



FINANCIAL CRIME SOLUTIONS

The rise of the mule

Identifying mule accounts and tracing financial crime
across the UK payments network

SECOND EDITION, OCTOBER 2019



Second edition

This second edition of 'The rise of the mule' is updated to include performance statistics and learnings six months since the launch of our capability to trace financial crime across the UK payment network in partnership with Pay.UK.

It demonstrates success beyond the initial proof of concept, detecting and tracing criminal activity across the payments network and within financial institutions to support and inform the efforts of investigators on the ground.

Contents

5	Introduction
6	Context: The rise of the mule
8	Proof of concept: a game-changing result
12	Live service: tracing financial crime in the UK
16	Benefits: Better outcomes for people, businesses and society
18	Conclusion



Introduction

The problem of money laundering and mule networks is not a new one. For years, people involved in organised crime have endeavoured to set up or take-over accounts for the express purpose of moving the proceeds of crime through a network in order to obscure their source and extract funds.

Until now, getting a complete picture of how these networks operated and how vast and connected they might be was also impossible since the number of accounts across multiple financial institutions (FIs) involved in the movement of money, and the total number of payments associated with one fraudulent transaction was large enough to make piecing together the data impractical.

"It is noted that there is a marked overlap between money laundering and terrorist financing – both criminals and terrorists use similar methods to raise, store and move funds."

Source: UK national risk assessment of money laundering and terrorist financing report, HM Treasury & Home Office

2
\$trillion
laundered globally
every year

The value of money laundered globally in one year is estimated at over \$2 trillion, representing 2–5% of global GDP. Money taken by criminals through fraudulent activities is rarely fully recovered, leaving FIs or their customers to bear the cost.¹ The impact on companies and individuals can be devastating, resulting in large financial losses, business closures and job losses. Research conducted by Populus on behalf of Vocalink, a Mastercard company, found that nearly half (45%) of businesses falling victim to invoice or mandate fraud either folded or lost thousands – and in some cases millions – of pounds.

70% believe that the fraudsters committing invoice redirection, mandate and CEO fraud are now 'ahead of the industry'

Source: Vocalink Business Fraud Report 2018–2019

321
\$billion
cumulative bank
penalties for non-
compliance

The prevention of financial crime including payment fraud and money laundering is also a costly challenge for FIs who have regulatory obligations to know their customers and understand the payments going through their systems; Cumulative bank penalties for non-compliance amounted to an estimated \$321 billion in 2017.²

¹ Source: United Nations Office on Drugs and Crime (UNODC)

² Source: BCG

The rise of the mule

Part of the reason for the rise and success of money launderers and mule networks is the speed at which modern payment systems enable money to be received and sent on, and the sheer volume of transactions.

