feedzai

eBook

AI and the Fight Against Money Mules: New Tools for an Old Crime



Table of contents

Following the money mule trail from aml to fraud ---- 3

From clueless to criminal: the mule typology ---- 4

- Unwitting money mules
- Witting money mules
- Purpose-built money mules

How ai manifests itself within mule networks ---- 5

Detecting money mules: signs, signals, and strategies ---- 6

Regional solutions to a global problem ---- 9

Conclusion ---- 10

Oleksii Vengerskyi,
Financial Crime SME

pwc

Tejal Kaur,
Fraud & Identity SME

feedzai



Following the Money Mule Trail from AML to Fraud

There has been a notable shift in the financial industry's focus on money mules. From primarily addressing Anti-Money Laundering (AML) concerns to a heightened emphasis on fraud prevention, banks have created purpose-built teams to tackle the rising mule problem. Traditionally, mules were seen mainly as tools to move illicit funds in money laundering schemes and terrorism/trafficking financing, prompting institutions to tackle their role through AML/CFT frameworks. Fraud teams were even discouraged from implementing rules that may inadvertently disrupt mule networks to not 'tip them off' or alert them to potential investigation activities.

However, with the rise of digital fraud and increasingly sophisticated scams, mules are now more frequently involved in fraud-related activities such as authorized push payment (APP) frauds. As a result, f inancial institutions (FIs) and regulators are broadening their strategies, integrating fraud detection measures alongside AML efforts to identify, disrupt, and shut down mule networks earlier in the financial crime lifecycle. This evolution reflects the growing recognition that mules are not just a money-laundering conduit but an integral part of broader fraud ecosystems. To reflect that, under PSR rules aligned with PSD3, liability for APP fraud is split between sending and receiving banks, holding both accountable for money mule activity and incentivising them to detect and prevent such fraudulent transactions.

From Clueless to Criminal: The Mule Typology

Unwitting Money Mules

Who they are
Individuals who are unaware that they are facilitating fraud. Often recruited through fake job ads, romance scams, or social media "opportunities." Easily manipulated and frequently repeat victims. Education is key to prevention.

What they're likely to do
- Believe they are helping someone or earning money legally
- Receive and transfer funds quickly
- Provide personal information or open new accounts at someone else's request
- Be shocked or distressed when informed of the crime

Witting Money Mules

Who they are
Individuals who suspect or know the activity is suspicious but choose to look the other way for financial gain. Students are often targeted to become witting money mules. Often harder to detect than unwitting mules due to the frequent legitimate transactions in and around the fraudulent activity.

What they're likely to do
- Accept money transfers or share access to their account
- Refrain from asking too many questions; prefer "plausible deniability"
- Rationalize the activity as "helping a friend" or "just doing a favor"
- Engage intermittently or test the waters before deeper involvement

Purpose-Built Money Mules

Who they are
Knowingly involved in criminal networks, often as repeat offenders or part of organized fraud operations. These are extremely high-risk mules and considered a core part of the fraud operation involved in everything from scams to account takeover.

What they're likely to do
- Use multiple accounts, aliases, or fake identities
- Regularly move high volumes of money
- Coach others to become mules or manage networks
- Use more sophisticated methods to avoid detection (e.g., layered transfers, mule accounts with fake businesses)

How AI manifests itself within mule networks

Money mules have long been a crucial component in the world of financial fraud, acting as middlemen who transfer stolen funds on behalf of scammers. However, with the emergence of artificial intelligence (AI), the dynamics of money mule operations are undergoing a significant transformation.

In the case of recruiting money mules via job scams, instead of trawling the dark web for compromised credentials and details of potential victims to recruit, fraudsters use social media. LinkedIn, for instance, can be used to identify those who are 'Open To Work' and then, by using their information and employment history, can use AI to tailor a job description or even interviews and onboarding processes, which are personalised enough to be able to lure unsuspecting 'employees'.

AI has also assisted fraudsters with recruitment via romance scams. Tooling techniques, such as automated chatbots and deepfake audio apps, take centre stage and scam consumers at scale with personalised interactions to increase chances of success.

