Lynx

AI Against Fraud & Financial Crime

Money Mule Detection

Fact Sheet

Where Fraud, AML, and Cyber Intelligence Converge

Benefits

76 + Billion	transactions protected annually
330 + Million	users protected every year
<50 Milliseconds	for 99.99% of transactions processed*
2400 +	transactions per second*
$1.6 Billion	our FIs saved

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

About Lynx

Founded 30 years ago as a nonprofit by AI experts from the Autonomous University of Madrid, Lynx has transitioned to the market in 2023, bringing cutting-edge AI-driven solutions for fraud prevention and financial crime combat. Our advanced technology illuminates real-time risks, streamlines tasks, and empowers organizations to focus on what matters. Trusted by top financial institutions, Lynx saves clients up to **$1.6 billion annually,** safeguarding over **76 billion transactions** and protecting more than **330 million consumers.** Our proprietary 'Daily Adaptive Model' ensures unmatched accuracy while maintaining industry-leading low false positive rates, driving effectiveness in financial crime prevention.

Our Mission

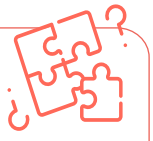
To lead the fight against fraud and financial crime through advanced AI technologies, continuous innovation, and deep industry expertise.

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

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** by using mule accounts.
- **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 $485.6 billion in projected losses globally.[2]

Financial crime is on the rise, 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[3], 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.[4]

Globally, there was a **10x increase in the number of deepfakes** detected across all industries from 2022 to 2023.[5]

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] Europol [2/3] Nasdaq [4/5] Sumsub

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?

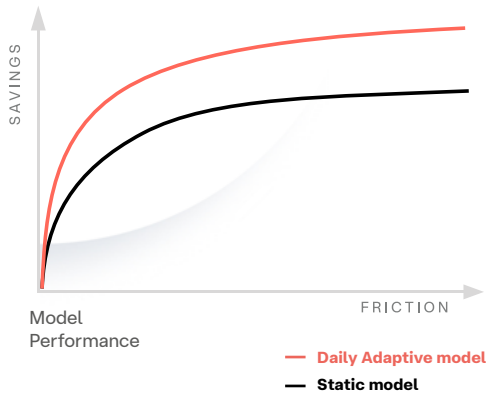
- Review every incoming transfer/transaction in real-time.
- Provide a 360-degree customer view, including all potentially risky transactions and accounts.
- Apply a risk score to the transfer/transaction based on the likelihood of association with illicit fund sources like APPF.
- Automatically flags and blocks 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' devices, cards transactions, incoming payments and locations. 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 it to flag if the account receiving and/or sending funds is a mule account. For example, the model can identify irregular sources of funds received by the account, potentially derived from APPF or other types of fraud, flagging the account as a mule.
- **Reduce losses**— Accurately identify mules. Reducing alert fatigue, complaints and risk. Address financial risk by identifying the mule account in real time and stop it from operating. The UK PSR regulation October 7th requires a reimbursement for APPF (scams) to be split 50/50 between sending and receiving FI's. Lynx identifies APPF inbound and prevents it flowing out significantly reducing losses.
- **Bespoke Models (DAM)**— Lynx builds models specific to each FI which automatically update daily. The models automatically adapt to the risks, behavior, products, and data of the FI. Enabling greater accuracy, 360 coverage, and reduced workload compared to traditional static models (transaction only data).
- **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.

Immediate Action Needed

New Regulation

Contingent Reimbursement Model Code (CRM) requires split reimbursement between the sending and recipient FI's in the UK.

To combat this FIs should 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]

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.

[5] Lending Standards Board

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.

Recognitions

Recognised as a Representative Vendor in the 2024 Gartner® Market Guide for Fraud Detection in Banking Payments.

Chartis Financial Crime and Compliance 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

datos INSIGHTS Risk Insights Spotlight Q4 2024

CB INSIGHTS Fintech 100 2024

Gartner, Market Guide for Fraud Detection in Banking Payments, 11 December 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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

- Rapid self-learning ML models improving improving accuracy daily
- Pre-configured financial behavioural models that update automatically
- Real-time financial behavioural monitoring
- Real-time monitoring of both APPF outbound and inbound
- Comprehensive 360-degree customer view and alert management
- Advanced easy-to-use configurable rules through a user interface (no programming needed)
- Just-in-time query and response dashboards and reporting
- Multi channel: Cards, Mobile, eBanking, ATM, Branch, P2P, Corporate, Acquirer, Telephony
- Automation of workflows from alerts

Technical Specifications

- SaaS or on-premises deployment options
- PCI-DSS and ISO27001 compliant
- Self-publishing API for easy integration
- Real-time optimized architecture for authorisation flow
- Low level code and in memory databases
- Real time response time (99.99%)*
- Extensible data models
- Strong model governance controls
- Optimised on Fraud vs Friction (VDR vs tFPR)

* on-premise deployment using TCP/IP socket average time to respond in milliseconds

Get in Touch
Website: **lynx**tech.com
Email: **info@lynxtech.com**

Developed by Lynx