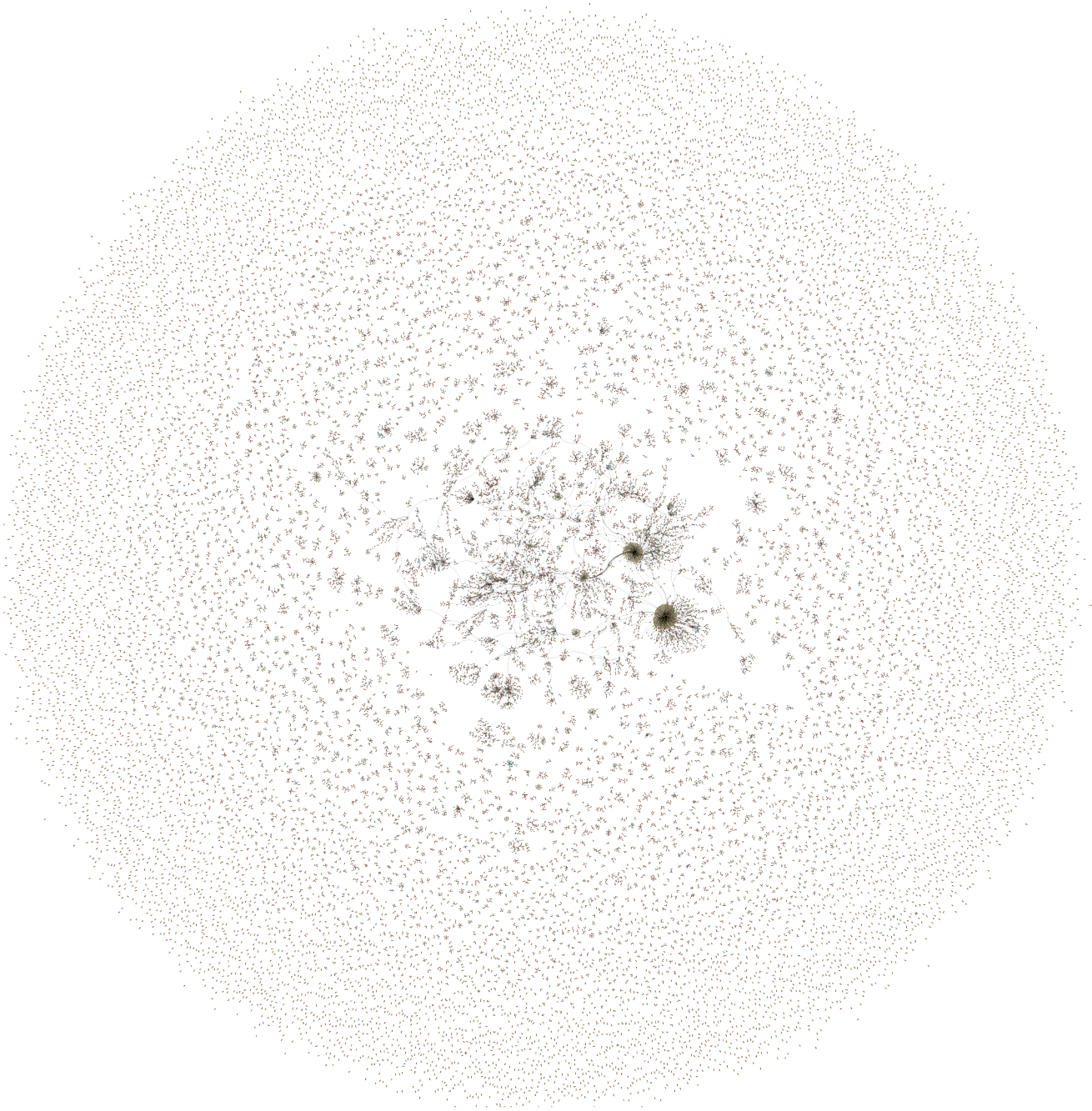
People and businesses benefit from the speed and convenience of transferring money 24/7; unfortunately, criminals are also quick to leverage the benefits of real-time payments to fund their activities and launder money.

The scale of the problem

Criminals will always look for the path of least resistance when operating, and modern payments systems offer them the ability to exploit speed to their advantage. The further away money moves from the victim's account, the harder it is to trace. Money now moves through payments systems faster than many existing technologies or manual anti-money laundering processes can identify and flag suspicious transactions.

Additionally, FIs currently only have a partial view of the scale of the problem. They are challenged in their ability to tackle the issue of money laundering because they don't have sight of a transaction once it leaves their four walls. What's more, financial crimes can be highly organised. Certain criminals employ mule accounts that are held at multiple FIs and endeavour to make the movement of monies associated with financial crime as normal as possible by breaking sums down into smaller amounts and dispersing them across multiple accounts. In isolation the data that banks hold on their customer accounts only provide part of the picture.

We believe that the best way to combat the speed and inter-bank reach of the criminals involved in money mule activity is to look holistically at the system, rather than trying to operate only within a subset of the data. Each FI has a number of powerful tools which can identify and stop the proceeds of crime, however these tools are only as good as the data that they see and no single FI can see the entire end-to-end payments flow across the banking network. A holistic view of the entire end-to-end payments flow also enables insights to be learned and applied to a single bank as well as across a network.

