STORIES THIS MONTH
January, 2025

TOP STORY

MuleHunter.AI: Adoption of AI/ML for rapid fraud detection

NEWS SNIPS FROM AROUND THE WORLD

REGULATORY UPDATE

Alert Against Illegal Payment Gateways

DOMAIN MATTERS

FATF – Travel Rule

TOP STORY

MuleHunter.AI: Adoption of AI/ML for rapid fraud detection

by Shivani Shetty

According to RBI's annual report for FY 2024, there have been over 29,082 cases of card and digital payment fraud, involving amounts exceeding ₹1,457 crores. A significant challenge in combating financial fraud lies in the use of money mule accounts, which facilitate illicit transactions.

To address this issue, the Reserve Bank Innovation Hub (RBIH), a subsidiary of the Reserve Bank of India (RBI) recently developed an in-house AI/ML solution for mule detection called MuleHunter.AI. It effectively analyses transaction and account detail-related datasets to predict mule accounts with higher accuracy and greater speed. Machine learning-based approach along with near-real-time monitoring and AI/ML-based pattern recognition has proven to identify more mule accounts within a bank's system. This will further enable financial institutions in quickly identifying and shutting down suspicious accounts, thereby preventing the flow of illicit funds and reducing digital fraud.

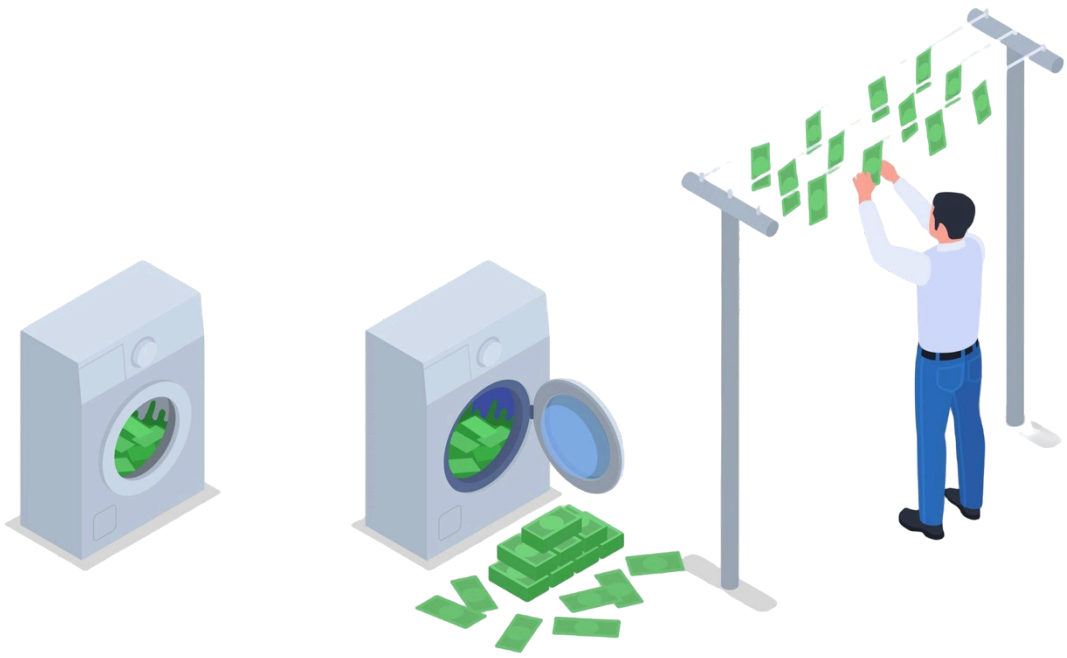
The adoption of AI/ML in mule account detection can significantly reduce false positives, ensuring faster turnaround times and detecting accounts that might otherwise go unnoticed. This is a transformative development for the industry as reducing false positives means streamlined compliance operations for financial institutions.

