FS Club
News Events Partnerships

The Future Of Fraud – An Interactive Discussion

Professor Michael Mainelli & Simon Mills, Z/Yen Group

Webclave

Thursday, 10 March 2022, 16:00 – 16:55 GMT

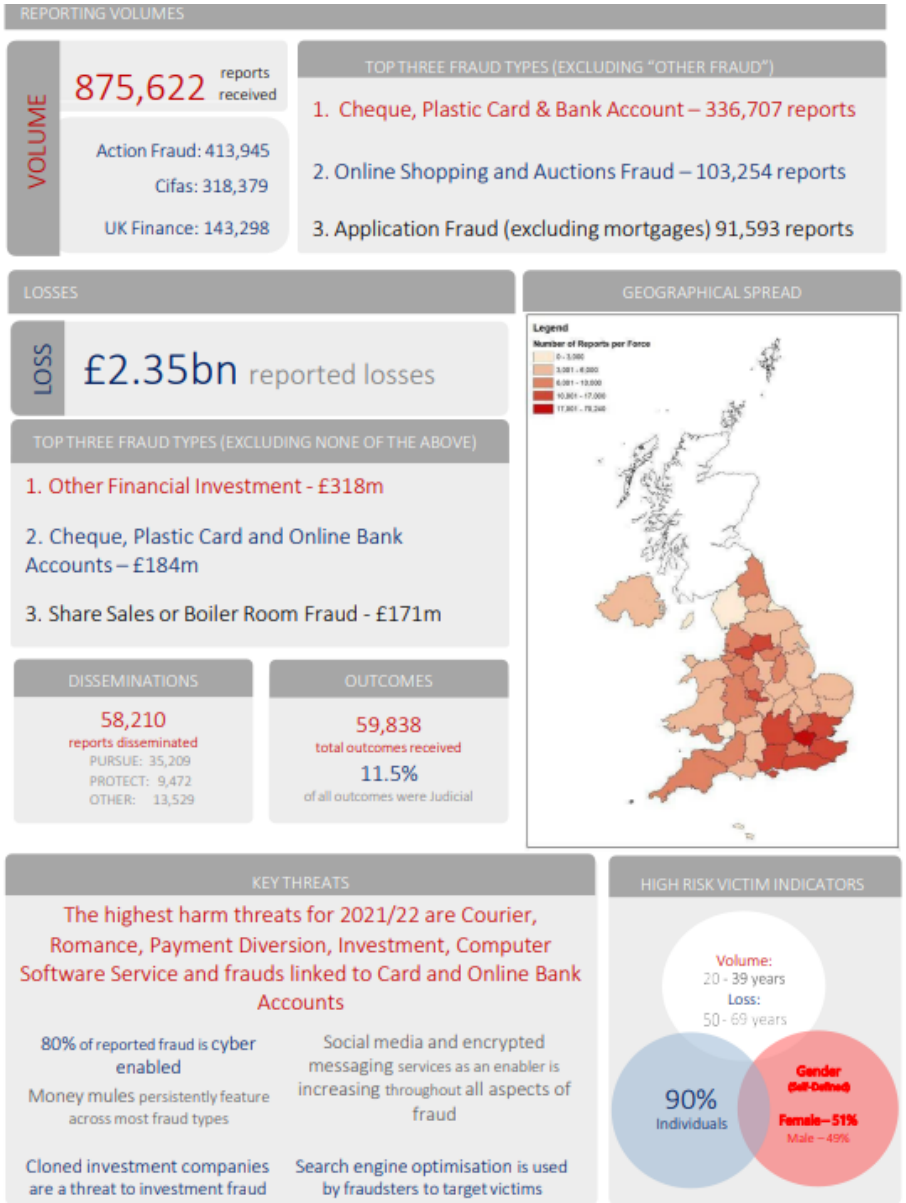
Welcome & introduction

Professor Michael Mainelli

Executive Chairman

Z/Yen Group

What Will The Fraud Landscape Of 2032 Look Like?



"Fraud has grown hugely in recent years and now accounts for 39% of all crime. Estimates from the Crime Survey for England and Wales (CSEW) showed there were 4.6 million fraud offences in the year ending March 2021. This compares to 3 million incidents of theft and 1.6 million incidents of violent crime. From March 2020 to March 2021, the volume of fraud incidents increased by almost a quarter (24%), in part due to a boom in Covid-related scams."

