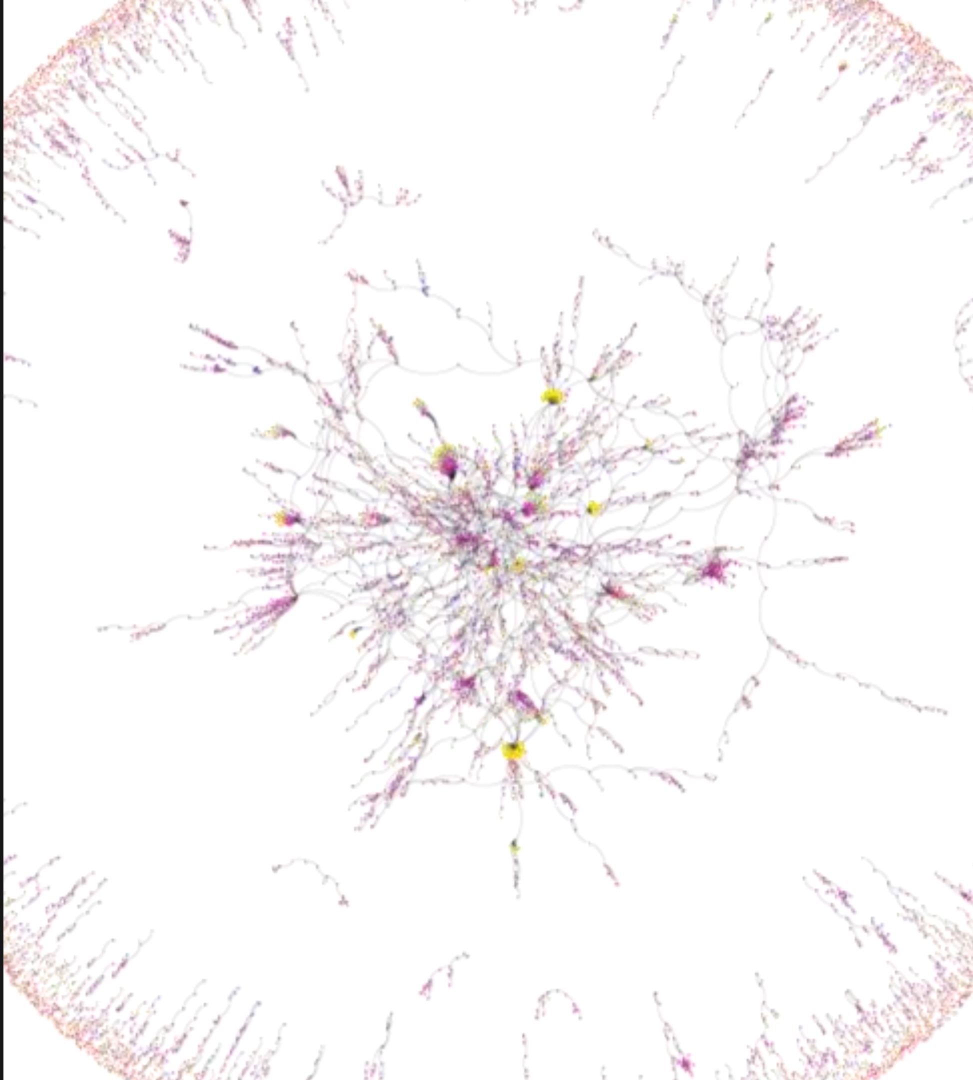
Uncovering Fraud and Financial Crime

Using AI and Machine Learning to Uncover Sophisticated Patterns of Fraud and Money Laundering

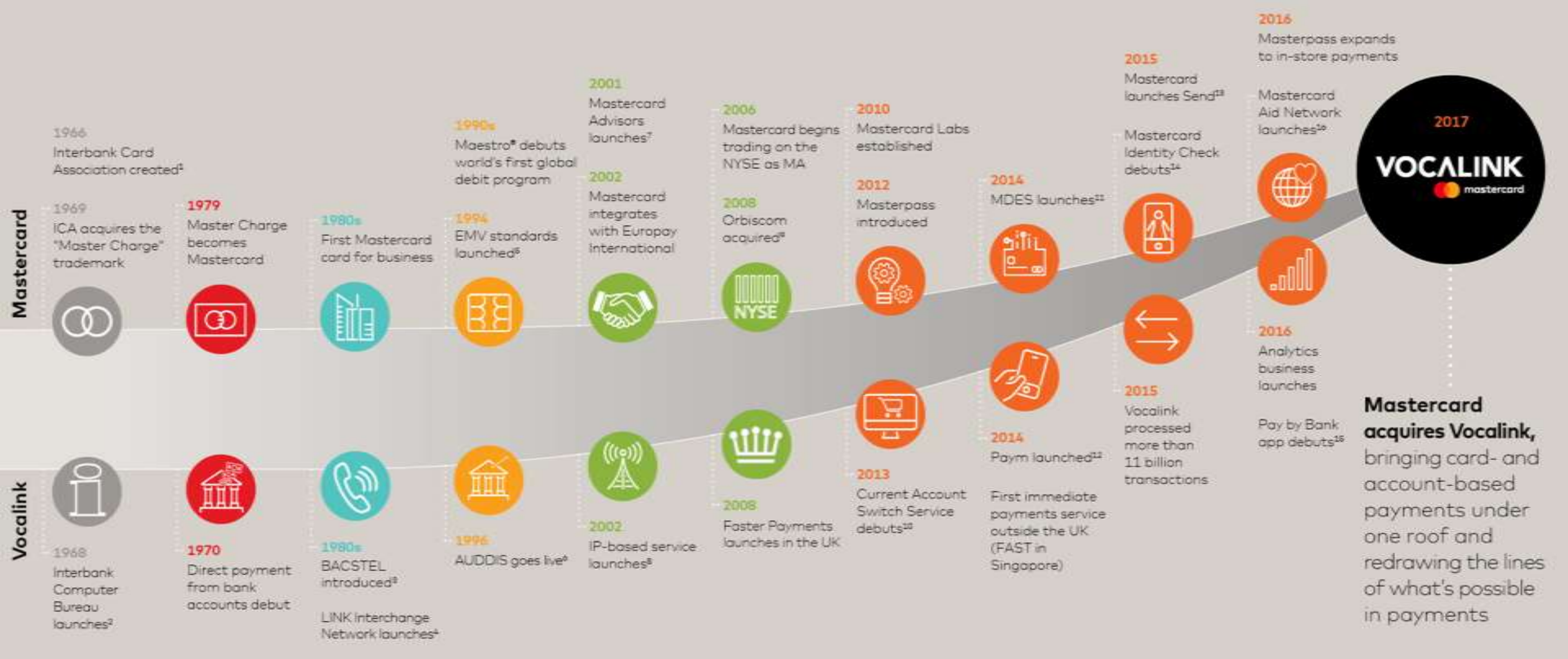
March 4th, 2020

Richard Luff
Director, Business Development

mastercard



Vocalink - Company history



Mastercard

1966
Interbank Card Association created[1]

1969
ICA acquires the "Master Charge" trademark

1979
Master Charge becomes Mastercard

1980s
First Mastercard card for business

1990s
Maestro® debuts world's first global debit program

1994
EMV standards launched[5]

2001
Mastercard Advisors launches[7]

2002
Mastercard integrates with Europay International

2006
Mastercard begins trading on the NYSE as MA

2008
Orbiscom acquired[9]

2010
Mastercard Labs established

2012
Masterpass introduced

2014
MDES launches[11]

2015
Mastercard launches Send[13]

Mastercard Identity Check debuts[14]