RBI's proactive stance on adopting AI/ML portrays its recognition of the growing threat posed by money mules and the need for innovative solutions to combat them. By encouraging the use of technologies like MuleHunter.AI, RBI is driving the industry toward smarter detection and prevention mechanisms, ensuring a safer financial ecosystem.

NEWS SNIPS FROM AROUND THE WORLD

by Neha Joy and Anna Paulin

[Collated from other publishers and sources on the Internet, as referenced after each snippet]



SIM Swap Scam - Quick action saves crores

Swift action by the cyber police successfully recovered Rs. 4.65 crore from the Rs 7.50 crore that had been transferred out of a victim's current account into multiple accounts operated by the perpetrator. The entire plan was executed over the weekend, with funds being moved to various bank accounts between December 21 and 23, resulting in siphoning of Rs. 2.9 crores.

Source: The Times of India

Cyber fraud investigation unearths a hidden nexus of Money Launderers

A recent Rs. 640 crore cyber fraud case exposed a sophisticated money laundering operation involving 5,000 mule accounts, orchestrated by financial experts with the use of advanced technology. The fraud proceeds were layered through Indian mule accounts followed by sequential transfer to a UAE-based payment platform. A significant portion of the funds was withdrawn in Dubai using cards issued by Indian banks, while part of the proceeds was converted into cryptocurrency.

Source: The Economics Times

Money mule agent caught while dismantling a cybercrime network

Police have arrested operatives involved in a cyber fraud case reported in Pune, including agents who managed a network of hundreds of mule bank accounts. The group was led by a Dubai-based Bank employee, serving as the key link between international cyber criminals and Indian operatives. The money was siphoned off from victims of fake online trading apps and investment scams, which were then channelled internationally via cryptocurrency.

Source: The Indian Express

792 arrested in Nigeria for Involvement in Crypto Romance Scam

Fraudsters involved in a crypto romance scam targeted victims from America and Europe on the pretext of romance. The victims were contacted through social media and messaging platforms by posing as romantic interests. Once the fraudsters established a fake relationship with victims, they would broach the idea of investing in crypto. The victims were then pressured to transfer money for fake cryptocurrency schemes. As stated by the FBI, criminals have turned to crypto more readily as an outlet for fraud because of its decentralized nature, the speed of irreversible transactions and the ability to move money around the world.

Source: Reuters

Klarna Bank Found Non-Compliant with Sweden's AML Regulations

Following an investigation, the Financial Supervisory Authority, Sweden's financial regulator, determined that Klarna Bank was non-compliant with its AML/CFT guidelines. The bank's AML program exhibits significant shortcomings, such as the absence of assessments addressing how the bank's products and services could potentially be used for money laundering or terrorist financing. Further, the bank has lacked comprehensive procedures and guidelines to identify all instances requiring customer due diligence measures.

Source: Financial Supervisory Authority Sweden

Bank frauds in India surged dramatically in the first half of FY25

There has been a significant rise in bank frauds during the first half of FY25, increasing eightfold to ₹21,367 crore, compared to 14,480 cases amounting to ₹2,623 crore during the same period in FY24. The number of frauds reported also rose sharply to 18,461 in FY25, according to the RBI's Report on the 'Trend and Progress of Banking in India 2023-24.' The report revealed gaps in fraud detection and reporting, highlighting the need for enhanced fraud surveillance mechanisms. Penalties imposed on regulated entities also significantly rose during FY24, with the total penalty amount more than doubling to ₹86.1 crore, driven primarily by public and private sector banks. RBI emphasized the importance of customer onboarding processes, transaction monitoring, adoption of advanced technology, and coordination between agencies to ensure a secure banking environment.