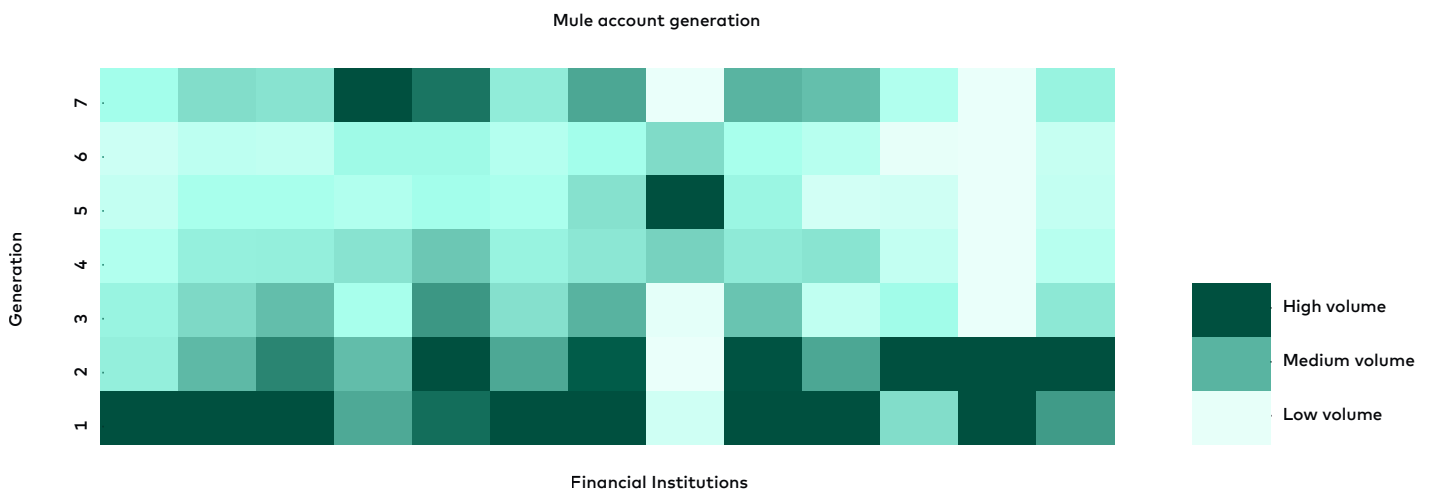


A graphic representation of all suspect money mule data from October 2018 to April 2019 inclusive. This clearly shows the central network of accounts, as previously evidenced in the original Proof of Concept and through further work. When zoomed in, the patterns and behaviours of the money laundering networks can clearly be seen.

A game-changing result

To tackle the problem of money laundering and mule networks, our team set about analysing a 'snap-shot' of payments data to identify, and trace suspected money mule activity across the UK payments infrastructure.

We undertook a proof of concept with 12 FIs and Financial Fraud Action UK (FFA UK) to prove the hypothesis that we could overlay payments data with cutting-edge analytical techniques to highlight the existence and scale of suspect mule accounts operating within the banking network and to map the movement of funds through the Faster Payments network.



Heatmap showing the distribution of suspect mule accounts through the stages of a mule network, against financial institutions in the UK

Starting hypothesis: our team could overlay payments data with cutting-edge analytical techniques to highlight the scale of mule accounts operating within the banking network and map the movement of stolen funds through the UK payments systems.

How we proved the hypothesis

We brought together two years' worth of Faster Payments transaction data in order to build a model of the UK's payments network, connecting nearly 100 million accounts across FIs and detailing over 357 million individual payment relationships. The 12 participating FIs represented the overwhelming majority of the UK interbank payments volume.³

The payments network is defined as a collection of bank accounts connected together by transactions that indicate a directed economic relationship between two accounts. For the purposes of this report, a money mule is a person who participates, sometimes unwittingly, in the transfer of illegally obtained money between different accounts. These proceeds of crime are transferred through a network in order to obscure their source, extract funds and make the recovery of stolen funds by FIs almost impossible.

The proof of concept had three agreed deliverables:

- Mule network visualisation: To provide graphical representations, insights and statistics of suspect money mule networks;
- Alert on mule accounts: to identify a proportion of suspect mule accounts within each participating FI's customer base not otherwise detected through the FI's existing mule detection strategies;
- Proceeds of crime path mapping: To trace funds from source through the payments network.

