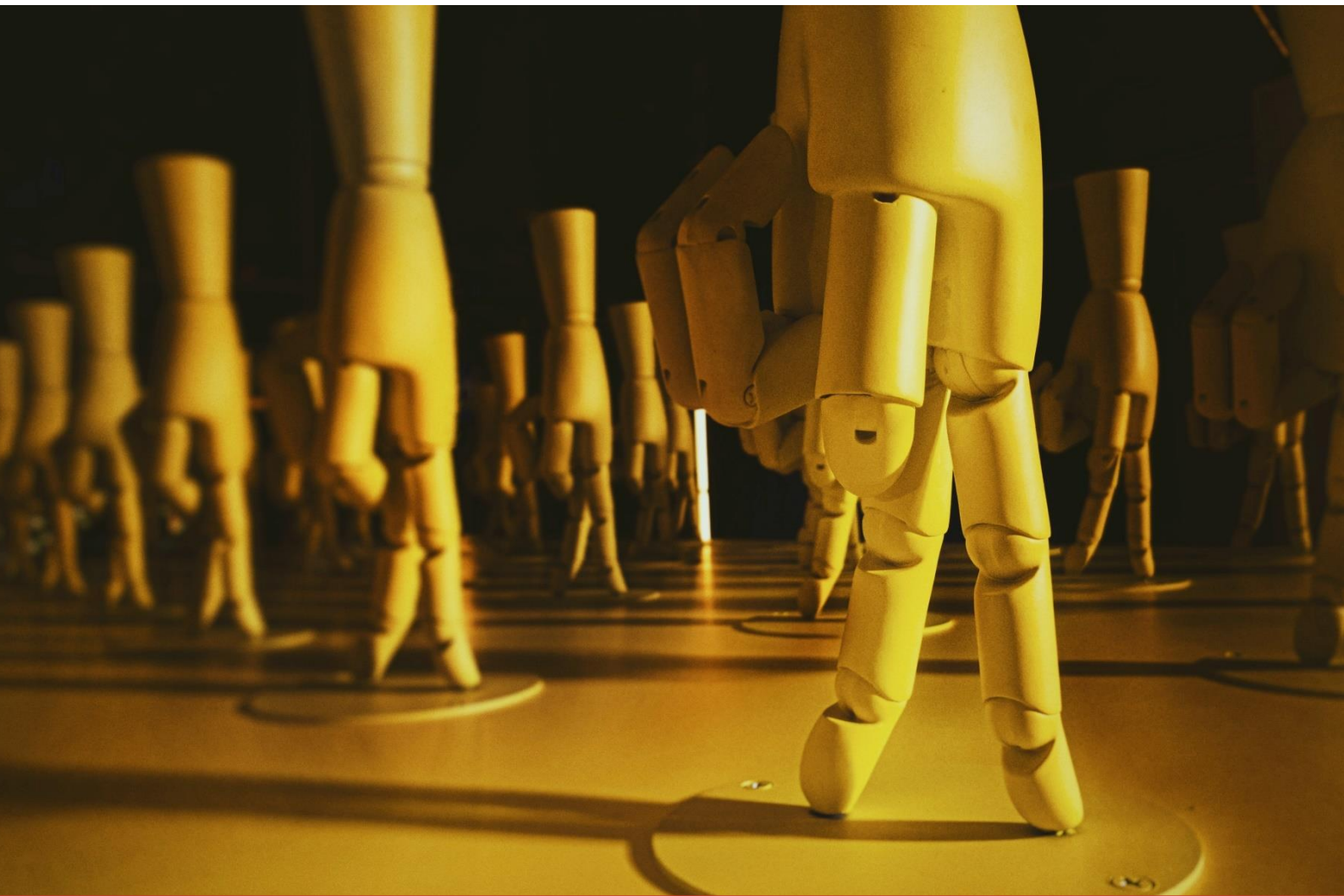


The Future Of UK Fraud

Challenging High-Volume, Automated Crime



The Future Of UK Fraud Challenging High-Volume, Automated Crime

June 2022

Principal Authors

Professor Michael Mainelli
Executive Chairman, Z/Yen Group

Simon Mills
Senior Associate, Z/Yen Group

www.zyen.com

© Z/Yen Group 2022

Executive Summary

This study focuses primarily on fraud as it affects individuals and consumers, i.e., large-scale, high-volume, automated fraud, where technology can make a difference. The time horizon is roughly a decade ahead. The output of this study provides four scenarios for readers taking a considered, forward-looking perspective on threats and opportunities.

The methodology included open-source desk research leading to the identification of a set of trends. Four scenarios were created and tested against the trends, against Dator's scenario classifications, and against Adams' risk/reward typologies. Five 'future narratives' were compiled and contrasted with the scenarios. The trends, scenarios and narratives were used to elicit feedback in a questionnaire and an online webclave. A viable systems approach was used to model two systems, the criminal system and the anti-fraud authority system, and then used to identify explorations for tackling fraud over the next ten years. These explorations, along with the scenarios, were used to set out a handful of 'challenge' themes as suggestions to guide the anti-fraud agenda over the next decade.

The four scenarios are:

- **Crumbling Capacity** – the United Kingdom (UK) and international environment grows increasingly fragile with increasing cross-border frictions that permit increasing fraud.
- **Island Kingdom** - social contracts between states and citizens have reached breaking points, and international relations have deteriorated so far that fraudsters operate cross-border with impunity.
- **Safe Neighbourhoods** – strong public agencies and strong local, ethical bonds combine with strong international cooperation to almost eliminate fraud.
- **Big Tech Country** - attempts to regulate big tech companies have failed but important 'customers' get the protection they 'deserve' from private providers.

The six challenge themes are:

- **Measure & Manage Fraud Systematically** - management tools - such as a clear chain of command, a clear network of support, a planning-implementation-evaluation management loop, and a fundamental re-engineering of people, processes, and organisation – should be applied consistently, at scale, in line with benefit-cost analysis.

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

- Automate Offensive & Defensive Tools For All Of Society – encourage data, information, and knowledge sharing, provide an open-source intelligence (OSINT) framework to help galvanise citizen action and support, citizens are empowered to easily notify and impede fraudsters, and anti-fraud authorities commission and use large-scale, automated systems for offence and defence.
- Nurture Global, Grassroots Coalitions - purposeful cooperation is sought with National NGOs and health authorities, international bodies, international payment providers, Big Tech firms, and high-fraud nations.
- Actively Provide A National Identity Infrastructure - incentivising the development of common identity systems infrastructure for use by the general public and by government in relations with citizens.
- Grow A Victim-Oriented, Zero-Tolerance, Anti-Fraud Culture - anti-fraud authorities treat victims as they themselves would wish to be treated, in a compassionate and open manner, the public actively involved in anti-fraud work with feedback on the progress of prosecution and recovery, and everyone jointly sharing knowledge and celebrating successes.
- Evaluate & Evolve – recognising that fraud evolves swiftly and thus counter-fraud needs to as well. Recognising that some low-level fraud may serve a purpose of inoculation is not incompatible with zero-tolerance.

'Fraud is good' only if it helps us to figure out what needs fixing, i.e., that we learn from it and strengthen our defences.

Contents

1. Why This Report?	6
Background	6
Objective & Scope	7
Methodology	8
2. Assessment Of The Fraud Landscape	10
Fraud In England & Wales	10
Categories of Fraud	11
Victims of Fraud	14
The Motivation Of Fraudsters	15
3. Trends Affecting Fraud	18
4. Four Scenarios For The Future Of Fraud	20
Scenario 1 - Crumbling Capacity	20
Scenario 2 - Island Kingdom	21
Scenario 3 - Safe Neighbourhoods	22
Scenario 4 - Big-Tech Country	22
Common Elements Between Scenarios	24
Testing For Reasonableness	26
5. Future Narratives	30
6. Viable Systems Analysis & Exploration Generation	41
7. Challenge Themes For The Next Decade (2023-2032)	52
1. Measure & Manage Fraud Systematically	52
2. Automate Offensive & Defensive Tools For All Of Society	52
3. Nurture Global, Grassroots Coalitions	53
4. Actively Provide A National Identity Infrastructure	54
5. Grow A Victim-Oriented, Zero-Tolerance, Anti-Fraud Culture	54
6. Evaluate & Evolve	55
APPENDIX 1 - Additional Sources	57
APPENDIX 2 - Trend Analysis	59
APPENDIX 3 – Synopsis Of Common Frauds	64
APPENDIX 4 – Questionnaire & Webclave Synopsis	67

1. Why This Report?

Background

Fraud is defined in the UK's 2006 Fraud Act as *“false representation, failure to disclose information when there is a legal duty to do so or abuse of position with the intention to make a gain (personal or for another); or cause a loss or the risk of a loss to the victim”*¹.

