منتدى الشراكة في مواجهة غسل الأموال وتمويل الإرهاب

AML/CFT Partnership Forum

اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل التنظيمات غير المشروعة

National Anti Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee

الأمانة العامة General Secretariat


# Fighting Financial Crime:
# AI & Data Analytics in Money Mule Detection

DWG | Digital Working Group

# Table of Contents

# Fighting Financial Crime: AI & Data Analytics in Money Mule Detection

A money mule is typically an individual who transfers or moves illegally acquired money on behalf of criminals, often as part of a larger financial fraud or money laundering scheme. They act as intermediaries, disguising the movement of illicit funds to evade detection by financial institutions and law enforcement. Some money mules knowingly participate in fraud, while others are tricked into it through scams, job offers, or social engineering tactics.

## Types of Money Mules

### Unwitting Mules

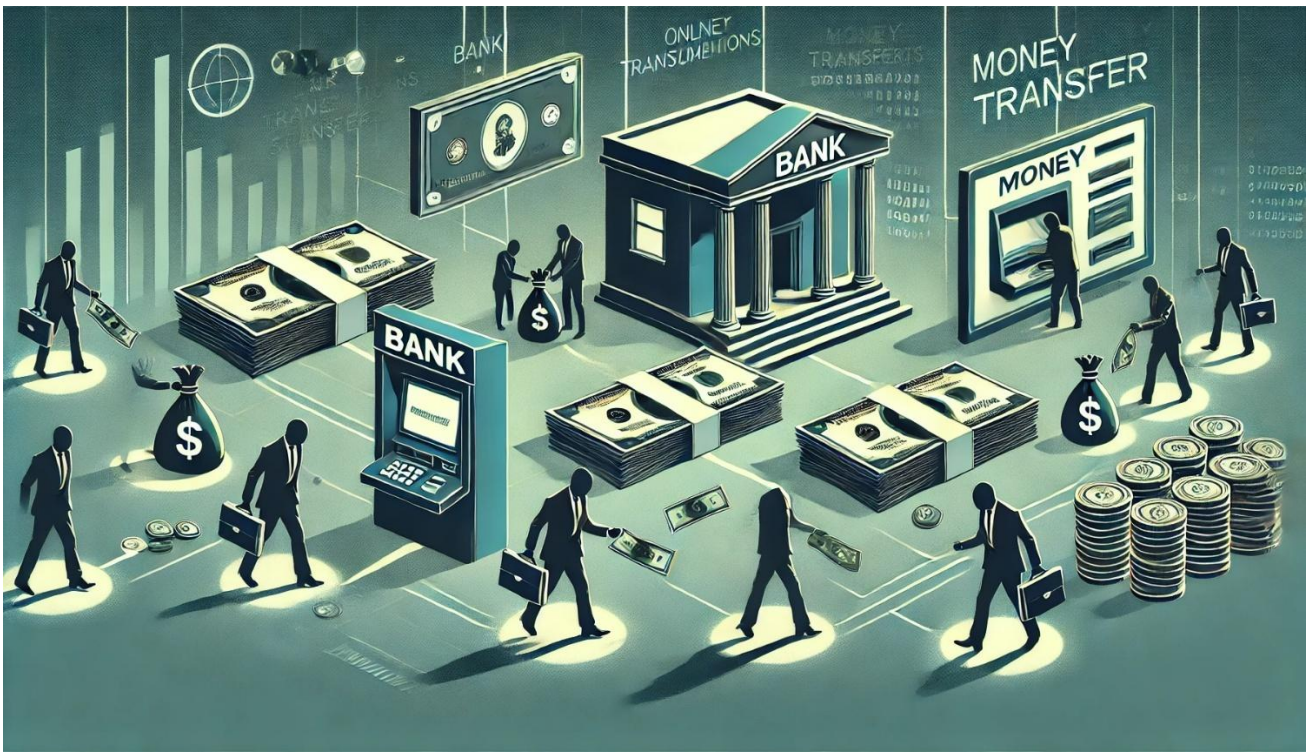
Individuals who are deceived into transferring money, believing they are engaged in a legitimate job or helping someone in need are often recruited through fake online job postings, romance scams, or phishing schemes. They may be unaware that they are facilitating financial crime.

