feedzai

Inbound Payment Fraud Detection and Mule Risk Modeling

Complying with Bank Negara Malaysia's Recommendations for Identifying Fraudulent Accounts

Contents

Inbound Payment Fraud: Shifting the Focus from Victim to Criminal

Stopping outbound payments that pose a high fraud risk has been the cornerstone of most financial institutions' fraud prevention strategy for years. However, with the emergence of authorized push payment (APP) fraud, this is arguably targeting the wrong person. It is the inbound payments that lead directly to the criminal accounts moving illicit funds, as opposed to the genuine account owner making what they believe to be a legitimate payment. Inbound monitoring provides more opportunities to capture fraud; not only preventing funds leaving victims accounts but also identifying mule accounts as funds arrive.

It is the inbound payments that lead directly to the criminals whereas with authorized fraud the genuine account owner is making what they believe to be a legitimate payment.

A mule account holder – whether witting or unwitting – is considered an accessory or accomplice to fraud and money laundering. According to Bank Negara Malaysia (BNM), mule account holders can be charged under Section 424 of the Penal Code for fraudulently concealing monies and for owning stolen goods under Section 29 of the Minor Offences Act 1955. The good news is that by using the latest fraud prevention techniques banks can identify mules before they inflict significant harm on customers.

Monitoring Inbound Payments and Identifying Mule Accounts

42%

of first-party current account fraud is now mule-related, with the fraud rate for current accounts rising by 13% in just three months.

Experian

Inbound payment fraud detection not only helps identify illegitimate funds, but also uncovers mule accounts into which they are initially received. The earlier the risk is identified, the higher the success rate of preventing those funds from being forwarded on. The problem of identification is made more complex by the fact that there are different types of money mules – whether witting or unwitting. These can vary across 1) the fraudster who opens the account themselves, 2) accomplices that either hand over their account and willingly transfer funds on request, or 3) others who are not aware there is anything illegitimate happening or are unaware that their account has been hacked and is being used to launder funds.

In all cases there is **three-stage lifecycle with opportunities to identify mules at each stage: Account Opening, Ongoing Activity and Inbound Payment Monitoring.**

Account Opening	Ongoing Activity				Inbound
					
Account Opening	**Limited Activity**	**Unusual Usage**	**Activity Increase**	**Beneficiary Creations**	**Receives Fraudulent Funds**
It isn't always possible to detect all mules at account opening. Some slip through the net.	No credits, no bills, no direct debits etc. are observed on the account.	Account accessed by multiple devices, same phone numbers or other common entities.	Following a period of dormancy, the account becomes active.	Beneficiaries are created but not paid. Often the account is 'prepped' ahead of receiving funds.	Account receives fraudulent funds. It is possible the risk could have been recognized and mitigated by this stage.
Risk Scale					
Low	Increased	Medium	Increased	High	Confirmed

1 Account Opening

The right account opening strategy provides the best opportunity to prevent witting mules and avoid the need for subsequent account closure processes.

2 Ongoing Activity

Often, seemingly good accounts can go bad. Changes such as intent, behavior and account characteristics can be identified during everyday use.

3 Inbound Payment Monitoring

Identify suspicious inbound transactions in real-time to freeze potentially fraudulent funds. Inbound payments can also be used as context to detect further attempts to move the money to a 2nd generation mule account.

3 Chances to Catch a Mule

1 Account Opening

Identify mules before they become active by flagging accounts that show signs of mule risk and record the features and triggers. Examples include:

- The device used at account opening has been used by known mules in the past.
- Similar data items, such as email or other personal details have been used across multiple applications.
- Online application typing patterns indicate either lack of knowledge of personal details or conversely familiarity with the form structure.
- A bot is being used to open multiple potential mule accounts at scale.

2 Ongoing Activity

Fraudsters often find it difficult to beat account opening controls when creating mule accounts themselves. Instead they lure genuine customers to process fraudulent funds on their behalf in exchange for a fee. These behavioral patterns can be recognized within the data when analyzed. Indicators include:

- Abnormal patterns in individual-specific behaviors and similarity with previous known mule patterns including transaction velocity, amounts and timings.
- Signs of financial distress within the account history of a user. Fraudsters often target customers that follow this pattern. Use machine learning models to operate a rolling future mule propensity score for predictive risk decisions.
- A feedback loop of data and entity linking. E.g. one device that has been used on a known mule suddenly accesses multiple other accounts. These accounts should be reviewed and additional scrutiny should be placed on them.

3 Inbound Payment Monitoring

Monitoring inbound payments coming into the bank can play a significant contribution to stop fraudsters in their tracks. Example checks include:

- If the payment amount fit with the usual credits received.
- How funds are moved upon receipt. E.g. an inbound payment followed by an immediate outbound payment for a similar amount should be monitored.
- Recent device usage and any links to known mule networks.
- Purpose-built machine learning models that reference output from previous steps in the mule monitoring process. E.g. a payment received by a customer with a high mule propensity score demands a different outcome.