The information age has aided an explosion in the rates of fraud. Fraud takes many forms, transcending geographical boundaries and jurisdictions. According to the Victims' Commissioner,² 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)³ year ending September 2021, are that fraud makes up more than 40% of all crime. A non-exhaustive list of the types of fraud currently prevalent in the UK is contained in Appendix 3. Research by UK Finance⁴ indicated that whilst unauthorised financial fraud losses across payment cards and remote banking decreased by five percent compared to 2019, by contrast, the criminal use of social engineering to defraud members of the public has grown markedly.

Although fraud does not command the same media attention as violent crime, members of the public are more likely to be victims of fraud than assault. Counter-terrorism policing will receive funding of over £1 billion in 2022/23. Anti-fraud work receives less than a fifth of this amount. Fraud is a sub-set of economic crime, and also abetted by economic crime vehicles.

“Our spending for national agencies fighting economic crime is around £850 million per year, set against the money laundering cost to the UK

¹ CPS *The Fraud Act (2006)* <https://www.cps.gov.uk/legal-guidance/fraud-act-2006>

² Victims' Commissioner 2021 *Who suffers fraud? Understanding the fraud victim landscape* <https://s3-eu-west-2.amazonaws.com/victcomm2-prod-storage-119w3o4kq2z48/uploads/2021/10/VC-Who-Suffers-Fraud-Report.pdf>

³ ONS 2022 *Crime in England and Wales: year ending September 2021* <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021>

⁴ UK Finance 2021 *Fraud The Facts 2021* <https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021>

economy of perhaps as high as £100 billion. No wonder conviction rates have been so low.”⁵

Lord Londesborough, House of Lords Debate, 9 March 2022

Yet the defence think-tank, Royal United Services Institute (RUSI), has identified fraud as a potential national security issue, which contributes to the funding of terrorist organisations, and may have the backing of rogue states.⁶

It is essential to remember that behind these dry figures are ruined lives, mental anguish, and erosion of the trust that allows society to function. Fraud is never a victimless crime.

“Transparency destroys secrecy: but it may not limit the deception and deliberate misinformation that undermine relations of trust. If we want to restore trust we need to reduce deception and lies, rather than secrecy”.

Onora O’Neill, 2002⁷

Z/Yen was commissioned to provide a swift survey of high-volume, automated crime, set out some scenarios to help guide thinking, and to provide some general recommendations for discussion.

Objective & Scope

This study is intended to challenge people to think about the basic behavioural contexts of fraud and move on to consider wider societal, technical, economic, and political aspects.

The study focuses primarily on the next decade of high-volume and large-scale fraud as it affects individuals and consumers, where technology can make a difference. The output of this study provides four scenarios against which the UK Government's emerging fraud strategy can be tested to ensure that it is forward-looking and takes account of anticipated threats and opportunities.

⁵ Lord Londesborough, Economic Crime (Transparency and Enforcement) Bill, House of Lords Debate, 9 March 2022 - [https://hansard.parliament.uk/Lords/2022-03-09/debates/70AD4617-20E7-4EF6-A69F-50EE4F3F1EF9/EconomicCrime\(TransparencyAndEnforcement\)Bill](https://hansard.parliament.uk/Lords/2022-03-09/debates/70AD4617-20E7-4EF6-A69F-50EE4F3F1EF9/EconomicCrime(TransparencyAndEnforcement)Bill)

⁶ RUSI 2021 *The Silent Threat - The Impact of Fraud on UK National Security* https://static.rusi.org/the_silent_threat_web_version.pdf

⁷ O’Neill, Onora 2002. *Trust is the first casualty of the cult of transparency* - <https://www.telegraph.co.uk/comment/personal-view/3575750/Trust-is-the-first-casualty-of-the-cult-of-transparency.html>

The report is intended to assist with:

- Informing future vision or high-level strategy, to ensure that priorities and objectives are rooted in a better understanding of the potential risks;
- Identifying challenges and opportunities that could arise in the future, and stress-test how well the assumptions which underpin a given plan or policy may stand up to a range of external conditions;
- Assessing the potential strengths and weaknesses of different strategic objectives or policy options;
- ‘Future proofing’ planned investments or other decisions that are under consideration to ensure that potential risks and unintended consequences are identified and considered as part of overall risk management.

Methodology

Z/Yen approached the study using Z/EALOUS, a six-stage problem-solving approach⁸ grounded in systems theory, viz. establish the endeavour, assess & appraise, lookaheads & likelihoods, options & outcomes, understanding & undertaking, securing & scoring. These six stages are reflected in the layout of this report (see Figure 1).

Figure 1 - Report Structure



Data was collected using desktop analysis. Details of sources are annotated within the text and additional reading is listed in Appendix 1. Trends were generated using societal, technical, economic, and political analysis, and assigned scores on their impact and likelihood. The trends and scenarios were sent for consultation with an expert community and two highly respected think tanks⁹, and amended according to their feedback. Five ‘future narratives’ were compiled and contrasted with the scenarios.

Scenarios were created against the backdrop of a ‘three horizons’ framework,¹⁰ tested against the trends, against Dator’s scenario classifications, and against

⁸ <https://www.zyen.com/about/methodologies/zealous/>

⁹ CSFI and Cityforum

¹⁰ Curry, A & Hodgson A 2011, *Seeing in multiple horizons: connecting futures to strategy*, Journal of Future Studies, 13, 1, 2011: <https://jfsdigital.org/wp-content/uploads/2014/01/131-A01.pdf>

The Future Of UK Fraud Challenging High-Volume, Automated Crime

Adams' risk/reward typologies. A viable systems approach¹¹ was used to model two systems; the criminal system and the anti-fraud authority system. An observe–orient–decide–act (OODA) loop¹² was applied to identify explorations for tackling fraud over the next ten years. These explorations, along with the scenarios, were used to set out a handful of 'challenge' themes as suggestions to guide the anti-fraud agenda over the next decade.

The assumptions, trends, scenarios, future narratives, models, and challenges underlying and developed through the research were tested at a webclave held on 10 March 2022¹³, which was attended by 51 representatives from academia, the public sector, the ICT Industry, the financial services sector, and fraud prevention specialists. Feedback from the webclave was incorporated into the report.

¹¹ **Beer, S 1984** *The Viable System Model: Its Provenance, Development, Methodology and Pathology* Journal of the Operational Research Society, vol. 35, no. 1 pp. 7–25, <https://doi.org/10.2307/2581927>

¹² **Luft A 2020** *The OODA Loop and the Half-Beat* <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>

¹³ **Z/Yen 2022**, *The Future Of Fraud - An Interactive Discussion* <https://fsclub.zyen.com/events/all-events/future-fraud/>

2. Assessment Of The Fraud Landscape

Fraud In England & Wales

Obtaining comparable fraud statistics for the United Kingdom is difficult. *“Fraud data are not designated as National Statistics.”*¹⁴ Before 2011, fraud offences were only recorded by the police. Questions on fraud were only introduced into the Crime Survey for England and Wales (CSEW) in October 2015. The CSEW estimated that only 15% of fraud offences were reported to the police in the year ending March 2019.

The CSEW also incorporates fraud offences collated by the National Fraud Intelligence Bureau (NFIB) from three reporting bodies: Action Fraud, Cifas, and UK Finance. It is possible that *“there may be some double or triple counting between these sources (Action Fraud, Credit Industry Fraud Avoidance¹⁵ (Cifas), and UK Finance). Experts believe this duplication to be so small as to have an insignificant effect on crime trends, but there is currently no simple cross-referencing method within NFIB to detect the scale of it”*¹⁶.

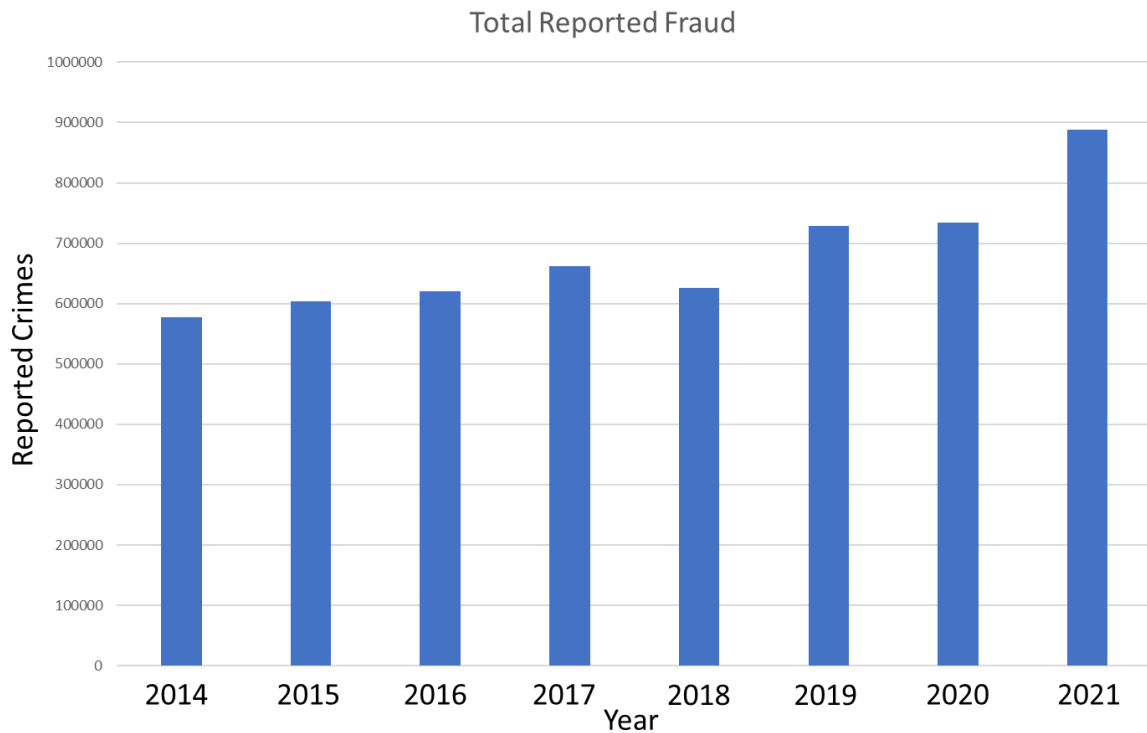
Although information on fraud in the UK is of variable quality, the data examined in the course of this study indicates a major increase in fraud over the last five years. If this trend continues unabated, fraud will have a significant impact on resources and public confidence in the state’s ability to protect citizens.