Victims Commissioner
13 October 2021

Today's Agenda - WEBCLAVE

- 16:00 – 16:05 Welcome & introduction: Michael Mainelli
- 16:05 – 16:15 Background to the research and some preliminary findings: Simon Mills
  - Trend analysis
  - Scenarios
  - Theoretical case studies
  - Systems theory applied
  - OODA brainstorming
  - Explorations
  - Challenge Themes
- 16:20 – 16:50 Audience input, discussion
- 16:50 – 16:55 Wrap up

Poll 1

How reliable are our fraud statistics?

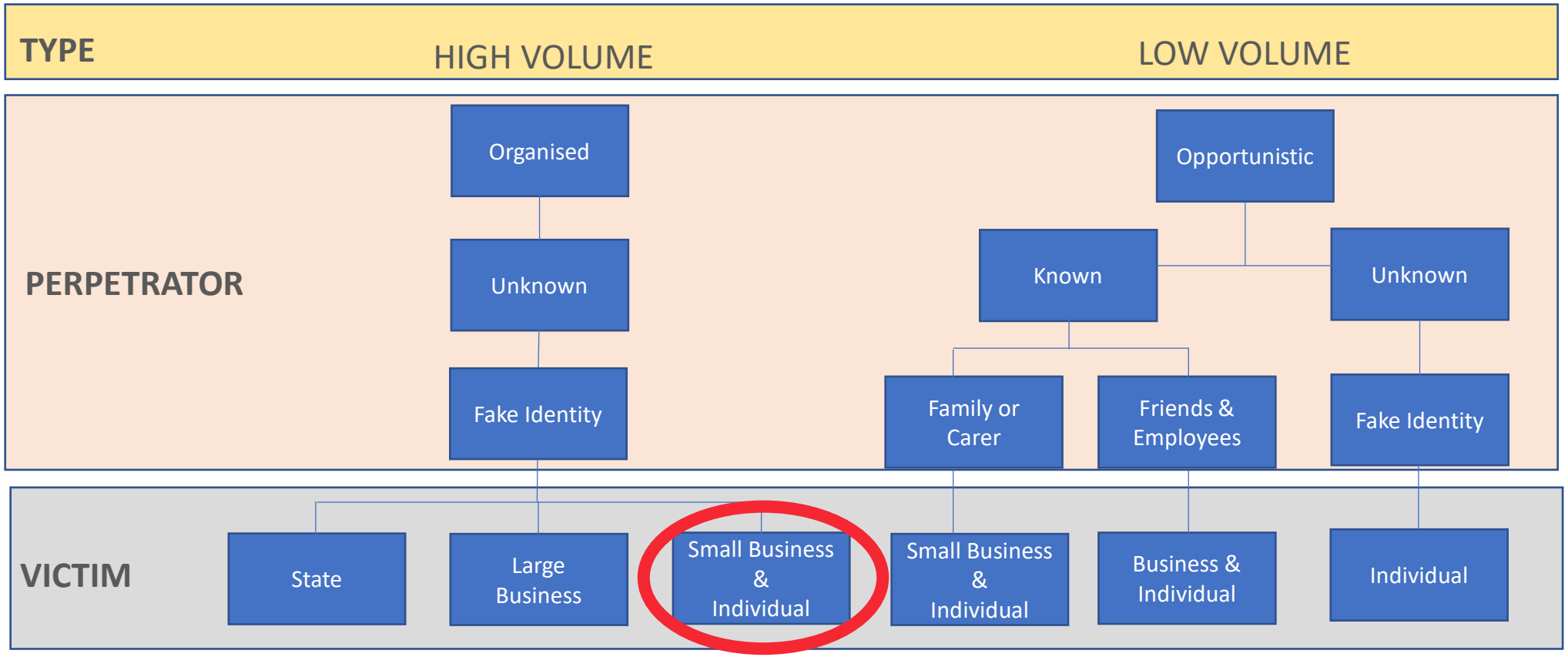
- Excellent
- Reliable enough for policy purposes
- Indicative of trends
- Useless
- Dangerous

Background & Preliminary Findings

Simon Mills
Senior Consultant
Z/Yen Group

Focus

Organised high volume fraud which targets individuals, sole traders, and small businesses



Types Of Fraud

- Card Not Present Fraud
- Confirmation Of Payee Fraud
- Account Takeover Fraud
- Romance Fraud
- Holiday And Ticket Scams
- Phishing, Vishing and Smishing
- Investment Scams
- Pension Scams
- Advance Fee And Lottery Scams
- Courier Scams
- Safe Account Scams
- Invoice Or Mandate Scams
- Property Scams
- Premium Rate Telephone Prize Scams
- Work At Home/Business Opportunity Scams