2016
Masterpass expands to in-store payments

Mastercard Aid Network launches[16]

Vocalink

1968
Interbank Computer Bureau launches[2]

1970
Direct payment from bank accounts debut

1980s
BACSTEL introduced[3]

LINK Interchange Network launches[4]

1996
AUDDIS goes live[6]

2002
IP-based service launches[8]

2008
Faster Payments launches in the UK

2013
Current Account Switch Service debuts[10]

2014
Paym launched[12]

First immediate payments service outside the UK (FAST in Singapore)

2015
Vocalink processed more than 11 billion transactions

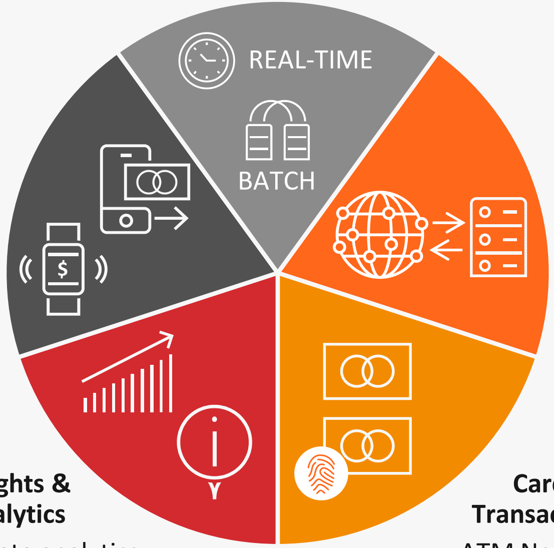
2016
Analytics business launches

Pay by Bank app debuts[15]

2017
VOCALINK mastercard

Mastercard acquires Vocalink, bringing card- and account-based payments under one roof and redrawing the lines of what's possible in payments

We’re at the heart of payments – both in the UK and worldwide



Payment Services
Account-based payments

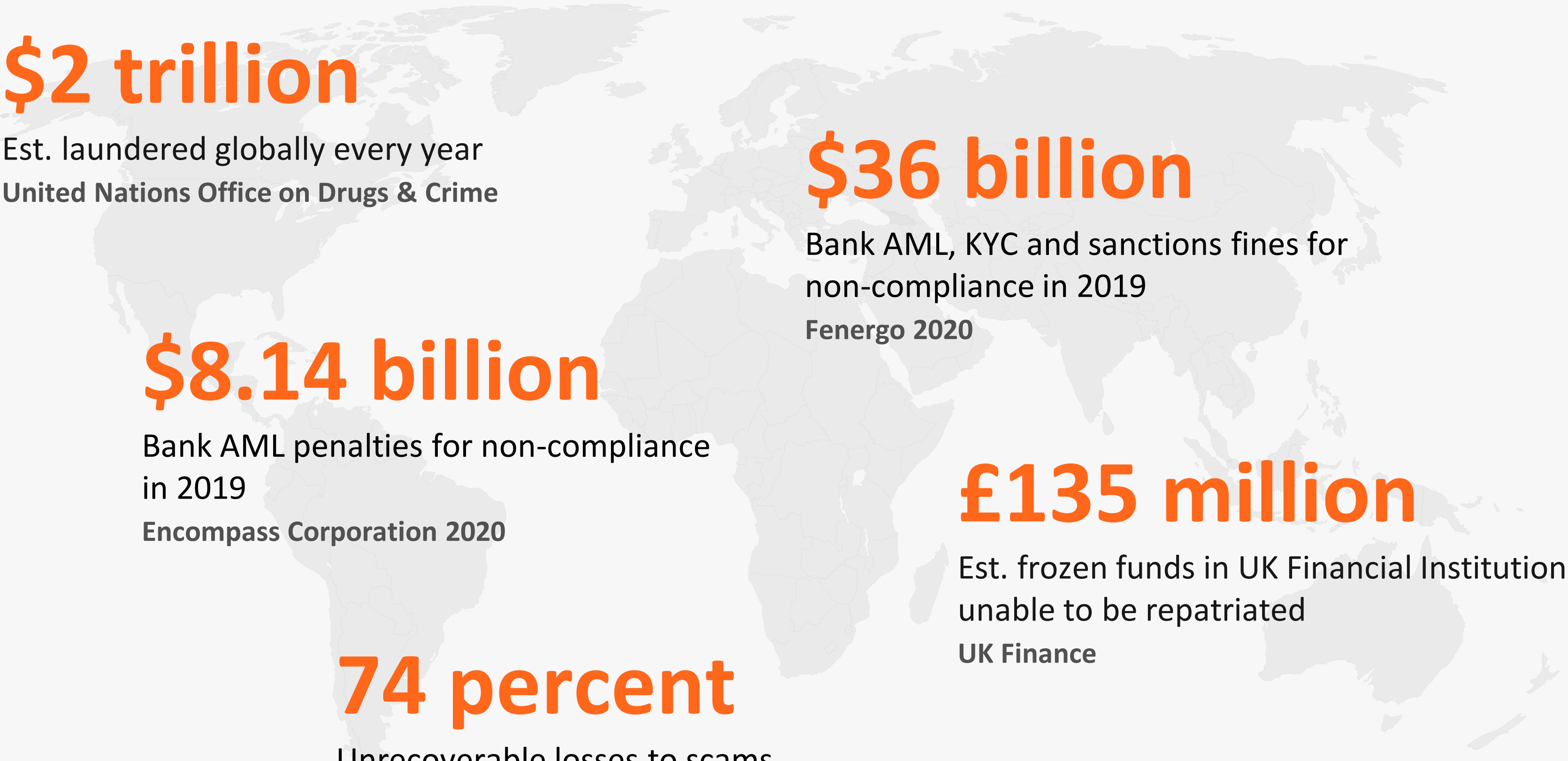
Alternative Payments
Zapp - Pay by bank account

Access
Gateway, routing and translation services

Insights & Analytics
Fraud & data analytics

Card Transaction
ATM Network

The current fraud and AML landscape | Pressure from all sides



$2 trillion

Est. laundered globally every year

United Nations Office on Drugs & Crime

$36 billion

Bank AML, KYC and sanctions fines for non-compliance in 2019

Fenergo 2020

$8.14 billion

Bank AML penalties for non-compliance in 2019

Encompass Corporation 2020

£135 million

Est. frozen funds in UK Financial Institutions unable to be repatriated

UK Finance

74 percent

Unrecoverable losses to scams

UK Finance

Scale of data to drive research

Machine learning algorithms and technology trained on significant volumes of payment and non-payment data