### Witting Mules

Individuals who suspect or know they are involved in an illegal operation but continue due to financial incentives might justify their actions by assuming they won't be caught or believing the risk is low.

### Criminal Mules

Individuals who are fully aware of their role in financial crimes and actively participate for profit are often connected to organized crime groups, cybercriminals, or terrorist financing networks. They help launder money through various financial channels, including cryptocurrency, shell companies, and offshore accounts.



# How Money Mules are Recruited

**Job Scams:** Fake remote job offers promising easy money for processing payments

**Romance Scams:** Victims are manipulated into sending or receiving money on behalf of their "partner"

**Social Media & Messaging Apps:** Fraudsters lure individuals through get-rich-quick schemes

**Phishing & Smishing Attacks:** Emails or messages claiming urgent financial transfers or rewards

**Referrals & Word of Mouth:** Criminals recruit within communities or networks to build a chain of money mules. Direct messages sent through instant messaging apps (e.g. WhatsApp, Viber, Telegram) or by email

# Most Targeted Individuals

Newcomers to the country (often targeted soon after arrival), unemployed people, students and those in economic hardship are typical targets.

The primary targets are individuals under the age of 35, including students, retirees, and homemakers. Recently, criminal groups have increasingly focused on recruiting younger individuals, particularly those between the ages of 12 and 21.

# Case Example

## Drug Mules

Drug cartels often recruit young individuals under the guise of legitimate job opportunities, providing them with freelance visas or other work permits. Once these individuals arrive in the target country, criminals instruct them to open bank accounts—primarily with digital banks due to their ease of access and minimal face-to-face verification requirements.

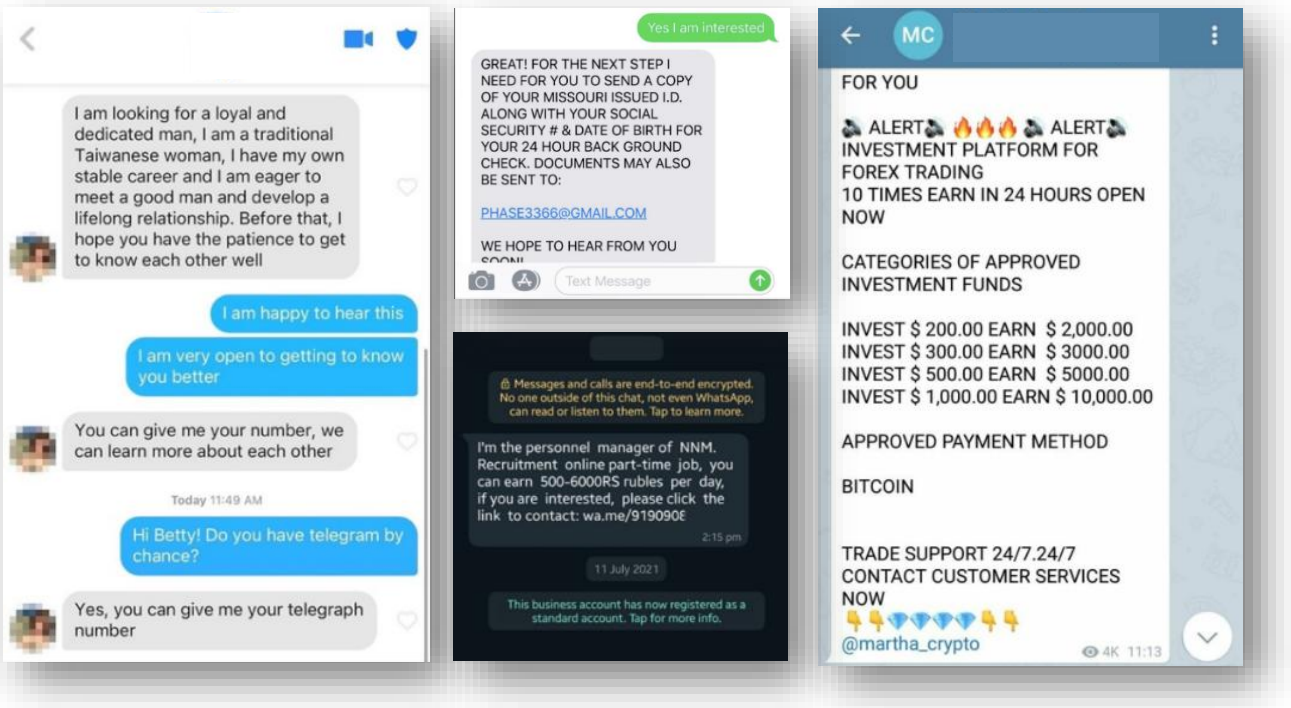
Once the bank account is set up, the criminals take control of its operations. Drug buyers are then directed to deposit cash into these accounts, effectively using them as temporary conduits for laundering illicit funds. A common pattern observed in such accounts includes a high volume of third-party cash deposits