Trend Analysis

Societal

Trend	Impact	Likelihood
Ageing Population	High	High
Inequality	High	Medium
Increase In Economic, Conflict And Environmental Induced Migration	Medium	High
Pressure On Social Care And Public Services	High	High
Pandemics	High	Low
Increasing Social Fragmentation And Tribalism	High	Medium
Increase In Environmental Disruption	Medium	High

Technical

Trend	Impact	Likelihood
Industrialisation Of Fraud	High	High
Advances In Quantum Computing	Medium	High
Advances In Technology And Interactions Between Technology And Society (AI, IoT, Metaverse etc)	High	High
Growing Digital Footprints	High	High
Ageing Security Systems	High	High

Economic

Trend	Impact	Likelihood
Inflation In Cost Of Basic Goods And Services	High	High
Global Recession	Medium	Medium
Continued Migration Of Retail Online	Medium	High
Disruption To Employment, Redundancy Of Certain Skills And Business Models	High	Medium
A Cashless Society	Low	High

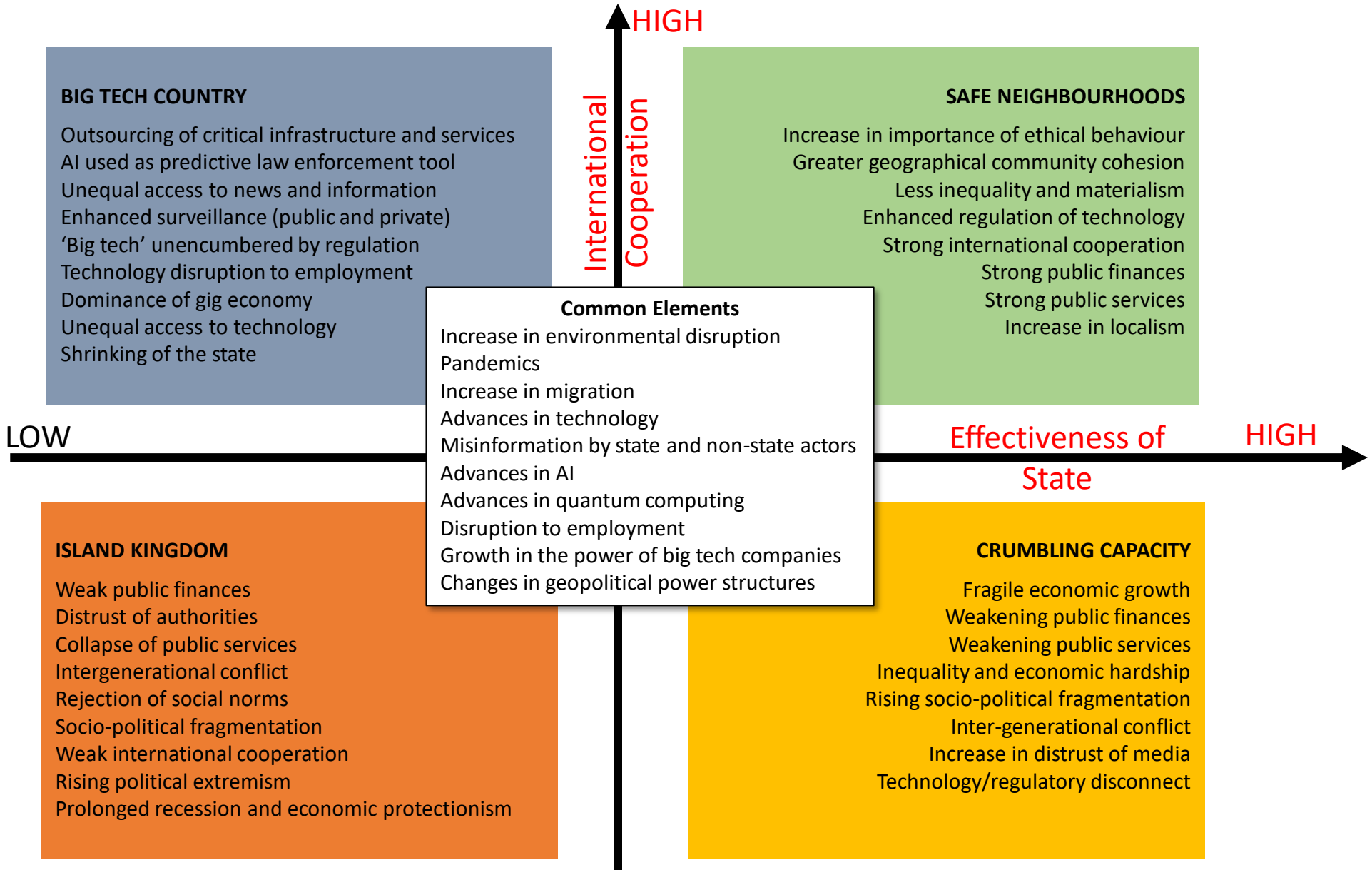
Political

Trend	Impact	Likelihood
Reduction In International Cooperation	High	Low
Increased Volume Of Misinformation By State And Non-State Actors	Medium	High
Growth In The Power And Influence Of Big Tech Companies	Medium	High
Divergence Between International Laws And Standards	Medium	High

Sound Out – Well Type Out…

Missing Trends, Important Trends To You?

Scenarios – Dator and Risk/Reward Typology Approaches



Poll 2

Which scenario best reflects your view of where we are headed?

- Big Tech Country
- Island Kingdom
- Safe Neighbourhoods
- Crumbling Capacity

Sound Out – Well Type Out…

Thoughts Or Observations On Scenarios?

Theoretical Case Study - Susan

Name:	**Susan Jones**
Age:	**68**
Details:	**Retired school teacher, widowed**
Location:	**Burnthome, Staffordshire**
Background:	**Susan is lonely and isolated. She met 'Martin' in a chatroom on a social media platform. 'Martin' says he is a retired engineer who lives in New Zealand. He is in fact the invention of a criminal gang located in Berlin, who are using the 'Martin' identity to defraud 18 women in 4 countries**

