FACT SHEET

Money Mule Detection

Technical Data Sheet

lynxtech.com

Lynx

About Lynx

Founded 30 years ago as an R+D center by AI experts from the Autonomous University of Madrid, Lynx entered the market in 2023, delivering advanced AI-based solutions for fraud prevention and financial crime prevention. Trusted by leading financial institutions, Lynx protects more than **129 billion transactions** and **over 330 million consumers annually.**

Our patented “Daily Adaptive Model” ensures unmatched accuracy while maintaining industry-leading low false positive rates, driving greater efficiency 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, preserve the integrity of macroeconomic financial systems, and protect them from potential harm.

Benefits

129 + billions
transactions protected annually

330 + million
users protected every year

< 50 milliseconds
for 99.99% of transactions processed*

2.400 +
transactions per second*

$1.6 billions
our FIs saved

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

The Problem

- Financial institutions (FIs) **face challenges in identifying and preventing illicit money flows in real time**, resulting in financial losses and regulatory compliance risks.
- Criminal organizations use **money mules** to **launder illicit funds** through mule accounts.
- **Automated attacks** and the use of machine learning by organized crime groups (OCGs) are **making detection increasingly difficult**. After achieving successful results, OCGs intensify their efforts, leading to an **increase in criminal activities** and the generation of more illicit funds.
- FIs are being overwhelmed by Authorized Push Payment Fraud **(APPF), which impacts their financial results through fraud losses, operational costs, and customer claims.**

The Scale of the Problem

Europol states that more than 90% of identified money mule operations are linked to cybercrime.[1] Illicit funds usually originate from criminal activities such as phishing, malware attacks, online auction fraud, e-commerce fraud, business email compromise (BEC), CEO fraud, romance scams, travel booking fraud, and many others.
A significant number of banks have limited preventive detection capabilities, exposing them to money mule activity. According to Gartner©, more than one-third (35%) of banks detect less than 60% of fraudulent transactions before losses occur, while only 31% detect more than 80% preventively; these detection deficiencies allow money mule activity to persist and amplify its impact.[2]
Criminals are highly organized and use the latest advances in AI to orchestrate complex attacks against financial institutions (FIs) and their customers.

Criminals require mule accounts to legitimize illicit funds; in this sense, they can be considered part of the logistical chain of criminal enterprises.

By identifying illicit funds and mule accounts in real time, we cut off the logistical arm and stop the flow of illicit money feeding the giant that is organized crime.

According to Europol, more than **90% of money mule operations** are linked to cybercrime.[1]

1 Europol. **2** Gartner©

The Solution

Lynx Money Mule Detection uses supervised machine learning to identify illicit sources of funds and mule accounts in real time. The platform combines incoming and outgoing transaction data to provide a complete 360-degree view for proactive fraud prevention.

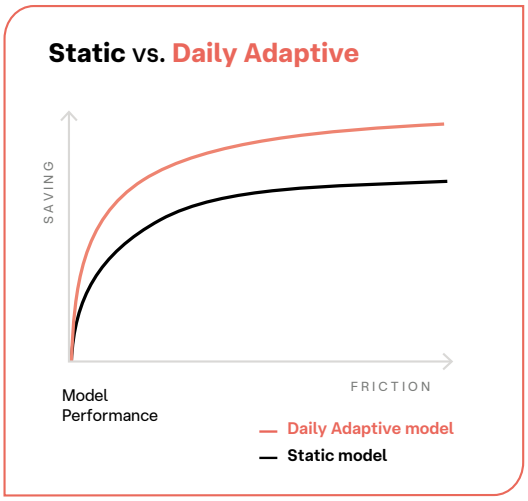
Block the account. Return the fraudulent funds to their rightful owners. Stop the flow of money to criminals.

How is it done?

- Reviews every incoming transfer/transaction in real time.
- Provides a 360-degree customer view, including all transactions and accounts potentially at risk.
- Applies a risk score to each transfer/transaction based on the likelihood of association with illicit sources of funds such as APPF.
- Automatically flags and blocks the activity of accounts identified as mule accounts.
- Generates alerts for immediate action by fraud prevention and anti-money laundering teams.
- Updates the model daily through the Daily Adaptive Model (DAM) process to achieve maximum accuracy and minimize false positives, enabling the real-time blocking of mule accounts and illicit funds.
- If mule account activity is detected, an alert is immediately sent to the anti-money laundering team. Recognizing that money mules constitute a form of money laundering and reporting it in real time not only ensures regulatory compliance for the financial institution (FI) but also helps law enforcement agencies identify and stop these criminals.
- Analyzes customer logins to identify suspicious patterns, such as multiple logins prior to a monetary transaction or unusually large distances between the first login and subsequent ones.