+20
BILLION
transactions, amounting to $trillions in value

+100
MILLION
unique accounts

+700
MILLION
money laundering data points

+375
MILLION
unique relationships

+100,000
money laundering motifs examined

+18
BILLION
business payments fraud data points

The fraud and AML challenge in account to account payments

With real-time payments comes real-time fraud

Fraudsters can steal and launder funds quicker than ever before

Fraudsters are getting smarter

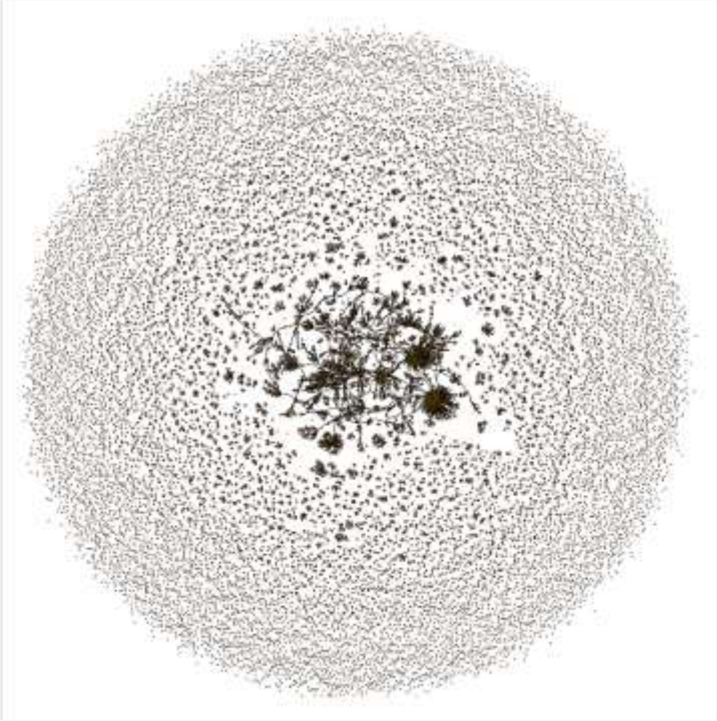
Increasing sophistication make financial crime harder to identify and harder to trace

Money is rarely recovered

The further stolen funds move away from the source, the harder they are to trace

Live - UK | Mule Insights Tactical Solution – Network Level Analytics

- The first network level solution of its kind - Globally
- Designed to provide additional intelligence to tackle fraud and money laundering to all participants involved
- Used to investigate known or suspect cases of money laundering, fraud or APP scams
- Assists in the tracing of dispersed illicit funds across the Faster Payments Scheme (FPS)



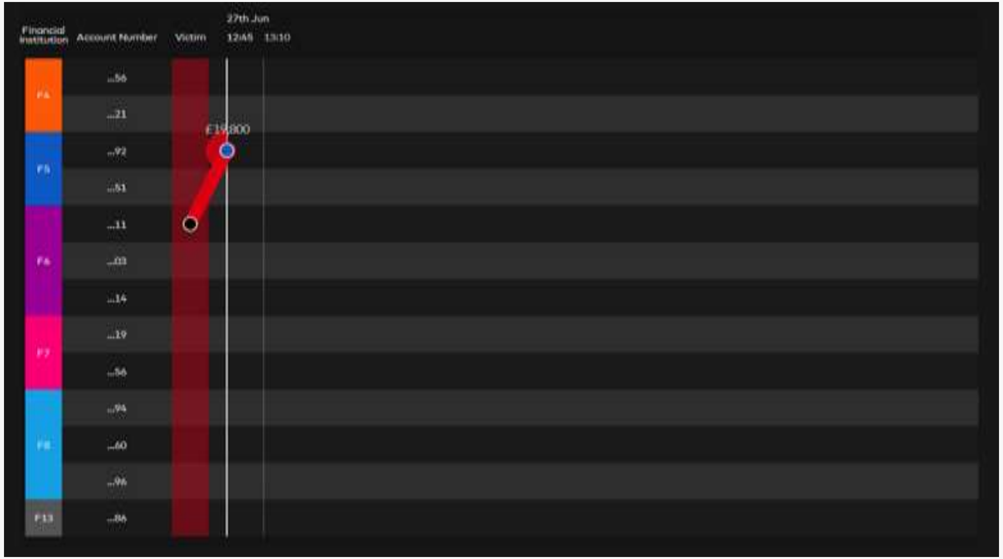
Real-time fraud & money laundering | The problem

Financial institution view

A bank’s view of money laundering is limited to the movement of illicit funds within its own accounts.

Once the funds leave the financial institution's accounts, it loses sight of them.

First movement of illicit funds



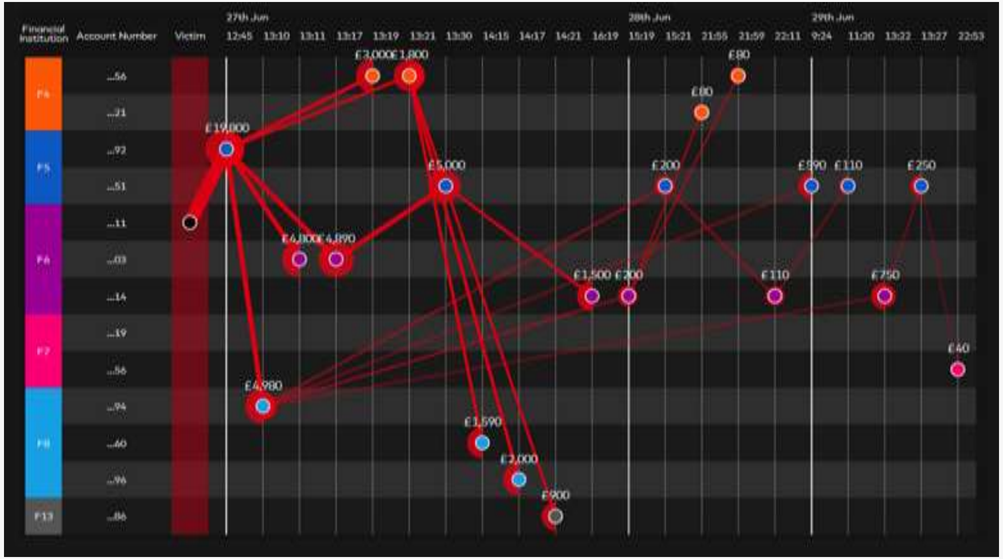
Real-time fraud & money laundering | The problem

Network view

Money launderers quickly move illicit funds between accounts across multiple financial institutions.