Attack Method: Romance Fraud: Martin and Susan have been corresponding for eight months. She has seen pictures of Martin's vineyard, and he has sent her a bottle of his wine. Martin has told Susan that he would like to come and visit her, but he is having difficulty buying the tickets because of New Zealand's strict anti-pandemic border controls. Could she buy them for him? He will pay her back. He sends her the website details for the transaction. The website is fake and designed to gain access to Susan's bank account.

Theoretical Case Studies – Differ By Scenario

SCENARIO 2: BIG TECH COUNTRY

- Susan has a new laptop computer but cannot afford a subscription to the latest AI enabled security software which would have alerted her to a potential fraud.
- Her only news sources are free feeds and she hasn't seen any articles about the recent surge in romance fraud.
- Susan's bank account is compromised and she loses £3,000 pounds. She reports the fraud, but her bank rejects liability.
- The outsourced national anti-fraud agency, which is a subsidiary of a large tech firm runs an AI engine which logs the potential fraud, and red flags the fake website. However, it is only contracted to collect, analyse, and pass on data, and there is no system to ensure the site is blocked.
- Europol is alerted and takes steps to close the fraud ring down, but although they make some local arrests, the website is hosted on a server in Honduras and they have limited success.
- As Susan doesn't have anti-fraud insurance as part of her household insurance, she has no means of paying for a recovery agent to get her money back. She is emailed a standard victim of fraud pack by Staffordshire Police.

SCENARIO 3: ISLAND KINGDOM

- Susan uses her phone to access the internet since her grandson stole her laptop.
- She has no malware detection capabilities installed.
- Susan's bank account is compromised and she loses £3,000 pounds. She reports the fraud, but her bank rejects liability.
- She contacts the local police, but they no longer deal with fraud.
- She searches online for advice on what to do if you are a victim of fraud and finds a website which offers help.
- The website is another fake and Susan loses more money.
- **Her personal details are shared on a social media stream mocking gullible old people and she receives hate mail.**