Additionally, the barrier to entry in the mule market has been lowered with the rise of Fraud-as-a-Service propositions, which offer less technically savvy fraudsters the ability to bulk order fictitious profiles and synthetic IDs. Other services offered by AI include the ability to generate content on a multi-language basis to recruit mules globally with minimal effort, whilst exploiting the advances in cross-border payment mechanisms.



Detecting Money Mules: Signs, Signals, and Strategies

AI-powered fraud detection systems offer several advantages over traditional methods, including analyzing vast amounts of data in real-time, recognizing complex patterns, and adapting to new or emerging threats. Traditional fraud detection methods, which rely on rule-based systems or simple algorithms, are often ill-equipped to handle the complexities of modern financial crime. These methods may flag obvious fraudulent transactions, but struggle to identify subtle or well-disguised activities. There are a number of signs, signals, and strategies that can be leveraged to increase mule detection.

Prevention across the entire fraud lifecycle
Leveraging device and behaviour at onboarding to determine whether an applicant looks legitimate. For example, synthetic IDs are often generated at scale, so detecting signs of automation during an application is a useful method of detection. We can connect the application to any subsequent transactions that are made in the account. For example, if an account is opened then left dormant for a period of time, if we then see that multiple incoming payments are received, we can detect these in real time and give the FI a clear line of investigation.

Thinking outside the 'whitebox'
While device profiling is commonly used to detect when a single device is associated with multiple accounts, a less common, but highly effective, method involves analyzing addresses to identify when multiple customers are linked to the same location. This technique often reveals smaller mule networks that register at obscure addresses, such as small takeaways or other businesses acting as fronts. These networks can then be fed into lists of higher-risk profiles to treat with an additional layer of scrutiny. From a treatment strategy perspective, increasing the hold period for potential mule accounts is often enough of a deterrent. It will most likely lead to the account being abandoned, particularly for purpose-opened mules.

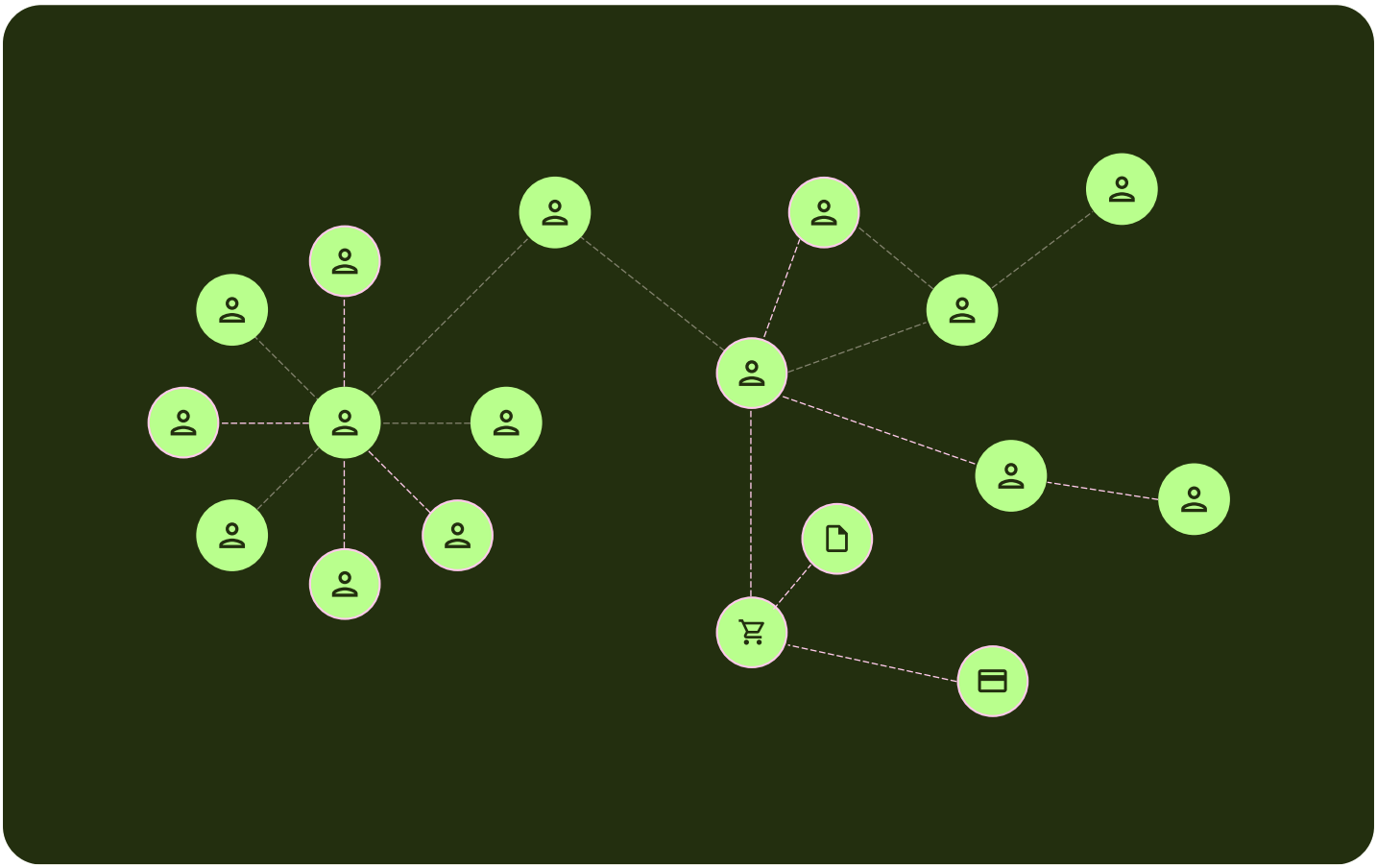
Targeted Prevention and Detection
In addition to AI, an essential aspect of targeted fraud detection is ensuring that the data going into the models is specific. For example, it is not enough to label a mule as a mule due to the distinct differences in behaviour of mules. Purposely opened mules, for instance, are much easier to detect than unwitting mules due to their behaviour. FIs should ensure their labels capture the variations of mule typologies. The impact of having this granular detail flowing into fraud detection models, the better and more accurate the decisioning will be across detection and false positives.