¹⁴ **Office of National Statistics (ONS)** *Police force area data tables - year ending September 2021* table p11
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/policeforceareadatatable>

¹⁵ <https://www.cifas.org.uk/> accessed 13/3/2022

¹⁶ **ONS** *Notes to accompany table A5, Note 23*
<https://www.ons.gov.uk/file?uri=%2fpeoplepopulationandcommunity%2fcrimeandjustice%2fdatasets%2fpolicforceareadatatables%2fyearendingseptember2021/pfatablesep21final26012022132100.xlsx>

Figure 1 - CSEW Data on Fraud 2014-2021



Source: CSEW

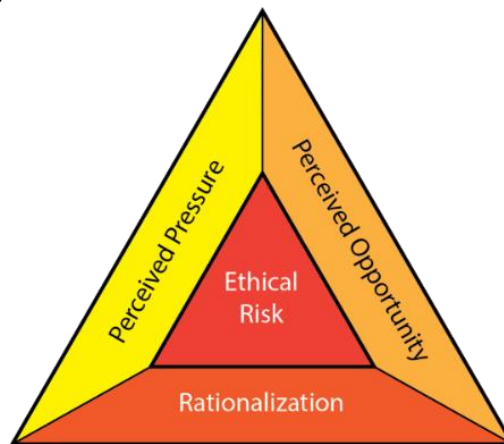
Reliable data on the average amount of loss per victim of fraud is scarce, However, in March 2018, the CSEW estimated that 31.1% of fraud victims experienced no financial loss. No data could be found on how much money is returned to consumers who are victims of fraud. CSEW findings from the year ending September 2021 showed that in over a quarter of incidents (26%) – more than 1.3 million cases - the victim was left out of pocket, experiencing a loss with only partial or no reimbursement.

Categories of Fraud

From the literature describing fraudsters' motivations and methods, until recently the "fraud triangle" was the dominant model¹⁷ (see Figure 2).

¹⁷ Albrecht S 2014 *Iconic Fraud Triangle endures* <https://www.acfe.com/article.aspx?id=4294983342>

Figure 2 - Fraud Theory



However, the fraud triangle is a poor fit for high-volume consumer-oriented fraud and does not map onto the type of fraud that is increasingly being conducted by organised criminal gangs.¹⁸ The advent of the internet has led to an explosion in the volume of fraud.¹⁹ Mass-marketing frauds and consumer scams were traditionally conducted via letter or telephone and required a significant input of time and resources, both in the gathering of intelligence and execution. However, the advent of email and social networking has greatly simplified the input and process phases of fraud, while greatly complicating anti-fraud authorities' task of tracking down criminals and bringing them to justice.

In short, the principal change is that online fraud now dominates high-volume consumer-oriented fraud. By implication, online fraud is highly mechanised (automated) and international. Levi (2008)²⁰ examines the settings for frauds in the context of crime networks, fraud opportunities, and a victim-centric typology of fraud. This is mirrored by the work of the Financial Fraud Research Center at Stanford which has developed a taxonomy of fraud²¹. Using this work as a framework allows the landscape of high-volume consumer fraud to be mapped and contextualised (see Figure 3).

¹⁸ **Huber D 2017** *Forensic accounting, fraud theory, and the end of the fraud triangle* Journal of Theoretical Accounting Research, 12(2), 28-48, 2017

<https://www.researchgate.net/publication/319333659> Forensic accounting fraud theory and the end of the fraud triangle

¹⁹ **Home Office 2013** *Cyber crime: A review of the evidence* Research Report 75

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

²⁰ **Levi M 2008** *Organized fraud and organizing frauds - Unpacking research on networks and organization*

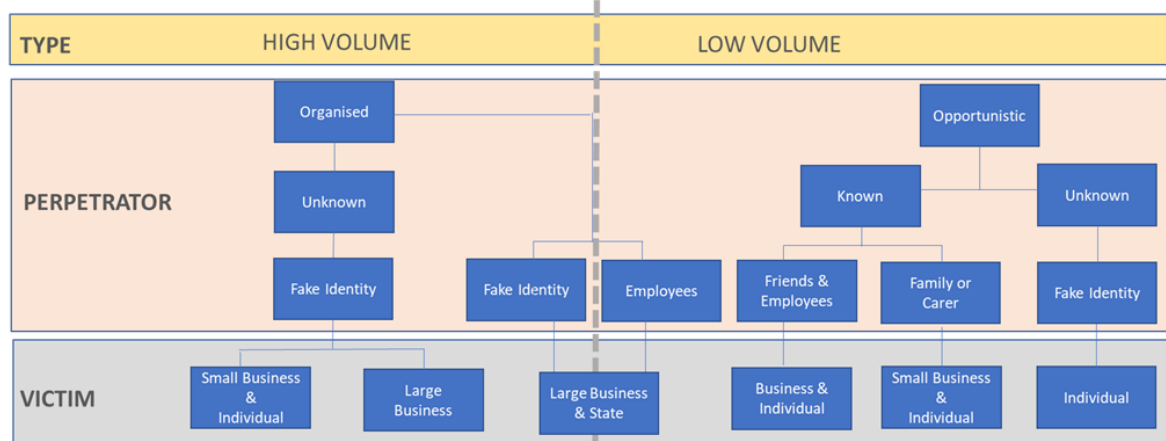
Criminology and Criminal Justice December 2008 <https://www.researchgate.net/profile/Michael-Levi-5/publication/249786379> Organized fraud and organizing frauds Unpacking research on networks and organization/links/0c960532755df02414000000/Organized-fraud-and-organizing-frauds Unpacking research on networks and organization.pdf?origin=figuresDialog download

²¹ **Stanford Centre On Longevity 2015** *Framework For A Taxonomy Of Fraud*

<http://162.144.124.243/~longevl0/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

Figure 3 - High-volume Versus Low-volume Fraud



[adapted from Stanford Centre On Longevity 2015, Framework For A Taxonomy Of Fraud]

This scope of this report is limited to high-volume fraud affecting small businesses and individuals. *In extremis*, the Stanford taxonomy might seem to suggest that low-volume fraud is simply opportunistic, which is an oversimplification. From the taxonomy, one might suggest that a distinction between high-volume and low-volume fraud is that high-volume is distinguished by a need to use automated systems to combat it. The volume of activity is so high that traditional manpower-based approaches to investigation and closure are of limited use. A recent report by the consumer rights organisation *Which?*, that drew on Action Fraud data, estimates that between April 2020 and March 2021, high-volume fraud increased by 33% year on year, resulting in UK losses of more than £2.3bn²². Appendix 3 contains a description of common frauds perpetrated in the UK.

²² Patchett M 2021 Scams rocket by 33% during pandemic, Which?
<https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

Table 1 – A Breakdown Of The Cost Of High-volume Fraud In 2021

Fraud Type	Reports	Total Cost (£ Million)	Average Cost To Victim £ ²³
Online retail and auction fraud	103,254	69	674
Advance fee fraud	38,844	52	1,345
Retail/consumer fraud	29,466	152	5,182
Banking fraud	27,773	183	6,622
Investment fraud	20,989	535	25,496
Computer fixing fraud	18,811	22	1,175
Romance Fraud	7,754	73	9,531
Phone fraud	5,073	1.5	296
Mandate fraud	4,681	145	31,126
Courier Fraud	4,373	21	4,802
Fake loan fraud	2,782	4	1,474
Ticket fraud	2,104	2	998

Source: Which?, 2021

Victims of Fraud

In October 2021 the Victims' Commissioner published research²⁴ on the fraud victim landscape. The findings, drawn from a variety of sources including CSEW data indicates *inter alia* that:

- There is little variation in victimisation across age groups for fraud in general, but certain groups were more vulnerable to particular types of fraud; for example, those aged 45-54 are the most likely to experience romance fraud; and younger people (18-24) are most likely to provide personal information in response to fraudulent invitations.
- Victimisation is greater in higher-income households (earning £50,000 or more) than lower-income groups.
- The use of technology and the internet, and security habits, have been linked to an increased risk of victimisation.