We created relationship-based views of the network by using our patented algorithm to build fund dispersion trees from confirmed frauds and scams – known as 'seed accounts' – to uncover accounts involved in money laundering activity– and plot their direct relationships with other accounts.

Through tracing funds across the banking network we built up a statistical understanding of how suspect money flows through it. It also allowed us to filter the entire UK payments network down to just those accounts and relationships that had been seen to demonstrate suspect mule behaviour.

³ We would like to take this opportunity to thank everyone – all twelve FIs, FFA UK (now UK Finance) and Faster Payments (now Pay.UK) – that took part in the proof of concept, and supported us throughout the process to help turn a hypothesis into reality.

Results and insights

A number of key insights were identified following the successful proof of concept and analysis of results:

- By volume, the majority of mule networks are short and linear; however, the presence of a large, highly-connected central mule network in the UK (composed of c.25% of all suspect mule accounts), was detected;
- Fraudsters have used accounts at all FIs to receive and send proceeds of a crime. Some FIs were targeted differently than others;
- Single fraud and money laundering cases can move through multiple FIs in incredibly short periods of time;
- A subset of FIs have mule accounts on their books that preferentially move money to/from one another, utilising existing, established relationships;
- Different behaviours in mule account activity have been observed within different FIs in terms of how deep within a mule network their accounts are used, and how illicit funds are extracted;
- Certain FIs tend to have a proportionately higher number of mule accounts which are involved either at the start point or towards the end of the chain in the dispersion of illegal funds;
- Controllers of a mule account move money into and out of accounts at different speeds depending on where in the mule chain an account is used;
- Seven major routes of extraction were identified as being the most common ways for criminals to extract illegal funds from the UK banking network;
- In some instances uncovered by our analysis, the pattern of the movement of illegal funds through the UK's payments systems is significantly different from that of legitimate money, which means suspect accounts behave fundamentally differently to 'normal' accounts and are therefore easy to identify; in other instances, the pattern of movement of illegal funds is designed to emulate the movement of legitimate money, which can make suspect accounts more difficult to identify
- The rate at which a mule account is re-used could represent how valuable it is to a criminal network, as well as indicating the impact of shutting down that particular account;
- The quicker a fraudulent transaction can be identified and traced, the more chances there are of identifying illegal funds and making possible its recovery.



Large connected suspect Mule network showing patterns of victims all sending to collector accounts either via intermediary mules or directly.

Live service: Tracing financial crime across the UK payment network

Vocalink, a Mastercard company, partnered with Pay.UK to develop a world-first, industry-level solution to detect and shut down criminal activity across the Faster Payments network. We announced the official launch of our capability to trace and alert financial crime – deployed under the name Mule Insights Tactical Solution (MITS) – in Q4 2018 after a successful pilot with scheme participants.

Our solution alerts financial institutions to suspect money laundering accounts within their portfolios, so they can act to avoid potential losses, fines and reputational risk. It does this by tracing suspicious payments as they move between bank and building society accounts regardless of whether the payment amount is split between multiple accounts, or those accounts belong to the same or different financial institutions.

It provides intelligence beyond an individual financial institution's partial view, enabling the industry to work together to shut down mule networks and disrupt fraud and money laundering, which amounts to millions of pounds annually.

"This new initiative is a significant milestone in the UK's fight against financial crime, giving the industry the potential to trace the flow of illicit funds on a greater scale and with more speed and accuracy than ever before.

"The effective introduction of [this solution] can help to tackle money-laundering practices head-on and further disrupt criminal activity... We believe this project can play an important role as one of the first stages in a cross-agency effort to disrupt the criminals who are responsible."