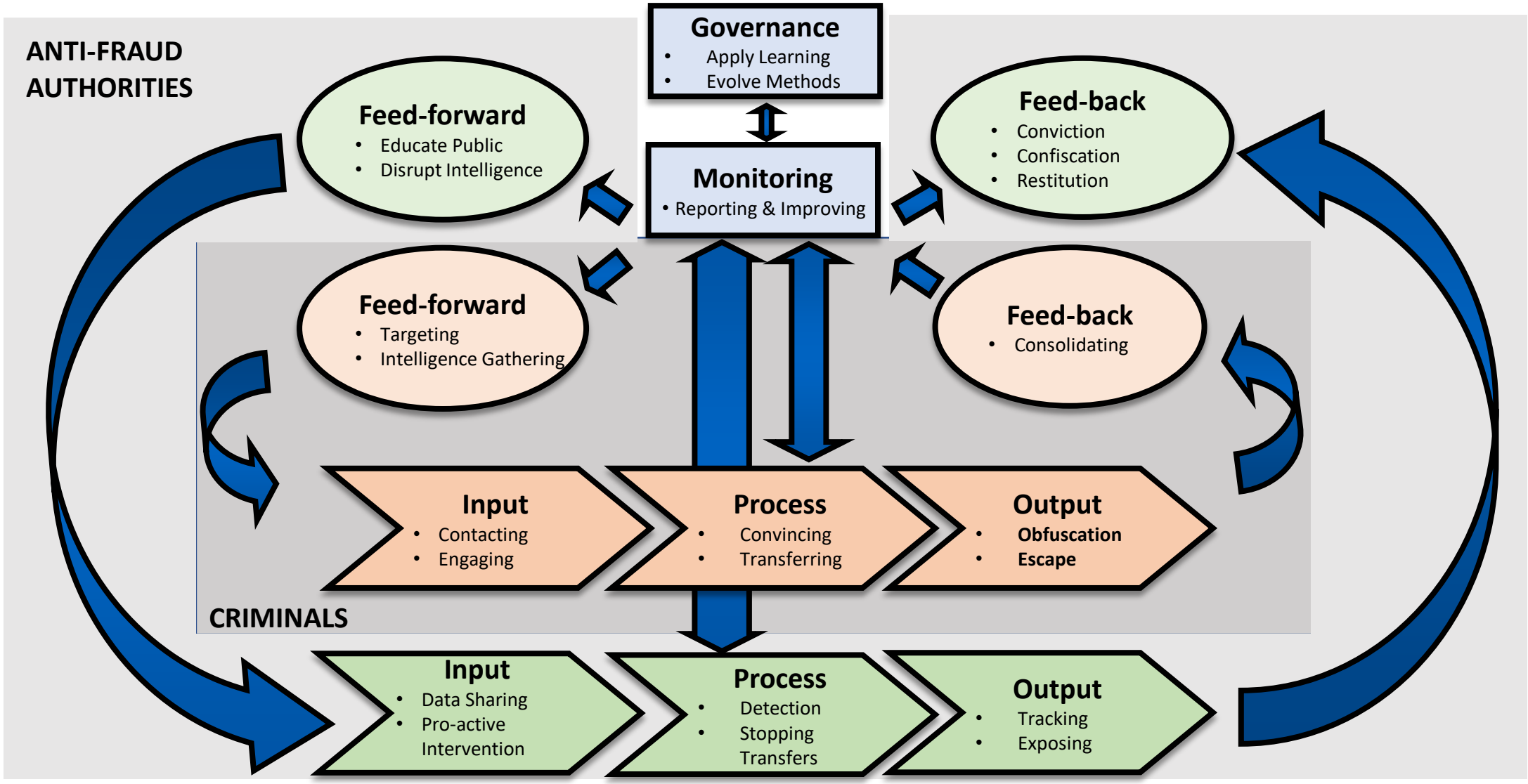
SCENARIO 4: SAFE NEIGHBOURHOODS

- Susan uses a desktop to access the internet. The desktop was recently refurbished by a local charity which helps retired people. The computer runs AI enabled security software.
- The software identifies the origin of the emails from 'Martin' and alerts her to the discrepancy. The software red flags the fake website.
- Her bank delays the transaction and alerts Susan to a possible fraud. The bank also alerts the NFIB and CIFAS who contact her local police force.
- A community support officer visits Susan and gives her information on how to spot and avoid fraud. A social worker visits Susan with information on local groups and activities she may want to join to help with her isolation.
- NFIB collates a report identifying the criminals and their methods which is sent to Europol.
- Europol identifies a pattern of fraud in other European countries and liaises with the police in Berlin who conduct an operation against the fraudsters, arresting them, seizing their equipment and freezing their bank accounts.
- **Details of all the financial institutions the fraudsters have had dealings with are published on an OSINT site.**

SCENARIO 1: CRUMBLING CAPACITY

- Susan uses an elderly laptop for accessing the internet and relies on free security software.
- She obtains her news from terrestrial television, and recently saw a documentary on fraud.
- Susan's bank account is compromised and she loses £3,000 pounds. She reports the fraud, but her bank refuses to accept any liability.
- She reports the crime to her local police force who alert the National Fraud Intelligence Bureau (NFIB).
- The NFIB log the report, but budget cuts mean the incident is given a low priority as the amount of money stolen does not meet the threshold for action and the criminals are based outside of the UK, which has recently ceased cooperation with Europol.
- A victim support officer is assigned to Susan, and they e-mail her a pamphlet on how to avoid fraud.