²³ NFIB reported mean loss may be skewed upwards if victims are more likely to report with larger losses.

²⁴ **Victims' Commissioner 2021** *Who suffers fraud? Understanding the fraud victim landscape* <https://s3-eu-west-2.amazonaws.com/jotwpublic-prod-storage-1cxo1dnrmkg14/uploads/sites/6/2021/12/VC-Who-Suffers-Fraud-Report-1.pdf>

- Loneliness and isolation may lead people to respond to and maintain involvement in scams - these people also have a lack of trusted people to consult.

Fraudsters know that the circumstances of certain individuals make them more vulnerable to fraud. Research by AARP (formerly the American Association of Retired Persons)²⁵ and others has identified the personality traits of people who are particularly vulnerable to fraud:

1. **Respect for authority** - Many common scams are perpetrated by criminals impersonating a public official.
2. **Desire to please** - For example a fraudulent email from a colleague, family member, or friend asking you for help.
3. **Previously victimised by a fraudster** - Criminals compile 'victim lists' that get sold to criminal rings.
4. **Friendly and approachable** - Many victims meet their scammer on social media via a friend request.
5. **Under stress** - People who are suffering from personal loss, illness, or financial difficulties can make irrational decisions.
6. **Lonely and isolated** - Many fraud victims report feeling lonely and isolated from family and friends which makes them susceptible to the fake friendliness of professional thieves.
7. **Live in a closed community** - Individuals within a closed community (by nature of religion, geography, or language) are particularly at risk from contagion with frauds such as pyramid schemes.²⁶

The Motivation Of Fraudsters

Although there is a large body of literature on 'white-collar crime', its primary focus is on low-volume opportunistic fraud and individuals who defraud organisations for whom they work. Studies that attempt to profile the perpetrators of high-volume fraud are much rarer. Such studies would be complicated by the fact that high-volume frauds are 'organisational' in nature, a 'day job' for many people.

²⁵ **AARP 2019** *7 Behaviors That Can Make you a Target for Scammers* <https://www.aarp.org/money/scams-fraud/info-2019/vulnerable-to-fraud.html>

²⁶ **Schiffauer L 2018** *Dangerous speculation- The appeal of pyramid schemes in rural Siberia* *Journal of Global and Historical Anthropology* 2018: Issue 81 <https://doi.org/10.3167/fcl.2018.810105>

In 2016 Chan *et al*²⁷ conducted an exploratory profiling study of online auction fraudsters. Their sample consisted of 121 individuals online auction offenders drawn from the database of the Hong Kong Customs and Excise Department, which maintains data pertaining exclusively to counterfeit goods. They found:

- 67% of the fraudsters were male, with a mean age of 30;
- 20% had a university education;
- 55% were employed;
- 64% were single;
- 64% lived with their parents;
- 80% were motivated by monetary considerations;
- 20% were motivated by the thrill.

Given the small sample size and the niche nature of the fraud committed, it is not possible to speculate whether this profile could be more broadly applied to high-volume fraud, but it does underline the need for more work understanding the motivational aspects of high-volume fraud organisations and their economics.

Interviews

As part of this research, unstructured interviews were conducted with 14 individuals. Three of the subjects were academics with expert knowledge of fraud and financial systems, four were senior managers in anti-fraud systems providers, one was from Age UK, and six individuals had been victims of fraud.

Observations from the interviews indicate environmental points worth noting:

1. The international nature of fraud is not just on the rise, rather it is endemic. Any fraudster has a target population in one country, servers in another, and payments systems in a third, and that's just for starters.
2. Data on fraud and anti-fraud is poor to non-existent. Many basic theories of vulnerability, e.g., are the mentally ill more susceptible? are the aged?, remain unproven. The effectiveness of anti-fraud techniques is largely unknown.
3. A lack of highly visible and successful prosecution, combined with widespread consumer contact with fraudsters (check your spam filter or answer your telephone during daytime fraud calls), leads to the impression

²⁷ Chan V *et al* 2016 *An Exploratory Profiling Study Of Online Auction Fraudsters* 10th IFIP International Conference on Digital Forensics (DF), Jan 2014, Vienna, Austria. pp.43-56 <https://hal.inria.fr/hal-01393758/document>

that fraudsters are never caught. The feeling of helplessness induced by the apparent lack of reprisal leads to a feeling that nothing can be done.

4. Public concern about fraud is hard to engage. There has been an inability to convey to the public the human impact of fraud, for example compared with domestic violence. Fraud is seen as just about money, regardless of the real and wider damage done. Victims are seen as complicit in fraud. Among the limited interviewees during the study, one made the statement that those defrauded *"...deserved to be because they were greedy. When will people learn when something is too good to be true that's because it is."* Another drew an analogy between fraud and car crime – *"You're a victim when you return from a meal and your locked car is stolen. You're an idiot when you hand the criminal the keys on your way into the restaurant."*

3. Trends Affecting Fraud

The trends driving and defining the future of fraud over the next 10 years were investigated using desk-research and societal, technical, economic, and political categorisations. These trends are not intended as predictions but as a framework for considering how fraud may evolve over the next ten years. Many of the trends identified are interlinked and synergistic. The trends are contextualised by their impact (the scale and depth of their reach) and likelihood (the probability of occurrence) as high, medium, or low. A summary of the trends is contained in Tables 2, 3, 4, and 5. A more discursive explanation of each trend is contained in Appendix 2.

The trends were lightly tested, a ‘sighting’ test, in a questionnaire to an expert community on 2 March. Respondents, though few, did not object to the trends but emphasised them differently at points. This was taken into account when assessing impact and likelihood.

Table 2 - Political Trends

Political	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

Table 3 - Economic Trends

Economic	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 – UK central bank digital currency (CBDC), positive impact	Medium	High

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

A cashless society – cryptocurrencies rather than CBDC, negative impact	High	Low
---	------	-----

Table 4 - Societal Trends

Societal	Impact	Likelihood
Ageing population	High	High ²⁸
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

Table 5 - Technological Trends

Technological	Impact	Likelihood
Industrialisation of fraud	High	High
Advances in quantum computing	Medium	High
Advances in technology and interactions between technology and society (AI, machine-learning, IoT, Metaverse, etc.)	High	High
Growing digital footprints	High	High
Ageing security systems	High	High

These trends enabled the construction of relevant scenarios.

²⁸ See Appendix 2, point IX.

4. Four Scenarios For The Future Of Fraud

Trend-based analysis can give a linear view of the future, encourage maintenance of the status quo, and miss potential disruptions (Grey Rhino²⁹ or ‘black swan’ events^{30 31}). ‘Scenario planning’ has been developed to describe plausible alternative futures, and is one way to avoid myopia or ‘tunnel’ vision. Scenarios are not predictions, rather they describe a range of possible futures or thought experiments. They are used to explore how trends, decisions, and uncertainties might play out over multiple pathways.

It is important to remember that scenarios, like the trends identified above are not predictions – they are broad brush caricatures that describe a range of possible futures that can be used as thought experiments to explore and learn from. Scenarios provide a useful framework for discussion as using scenarios allows people to explore the implications of other possible—or probable—future worlds and to build these into their plans.

This study produced four scenarios that can be used to help structure analysis, responses, and strategic themes by anti-fraud authorities, these are detailed below. Figure 4 illustrates this graphically – the x axis showing the degree of influence the state holds (note that influence does not necessarily equate to effectiveness) the y axis shows the degree of international cooperation.

Scenario 1 - Crumbling Capacity

This scenario explores a UK, and international environment, growing increasingly fragile in the face of rising inequality, increased impacts from a changing climate, and increasing economic disruption as a result of technological and geopolitical changes that increase cross-border frictions. The UK state is powerful locally, but disorganised. Internationally, increased frictions reduce international cooperation. The UK largely deals with fraud through today’s multiplicity of forces and agencies. The scenario underscores the difficult choices policy makers and law enforcement agencies might face, in terms of prioritising resources, in the context of adverse global and domestic conditions.