Source: The Economic Times

Operation Destabilise exposes global money laundering network

Operation Destabilise, an NCA-led investigation, has disrupted Russian money laundering networks Smart and TGR, which operated globally to launder funds for criminals, including the Kinahan crime syndicate and Russian elites bypassing sanctions. These networks facilitated illicit transactions by exchanging cash for cryptocurrency, enabling criminal groups to reinvest in drugs and weapons while avoiding physical cash transfers. The scheme was coordinated across more than 30 countries with UK-based couriers conducting cash handovers in exchange for the equivalent cryptocurrency. This swapping method allowed criminals to launder billions while hiding the source of funds. The collaborative efforts between OFAC, the UK's NCA, and international law enforcement have resulted in 84 arrests and £20m in asset seizures.

Source: NCA

Crypto wallet linked to ponzi scheme frozen in Argentina

Argentine authorities have taken action against a crypto wallet containing $3.5 million in Tether (USDT) during an investigation into the alleged Rainbowex Ponzi scheme. In addition to the wallet, several other cryptocurrency and traditional bank accounts linked to the accused have been frozen. Rainbowex allegedly lured investors with promises of extraordinary returns, advertising daily gains that compounded to an annual rate of nearly 3,500% and sent "signals" via Telegram advising which cryptocurrency to buy and the expected returns. The scheme was revealed to be a Ponzi operation only after investors began facing issues with withdrawals. Authorities estimate that thousands of individuals, particularly residents of San Pedro, Buenos Aires, have fallen victim to the scheme.

Source: Buenos Aires Herald

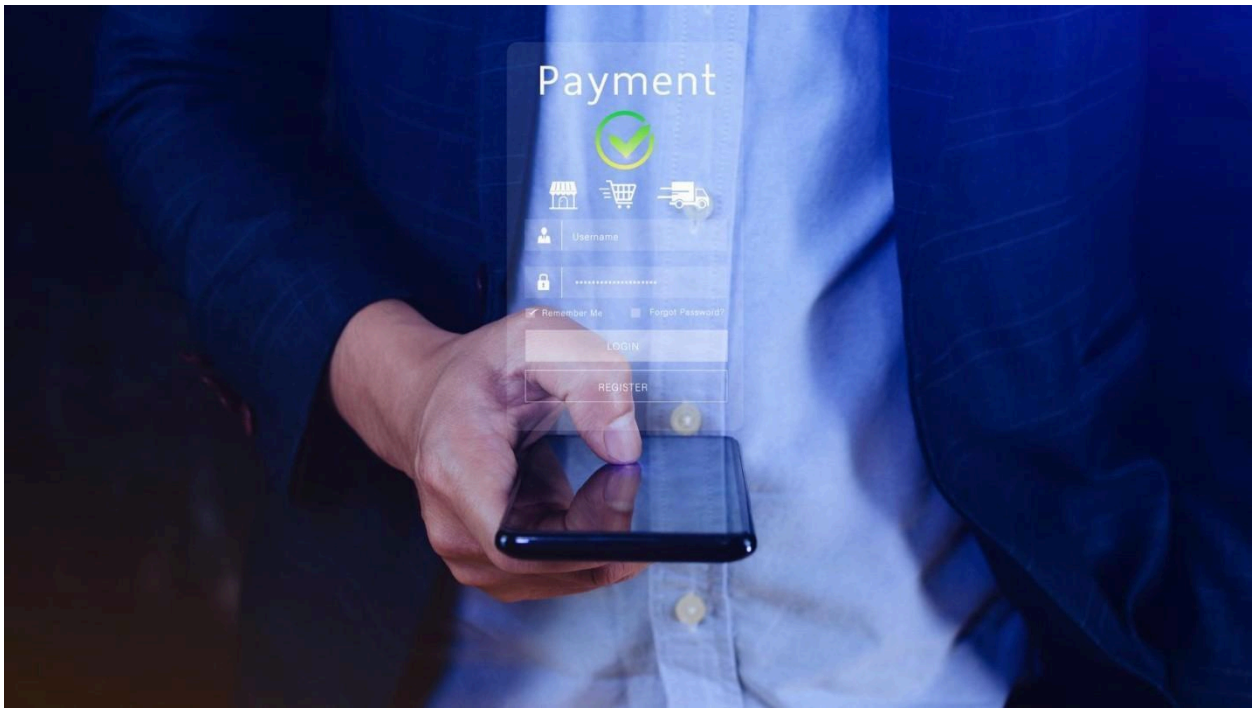
Bank of America faces regulatory action over AML deficiencies