For example:

- More than 15 distinct third-party cash deposits in a single week
- More than 30 distinct third-party cash deposits within a month

Additionally, a key red flag in these schemes is the use of a single device to control multiple mule accounts. Drug traffickers or their handlers often manage several such accounts from the same phone or computer, enabling them to efficiently move money while minimizing their own exposure

Sample illustration of scam messages:




## Money Mule & Shell Companies

Shell companies, established either in Mainland or Free Zones, are often used as conduits for laundering illicit funds, with money mules playing a central role in the process. Criminal networks recruit money mules—either knowingly or unknowingly – to facilitate structured cash deposits. These deposits, made in both local and foreign currencies (where allowed), are strategically layered across multiple shell companies to obscure the illicit origins of the funds. By using multiple mules, criminals create complex transaction trails that make detection by financial institutions and regulators more challenging.

Unlike legitimate businesses, these shell companies typically lack real operations, employees, or inventory, existing solely to move money under a legal guise. Many of them operate in industries that naturally involve high cash flow, such as travel agencies, salons, and online retail stores, making it easier to justify frequent transactions. Mules are often directed to deposit cash into these accounts in small increments, ensuring transactions stay under reporting thresholds while enabling the steady movement of illicit proceeds.

## Money Mules in Hawala Transactions

Money mules play a crucial role in facilitating Hawala transactions by acting as intermediaries who collect and deposit cash into accounts controlled by Hawala operators, known as Hawaladars. These mules can be individuals or small business owners, such as shopkeepers and travel agents, who disguise illicit funds as legitimate business transactions. By integrating these deposits into daily commercial activities, the Hawala network effectively avoids detection while maintaining the flow of unregulated money transfers. Once deposited, the funds are either transferred to other mule accounts or directly to Hawaladars, who settle the transactions through informal financial adjustments or trade-based money laundering methods. Since Hawala operates outside traditional banking systems, the use of mules provides anonymity, minimizes regulatory oversight, and ensures that funds can be moved across borders without leaving a traceable financial footprint.

# Red Flags for Identifying Money Mule Activities

**Discrepancies in account holder personal information and transaction details** - (information used during onboarding (KYC) and information used in transaction messages like address/name/phone number mismatch) indicating fraudulent activity

**Deposits followed by immediate withdrawals** - Withdrawing >90% of the amount which is deposited in the account which is a common tactic used by money mules to withdraw funds immediately

**Unusual transaction patterns** - Monitoring for unusual transaction patterns, such as frequent small deposits followed by large withdrawals, can help identify potential money mule activities. These patterns may indicate attempts to structure transactions to avoid detection

**Number of customers sharing a single device** - Multiple accounts accessed from the same device (e.g. mobile phone) indicate potential control by a single individual or group. This tactic is used to manage numerous mule accounts without exposing multiple devices