—Paul Horlock, Chief Executive of Pay.UK

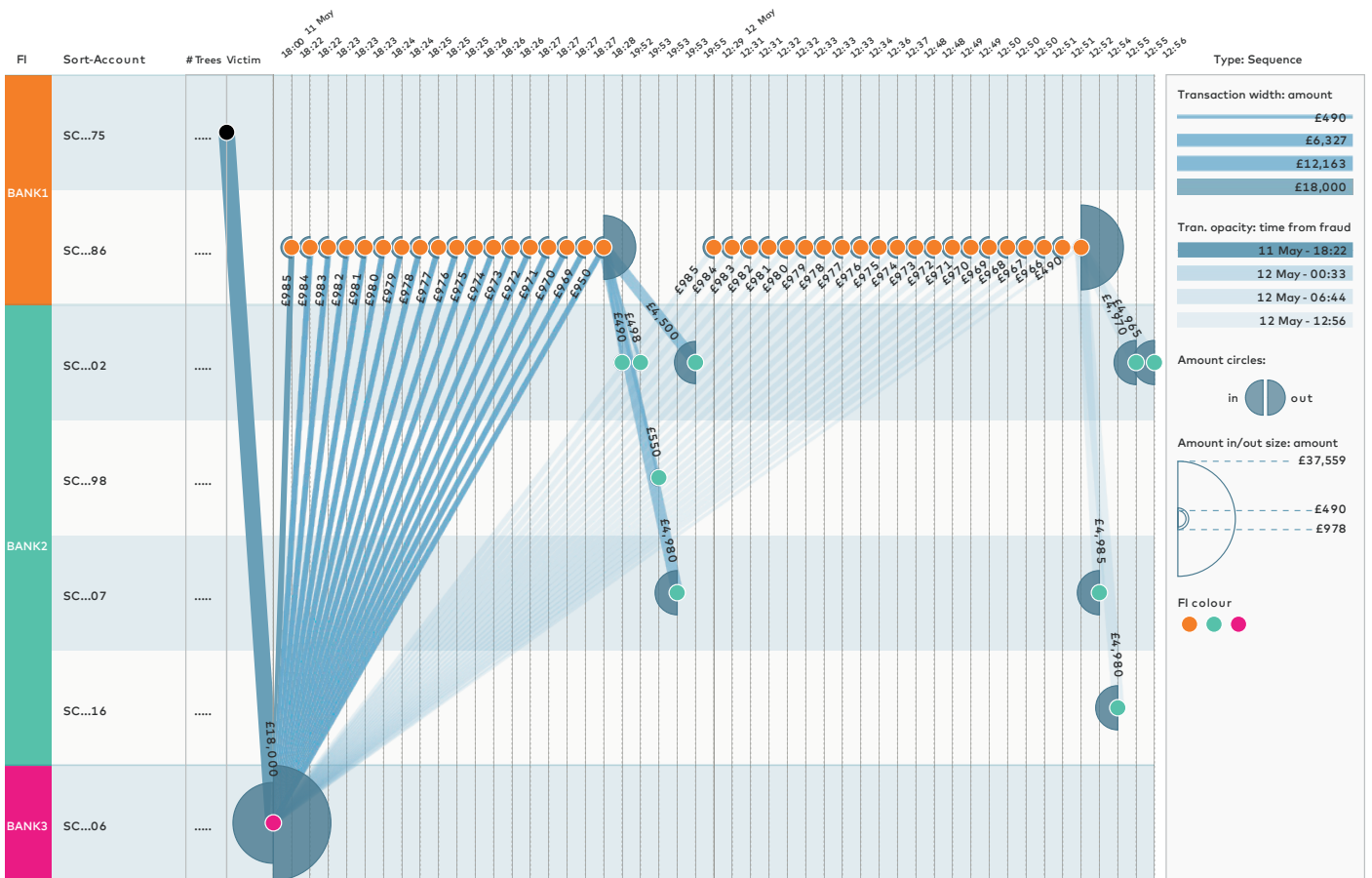
Within a few weeks of going live, the following results had been achieved:

- Thousands of UK accounts were subjected to further investigation due to suspicious activity – a notable percentage of which were subsequently identified as mules.
- Multiple, large, well-concealed money laundering rings were uncovered – where money was being moved between networks of accounts and institutions.
- Hundreds of mule accounts previously completely unknown to authorities were identified.

Our solution to trace and alert financial crime was recognised with the Rising Star Award for 2018 at the Corporate Entrepreneur Awards.

“The innovative data science behind our solution enables us to spot and trace and alert financial crime like never before. By coming together, connecting the dots and then identifying how the laundered money is split, layered and dispersed across the whole banking network... It showcases industry collaboration at its very best.”

—David Rich, Executive Vice President, Real-time Services



An example dispersion tree showing rapid dispersal of funds – likely an automated attack.

