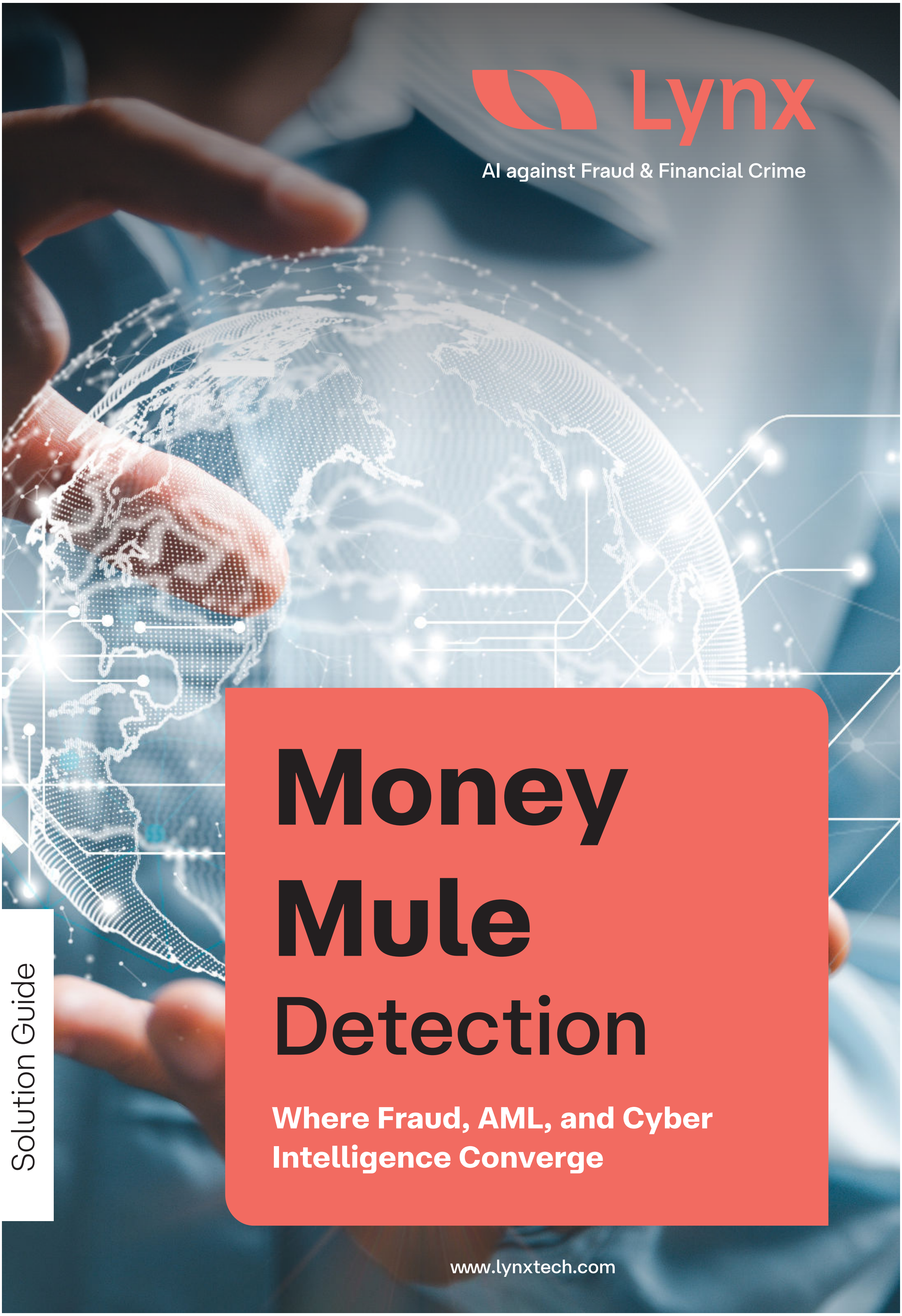


Lynx

AI against Fraud & Financial Crime

Solution Guide

Money Mule Detection

Where Fraud, AML, and Cyber Intelligence Converge

www.lynxtech.com

Money Mule Detection

Where **Fraud, AML,** and **Cyber Intelligence Converge**

The Problem

- Financial Institutions (FIs) struggle to identify and prevent illicit money flows in real time, leading to financial losses and compliance risks.
- Criminal groups utilize money mules to launder illicit funds, utilizing mule accounts for laundering.
- Automated attacks and the use of machine learning by Organized Crime Groups (OCGs) make detection increasingly difficult. Experiencing success, OCGs intensify their efforts, resulting in an upsurge in criminal activities and the generation of more criminal funds.
- FIs are overwhelmed with Authorized Push Payment Fraud (APPF), which hits their bottom line in fraud costs, operations, and customer complaints.