Automatic Daily AI Retraining Agent

Daily Adaptive Models represent the latest advancement in fraud prevention.
The daily AI retraining agent continuously updates the models using the latest genuine user behaviors and fraud patterns. The self-learning profiles are based on devices, card transactions, received payments, and the locations of real users.
Real-time data enrichment, enabled by Lynx's in-memory database, allows the rapid and accurate identification of fraudulent behaviors and activities.
The Daily Adaptive Model reduces friction and prevents more fraud.



Advantages of Lynx Money Mule detection

- **Real-time defense:** The Lynx Money Mule model combines incoming and outgoing transactions, enabling it to identify whether 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, and flag the account as a mule account.
- **Loss reduction:** Accurately identifies mule accounts. Reduces alert fatigue, complaints, and risks. It addresses financial risk by identifying mule accounts in real time and preventing them from operating. The UK PSR regulation of October 7 requires APPF (scam) reimbursement to be shared 50/50 between sending and receiving financial institutions (FIs). Lynx identifies incoming APPF transactions and prevents them from leaving, significantly reducing losses.
- **Tailored Models (DAM):** Lynx builds institution-specific models for each FI that are automatically updated daily. The models automatically adapt to the FI's risks, behaviors, products, and data. This enables greater accuracy, 360-degree coverage, and workload reduction compared to traditional static models (transaction data only).
- **Comprehensive view:** Centralizes the monitoring of incoming and outgoing transfers into a single solution, providing real-time scoring and a complete 360-degree view.
- **Standalone or part of a broader solution:** The Lynx Money Mule model can be used as a standalone component to provide real-time scoring to an existing fraud solution. This can help improve fraud detection accuracy by efficiently addressing this specific challenge without requiring complex integrations, while effectively supporting financial institutions. Alternatively, the Lynx Money Mule model can be used as part of Lynx's end-to-end fraud prevention solution to accurately identify fraud and mule activity in both incoming and outgoing transfers.

Lynx successfully prevented €7 million in mule account losses at a leading UK bank.

65% ADR
Account detection rate of money mules

70% VDR
Value (amount) detection rate

< 10
False positives for 10.000 transactions

Need for Immediate Action

More Sophisticated Criminal Activity

- The rise of synthetic identities, driven by the widespread adoption of AI, makes it easier for criminals to create mule accounts.
- Criminals leverage advances in AI to orchestrate complex attacks with minimal resources, using bots and social media to amplify their reach.
- Although digital onboarding aims to streamline identification and verification processes, it has unintentionally facilitated the proliferation of mule accounts, especially with the rise of deepfakes.
- Crime-as-a-Service (CaaS) fuels more data breaches, identity theft, and new account fraud, as criminal groups offer subscription-based services for advanced attacks.

Banking Trends in the United Kingdom

- Real-time payments enable criminals to move illicit proceeds rapidly, at an unprecedented pace and without detection.
- All banking operations, including onboarding, product applications, approvals, and transactions, now occur in real time.
- The lack of strong digital customer identities, supported by device profiles, geolocation data, and behavioral biometrics during onboarding and subsequent interactions with the financial institution, represents a significant risk.

Next Steps

Stop the Mules, Stop the Crime

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

The Impact

Imagine a world where criminal networks are unable to operate because their financial channels are blocked at every step.

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

- Fast self-learning ML models that improve their accuracy on a daily basis.
- Preconfigured financial behavior models that are automatically updated.
- Real-time financial behavior monitoring.
- Real-time monitoring of incoming and outgoing APPF cases.
- Comprehensive 360-degree customer view and alert management.
- Advanced rules that are easy to configure through a user interface (no coding required).
- Real-time dashboards and reporting for monitoring and response.
- Multi-channel support: cards, mobile, online banking, ATMs, branches, P2P, corporate banking, acquirers, and telephony.
- Workflow automation based on 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 authorization flows.
- Low-level code and in-memory databases.
- Real-time response time (50ms for 99,99% transactions)*.
- Expandable data models.
- Strong model governance controls.
- Optimized for Fraud vs. Friction (VDR vs. tFPR).

Lynx

About Lynx

Established 30 years ago, Lynx is an AI-driven software company dedicated to solving clients' most pressing challenges in fraud and financial crime. Our solutions utilize advanced AI technology to proactively identify and prevent fraud and financial crimes in real time, establishing new standards for accuracy, speed, and scalability for multinational organizations.

Industry recognition

Gartner

Chartis

datos INSIGHTS

FStech
Anti-Fraud Solution of the Year

pay360 AWARDS
Best Initiative in Utilising Data or AI. 2025

Get in Touch

web: lynxtech.com
email: info@lynxtech.com