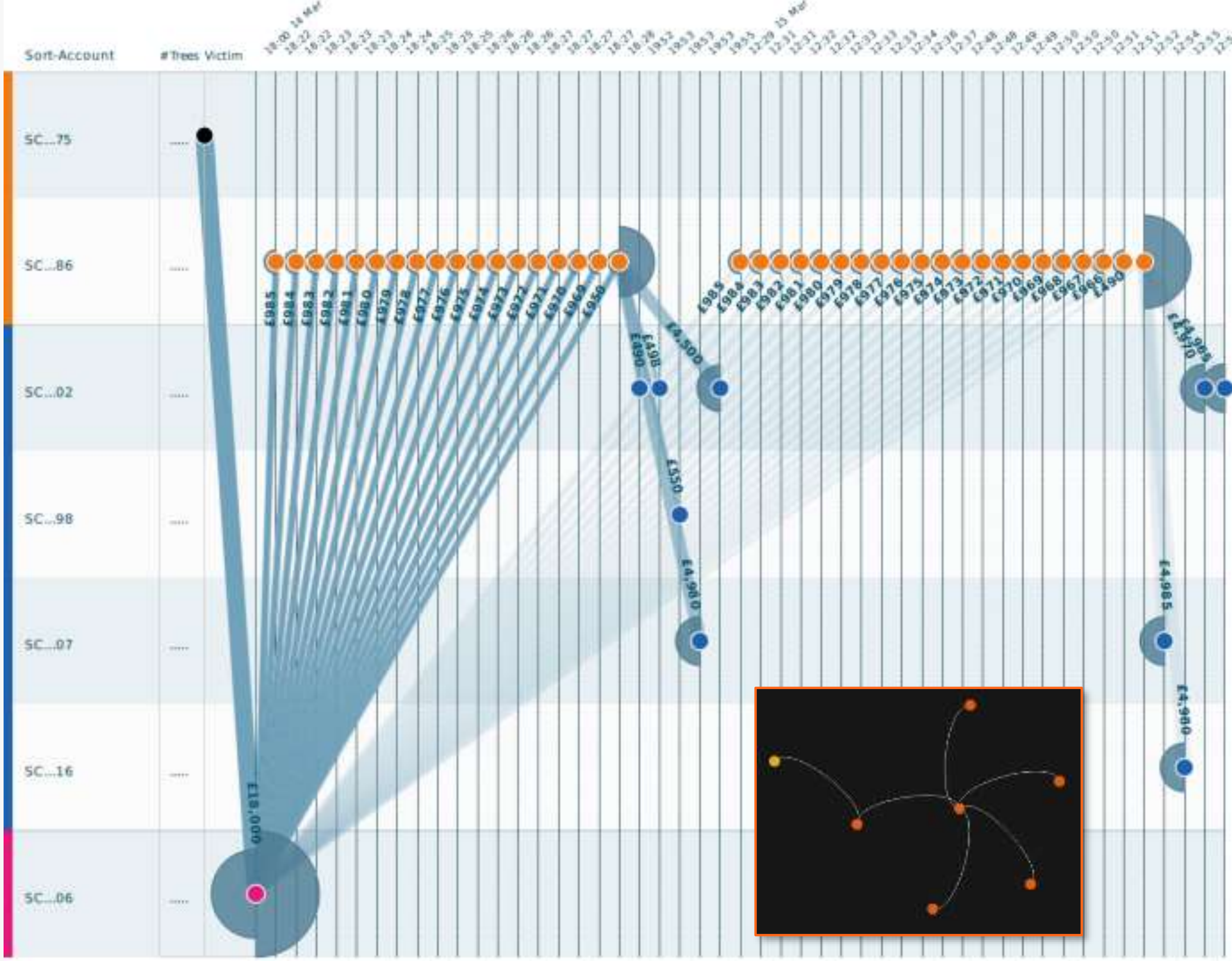
The further away they move, the lower the chance of tracing or repatriating illicit funds.

Subsequent movements of illicit funds



Rapid dispersal

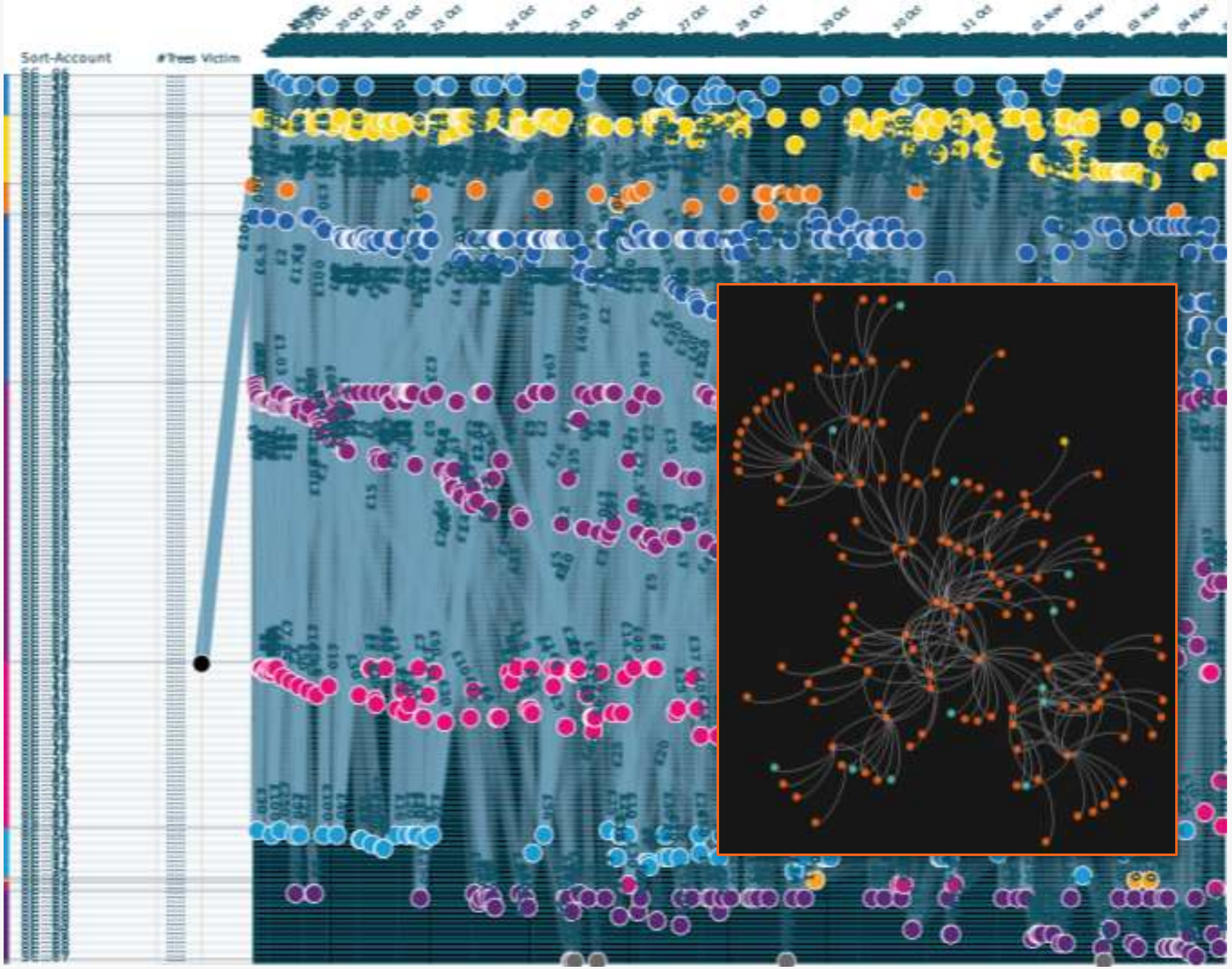
- Automated disbursement attack
- Rapid movement from 1st generation mule to other mules in order to hide funds
- Decreased payment amount by £1 every time