With sufficient suspicion resulting potential actions could be to freeze funds in real-time, place account level blocks, or provide watch flags on accounts for future activity.

With sufficient suspicion, resulting potential actions could be to freeze funds in real-time, place account level blocks, or provide watch flags on accounts for future activity.

The Feedzai Difference

Feedzai not only identifies mule accounts via transaction-based rules and models to stop payments as they hit accounts, but also combines contextual session data, such as device identification to uncover and take down large mule networks at scale. This approach of monitoring account risk across the lifecycle from onboarding, right through to fraudulent funds being received is the most effective way to catch mules.

Feedzai's AI-first patented decision intelligence has been independently endorsed to improve detection rates whilst lowering false positives.

Anomaly Detection at Scale

Feedzai analyzes vast quantities of data, over much longer time windows in order to understand each individual's unique behavior. It identifies anomalies accurately across multiple channels with customer-centric profiles using precise analysis of behavior, device, network, inbound and outbound payments, and user activity - all on a single, scalable platform.

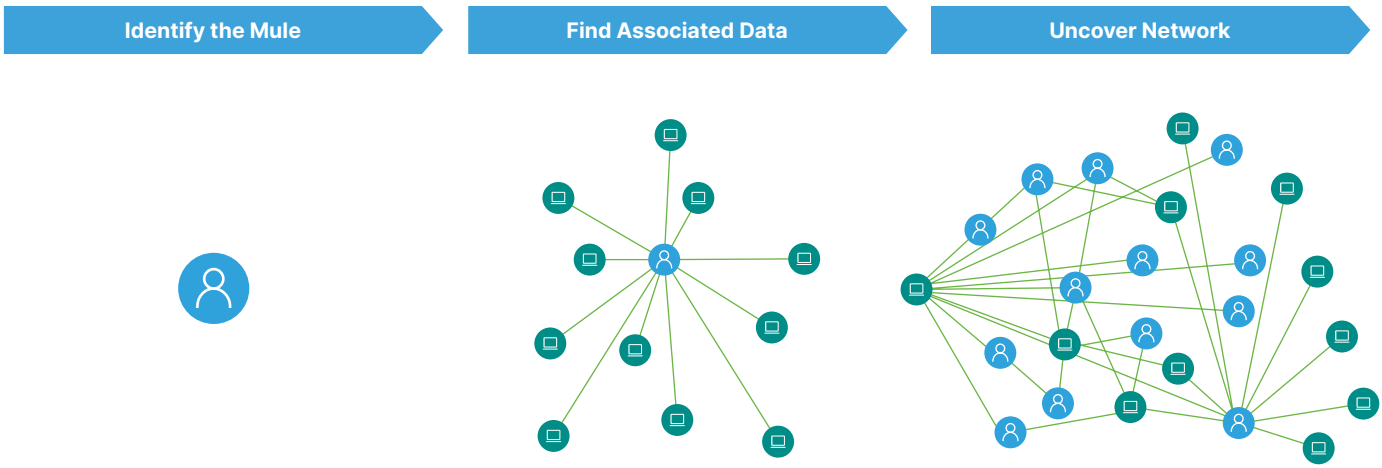
3-in1 Risk Analytics

Feedzai analyzes vast quantities of data, using precise analysis of behavior, device, network, inbound and outbound payments, and user activity.

Easier Decisioning

Feedzai provides fraud analysts and compliance investigators with clear risk explanations with full context to drive faster decisioning. In addition, our Visual Link Analysis connects more complex scenarios to:

- Stop coordinated attacks and complex financial crime patterns.
- Follow the money flow and intuitively guide investigators through relationships.
- Identify new rules to detect and block identified patterns.
- Share insights with compliance teams.