**Multiple devices used by a single customer** - Frequent device changes by the same user suggest attempts to conceal activities or involve different handlers and may indicate coordinated efforts to obscure the true user or enable criminal networks

**Login from high-risk geographies** - Access from regions known for financial crime or lacking strict regulations. High-risk locations may serve as operational bases for criminal organizations

**Logging in during odd Hours** - Activity outside normal banking hours may indicate remote operation by handlers in different time zones, suggesting urgency in moving illicit funds quickly to avoid detection

**Frequent changes in contact details (Phone number, Email ID, etc.)** – Rapid updates to contact information can signal attempts to evade detection or impersonate legitimate users to help disconnect fraudulent activities from initial identification details

**Rapid movement of funds** - Quick transfers between accounts are a classic sign of money laundering and often used to layer transactions and create complex money trails

**Multiple counterparties in transactions** - Numerous unique counterparties indicate structuring and placement of illicit funds, thereby diversifying the money trail, making it harder to trace the original source

**Transactional counterparty of known mule** - Interaction with accounts previously flagged as mules suggests involvement in a broader network

**Same contact details (Email ID, phone number) of known mules** - Shared contact information among multiple accounts links them to a single orchestrator

**Cross-border transactions** - International transfers are common in layering stages of money laundering. Provides a means to evade domestic regulatory scrutiny

**Activity at different ATMs** - Using various ATMs in multiple locations increases anonymity, enabling rapid cash withdrawal before accounts are flagged

**Common contact details shared by multiple customers** - Shared details suggest coordinated account creation or use by criminal groups and useful in identifying collusion among account holders

**High proportion of transactions from or to same or few Counterparties** - Concentrated transactions may indicate funnel accounts used to collect or distribute illicit funds

**Nationality of countries with high money mule prevalence** - Account holders from regions notorious for mule recruitment may pose increased risk

**Multiple logins in a single day** - Frequent access may indicate multiple users or urgent fund transfers. Suggests accounts are under the control of criminal handlers

**Transactions exceeding expected profile** - Large or frequent transactions inconsistent with the customer's profile can signal mule activity. Crucial for detecting sudden deviations in behaviour

**Unusual ATM activity** - Repeated withdrawals in quick succession or in different locations suggest illicit cashing out

**Newly opened accounts** - Recently opened accounts with immediate high activity may be set up solely for criminal use and highlights potential front accounts for laundering operations

## Small cash deposits and multiple counterparties

To identify accounts involved in collection of proceeds from predicate offense the following red flags may be considered and scenarios developed:

- Frequent small deposits of cash (For example, ranging from 300 -1200 AED)
- Accounts with daily deposits and withdrawals (indicating high volume of transactions, for example > 30)
- Transactions to/from multiple beneficiaries (number of counterparties, for example > 15)
- Deposits followed by multiple withdrawals (withdrawing > 90% of the total deposit amount in 1 month)

## Additional methods to identify money mules

- **Behavioural Analytics** - Implementing behavioural analytics can help detect anomalies in customer behaviour. For example, if a customer who typically conducts small, local transactions suddenly starts making large international transfers, it may indicate money mule activity
- **Machine Learning Models** - Developing and deploying machine learning models can enhance the detection of money mule activities. These models can analyse large volumes of transaction data to identify patterns and anomalies that may indicate money laundering.
- **Collaboration with Law Enforcement** - Financial institutions should collaborate with law enforcement agencies to share information and intelligence on money mule activities. This collaboration can help identify and disrupt criminal networks involved in money laundering

# Role of AI in detecting money mules


Artificial Intelligence (AI) plays a crucial role in detecting money mules by leveraging advanced algorithms and data analytics to identify suspicious activities and patterns. Here are some key ways AI contributes to money mule detection.

Anomaly Detection: AI algorithms can analyse vast amounts of transaction data to identify anomalies that deviate from normal behaviour. These anomalies may indicate potential money mule activities, such as unusual transaction patterns or rapid movement of funds.