mastercard

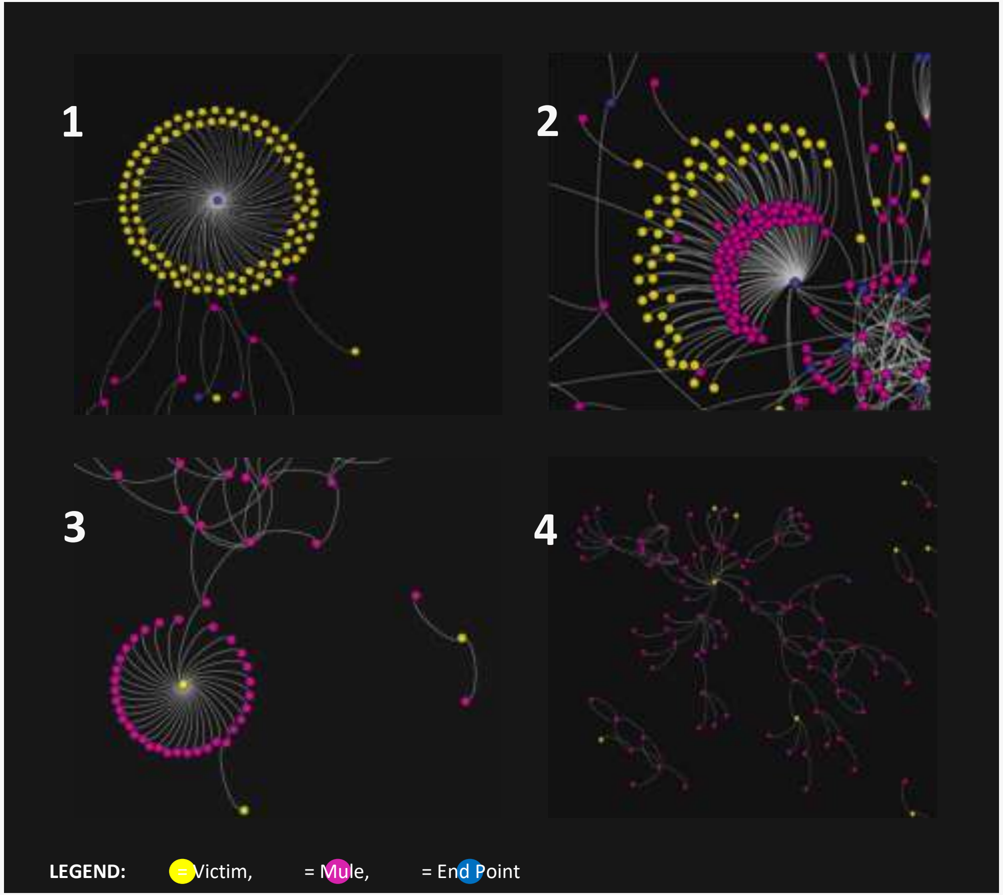
Extreme networks

- Extreme movement of funds
- Small amounts moved between hundreds of accounts
- Many references to raffles and lottery
- Deep network with over 70 generations and 200 accounts



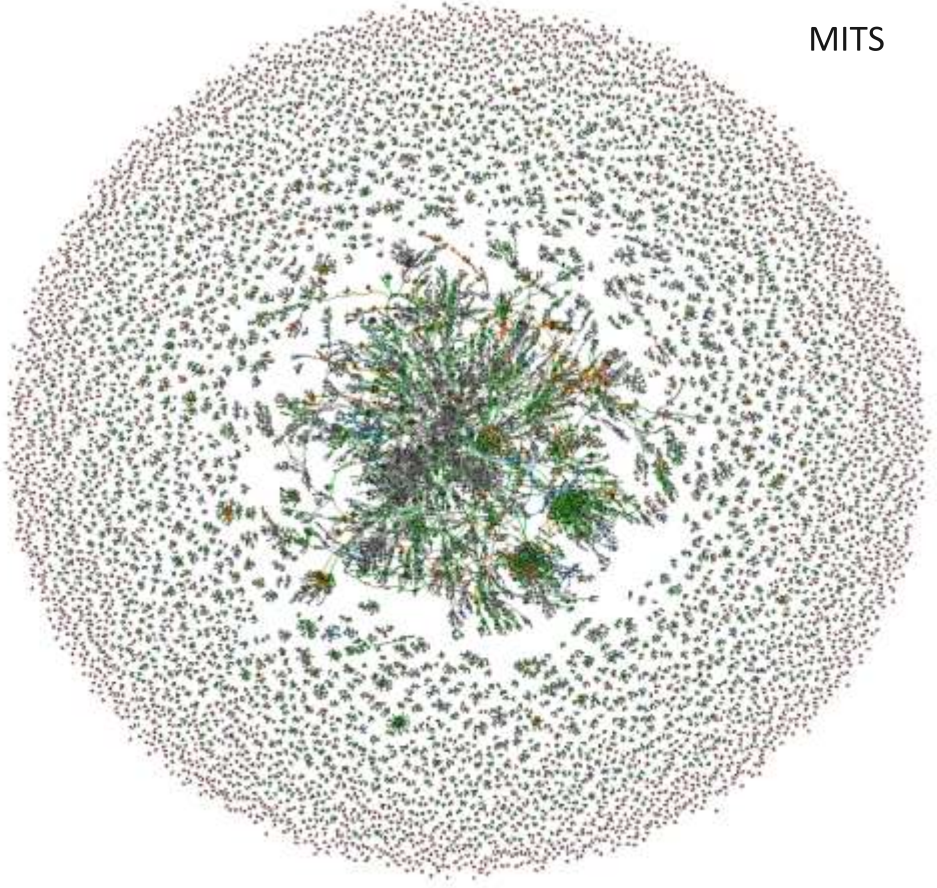
Patterns of exploitation

- A number of victims of a fraud or scam with one egress point, likely phishing or account takeover
- Typical flow from victims to multiple mules to one egress point
- One victim connected to multiple mule accounts
- Broader dispersion tree showing flow of laundering