Omnichannel profiling of mule behaviour

Once you've got the keys to the front door, why stop there? FIs investigating mule activity have found that these accounts often span beyond bank transfers into card products as well. That's why an omnichannel view of the customer is essential, because mule behaviour is rarely confined to a single channel. A mule might receive illicit funds via online transfer, withdraw cash from an ATM, spend through a card, or use one of the financial instruments (mainly checks, and other monetary instruments) . Seen in isolation, each action may look perfectly normal. But viewed together, the pattern tells a different story. Criminals thrive on the blind spots between channels and an omnichannel view eliminates those blind spots.

Visual Link Analysis

Tooling that shows the links between mule accounts turns raw data into network maps that show how accounts, phone numbers, devices, and IPs are interconnected, which is valuable across the breadth of fraud teams. Link analysis can reveal patterns of mule behavior, like multiple accounts funneling money to one central account, clusters of low-value transfers at similar times, and shared device fingerprints across accounts. This gives all audiences a clear insight into the 'full picture' around mule activity.



Anomaly Detection, Behavioral Analytics and Machine Learning for Pattern Recognition
In Machine learning (ML), a subset of AI, allows fraud detection systems to continuously improve their ability to identify fraud. As the system processes more data, it learns to recognize new fraud patterns and adapt its detection algorithms accordingly. For example, if a criminal organization changes tactics, the AI system can quickly identify these new methods based on the patterns of previous activities, helping to detect money mule operations even if they don't fit traditional fraud models.

Real-Time Inbound/Outbound Monitoring and Decision-Making
When money moves fast, your defences need to move faster. AI-powered systems allow banks to spot and act on suspicious transactions in real time. And it's not just about catching bad actors on the way out, many banks are turning their attention to what's coming in. Inbound payment profiling helps financial institutions stop mule activity before the money even lands. By analyzing payment patterns and traffic trends, banks can flag risky accounts early—sometimes before they've moved a single cent out.