²⁹ Rothstein Publishing <https://www.rothstein.com/gray-rhinos/> accessed 14/03/2022

³⁰ **Taleb N 2009** The Black Swan: The Impact of the Highly Improbable, Penguin ISBN-10 : 0141034599

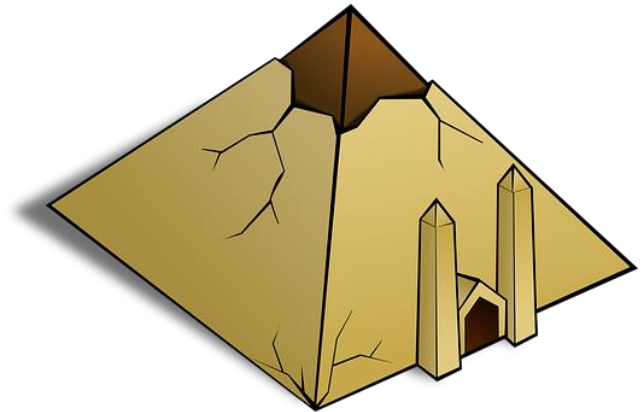
³¹ <https://www.garp.org/risk-intelligence/culture-governance/swans-rhinos-and-elephants-are-animating-risk-debates>

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

Elements:

- Fragile economic growth;
- Weakening public finances;
- Weakening public services;
- Inequality and economic hardship;
- Rising socio-political fragmentation;
- Inter-generational conflict;
- Increase in distrust of media;
- Technology/regulatory disconnect.



Scenario 2 - Island Kingdom

This scenario explores a world in which the attributes of Crumbling Capacity have played out to their logical conclusion. Economic, geopolitical, and environmental crises have fed each other and pushed economies into deep recessions. The social contract between the state and citizens has been pushed to breaking point, and international relations have deteriorated creating favourable conditions for fraudsters to operate with a degree of impunity. Lawless zones exist around the world where fraudsters have unfettered access to machinery and energy. Their giant quantum computing botnet capacity dwarfs almost any nation's individual capacity, and gives them an edge on using portfolio analysis to optimise revenues. The UK's newly-formed Action on Fraud (AoF) unit does what it can nationally, though international gangs easily compel online communities, particularly business ones, to pay extortion fees to continue with minimal interruption from their 'for hire' online bot 'divorce networks' that deliberately incite divisiveness in communities.

Elements:

- Weak public finances;
- Distrust of authorities;
- Collapse of public services;
- Intergenerational conflict;
- Rejection of social norms;
- Socio-political fragmentation;
- Weak international cooperation;
- Rising political extremism;
- Prolonged recession and economic protectionism.

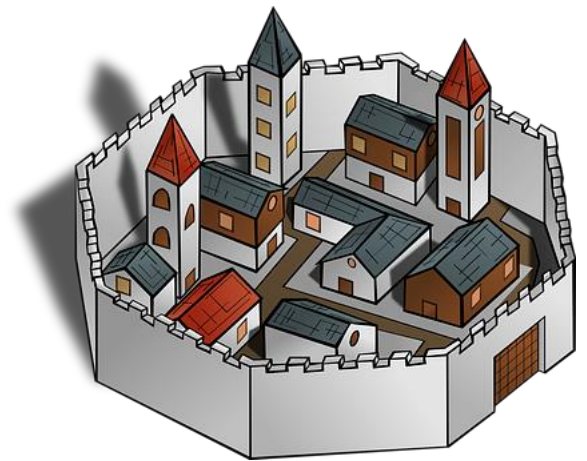


Scenario 3 - Safe Neighbourhoods

In this scenario, increased fraud has been prevented and globalisation has reduced. The national economy is more increasingly 'managed'. Strong public finances support effective public services, inequality has declined, and the strong bonds which people have with their local geographical communities have enhanced the importance of ethical behaviour. Strong international cooperation has enabled the effective harnessing of big tech companies in the public interest. The combination of local, national, and international has almost eliminated fraud. In the UK, the Super Anti-Fraud Squad (UK-SAFS) works closely with the United Nations' Global Online Policing Service (UN-GOPS).

Elements:

- Increase in importance of ethical behaviour
- Greater geographical community cohesion
- Less inequality and materialism
- Enhanced regulation of technology
- Strong international cooperation
- Strong public finances
- Strong public services
- Increase in localism



Scenario 4 - Big-Tech Country

This scenario envisages a future in which attempts to regulate big tech companies have failed. Trustworthy information is available to those who can pay. Regulation cannot keep pace with online services. Most public services and infrastructure, including some policing and law enforcement functions, are provided by the private sector. Employment patterns have been irreversibly disrupted, with the majority of workers on zero-hours contracts in the gig economy. Personal identity and brand identity are inseparable. AI is used widely in both law enforcement and sentencing. The Consortium, a group of the largest Big Tech firms, share information and processes to help police their online markets and communities.

The Future Of UK Fraud

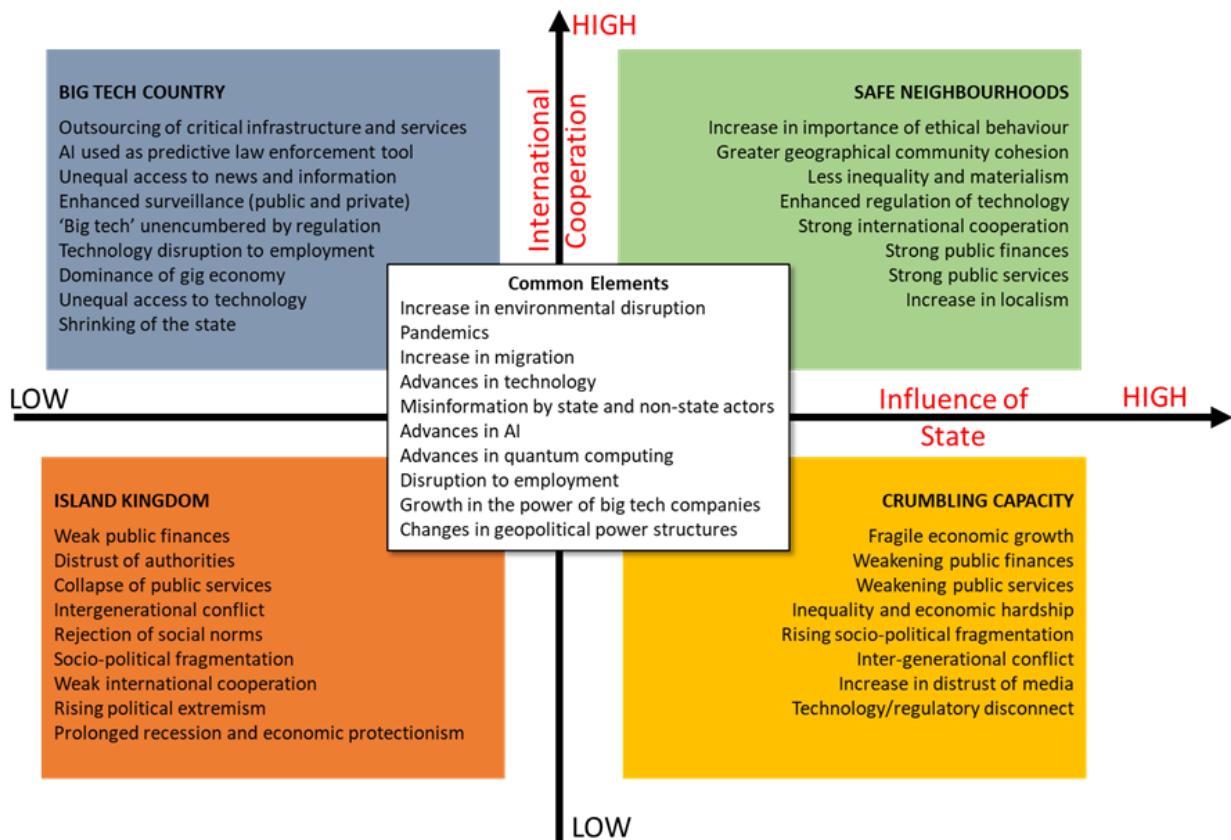
Challenging High-Volume, Automated Crime

Elements:

- Outsourcing of critical infrastructure and services;
- Artificial Intelligence (AI) is routinely used as a predictive law enforcement tool;
- Unequal access to news and information;
- Enhanced surveillance (public and private);
- ‘Big tech’ unencumbered by regulation;
- Technology disruption to employment;
- Dominance of gig economy;
- Unequal access to technology;
- Shrinking of the state.



Figure 4 – Four Scenarios



Common Elements Between Scenarios

Although the scenarios are broad-brush caricatures of possible futures, each of them has its origins in the world of today. As a result, they share common elements drawn from the set of current trends. These can be summarised as follows:

- Environmental disruption caused by anthropogenic climate change, including floods, droughts, storms, and wildfires will increase, placing strain on infrastructure and services and adding anxiety to people's lives.
- Changes in geopolitical power structures may change the world order, with new actors, with different priorities taking the lead in international bodies.
- As the world recovers from Covid-19 the public are likely to be receptive to rumours of new pandemics (although these have a very low probability)
- The economic fallout of Covid-19, the current conflict in Ukraine, ongoing and future conflicts in Africa, increasing droughts, floods, and extreme weather events are likely to mean that large numbers of migrants and refugees will cross international borders in search of new lives.
- Technology will advance, and new applications for technology will be found, some of which may affect society in ways we cannot imagine. People may retreat from the world into virtual fantasy lands in 'the Metaverse', or their lives may be enhanced by a virtual information-rich overlay. There is a feedback loop between technology and inequality. Technology inequalities create vulnerabilities that can be abused by criminals or leave individuals open to fraud. Technological developments could increase the "chasm" between rich and poor, and between skilled and unskilled technology users.
- The use of 'weapons of mass distraction' by state and non-state actors is likely to increase. Russia has used *maskirovka*³² techniques against the west for many years. There is evidence that the Chinese state is learning from their example, and extremists, ideologues, and nihilists continue to exploit the unwillingness of tech companies to in any way constrain their role, despite the corrosive effect of some activities on their 'platforms'.
- There will be advances in AI and new applications for AI systems. Some will undoubtedly benefit society by improving planning and decision making, others such as AI-powered surveillance and law enforcement may be a double-edged sword.