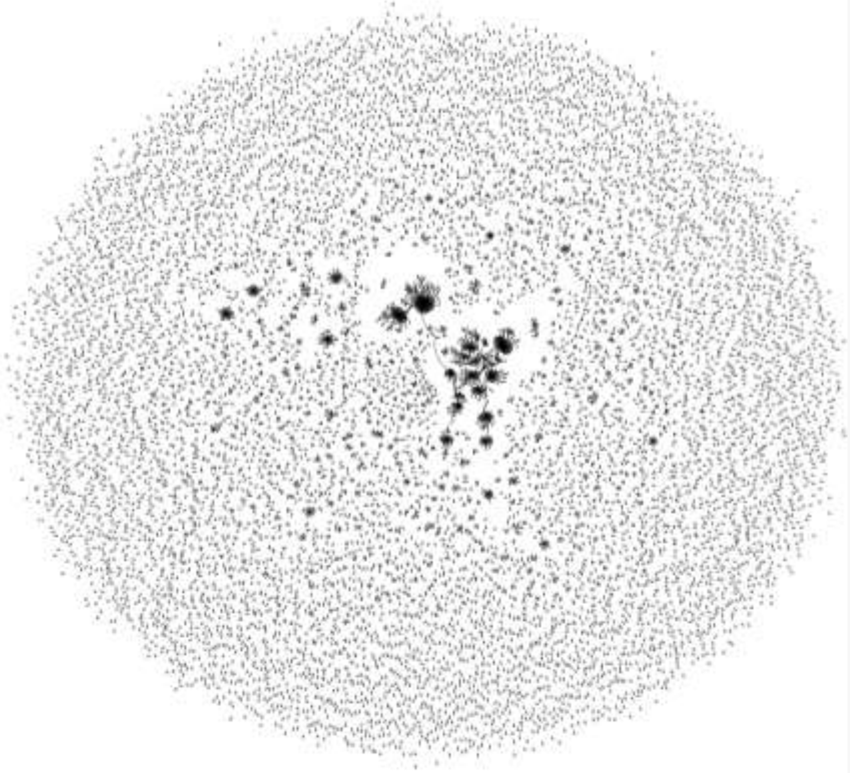


Trace and Alert (MITS) to date | Networks

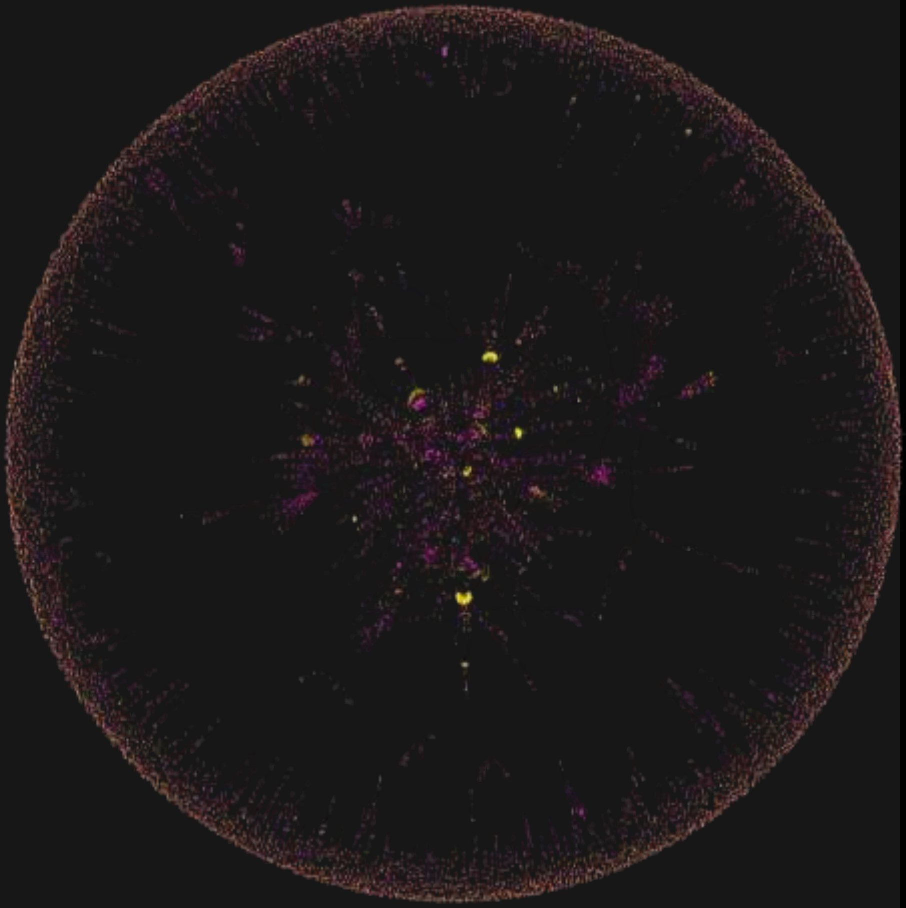
MITS

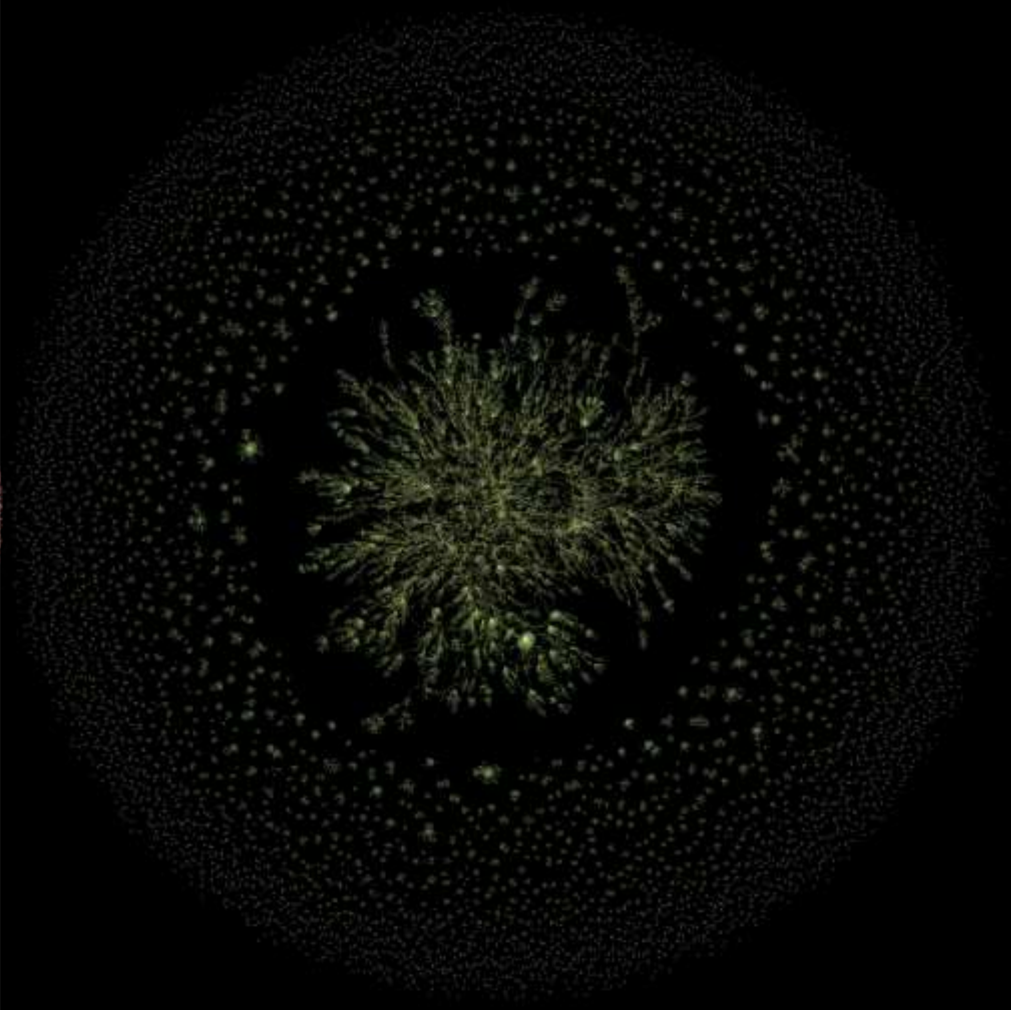


Random UK



Sophistication is on the rise





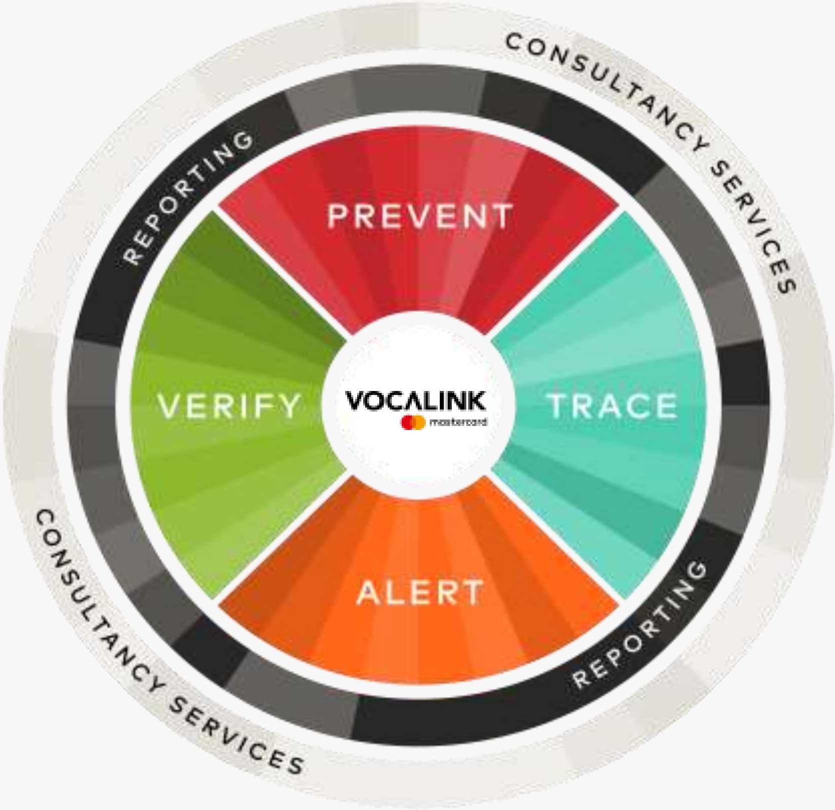
mastercard

New Initiatives

- New Participants
- Government (Use cases to support fraud reduction, ID and more)
- Law enforcement
- International The Clearing House (U.S) – Trace and Alert

Evolution - Prevent:

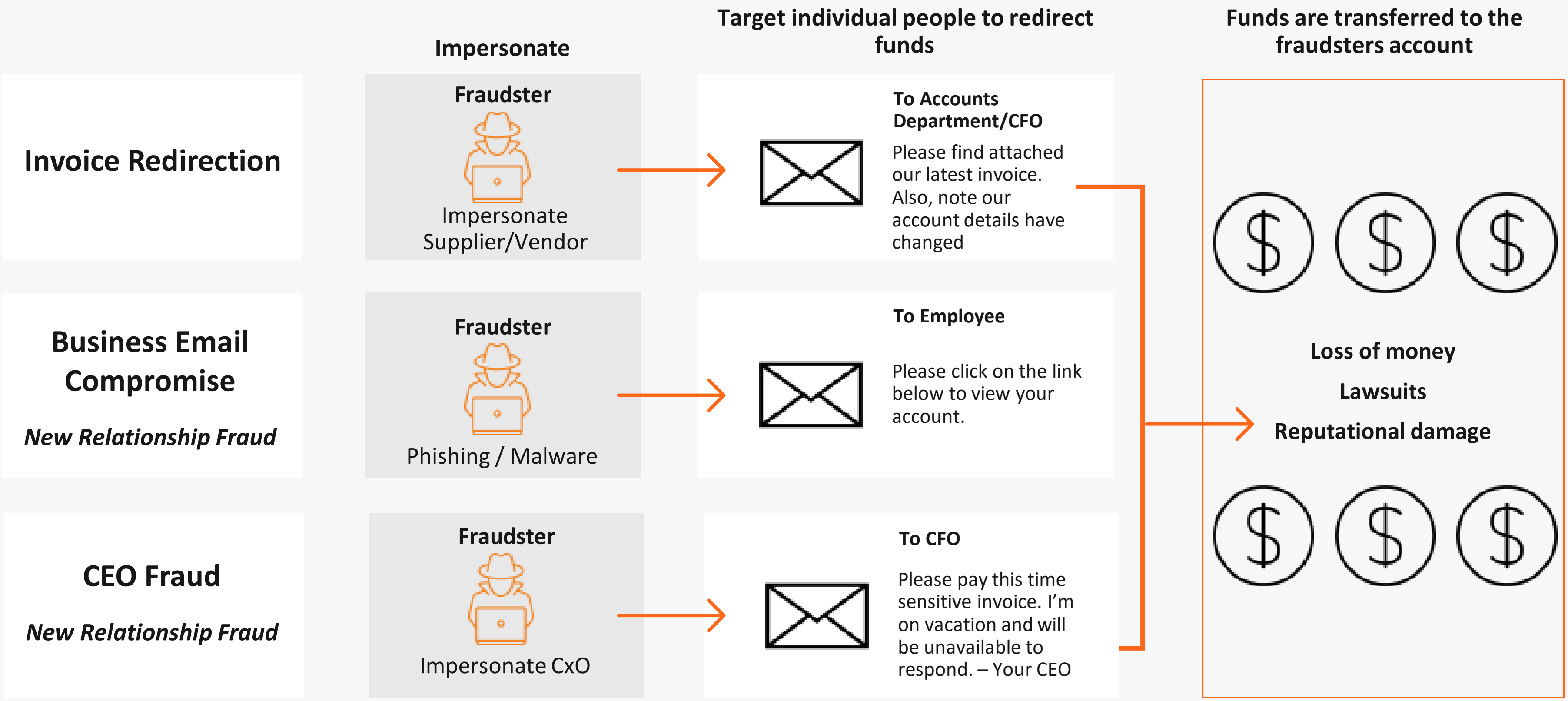
- CHAPS (BoE)
- Cheque
- Retail (Scams / APP)
- Enhancements to existing Prevent - Business solution



Prevent - Business Fraud

Protecting customers from payments-related fraud

Problem | Through social engineering and cyberattacks, fraudsters trick businesses into making payments into accounts they control



Impersonate

Target individual people to redirect funds

Funds are transferred to the fraudsters account

Invoice Redirection

Fraudster

Impersonate Supplier/Vendor

To Accounts Department/CFO

Please find attached our latest invoice. Also, note our account details have changed

Business Email Compromise

New Relationship Fraud

Fraudster

Phishing / Malware

To Employee

Please click on the link below to view your account.