The Office of the Comptroller of the Currency (OCC) released a cease-and-desist order against Bank of America after discovering deficiencies in its Bank Secrecy Act (BSA) and sanctions compliance programs. Compliance programs of the bank depicted shortcomings in reporting suspicious activities and customer due diligence processes. OCC also identified deficiencies in internal controls, governance, and training components of the bank's BSA compliance program. The order mandates Bank of

America to improve its AML and sanctions compliance, including hiring an independent consultant for assessments and lookback reviews of suspicious activity.

Source: OCC

REGULATORY UPDATE



Alert Against Illegal Payment Gateways

by Amruta Raje

Indian Cybercrime Coordination Center (I4C), MHA has issued an alert against illegal payment gateways.

Key points to note are as follows:

- Current accounts and saving accounts are scouted through social media
- An illegal payment gateway is created using mule bank accounts
- These mule accounts are controlled remotely from overseas
- These mule accounts are given to criminal syndicates for accepting deposits on illegal platforms like fake investment scam sites, offshore betting and gambling websites, fake stock trading platforms etc.
- Funds are immediately layered to another account as soon as the crime proceeds are received. Bulk payout facilities provided by banks are misused for the same.

Some of the payment gateways identified during operation are PeacePay, RTX Pay, PoccoPay and RPPay. Banks are advised to deploy necessary checks to identify

misuse of bank accounts that are used for setting up illegal payment gateways.

Source: PIB

DOMAIN MATTERS

FATF – Travel Rule

by Amruta Raje

The Financial Action Task Force (FATF) Recommendation 15 emphasizes regulating virtual asset service providers (VASPs) for AML/CFT purposes, requiring their licensing or registration, and implementing effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

In alignment with Recommendation 15, this article outlines the Travel Rule under Recommendation 16.

The Travel Rule applies to VAs and VASPs and other obligated entities such as financial institutions (FIs) when conducting VA transfers on behalf of a customer. The travel rule also applies to Intermediary VASPs.

This includes:

- a traditional wire transfer
- a VA transfer between a VASP and another obliged entity (e.g., between two VASPs or between a VASP and another obliged entity, such as a bank or other FI), or
- a VA transfer between a VASP and a non-obliged entity (i.e. an unhosted wallet).

VASPs must obtain, hold, and submit the following information for originators and beneficiaries:

- the name of the originator
- the originator account number where such an account is used to process the transaction
- the originator's address, national identity number, customer identification number, or date and place of birth
- the name of the beneficiary
- the beneficiary account number where such an account is used to process the transaction.

Countries may adopt a minimum threshold of USD/EUR 1000 for VA transfers. For transfers below this threshold, VASPs must at least collect the name of the originator and the beneficiary, and the VA wallet address for each, or a unique transaction reference number.

For transactions involving unhosted wallets, FATF does not mandate originating VASPs and FIs to submit required information to individuals who are not obliged entities. However, they must obtain originator and beneficiary information from their customer and may impose additional controls or limitations on such transfers.

Without adequate regulation, virtual assets risk becoming a haven for financial crimes, including money laundering and terrorism financing. To address these concerns, the FATF has been closely monitoring developments in the cryptosphere and has issued global, binding standards to prevent the misuse of virtual assets for money laundering and terrorist financing.

The successful implementation of the Travel Rule will ensure transparency, deterring illicit activities in the cryptosphere. All participants need to develop the technology to comply with FATF requirements, particularly concerning the Travel Rule. VASPs and

other obliged entities should take requisite steps to scrutinize VA transfers and meet their obligations for suspicious transaction reporting (STR) and sanctions compliance.

Please write to connect@naviage-change.com to know more.