Our solution provides yet another barrier to fraudsters and is a further step towards the industry's wider goal of reimbursing victims of fraud who have had their money stolen. This marks a vital step forward for the industry in the fight against organised financial crime, as well as an opportunity to help reduce the impact of fraud on both FIs and their customers.

Case 1 Network of traced funds

After a bank received a notification from a customer that they were a victim of fraud, details of the fraudulent transaction were traced across the payment network. It was discovered that the account was a fourth-generation mule account within a complex network.

The account activity was typical of a mule: receiving a large volume of funds and rapidly paying them out. The majority of funds were being sent on to another account within the same bank, which upon investigation was also found to be receiving large volumes of funds and distributing them further.

As investigations progressed, a fraud ring of over **70 active accounts** was uncovered and shut down.

Case 2 The business account

Following an initial alert that raised suspicions regarding a business account it was blocked. However, the account holder did not make contact to find out why raising further suspicions. Upon profiling the account, the bank found an unusual number of credits from different sources that in no way matched expected account activity for the business.

Using our solution the bank checked where the account had been receiving the credits from and who else had been receiving or sending funds to these accounts, which revealed the business account was participating in a fraud ring.

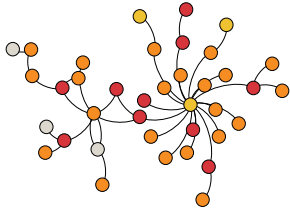
Investigations are ongoing, but so far **29 active suspect** accounts have been identified.

Case 3 Organised crime ring

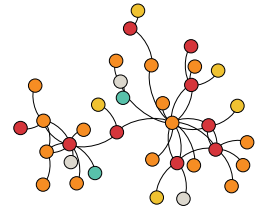
One account highlighted as a suspect mule by our solution was linked to a further **15 accounts** that appeared to be part of the same organised crime ring. There was evidence of payments being cycled between some of the accounts.

All accounts have now been blocked.

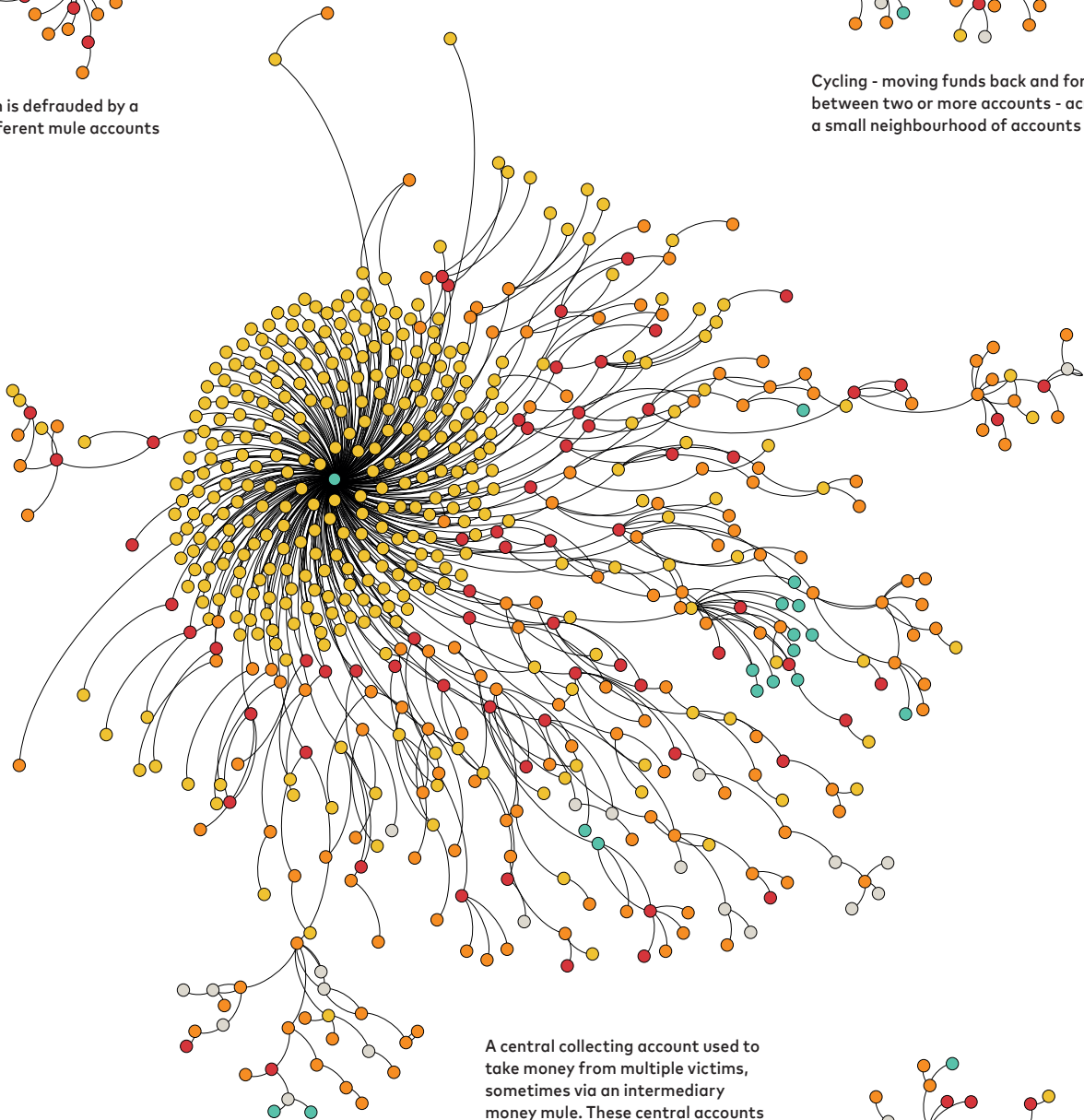
Images of the maps produced by MITS of these fraud networks are available on request.