CEO Fraud

New Relationship Fraud

Fraudster

Impersonate CxO

To CFO

Please pay this time sensitive invoice. I'm on vacation and will be unavailable to respond. – Your CEO

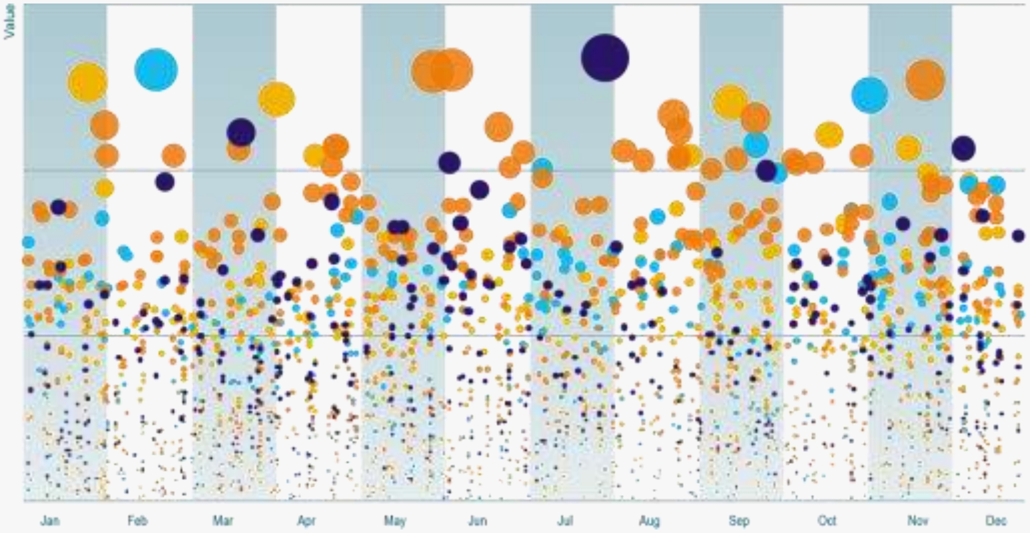
Loss of money

Lawsuits

Reputational damage

Targeting business payments fraud

- Risk for these types of fraud are distributed across time and amount
- Limited correlation between risk and size of payments
- Machine learning is the only tool capable of weeding out the frauds from the legitimate



$ 26B

Est. global CEO / BEC fraud losses
Oct 2013 to Jul 2019

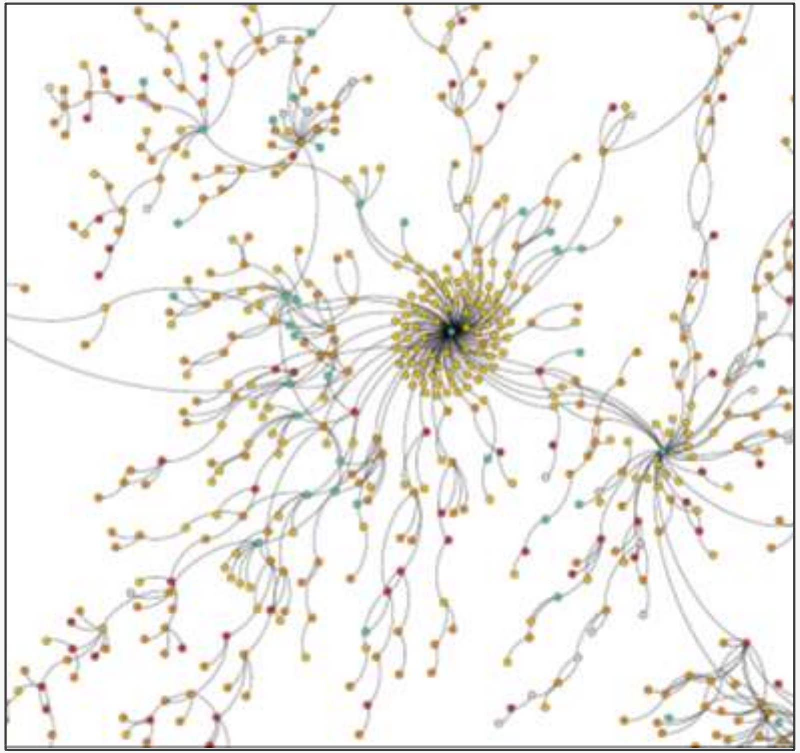
$ 158K

Av. amount lost per BEC/CEO incident
Oct 2013 to Jul 2019

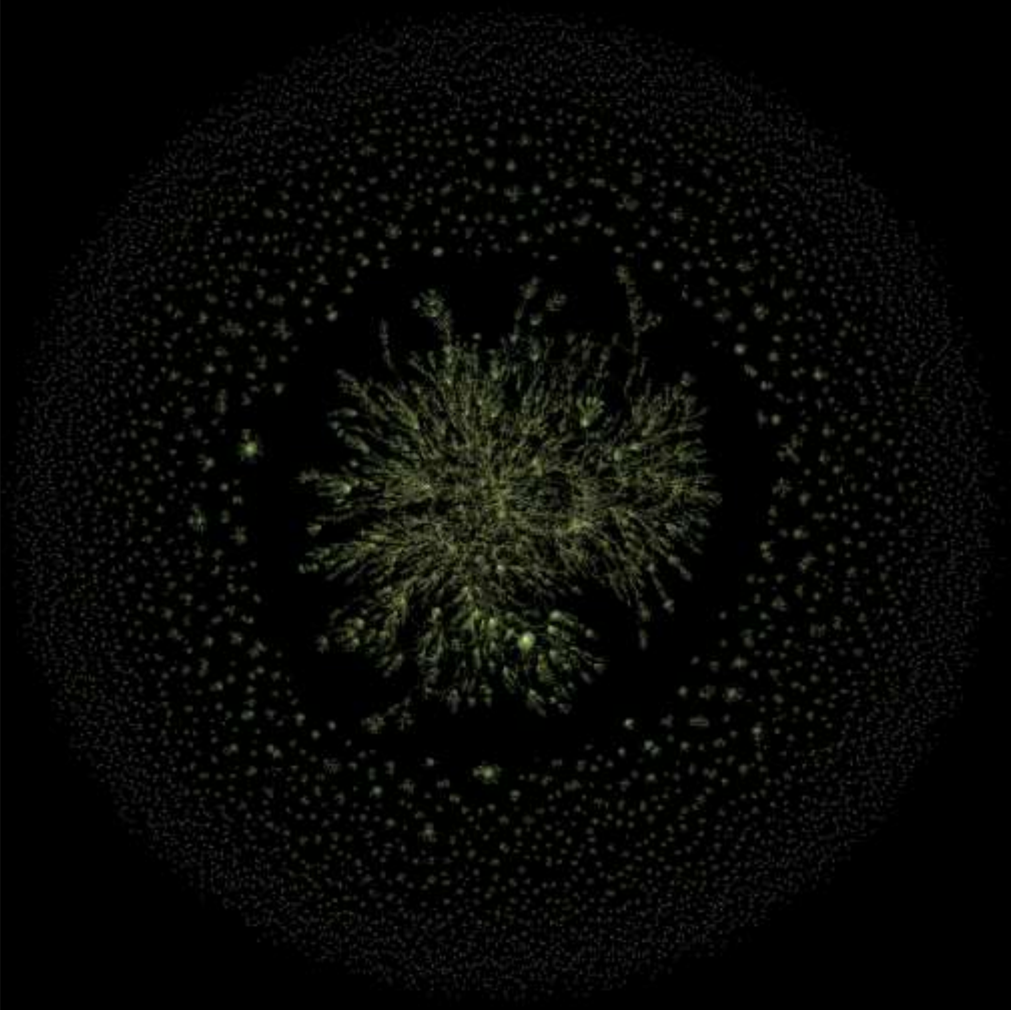
mastercard

Summary: AI techniques can be used to tackle multiple types of sophisticated criminal behaviour

- Trace and alert on financial crime across payment networks and geographies
- Prevent instances of fraud
- Has the potential to support numerous use cases in the public sector (subject to relevant permissions)
- Supports anti-bribery / corruption regulatory requirements
- Suffocate illicit funds which finance real life issues globally – e.g. human trafficking, drugs and terrorism



Thank you



mastercard