Systems Theory



OODA Applied

Observe
- Gather & record
- Share

Orient
- Analyse
- Test

Decide
- Categorise
- Value

Act
- Offensive
- Defensive
- Economic

Feedforward – Pre-bunking & Inoculation
Input – Detection & Blocking
Process – Interference & Trapping
Output – Prosecution & Recovery
Feedback – Sharing lessons
Monitoring – Reporting & Improving

Sound Out – Well Type Out…

Missing Possible Actions?

Explorations

Heighten authority trust levels
Reduce and control digital footprints on social media
Attack dark web marketplaces
White hat spear phishing attacks
Mandate data breach insurance so that breaches are fully dealt with
Record direct usage of government registers, e.g. electoral roll or Companies House for collecting information
Promote two-way identity proof as the norm for all transactions
Promotion of .uk style domains and registrations that tie organisations to government-validated registers, e.g. Companies House
Zero-tolerance for phone call non-identification, and abuse of mass marketing registries
Establishing a pay-to-read norm for mass emails, i.e. cost-based anti-spam systems, thus distinguishing legitimate contact from pure spam
Licensing large-scale emailers, with or without cost
Government identity 'infrastructure' system (not necessarily 'government identity cards')
'Nudging' two-factor and biometric authentication
Metaverse 'officers', human and AI
Mandate full compliance by payment providers with Confirmation of Payee
Implement a scaled cooling off period, e.g. 2 day minimum holding plus 1 day per £x,000 Timing and limit restrictions on overseas credit card usage
Create supra-national 'closing down' teams
Encourage more active use of transaction-by-transaction notification
Target finding large-scale activity hot spots in the UK, e.g. large scale emails, large quantities of suspicious processing
Slow banks down on multi-account transfers between institutions
Government and/or ISP automatic tagging, e.g. banners, of emails emanating from highly suspicious regions abroad
Encourage reporting of frauds
Provide timely and transparent reporting to victims
Providing private sector with OSInt tools such as inbound internet traffic analysis for the UK as a whole, or cryptocurrency tracing services to follow payment trails
Remove obstacles to private sector information sharing, particularly liability
Examine closely fiat-to-crypto and crypto-to-fiat conversion zones
Working with multi-lateral institutions, e.g. OECD, BIS, publish very regular, e.g. monthly, international fraud comparisons
Publish lists of financial services firms convicted fraudsters used
Publish lists of ISPs used by convicted fraudsters and the volumes of emails for use by mail servers to assess risk
Set standards for 'prediction' that the national anti-fraud community should be assessed upon, why can't we predict the likely amount of fraud in which categories for the following week?
Work with insurers on setting notification times beyond which fraud is not covered, in order to speed up reporting times
Daily publication of the national fraud situation, a fraud 'weather report', hot scams, recovery rates, recovery times, etc.
Consider support and encouragement for OSInt 'digital vigilantes' and/or 'bounty hunters'
Set up automated genetic-algorithm AI penetration testers
Create a market for the prosecution of fraud
Government timestamping services
Government documents issued electronically

Challenge Themes?

- Developing a trusted ‘no tolerance’ fraud culture
- Providing government supported identity ‘infrastructure’
- Concerted international cooperation
- Working with OSINT and social support services
- Working with global payments infrastructure to control access, timing, and flows
- Taking a ‘victim-oriented’ approach to processes, e.g. reporting speed and clear actions

Poll 3

Please rate the challenge that resonates most:

- Creating a zero-tolerance, victim-orientated fraud culture
- Providing government supported identity ‘infrastructure’
- Concerted international cooperation
- Working with OSINT and social support services
- Control access, timing, and flows in payment infrastructure

Sound Out – Well Type Out…

Missing Challenge Themes?

Comments, Questions & Answers (?)

Comments, Questions & Answers (?)

Thank You For Participating

Forthcoming Events

- **14 March**, 15:00 - 15:45 **Leading Beyond The Ego – It's What Future Stakeholders Will Expect**; John Knights
- **16 March**, 16:00 - 16:45 **Crypto Scams & What You Can Do About Them**; Sam Roberts
- **17 March**, 10:00 - 10:45 **A Shining Light On A Naughtie World**; Professor Bob Garratt

https://fsclub.zyen.com/events/forthcoming-events/

Watch past webinars https://www.youtube.com/zyengroup