EUROPOL

According to Europol, more than

90% **of money mule transactions** are linked to cybercrime.[1]

The Magnitude of the Issue

Europol states that over 90% of identified money mule transactions are linked to cybercrime.[1]

In 2023, fraud scams and bank fraud schemes totaled $485.6B in projected losses globally.[2]

Financial crime is rising, and money mules are real-time facilitators of organized crime. "In 2023, an estimated $3.1 trillion in illicit funds flowed through the global financial system,"[2] as reported by Nasdaq.

The **top five types of identity fraud** in 2023 are AI-powered fraud, money muling networks, fake IDs, account takeovers, and forced verification.[3]

Globally, there was a **10x increase in the number of deepfakes** detected across all industries from 2022 to 2023.[4]

Criminal activities generating illicit funds range from phishing and malware attacks to various forms of fraud, such as online auction scams, e-commerce fraud, business email compromise (BEC), romance scams, booking fraud, and many others.

Criminals are organized and using the latest advancements in AI to orchestrate complex attacks on FIs and their customers.

Criminals need mule accounts to legitimize their illicit money; in that sense, you can see it as a logistics chain of the criminal enterprise. **By identifying illicit funds and mule accounts in real time, we cut off the logistics arm and stop illicit money flowing to the monster that is organized crime.**

(1) https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling
(2) https://www.nasdaq.com/global-financial-crime-report
(3/4) https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/

Immediate Action Needed

New Regulation

In the UK, the Lending Standards Board (LSB) outlined the Contingent Reimbursement Model Code (CRM). Historically, this code was optional to FIs; however, that changes on October 7th, when it becomes mandatory to all FIs in the UK.

Financial Institutions subscribing to this code require that firms receiving Authorized Push Payment Fraud (APPF) must implement profiling for inbound payments. This measure enables firms to prevent the onward movement of funds if there is suspicion that the credited funds result from an APP scam.[5] It's anticipated that the upcoming mandatory reimbursement rules will have similar requirements.

More Sophisticated Criminal Activity

- The rise of synthetic identities, fueled by widespread AI adoption, simplifies mule account setup for criminals.
- Criminals leverage AI advancements to orchestrate intricate attacks using minimal resources, utilizing bots and social media to amplify their reach.
- While digital onboarding aims to streamline the identity and verification (ID&V) process, it has inadvertently facilitated the proliferation of mule accounts, especially with the rise of deepfakes.
- Crime as a Service (CaaS) drives more data breaches, identity theft, and new account fraud as criminal groups offer subscription services for advanced attacks.

UK Banking Trends

- Real-time payments allow criminals to swiftly move illicit proceeds at an unprecedented pace without detection.
- All banking transactions, including onboarding, product applications, approvals, and transactions occur in real time.
- The UK Financial Conduct Authority highlighted, "*We observed instances where firms are onboarding customers sharing a single device without a clear justification. This aligns with typical mule behavior, indicating potentially unauthorized account usage.*"
- The absence of robust digital customer identities, supported by device profiling, geolocation data, and behavioral biometrics during onboarding and subsequent interactions with the financial institution, poses a significant risk.

[5] https://www.lendingstandardsboard.org.uk/wp-content/uploads/2023/10/LSB-CRM-Code-V5.0-17-October-2023.pdf

The Solution

Lynx Money Mule Detection uses supervised machine learning to identify illicit sources of funds and mule accounts in real-time.

By combining incoming and outgoing transaction data, Lynx provides a comprehensive user view for proactive fraud prevention and money mule detection.

Block the account. Return the fraudulent funds to their rightful owners. Stop the money flowing to criminals.

What does it do?

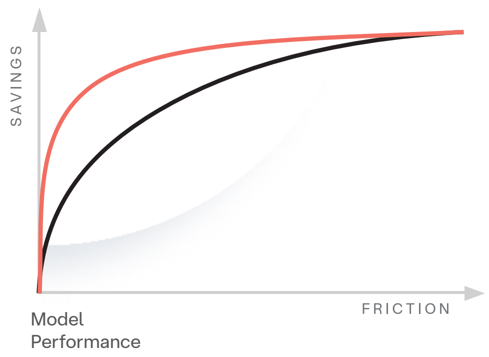
- Review every incoming transfer/transaction in real-time.
- Provide a 360-degree customer view, including all potentially risky transactions and accounts.
- Apply a risk score to the transfer/transaction based on the likelihood of association with illicit fund sources like APPF.
- Automatically flag and block further activity on accounts identified as mule accounts.
- Generate alerts for immediate action by the fraud and AML teams.
- Updates model daily using the Daily Adaptive Model (DAM) procedure for the highest accuracy and minimal false positives, enabling real-time blocking of mule accounts and funds.
- If money muling is identified, an immediate alert is sent to the AML team. Recognizing money muling is a form of money laundering and reporting this in real-time not only ensures regulatory compliance for the FI but also helps law enforcement identify and stop these criminals.