³² Moore C 2019 *Russia And Disinformation: Maskirovka* <https://crestresearch.ac.uk/resources/russia-and-disinformation-maskirovka-full-report/>

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

- It is likely that in ten years' time consumer versions of quantum computers will be available, vastly increasing the processing power available to the public. Although applications for quantum computing are currently in their infancy and restricted to a few esoteric fields, it is likely that new applications will be found, particularly in robotics, artificial intelligence, and communications, which will impact society in unknown ways,
- Technology-related disruption to employment and the redundancy of certain skills and business models will affect society at all levels. White-collar and retail workers, in particular, are likely to be affected, and new graduates may struggle to find employment appropriate to their level of qualification.
- The growth in the power and influence of big tech companies has been largely unchecked. Political will and international cooperation will be required to ensure that big tech's capacity to benefit, rather than damage, society and democracy comes to the fore.

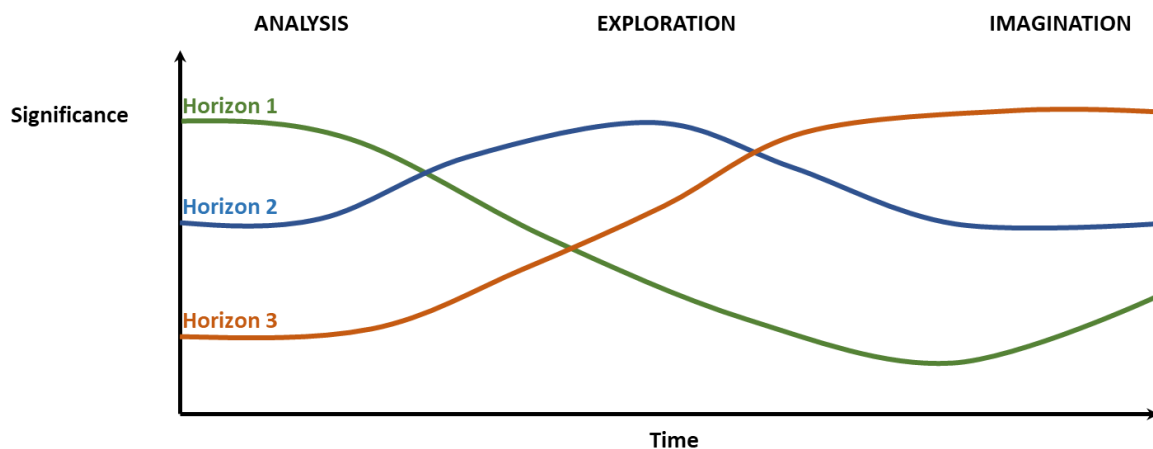


Testing For Reasonableness

The scenarios were compared with a 'three horizons' framework³³ (see Figure 5), which challenges scenario creators to make assumptions explicit, and then to explore emerging change as a way to reframe possible outcomes:

- **Horizon One** – These are important drivers of the world today. Horizon One drivers are likely to be well understood. They are useful for short-term planning – over two to three years – they affect the operating environment today but may well be less important in the future.
- **Horizon Two** – These are the drivers that are causing the operating environment to change. They may not affect the world today, but they are clear drivers with a predictable outcome that will affect the forecastable future. Horizon Two drivers are likely to be the most important for medium-term strategies encompassing the next five to ten years.
- **Horizon Three** – These are drivers that are early indicators of change and portents of trends to come. Horizon Three drivers may become important in the long-term future and may affect issues in the longer term. Although they may be flagged as weak signals they should not be discounted.

Figure 5 - Three Horizons To Classify Drivers Of The Future



The conclusion was that the scenarios appeared to map across all three horizons, though each scenario could be seen to be 'centred' on one horizon, viz.:

- Crumbling Capacity – Largely centred on Horizon One, approximately two years out.
- Island Kingdom – Largely centred on Horizon Two, approximately five years out.

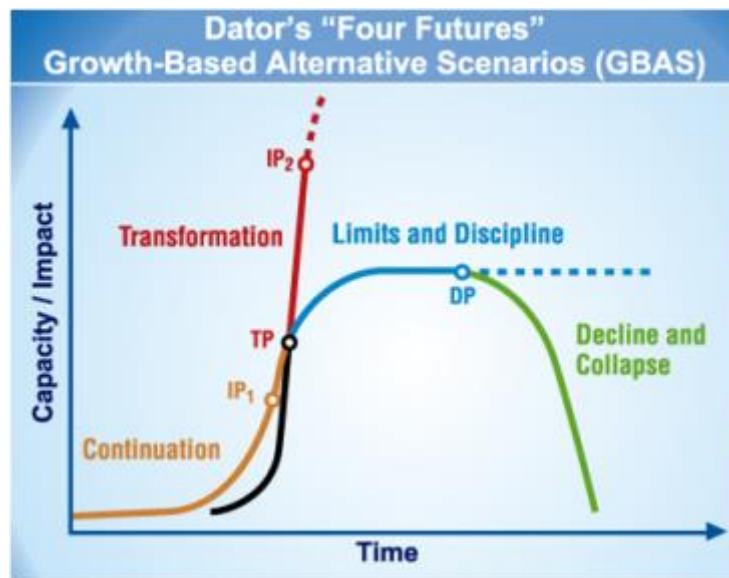
³³ Curry, A & Hodgson A, *Seeing in multiple horizons: connecting futures to strategy*, Journal of Future Studies, 13, 1, 2011: <https://ifsdigital.org/wp-content/uploads/2014/01/131-A01.pdf>

- Safe Neighbourhoods – Largely centred on Horizon Three, approximately eight years out.
- Big Tech Country – Largely centred on Horizon Two, approximately five years out.

To further test the breadth of the scenarios, they were mapped against Jim Dator's³⁴ four growth curves, see Figure 6:

1. Continuation (the initial phase of slow or fast exponential growth)
2. Limits and Discipline (the saturation phase of S-curve growth)
3. Decline and Collapse (the decline and recycling phase of life cycle growth)
4. Transformation (super-exponential growth)

Figure 6 – Dator's Four Growth Curves



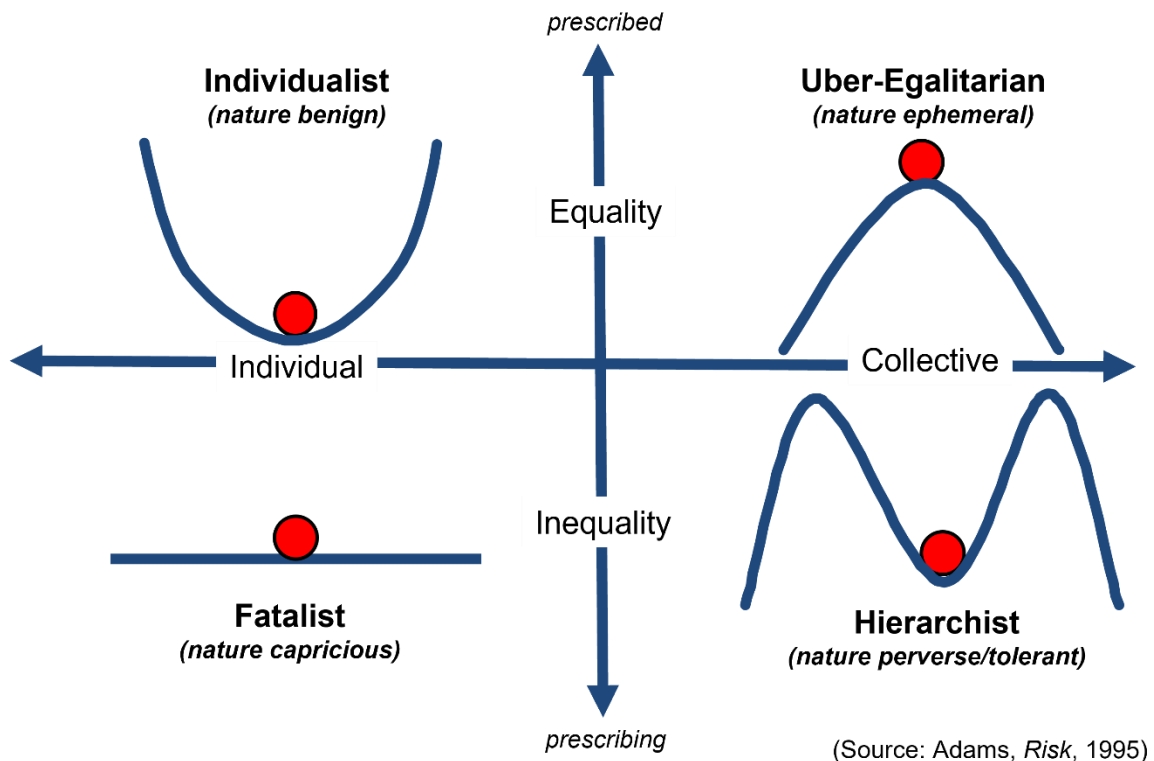
The scenarios mapped well against Dator's four recurring stories:

1. **Crumbling Capacity** - Continuation (business as usual, more of the status quo growth).
2. **Big Tech Country** - Limits and Discipline (behaviours to adapt to growing internal or environmental limits).
3. **Island Kingdom** - Decline and Collapse (system degradation or failure modes as crisis emerges).
4. **Safe Neighbourhoods** - Transformation (new technology, business, or social factors that change the game).