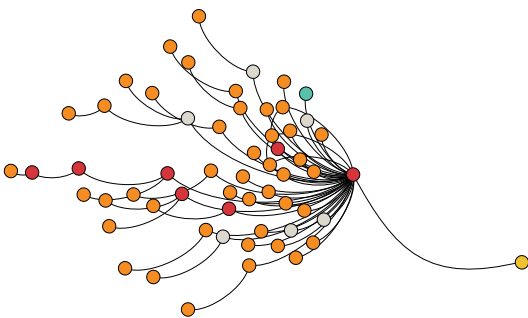
A single victim is defrauded by a number of different mule accounts



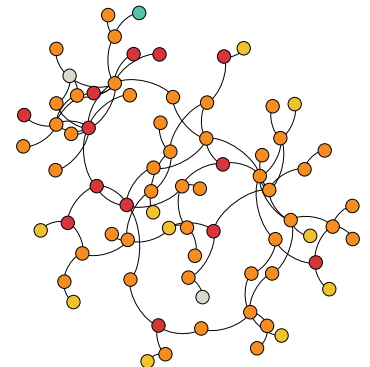
Cycling - moving funds back and forth between two or more accounts - across a small neighbourhood of accounts








A central collecting account used to take money from multiple victims, sometimes via an intermediary money mule. These central accounts are often money transfer services



A single victim loses money to a mule who sends funds out to a number of other accounts in their network



A neighbourhood with multiple cyclical connections spanning many suspect mules

-  legitimate
-  victim
-  suspected mule
-  confirmed mule
-  end point (algorithm can no longer trace)

Better outcomes for people, businesses and society

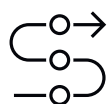
Our ability to trace and alert on financial crime is proven effective at detecting criminal activity across entire payment networks.

Using the consortium of intelligence gained throughout this work, our solution can now be engaged either at individual bank or scheme level anywhere in the world. It is quickly and effectively implemented with clear and proven advantages for FIs and schemes, enabling them to deliver benefits to their customer base and society as a whole. And, as money laundering is certainly not limited to domestic markets, we will begin to identify the corridors of illicit money movement cross-border as we deploy our financial crime platform globally.