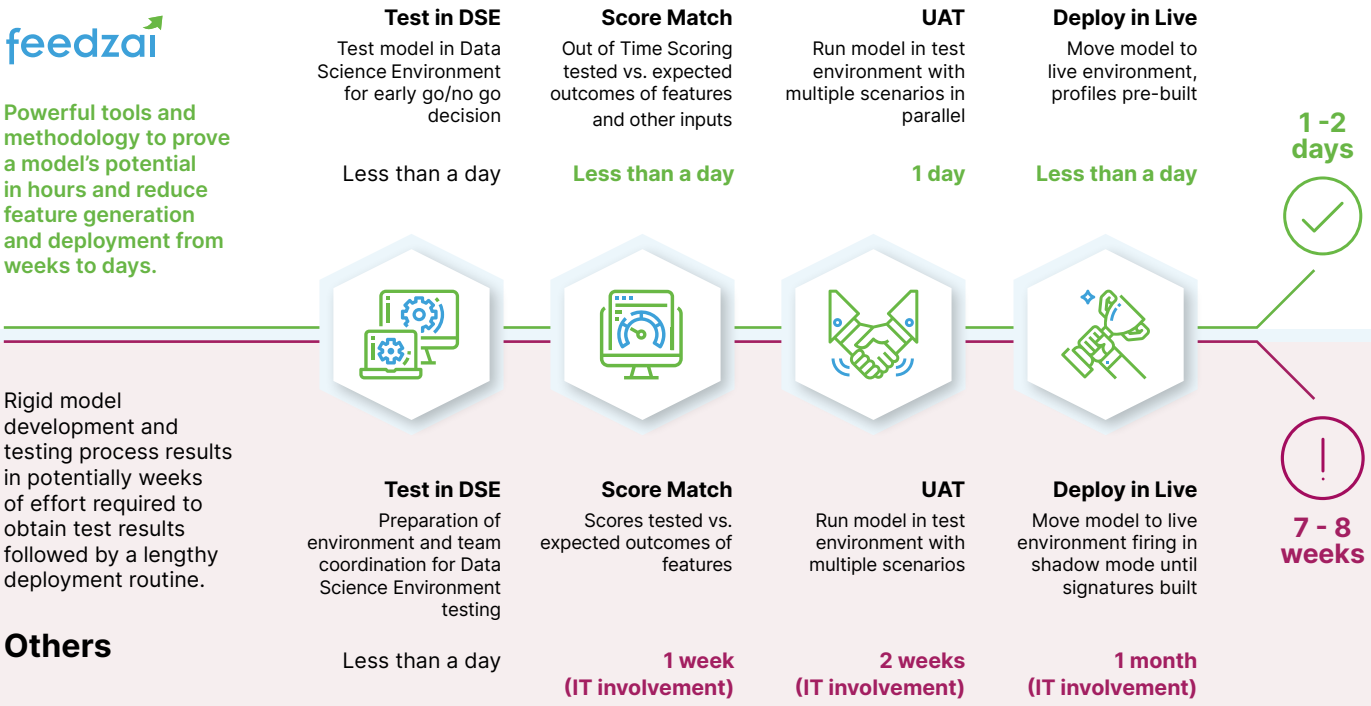
Find previously unidentified risks and proactively protect customers.
Feedzai provides multiple approaches to link analytics and known risk list management.

Link Analysis - Uncovering the Network Connection

Faster Adaptation

Feedzai changes the game for data scientists' ability to respond much more rapidly to evolving fraud threats. Our Automated Machine Learning (AutoML) techniques automate data exploration, feature engineering, model training, and evaluation steps of the data science workflow. Here are just some of the differences offered by Feedzai's AutoML capabilities:

- New features **do not need to wait for data**
- **No need to move data** to build models
- Possibility to bring **own models**
- Models that can be **immediately simulated and deployed** with IT involvement as optional



Model Deployment in Days, not Weeks

Case Study

Background
Top European Bank Targeted by Cybercriminal Gang

One of Europe's largest digital banks was targeted by a cybercriminal gang using the Bank as a clearinghouse. The Bank had over 1.2 million clients and $10 billion in customer assets. The gang had published a network of advertisements offering to sell consumer goods at steep discounts. Unfortunately for people who responded to these ads, all they received after transferring their funds to money mule accounts was disappointment.

Challenge
Shut Down Active Money Mule Accounts

The Bank's goal was to shut down active money mule accounts and prevent new instances of online account opening fraud to stop this criminal enterprise. Additionally, the Bank wanted to collaborate with local authorities to identify and help prosecute money mule account owners.

The Bank's goal was to shut down active money mule accounts and prevent new instances of online account opening fraud.

Solution

BionicIDs Uncovered Criminal Network of Mules

Feedzai's BionicID analyzes customers' behavioral biometrics, network, device, and malware data.

Feedzai creates BionicIDs as a unique identifier for each customer at scale. Each BionicID analyzes customers' behavioral biometrics, network, device, and malware data. Through this analysis, Feedzai quickly gathered profiles of known fraudsters, based on their BionicIDs. These are used to link to other accounts to discover which ones were "owned" by the same person, and uncovered any other criminals linked to that money mule account. For example, the Bank's analysts determined that the illegitimate accounts set up for this advertising scam were opened using stolen or synthetic identities (an identity made up of a blend of real and fake information).

Results

Feedzai Identified and Blocked hundreds of Money Mule Accounts

All of these accounts were created and used to process funds generated from the same fake classified advertisement scam. Using BionicID data of the known bad actors, analysts were then able to quickly create rules so that the Bank could automatically freeze offending accounts in real-time, preemptively stopping fraud before it happened. Additionally, fraud specialists used Feedzai's Fraud Hunter to gather more identifiable information of bad actors, and hand it over to the police to help them with their investigation into other money mule activity.