³⁴ **Foresight University** Chapter 4 Models -Foundations For Organisational Fore Sight
<https://www.foresightguide.com/dator-four-futures/>

Finally, again to test breadth and reasonableness, scenarios were assigned to Adams'³⁵ classification of risk/reward personalities (see Figure 7).

Figure 7 - Four Elementary Risk/Reward Typologies



Each character, organisation, and scenario can be represented by a 'ball' on a slope. The risk/reward profile is best visualised as what might destabilise the ball. Taking each quadrant in turn:

- 1. Fatalist - Unsettled Times** - The Fatalist sees nature as capricious. Nothing they do changes the way the ball moves. At first glance, the Fatalist is uninteresting, but over time it seems to be the quadrant of the majority.
- 2. Individualist - Free for All** - The Individualist is almost a parody of an 80's yuppie. It would take a complete catastrophe to disturb their ball. Nature is benign – it won't hurt him or her. Fraud? Well, after all the money has to go somewhere.
- 3. Über-egalitarian – Control Freaks** - The Über-egalitarian is almost a parody of a 60's or 70's socially-conscious individual – Earth Day, the Good Life, sandals. The ball is barely being held stable. Nature is ephemeral, about to be overwhelmed at any minute. The battle cry is often "there ought to be a law...".

³⁵ Adams J 1995 Risk, Routledge ISBN0-203-49896-8

4. Hierarchist - Power Brokers - The hierarchist sees nature as something to be overcome, but manageable. The little ball is stable within 'normal conditions', but extremes are to be avoided. The hierarchist is a natural bureaucrat and loves decisions based on sound thinking, however irrational the result.

Individuals inhabit different positions at different times in different circumstances for different decisions. One may be a fatalist about comet disasters – stuff happens; an individualist about one's children's education – why can't I have school vouchers?; a hierarchist about corporate rules – we need to enforce our expenses policy; and an über-egalitarian about corporate pollution – it's a crime; it shouldn't happen.


The scenarios mapped well against Adams' typologies:

- 1. Crumbling Capacity** – Fatalist.
- 2. Big Tech Country** – Individualist.
- 3. Island Kingdom** – Über-egalitarian.
- 4. Safe Neighbourhoods** – Hierarchist.

5. Future Narratives

To further test the scenarios' reasonableness, we created victims' stories from 2032. Each victim's case was fed into the scenarios and the outcomes under each of the scenarios were mapped. These are their stories:

Future Narrative 1 - Susan's Story

	<p>Name: Susan Jones</p> <p>Age: 68</p> <p>Details: Retired school teacher, widowed</p> <p>Location: Burntvale, Staffordshire</p> <p>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</p>
<p>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.</p>	
<p>SCENARIO 1: CRUMBLING CAPACITY</p>	
<ul style="list-style-type: none">• Susan uses an elderly laptop for accessing the internet and relies on free security software.• Susan loses £3,000. 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 logs the report and wishes to help, 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 contacts her. NFIB e-mails her prepared materials on how to avoid fraud.	
<p>SCENARIO 2: BIG TECH COUNTRY</p>	
<ul style="list-style-type: none">• Susan has a new laptop computer but cannot afford a subscription to the latest AI-enabled security software which would have alerted her to potential fraud.	

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

- Her only news sources are free feeds and she hasn't seen any articles about the recent surge in romance fraud.
- Susan loses £3,000. She reports the fraud, but her bank rejects liability.
- The national anti-fraud agency (a subsidiary of a large tech firm) runs an AI engine that logs the potential fraud, and red flags the fake website. However, the national anti-fraud agency is contracted to collect, analyse, and pass on data. There is no system to ensure the site is blocked.
- Had Susan conducted more online commercial activity in the past, The Consortium might have helped her with pursuing the fraudster and perhaps even recovery with one of their special 'flying units'. She might have been able to pay with her Consortium points gained from buying and selling online.
- Europol is alerted and takes steps to close the fraud ring down. They make some local arrests, however the website is hosted on a server in Honduras resulting in 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. Staffordshire police support is limited to standard information packages provided to victims in such cases.

SCENARIO 3: ISLAND KINGDOM

- Susan uses her phone to access the internet since her laptop went missing.
- She has no malware detection capabilities installed on her phone.
- Susan loses £3,000. She reports the fraud, but her bank rejects liability.
- She contacts the local police, with limited results. They suggest contacting
- AoF take her details, but nothing happens.
- She searches online for further advice on what to do if you are a victim of fraud and finds a website that 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, resulting in her receiving 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 possible fraud. The bank also alerts the UK-SAFS 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.
- UK-SAFS 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

The Future Of UK Fraud Challenging High-Volume, Automated Crime

equipment, and freezing their bank accounts. UN-GOPS is also brought in to coordinate and speed closure and apprehension.

- Details of all the financial institutions the fraudsters have had dealings with are published on an OSINT site.
- Sheepishly, Susan holds a private ‘Fraud Confession’ party with her few friends. It has become the socially ‘aware’ thing to do.

Future Narrative 2 - Kiran’s Story

	Name:	Kiran Williams
	Age:	47
	Details:	Self-employed plumber, lives with his wife and two children
	Location:	Hackney, London
	Background:	Kiran’s business debit card details were obtained by a criminal gang operating out of Brighton, using information purchased from a data broker based in Miami.

Attack Method: CNP Fraud (Card Not Present). Several transactions are made using Kiran’s credit card in a variety of locations.

SCENARIO 1: CRUMBLING CAPACITY

- Kiran contacts his bank to query several transactions when he receives his statement.
- The bank logs the purchases as suspicious, replaces Kiran’s card, and alerts the National Fraud Intelligence Bureau and Cifas.
- The NFIB logs the report, but the incident is given a low priority as the amount of money stolen does not yet meet the threshold for action. Once further frauds take place the NFIB will determine whether there is a pattern and reprioritise the case.
- After another six months, a pattern begins to emerge and NFIB contacts the police in Brighton, who raid an address but fail to make any arrests.
- Kiran’s personal bank account is subject to CNP fraud. He contacts his bank and the cycle repeats.
- The bank refunds Kiran’s money 12 months later and a victim support officer is assigned to, and contacts, Kiran. They e-mail him prepared materials on how to avoid fraud.

SCENARIO 2: BIG TECH COUNTRY

- Kiran contacts his bank. As the bank has no physical offices, this is done through an AI agent.
- The AI agent logs the incident and alerts the outsourced national anti-fraud agency, which is a subsidiary of a large tech firm.

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

- The AI engine at the national anti-fraud agency logs the potential fraud and using metadata from the transactions identifies the internet protocol (IP) address from which the frauds were committed.
- Local law enforcement is alerted, Closed Circuit Television (CCTV) footage from the locality is used to identify the criminals' address, and subversion software is deployed to penetrate Internet of Things (IoT) devices linked to the IP address.
- Recordings of conversations within the property are collected and a security team is dispatched to raid the premises and arrest the suspects.
- The national anti-fraud agency, in turn, enlists the aid of The Consortium which helps further immobilise the fraudsters' online activity.
- The bank refunds Kiran's money and he is emailed when an arrest is made.


SCENARIO 3: ISLAND KINGDOM

- Kiran contacts his bank, which denies liability but does issue another card.
- Kiran's credit record is marked.
- The bank alerts AoF to the fraud which collates annual statistics to distribute to their membership.
- Kiran contacts the police who e-mail him prepared materials on how to avoid fraud.

SCENARIO 4: SAFE NEIGHBOURHOODS

- Kiran's bank flagged up the suspicious transactions before Kiran was aware of them and blocked the payments.
- The bank alerts UK-SAFS who contact Kiran's local police force.
- A community support officer visits Kiran and gives him information on how to spot and avoid fraud.
- UK-SAFS collates a report identifying the criminals and where they obtained their information which it shares with international agencies, especially UN-GOPS.
- The criminals are located using the metadata associated with the transactions and arrested.
- The FBI raids the data broker in Miami and takes down a darkweb marketplace, obtaining information on international clients which it shares with local police forces. The fraudsters are arrested equipment is seized and bank accounts are frozen.
- Details of all the financial institutions the fraudsters have had dealings with are published on an OSINT site. The most culpable financial institution tips over a threshold that triggers the financial regulator to shame it nationally, hurting its business. It publishes a public apology and undertakes a thorough anti-fraud reform programme.
- Kiran posts the personal story of his fraud and what happened on his social media pages.

