feedzai

Case Study

Feedzai's Digital Trust Helps Challenger Bank Take on Money Mule Networks and Protect Customers

Key Results

400
money mule accounts identified 2 weeks after deploying Digital Trust

<15 mins
to block 400 mules

Company
One of Europe's largest digital banks, with more than 1.2 million clients and $10 billion in customer assets.

Industry
Financial Services
Challenger Bank

The Challenge:

Shut Down Active Money Mule Accounts

One of Europe's largest digital banks was targeted by a cybercriminal gang using the Bank as a clearinghouse. The Bank has 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.

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.

What is a money mule?

A money mule is an individual who opens a bank account at a legitimate financial institution to accept stolen or ill-gotten funds. These accounts can be opened by either witting or unwitting money mules. Witting money mules know they are part of something criminal or nefarious. Unwitting money mules, on the other hand, do not realize they are involved in something illegal.

Unfortunately, the Bank's fraud prevention team could not get in front of the bad actors fast enough to identify them when they opened a new account. By the time analysts identified the money mules, bad actors had cashed out one account and moved on to another. The analysts could only locate a few illegitimate money mule accounts early on due to fraudulent behavioral patterns, like having a short account lifespan with money remaining in an account for less than a day before being transferred out of the Bank.

But with so many fraudulent accounts, it proved to be impossible to keep up with the volume and speed at which they were being flipped.

Tracking down bad actors working as money mule herders and detecting accounts they had compromised or were in the process of compromising seemed to be an insurmountable problem.

The Bank needed a solution that would:

Identify bad actors operating money mule scams in their online banking systems

Reveal how the money mules networks operated to prevent additional mule accounts from being created

Protect legitimate customer accounts from getting compromised and turning everyday people into money mule victims

Additionally, the solution needed to identify money mule accounts first opened by bad actors at the beginning of their fraud campaign so they could be traced back to their owner and the information handed to authorities for prosecution.

How Feedzai's Digital Trust Uncovered Money Mule Operations

The Bank identified Feedzai as the only vendor capable of providing behavioral biometrics, network, and device intelligence solutions that would let the Bank's fraud prevention team actively hunt down bad actors operating in their online banking system. Feedzai Digital Trust creates a BionicID™ for every user, good or bad. BionicIDs are created using hybrid AI models, including Deep Learning, to analyze behavioral biometrics, behavioral analytics, device, and network data. BionicIDs are continually updated and analyzed at every interaction to thoroughly Know Your User (KYU) and verify their identity.

Here's how the Bank unmasked this financial crime ring with the help of Digital Trust:

Step 1

Once fraud has been detected, analysts use the Hunter tab in the Feedzai Management Console to perform online forensic analysis of the event and correlate all associated data relevant to that attack. Utilizing BionicIDs allows banks to catalog and cross-reference user information with customer data so that fraud teams are able to trace malicious activity back to individual actors in a highly effective manner.

Step 2

Feedzai analyzes the dynamic context of each fraudulent banking session to understand which devices, broadband networks, and geolocations, amongst other factors, were in use for money mule scams. It also detects the interrelationships between users' behavior and their environment, mapping these relationships graphically. Once these interrelationships are established, it is a simple process to perform link analysis between similar data types to identify the attack's origin.

Step 3

Once the money mule red flags were identified, rules were created to block attacking accounts from further operation, stopping future fraud attempts and cutting fraud off at the root. The Bank used this intelligence to understand the "modus operandi" of fraudsters and uncover complex fraud scenarios in order to predict and prevent future fraud campaigns.

Step 4

Additionally, the Bank now utilizes customer account information associated with attacking accounts to locate the owners and hand their information over to authorities for follow-up criminal investigations into money mule scams.

Results:

Feedzai identified and blocked over 400 money mule accounts.

The Bank uses Feedzai to profile fraudsters through their BionicIDs. It then used this data to link BionicID elements to other accounts to discover which ones were "owned" by the same person, or 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). When this information was analyzed using BionicID data, it was determined these fraudulent accounts were being accessed from the same device, or over the same Wi-Fi network. This information allowed the Bank to determine that the same bad actor controlled numerous money mule accounts, despite the fact that they were created under different names.

Feedzai identified and blocked over 400 money mule accounts early in the Bank's investigation. 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.

"Feedzai Digital Trust has proved invaluable to us. Firstly, it allowed us to rapidly identify an entire network of mule accounts in time for us to freeze them and halt any fraud before it could happen. Secondly, it enabled us to discover and profile the fraudsters themselves, so they can no longer attempt to commit fraud at our Bank.

Head of Bank Security,
Major Digital Bank

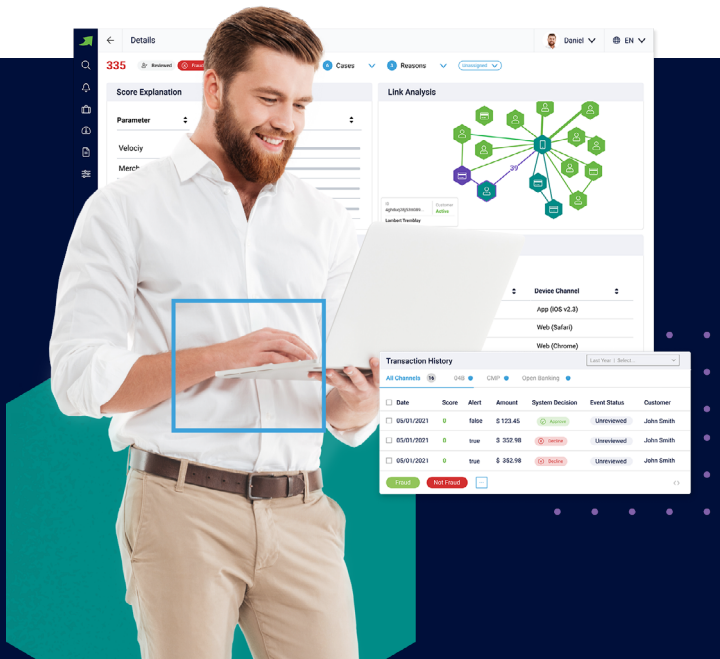
Brands Trust Feedzai

citi LLOYDS BANK Cuscal fiserv.

feedzai

See our technology in action.

Request a demo



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