Pattern Recognition: AI can recognize complex patterns in transaction data that may be indicative of money mule activities. For example, AI can identify patterns of deposits followed by immediate withdrawals or the use of multiple accounts to move funds.

Behavioral Analytics: AI can analyse customer behaviour to detect deviations from typical behaviour. For instance, if a customer who usually conducts small, local transactions suddenly starts making large international transfers, AI can flag this as suspicious

Machine Learning Models: AI-powered machine learning models can be trained on historical transaction data to identify features and patterns associated with money mule activities. These models can then be used to predict and detect potential money mule accounts in real-time

Natural Language Processing (NLP): AI can use NLP techniques to analyse unstructured data, such as emails, social media posts, and chat messages, to identify potential money mule recruitment activities. For example, AI can detect keywords and phrases commonly used in job scams or romance scams

Network Analysis: AI can perform network analysis to identify connections between different accounts and entities. This can help uncover money mule networks and their links to larger criminal organizations.

Real-Time Monitoring: AI can provide real-time monitoring of transactions and customer behaviour, enabling financial institutions to detect and respond to suspicious activities promptly. This can help prevent money mule activities before they escalate.

## Challenges in detecting money mules

Lack of Awareness and Training: Many individuals, including service provider employees and customers, may not be fully aware of the concept of money mules and how they operate. This lack of awareness can lead to missed red flags and inadequate responses to suspicious activities

Sophisticated Recruitment Techniques: Criminals use advanced social engineering tactics to recruit money mules, often targeting vulnerable individuals through job scams, romance scams, and social media. These techniques can make it difficult to identify and prevent recruitment efforts

High Volume of Transactions: Financial institutions process millions of transactions daily, making it challenging to identify suspicious activities among the vast amount of data. The sheer volume of transactions can overwhelm traditional monitoring systems

False Positives: Traditional rule-based systems often generate a high number of false positives, leading to significant effort and resources spent on investigating non-risky transactions. This can result in alert fatigue and reduced efficiency in detecting actual money mule activities

Evolving Tactics: Criminals continuously adapt their methods to evade detection, making it difficult for financial institutions to keep up with new tactics. This requires constant updates to detection models and monitoring systems

Data Quality and Availability: Effective detection relies on high-quality and comprehensive data. Incomplete or inaccurate data can hinder the ability to identify suspicious patterns and behaviours. Additionally, obtaining labelled data for training supervised machine learning models can be challenging

Cross-Border Transactions: Money mule activities often involve cross-border transactions, which can complicate detection efforts due to varying regulations and standards across different jurisdictions. Coordinating with international law enforcement agencies can also be challenging

Privacy and Compliance Concerns: Implementing advanced monitoring and detection systems must balance the need for privacy and compliance with regulatory requirements. Ensuring that detection methods do not infringe on customer privacy while effectively identifying suspicious activities is a delicate balance

Resource Constraints: Financial institutions may face resource constraints, including limited budgets and personnel, which can impact their ability to implement and maintain effective detection systems. This can lead to gaps in monitoring and response capabilities

Integration of AI and Machine Learning: While AI and machine learning offer promising solutions for detecting money mule activities, integrating these technologies into existing systems can be complex. Ensuring that models are accurate, explainable, and free from bias requires significant effort and expertise.