Daily Adaptive Models

Daily adaptive models are the latest breakthrough in fraud prevention.

Lynx’ Daily Adaptive Models (DAM) continually update by leveraging the latest genuine user behavior and fraud patterns. Self-learning profiles leverage genuine users’ connected devices, card and account transactions, beneficiary and incoming payments and geographic location of users. Real-time data enrichment, facilitated by Lynx’s in-memory database enables swift and precise identification of fraudulent behavior and activities.

Static vs **Daily Adaptive**



As you move towards the daily adaptive model, you **reduce friction** and **stop more fraud.**

By joining this fight, you're not just doing a job
You're safeguarding the future of millions of genuine users.

Advantages of Lynx Money Mule Detection

- **Real-time defense**—The Lynx Money Mule model combines both incoming and outgoing transactions, enabling the model to flag if the account receiving and/or sending funds is a mule account. For example, the model can identify if there are irregular sources of funds received by the account, which could be derived from APPF or other types of fraud and flag the account as a mule account.
- **Reduce losses**—Stopping money from flowing out of the FI can significantly reduce losses. As of October 7, 2024, the UK Contingent Reimbursement Model Code (CRM) will require FIs to refund victims for any APPF-related transactions.
- **Reduce Operational costs**—Accurately identify mules. Reducing alert fatigue, complaints and risk.
- **Holistic View**—Centralize monitoring of incoming and outgoing transfers with a single solution, offering real-time scoring and a comprehensive 360-degree view.
- **Standalone or part of a solution**—The Lynx Money mule model can be used as a standalone component to provide real-time scores to an existing fraud solution. This can help enhance fraud detection accuracy, addressing this specific challenge effectively without the need for complex integrations, thereby supporting financial institutions efficiently. Or utilize the Lynx money mule model as part of the Lynx comprehensive Fraud Prevention solution to accurately identify fraud and mules for outgoing and incoming transfers.

Next Steps

Stop the Mules, Stop the Crime

Money mules are a critical link in the chain of financial crime, facilitating the movement of illicit funds across the globe. By disrupting this flow, we not only protect countless victims but also cripple the operational capacity of criminal enterprises.

Your Impact

Imagine a world where criminal rings can't operate because their financial pipelines are blocked at every turn.

Try a POC and find out **how much money you could save!**

How many undetected or dormant warmup **mule accounts** do you have?

How much **money could you save your company?**

Product Features

- Pre-configured model that learns customer financial behavior and mule activity
- Comprehensive financial behavioral monitoring
- Real-time monitoring capabilities
- Utilization of Daily Adaptive Model for continuous updates for accuracy
- 360-degree view of your customers
- Sophisticated rules engine for advanced threat detection
- Multichannel tuning for diverse monitoring needs
- No code configuration

Technical Specifications

- Dual deployment options: on-premises & cloud-based solution
- Compliance with PCI Data Security Standard (PCI-DSS)
- Flexible and data-agnostic interface (Flex)
- ISO 8583 and ISO 20022 compatible
- Self-publishing API capability
- Supervised learning techniques
- Utilization of in-memory databases
- Low-level code access
- Rapid 25 ms response time*
- Capability to handle 2400+ Transactions Per Second (TPS)*

* on-premise deployment using TCP/IP socket

About Lynx

Lynx utilizes the most advanced AI for fraud prevention, honed over its 25-year history. Born out of the UAM — Autonomous University of Madrid data science program, Lynx is trusted by top financial institutions globally to significantly reduce fraud-related losses. We save our Tier 1 banking clients up to $500 million per year in fraud costs, and process more than 66 billion global payments and transactions annually. In 2023, we secured investment to scale our capabilities.

Our innovative AI-led approach illuminates real-time risks, eliminates mundane tasks, and empowers organizations to focus on what really matters.

Our Mission

To lead the fight against fraud and financial crime through advanced AI technologies, continuous innovation, and deep industry expertise.

By preventing fraud and financial crime, we help bring **trust**, maintain the **integrity** of macroeconomic financial systems and **protect** you from harm.

Benefits

66 + billion	transactions protected annually
300 + million	users protected every year
Real-Time	model processing
<25 millisecond	response time*
2400 +	transactions per second*

* Known performance where connection is TCP/IP socket and the solution is on-premise.

The right technology can unify teams, streamline processes, and boost insight for a complete defense against advanced attacks. At Lynx, collaboration is vital to outsmarting evolving threats and protecting FIs. Join us in this collective endeavor.

Find out more on the convergence of Fraud and AML

Get in Touch
Website: lynxtech.com
Email: info@lynxtech.com

Developed by Lynx