Local Network Data Integration
Many money mule operations involve international transactions, making it challenging for financial institutions to track illicit funds. Mastercard's CFR (Consumer Fraud Risk) and Trace are two important tools designed to f ight money mules and broader financial fraud. They provide insights that banks cannot easily generate on their own using Mastercard's network-wide intelligence. A bank knows what happens inside its own walls, not what happens before or after the money enters or leaves its accounts. Mastercard has a view across the whole payments network, seeing fraud patterns across multiple banks, PSPs, fintechs, and geographies. A future iteration of this concept would be cross-border collaboration to detect patterns of fraudulent activity that span multiple countries, enhancing the effectiveness of fraud detection efforts in an international environment.



Regional solutions to a global problem

Through policy introduction, adoption of the above strategies, and coordinated education efforts from governments and financial institutions around the world, we see real momentum in disrupting mule operations. A few examples include:

- **Thailand** has intensified its crackdown on mule accounts in response to a dire scam landscape. Law enforcement, working closely with FIs, has shut down over 135,000 mule accounts and facilitated over 869 arrests since the start of 2025.

- **Europol's 'EMMA' (European Money Mule Action)** initiative also boasts the identification and closure of thousands of mule accounts and arrests of hundreds of recruiters.

- **Singapore** has implemented harsher consequences for those involved in criminal mule activity, including first-time offenders. This tougher stance has been commended for its effectiveness in curbing mule operations in the region.

- **Australia** is tackling organized mule networks through joint efforts by the Australian Criminal Intelligence Commission, Federal Police, and banks. Public awareness programs like Scamwatch have helped to educate consumers and encourage reporting of mule recruitment scams.

Conclusion

The battle against money mules has entered a dynamic new phase, moving beyond basic anti-money laundering/Counter-terrorist financing tactics to a comprehensive defense incorporating fraud prevention, instant detection, and sophisticated data analysis. Artificial intelligence both enables and deters crime, empowering criminals to refine their recruitment strategies while simultaneously providing financial institutions with the means to identify and dismantle mule networks with unprecedented speed and precision. Faced with stricter regulations and shared responsibility within the payment system, the industry is innovating with detailed classifications, cross-channel oversight, and international partnerships. This fusion of technology, regulation, and public awareness is generating significant progress in the worldwide effort to stop money mules, making it harder for criminals to misuse the financial system and highlighting the ongoing need for ingenuity and collaboration across all sectors.