Read the full case study here

Case Study

The Benefits of Inbound Payment Fraud Detection

As fraudsters grow increasingly sophisticated, inbound payment and mule monitoring is a critical differentiator for keeping fraudsters in check. Here are some of the reasons why top financial institutions are now adopting this approach.

Remove Criminal Accounts

When bad actors and witting mules realize they keep getting blocked then they will turn elsewhere. Secure your reputation as a financial institution with legitimate transactions and customers.

Enhance Outbound Fraud Detection

The current practice of only monitoring outbound payments gives an incomplete view of customer risk. Whilst this was adequate in the past for unauthorized fraud typologies such as account takeover, the same cannot be said for authorized fraud. Tracking flows into and out of an account within the same risk model both improves accuracy and also identifies illegitimate use sooner.

Keep More Customers Safe

With better defence against mules, genuine customers will benefit from fewer unnecessary interventions and appreciate efforts to stop banking fraud. At the same time, you may even win over customers against competing institutions. If you stop a fraudulent transaction and return it to the rival bank's customer, the customer is more likely to give your bank a second look.

Move from Reactive to Proactive AML Monitoring

As well as the obvious fraud losses, mule accounts also pose a money laundering compliance risk. Malaysian governing authorities can look to their global peers for inspiration on keeping consumers educated and safe. For example, as a direct result to a large increase in mule activity, INTERPOL launched #YourAccountYourCrime campaign, to address the problem and highlight the need for financial institutions to keep accounts safe from criminal misuse.

Detecting illegitimate inbound payments enables an institution to gather compelling evidence for suspicious activity reporting and adopt a much more proactive approach to identifying problem accounts sooner.

Extensible as a Value-added Service for Corporate Banking

Many companies' payment receivable processes suffer from poor internal controls. 85% of companies are either already or planning to invest in fraud prevention. There is potential to adapt retail inbound payment risk models to provide competitive differentiation for corporate and SME banking.

Lead Industry-Wide Change

Demonstrating the value of inbound payment monitoring enables organizations to stand out as market leaders in fighting fraud. By demonstrating protection for customers of other payment institutions as well as its own, a bank can set new standards for consumer trust and doing the right thing for society.

85%

of CFOs are Prioritizing Fraud Controls for Incoming Payments

Pymnts.com

Inbound Payments: The Fraud & AML Intersection

Inbound Payments

Using The Right Data With The Right Analytical Approach

Historical Knowledge

- Applied known bad learnings from existing projects - both Fraud & AML
- Apply proven principles from previous research and factor in known mule risks
- Combine with anomalies on a user-by-user basis, analysing user history in real-time
- Consider historic data feed from bank where available to expedite model process

Transaction Analysis

- Decision based on amount, sender, reference, CoP results and other feeds
- Applying proven principles from outbound decisions to inbound events
- Apply metrics to recognize inbound payment ratios, payment velocities etc.
- Blend together with outbound payment history for best results

Contextual Data

- Augment transactional data with user and relationship data
- Ideas include age of account, other holdings, account status, user age etc.
- Capture any existing customer segmentation or flagging processes
- Leverage where applicable ongoing user risk score

Analytically Driven

- Start with rules and gradually develop rule complexity
- Explainable rules can eventually become models when enough data exists
- Use inbound events to influence subsequent outbound event decisioning
- Link analysis post event for additional capture

Inbound Payments
Using The Right Data With The Right Analytical Approach

Best Practice Tips

Feedzai offers both a fully-serviced cloud solution and proven practical expertize as we recognize that technology is only one part of the solution. Here are some additional hints and tips for market-leading mule account detection:

- Distinguish mules operationally. Identify mule propensity and flag accounts at the earliest opportunity - monitor these accounts as high risk or even close them before they have received funds. There is often a pattern of mule accounts remaining relatively inactive for a time after creation.
- Apply rules and ML models to improve ongoing account monitoring and intervene proactively.
- Adopt a multi-channel approach to avoid mules exiting funds via branch or card payments for example.
- Use machine learning models that include non-monetary events for precise decisioning.
- Increase education amongst customer base.
- Introduce robust account tagging, reporting and internal awareness.

Assess your readiness For Inbound Payment Fraud Detection

Schedule a free consultation today

feedzai

Fraud and Financial Crime Solutions

Transact in Trust

Feedzai is the world's first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime. The world's leading financial organizations trust Feedzai to safeguard trillions of dollars of transactions and manage risk while improving the customer experience.

Account Opening | Anti-Money Laundering Suite| Digital Trust | ScamPrevent | Transaction Fraud

Request a demo

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