.com

Email: info@lynxtech.com

Learn More

Interested in learning how to take immediate action against money mules and block incoming illicit funds? Read Lynx's Money Mule Detection Solution Guide for effective strategies and insights.

Take Action

Ready to take the next step?

Reach out to explore a Proof of Concept (POC) tailored to your institution. Lynx will analyze your transactional data to demonstrate the effectiveness of our money mule detection model compared to traditional solutions—no Personally Identifiable Information (PII) required. Discover how many undetected or dormant mule accounts you have, and find out how much money you could save.

About the Author

Greg Hancell

Head of Product - Fraud

Greg Hancell

Head of Product for Fraud Prevention at Lynx, I lead a talented team to develop cutting-edge fraud prevention products. With experience in server-side analytics and building global fraud consultancy teams, I focus on reducing financial crime through innovative solutions.

About Lynx

Lynx utilizes advanced AI for fraud prevention, honed over 25 years. Originating from the Autonomous University of Madrid data science program, Lynx is trusted by leading financial institutions globally to significantly reduce fraudrelated losses. Processing over 66 billion transactions annually, Lynx's AI-driven approach illuminates real-time risks and empowers organizations to focus on crucial tasks.

Contact Us

Get in touch with us:

Website:

www.lynxtech.com

Email:
info@lynxtech.com

Chartis
Financial Crime and Compliance50 2024

Chartis
RiskTech Quadrant®
Category Leader
Enterprise Fraud Solutions, 2024

Chartis
RiskTech Quadrant®
Category Leader
Payment Fraud Solutions, 2024

Chartis
RiskTech Quadrant®
Best of Breed
Name and Transaction Screening Solution, 2024