Supporting Industry Efforts

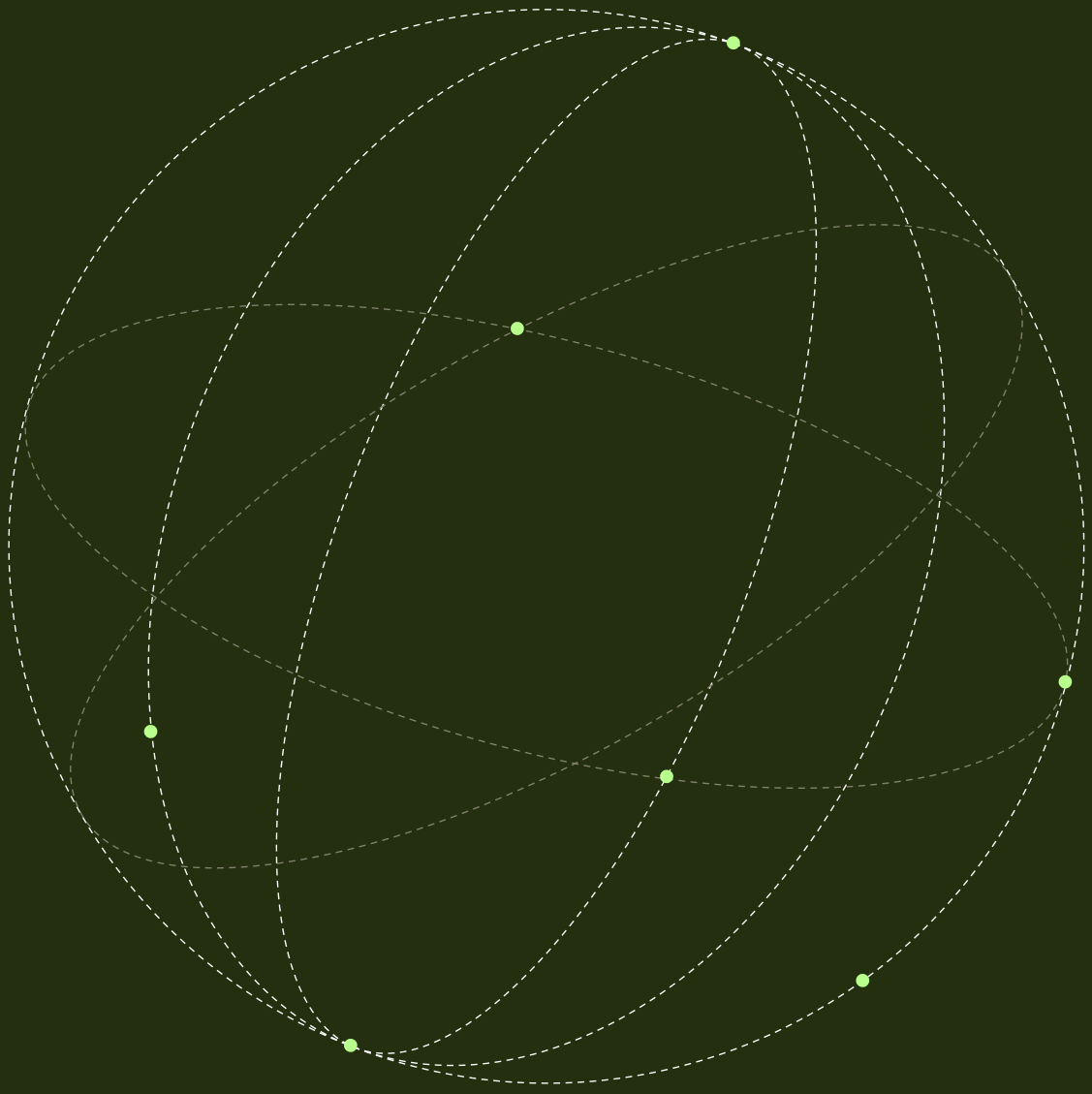
Feedzai is the world's first end-to-end financial crime and risk operations platform, protecting people and payments with AI-native solutions that stop fraud and manage compliance. With integrated data orchestration, Feedzai empowers financial institutions to dynamically access, manage, and act on the right data in real time. This accelerates decisions across onboarding, authentication, and transaction monitoring to ensure mules are dealt with effectively throughout the fraud lifecycle. Trusted by the world's leading banks, payment providers, and fintechs, Feedzai safeguards trillions of dollars in transactions while reducing customer friction and protecting user privacy.

Through our collaboration with PwC, we offer tailored strategies to help you identify and dismantle money mule networks. Our comprehensive approach enhances prevention across all channels, ensures compliance with evolving regulations, and contributes to the global fight against financial crime. PwC's experience in uplifting and designing robust operating models for fraud and AML, combined with our advanced detection technologies, keeps you one step ahead of criminals engaged in fraudulent activities and money laundering schemes.

The time to act is now. If you're interested in learning more about industry-leading practices or want to ensure alignment with current fraud and AML regulations, don't hesitate to contact our teams. Discover how we can revolutionize your prevention efforts. Together, we can create a more secure financial ecosystem, protecting your business from both fraud and money laundering threats.

"Trusted by the world's leading banks, payment providers, and fintechs, Feedzai safeguards trillions of dollars in transactions while reducing customer friction and protecting user privacy."

feedzai



Feedzai is the world's first end-to-end financial crime prevention platform, protecting people and payments with AI-native solutions that stop fraud and financial crime. Leading financial institutions trust Feedzai to manage critical risk and compliance processes, safeguarding trillions of dollars of transactions, while improving the customer experience and protecting the privacy of everyday users.

Recognized by IDC datos INSIGHTS Celent. Chartis

Identity | Orchestration | Fraud | Anti-Money Laundering

sales@feedzai.com info@feedzai.com feedzai.com