Digital Working Group

# Workflow for Machine Learning Model Development to Detect Money Mule Accounts

1. **Business Objective** - Identify key stakeholders and define business objectives with success criteria
2. Red Flag Identification - Identify red flags based on internal data and external references such as regulatory guidance, published articles, or case studies. Example: *Rapid fund movement, multiple accounts using the same device, and frequent logins during odd hours*
3. **Identify Critical Data Elements and Data Sources** - Determine the essential data fields and their sources required for feature generation. Ensure proper data lineage (understanding the origin and flow of data) to maintain consistency and quality
4. **Data Collection Preprocessing** - Develop features for each identified red flag. Clean and pre-process data to make it suitable for modelling. Example: *handling missing values, outlier treatment, normalize*
5. **Feature Engineering and Feature selection -** Generate new features based on red flags and other relevant indicators. For example: *develop new transactional features for rapid movement of funds, e.g.withdrawals >90% of deposits, identify key features for model development using techniques like correlation analysis, variable importance etc*.
6. **Model Selection -** Select appropriate modelling technique. If labelled data (e.g., *known mule accounts*) is available, consider using supervised algorithms like Logistic Regression or LightGBM. If labels are unavailable, consider unsupervised algorithms[1] like K-Means Clustering or Autoencoders. Select appropriate techniques to handle class imbalance
7. **Train - Test Data Splitting -** Divide the data into training, testing, and out-of-time (OOT) windows for model validation. OOT data helps evaluate the model's ability to generalize to unseen scenarios
8. **Model Training and Evaluation -** Train the model using different algorithms, such as Logistic Regression, Random Forests, or LightGBM, to find best-performing models
9. **Model Evaluation -** Optimize hyperparameters to improve model performance. Use cross-validation techniques to ensure the model generalizes well. Use metrics such as Recall or F1-Score to evaluate performance, focusing on minimizing false negatives

[1] Unsupervised algorithm provides general anomaly detection compared to supervised algorithm

10. **Responsible AI (RAI) Principles -** Ensure the model adheres to RAI principles such as explainability, fairness, and bias testing. Use tools like SHAP or LIME for explainability and fairness metrics to detect bias in predictions
11. **Data Quality Management Framework -** Establish a framework to monitor the quality of input data. Define metrics and processes to ensure the integrity and reliability of the data feeding into the model
12. **Model Monitoring Framework -** Design a framework for continuous model monitoring. Track metrics such as Population Stability Index (PSI), Characteristic Stability Index (CSI), Gini coefficient, and AUC to ensure the model remains stable and effective. Set thresholds and determine monitoring frequency in agreement with stakeholders
13. **Stakeholder Communication -** Share the final model performance, monitoring plans, and Responsible AI assessment with all relevant stakeholders. Obtain approvals before deploying the model into production.
14. **Model Deployment -** Develop pipelines for both feature engineering, trained model and prediction pipelines. Automate data processing and predictions to seamlessly integrate the model into operations.

## References & Further Reading

https://www.fic.gov.za/wp-content/uploads/2024/06/Financial-Crime-Insights-Money-mules.pdf

https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

https://www.justice.gov/civil/consumer-protection-branch/money-mule-initiative

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/money-mules

https://www.interpol.int/en/Crimes/Financial-crime/Money-mules-what-are-the-risks

https://www.biometricupdate.com/202501/biocatch-puts-spotlight-on-money-mule-problem-biometric-solution?

https://financefeeds.com/majority-of-uk-money-mules-are-under-30-says-report

https://lynxtech.com/resources/articles/money-mules-where-fraud-aml-and-cybersecurity-converge/

**Authored by:**

**Dr Yoonus Ahammed** (Member, DWG)

**Ms Indu Konuganti** (Special contributor)

**Reviewed by**:

**Nishanth Nottath, Mark Newfield, David Shepherd, Nipun Srivastava, Wai Lum Kwok, Bhavin Shah, Javier Pimentel, Lana Kershaw**

**Title:** Fighting Financial Crime: AI & Data Analytics in Money Mule Detection

**Compiled by:** Digital Working Group of the AML/CFT Partnership Forum, a Public-Private Partnership platform set up under the Executive Office of the Anti-Money Laundering and Counter Terrorism Financing in the United Arab Emirates.



**Disclaimer:** Despite the careful efforts made by DWG to prevent errors or omissions in this document, any unintentional mistakes or omissions are not intended. The information presented herein is solely for reference, educational, and awareness purposes and is subject to change without notice. It is important to acknowledge that DWG or any affiliates cannot be held responsible for any damage, loss, or other consequences arising from activities undertaken based on the information provided in this document.

**Languages:** English

**Number of pages:** 11 (including cover)

**Edition:** 1st edition

**Month and year of publication:** March 2025