Fishing for Mules with Nets

Authors: Andreas Schaefer, Jen Houle, Daniel Clegg

Institution: Royal Bank of Scotland

Financial fraud is a pervasive and ever-changing problem. Fraudsters successfully stole £1.2bn in 2018 using scams and fraud\(^1\). To access this money, criminals must launder the funds acquired. Often this activity is related to organised crime, drug and people trafficking and funding of terrorism. Stopping this activity benefits society as a whole.

One such method of money laundering is using a ‘money mule’: a person who receives criminal funds into his or her bank account and sends it on to the scam operator in return for a small commission. In the UK, money mule activity is increasing and now accounts for 25% of all types of fraud reported through the CIFAS national fraud database\(^2\). Banks have a duty to prevent the laundering of fraudulent funds in order to protect their customers and society.

In addition, there is an increased focus on money mules within the UK financial services industry with the introduction of the Industry Code on Authorised Push Payment (APP) Scams in 2019. 2018 saw a gross loss of £354m through APP Scams\(^3\).

A money mule is not an isolated person – they are connected to the scam operator and other mules through a complex web of financial transactions. Typically, money mules are found by financial institutions in a manual process where a tip is received from another bank or the police and connections in disparate bank databases are pieced together manually to find related mule accounts. It is laborious and time-consuming for a fraud investigator to collate these data items. We introduced a novel network analysis tool to replace this manual collation process.

Instead of manually connecting together a few data items to find money mules, our tool links together millions of banking event data records to find suspicious connections. Many standard fraud-finding techniques rely on analysing discrete data, meaning that connections between bad actors cannot be identified. Where common statistical models struggle because of class imbalance, graphs offer a simple and accessible approach. Starting from known bad actors, we connect customers, accounts, and transactions in a network graph. Adding information is important but exacerbates the “small world” problem. This is when the neighbourhood of a node becomes too large to investigate for a human. We worked with fraud investigators to target our network graph to only show the most suspicious links, for instance by filtering out highly connected nodes using ego nets or shortest paths. Based on fraud investigator feedback, we created a companion visualisation tool which visualises a simplified local neighbourhood of connections around known bad actors in our network.

Now, when a fraud investigator is looking for money mules, they can use our network visualisation of known bad actors to find connected money mule accounts. This means that investigators no longer need to manually piece together the connections which previously took days.

Instead, they can see suspicious accounts at a glance, and complete an investigation in far less time than previously. Our solution gives our people the chance to investigate data rather than generate it.

Since implementation of the mule network and visualisation tool, the volume of cases actioned by investigators has shown a material increase. Investigations have become more efficient and effective and we have been able to reduce the adverse impact of financial crime on our customers and society.

In addition, the use of the network tool has been expanded to visualise the networks of suspected fraudsters in specific complex fraud investigations across both personal and business banking within the bank.

The solution has been developed in an agile fashion with immediate application in mind. This means that it is built with the capability of continuously adding new data sources. Through this it is also capable of integrating the output of statistical and ML models.