Benefits for society



Investigate criminal networks: Our solution enables an FI to identify and flag accounts and entire networks involved in the theft and laundering of money to fund organised crime;



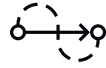
Assist in the repatriation of stolen funds: It can trace money through the payments system faster than was previously thought possible, identify where funds are resting in various accounts, give FIs the information they need to freeze these accounts. This gives FIs the information they need to freeze these accounts, and may enable them to repatriate and return funds to the victim;¹



Support the fight against organised crime: We enable the speedy closure of mule networks, and a fast and accurate way to monitor mule network, therefore giving criminals fewer avenues to use when attempting to steal money from the public.

¹ Vocalink have previously piloted a fund repatriation solution with industry partners, and through this work, they have developed an algorithm which could potentially repatriate funds in the future. Follow updates at vocalink.com

Clear and proven advantages for financial institutions



Significant resource efficiencies: Participating FIs have fed-back that our solution helps them realise key resource efficiencies, including:

- Ensuring scarce resources are focussed in the right areas;
- Improving detection rates;
- A faster speed of response, reducing consumer impact and dissuading criminals from targeting the participating institution.



Deep mule account detection: We deliver significant benefits to participating FIs by enabling them to reduce money laundering activity through the targeted closure of deep mule accounts.



Early warning of 'test' transactions: A proportion of analysed accounts showed a 'test' transaction had been made ahead of the main 'payload' of laundered money being moved into the account. The ability to pre-empt activity by alerting FI's to 'test' transactions improves their ability to:

- Hugely disrupt criminal activity at the very start of activities;
- Prevent fraud and money laundering from actually taking place;
- Save valuable time and resource through prevention of cases that may have occurred were the account to have remained open.



Identification of high risk 'endpoint' accounts: Analysing endpoints where funds exit a payment system enables the identification of suspect accounts which repeatedly receive funds connected with criminal activity. This close monitoring of customers transactions sent to known high risk endpoints enables:

- Greater prevention and recovery of funds exiting both the banking system and each participating institution;
- Fewer attempts at using participating institutions' accounts to extract funds;
- Disruption of criminal networks' "usual" methods of fund extraction.



Help to maintain regulatory compliance: We give FIs timely, fact-based insights that enable them to better understand the payments going through their systems.

Conclusion

Modern payment systems are being exploited rapidly to move the proceeds of crime between accounts, to a large degree thwarting the analysis and efforts by FIs to identify and trace illicit funds and create a path for repatriation.

Our proof of concept proved that money mule networks extend across the industry; they are not localised and affect all FIs. There is a fundamental difference in the behaviour of suspect mules compared with normal accounts and they move money rapidly through networks of accounts in order to hide the true origins of funds.

It also showed that overlaying payments data with cutting-edge analytical techniques makes it possible to quickly and efficiently identify patterns of mule dispersions both for an individual FI and across a payment network. And it shows our approach makes it possible to identify rogue, individual patterns of behaviour that – in isolation – are unremarkable, but seen together start to betray simple, consistent behaviours that are a strong indication of illegal financial activity.

Its findings have a number of implications for consideration by the financial services industry around the world:

- Confirmation that the extent of the money mule networks is not localised, but affects all FIs.
- Proof that working together to combat money mules is the best way to make a significant impact.
- That the efficacy of our solution will continue to improve with increased participation of FIs, and the addition of more sources of data over time.

Six months since launch of a live service with Pay.UK, our solution to trace financial crime has already achieved considerable results beyond the initial proof of concept, leading to the discovery of active mule accounts that were previously unknown to financial institutions and authorities. Our capabilities go far beyond what any individual in-house fraud or anti-money laundering tools can do in isolation and enable truly collaborative financial crime prevention, helping both individual banks as well as payment operators and schemes to further protect their customers.

Financial crime solutions

Our award-winning financial crime solutions help our customers better verify payment requests and recipients and prevent financial crime before it occurs. Our network-level solutions allow us to trace illicit funds across the payments network and alert financial institutions to suspect mule accounts so they can investigate and close them down. They can be engaged either at individual bank or scheme level, or across entire payment networks anywhere in the world.

For more information

vocalink.com/financialcrimesolutions
info@vocalink.com



Contact us

info@vocalink.com
vocalink.com

Head Office

1 Angel Lane
London
EC4R 3AB
United Kingdom