Future Narrative 3 - Viktor's Story

	<p>Name: Viktor Hirzhov</p> <p>Age: 24</p> <p>Details: Came to the UK with his mother and sister as a refugee from Ukraine in 2022. Viktor is an accountant. He suffers from anxiety and has been prescribed propranolol by his GP.</p> <p>Location: Lives in Redhill Surrey, in a flat jointly owned with his husband David.</p> <p>Background: Phone number obtained from a spear-phishing attack on his local GP which stole the details of patients suffering from mental health issues. The attack was made by Albion Arise, a far-right anti-migrant group. Albion Arise was covertly established by Russia, and is used as a front for harassing the Ukrainian diaspora.</p>
---	--

Attack Method: WhatsApp Scam. Viktor receives a WhatsApp message purporting to be from his sister claiming that a bailiff is at her door threatening to impound her possessions unless she pays a £1,800 fine. The bailiff has already taken her phone, so she is using her neighbour's phone to contact Viktor, hence the unrecognised number. Viktor immediately transfers the funds to the 'bailiff's' account.

SCENARIO 1: CRUMBLING CAPACITY

- Viktor contacts his bank as soon as he realises he has been scammed, but they will not refund the money.
- The bank logs the transfer as fraudulent and alerts the National Fraud Intelligence Bureau and Cifas.
- The NFIB logs the report and notes a pattern targeting Ukrainians. Local police forces are informed.
- After twelve months NFIB links the attacks to Albion Arise and begins tracing the organisation's bank accounts. NFIB notes that money transferred to a network of fifteen accounts is used to buy cryptocurrency, after which the trail goes cold. The active accounts are frozen.
- A year after the attack, Viktor is contacted by Surrey Police who warn him he is a potential target for Albion Arise and e-mail him a pamphlet on how to avoid fraud.

SCENARIO 2: BIG TECH COUNTRY

- Viktor contacts his bank, whose AI agent logs the incident and alerts the outsourced national anti-fraud agency. Kiran is emailed an incident number.

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

- The AI engine at the national anti-fraud agency logs the potential fraud and using metadata from the transactions, identifies the fraudulent accounts, alerting the banks that own them who shut them down.
- The national anti-fraud agency, in turn, enlists the aid of The Consortium which helps further immobilise the fraudsters' online activity.
- As Kiran has opted for anti-fraud cover as part of his household insurance. He contacts his insurance company with the incident number. His insurer's AI requests information from the bank AI and the national anti-fraud agency the claim is approved.
- The insurance company refunds Viktor's money, less a 25% handling charge, which is paid to the national anti-fraud agency.


SCENARIO 3: ISLAND KINGDOM

- Viktor contacts his bank, which denies liability.
- The bank alerts AoF to the fraud who collate annual statistics to distribute to their membership.
- Albion Arise publishes Viktor's address and photo on their website. Kiran receives hate mail and is threatened on the street.
- Kiran contacts the police who e-mail him prepared materials on how to avoid fraud.

SCENARIO 4: SAFE NEIGHBOURHOODS

- Viktor's bank initiated an automatic two-day delay on executing the transaction as it exceeded £1,000.
- The transaction is stopped immediately when Kiran informs them of possible fraud.
- The bank alerts the UK-SAFS who contact Kiran's local police force.
- A community support officer visits Kiran and gives him information on how to spot and avoid fraud. Viktor is assigned a case officer who keeps him informed of the investigation.
- UK-SAFS collates a report identifying the criminals and where they obtained their support which it shares with international agencies, especially UN-GOPS.
- UK police forces cooperate to take down the criminals. Albion Arise is proscribed and its websites are removed.
- The Danish police raid a crypto currency server in Randers and obtain information on international clients which they share with UK forces via UK-SAFS. The cryptocurrency wallets of the fraudsters are seized and residual funds are returned to the victims.
- Details on the origins of Albion Arise are released to the press who publish an expose.
- Details of all the financial institutions the fraudsters have had dealings with are published on an OSINT site.
- Viktor is too nervous about his personal circumstances to publicise things, but his community support officer helps him conduct a small online discussion about fraud and what to do about it with people from his church group.

Future Narrative 4 - Jahinda's Story

	<p>Name: Jahinda Patel</p> <p>Age: 34</p> <p>Details: Married, with two young children, Jahinda is a customer support teleworker</p> <p>Location: Leeds</p> <p>Background: The scam is almost fully automated and runs on a cloud-based, semi-autonomous, machine-learning algorithm (MLA), which has targeted 18 million women in 43 countries. Victim interactions are mediated through an automated chatbot that has scripted responses tailored to different cultures and languages.</p>
---	---

Attack Method: Business opportunity scam. Jahinda responds to an advertisement she saw on Facebook offering an opportunity to supplement her income by creating non-fungible tokens (NFTs) at home. Several of her friends have seen the advertisement and are participating. The advertisement leads to a well-designed website with contact details. She has an online chat with a nice lady who explains the process for creating NFTs – for a fee, Jahinda can download special 16 x 16 grids which she and her children can colour in any way they like. The company will turn them into NFTs which can be sold for hundreds, maybe even thousands of pounds. She is told that there is a small upfront fee for the grids and that a commission is charged when the NFTs are sold. The commission must be paid in advance before money 'earned' can be released.

SCENARIO 1: CRUMBLING CAPACITY

- Jahinda has been involved in the scheme for several months, but her doubts are growing. She has already spent £300 on the grids but she has been told she has to pay a commission fee of £1,200 before she will be paid the £7,000 her NFTs have been sold for. She speaks to several of her friends who are involved in the scheme and only one has received payment, with quite a bit of money still on account. The others have paid the commission but are still waiting for their earnings.
- She contacts action the Citizens Advice consumer helpline for advice, they advise her to contact Action Fraud.
- Action fraud alert NFIB, who log the incident and alert Yorkshire Police.
- A police officer telephones Jahinda and takes details of the incident including details of the website and a description of the woman she spoke with. However, Jahinda is unwilling to involve any of her friends.
- NFIB traces the funds Jahinda has paid to a company registered in Jakarta, they inform the Indonesian authorities and Facebook.
- Facebook refuses to take down the ads until Indonesia formally prosecutes the company concerned.

The Future Of UK Fraud Challenging High-Volume, Automated Crime

- A year later Jahinda has not heard anything more, and several of her friends have lost a considerable amount of money.
- The machine-learning algorithm continues to run and has now contacted over 30 million women in 73 countries.

SCENARIO 2: BIG TECH COUNTRY

- The Citizens Advice Bureau (CAB) no longer exists but Jahinda uses the Action Fraud gateway to log her case.
- The AI at her bank has flagged the transactions Jahinda made with the fraudsters and would have queried a larger transaction, as well as imposed a cooling-off payment period.
- The AI engine at the national anti-fraud agency logs the potential fraud, and notifies The Consortium. Although the machine-learning algorithm remains elusive, the national anti-fraud agency, with help from The Consortium, traces the money transfers to a series of accounts owned by a company registered in Jakarta, where it searches the Ministry of Trade's list of Surat Izin Usaha Perniagaan and identifies the company directors.
- A request is made to the Indonesian Ministry of Trade (MoT) and the Indonesian police service to investigate.
- The Consortium takes down the advertisements across all markets once the Indonesian authorities confirm an active investigation.
- Action Fraud email Jahinda with an update on progress, she shares it with her friends who stop dealing with the fraudsters, however, their money is not recovered.
- The machine-learning algorithm continues to run and has now contacted over 30 million women in 73 countries.

SCENARIO 3: ISLAND KINGDOM

- CAB no longer exists and the AoF gateway has minimal functionality.
- Jahinda voices her concerns to her friends, who ostracise her for several months until they realise that they too will not be paid.
- The fraudsters continue trading.
- The machine-learning algorithm continues to run and has now contacted over thirty million women in seventy-three countries.

SCENARIO 4: SAFE NEIGHBOURHOODS

- CAB advises Jahinda to contact UK-SAFS. UK-SAFS log the incident and alert Yorkshire Police. UK-SAFS also starts a low-level notification of UN-GOPS.
- The AI at her bank has flagged the transactions Jahinda made with the fraudsters and would have imposed an automatic one-day cooling-off period had Jahinda attempted to transfer a larger sum.
- Yorkshire police assign a community liaison officer to Jahinda who visits her and takes details of the crime. The community liaison officer also visits the local Imam who alerts the local community to the fraud and advises anyone affected to contact the police.
- Thirty women come forward to report the crime and Yorkshire Police update UK-SAFS. UN-GOPS is automatically also notified.

The Future Of UK Fraud

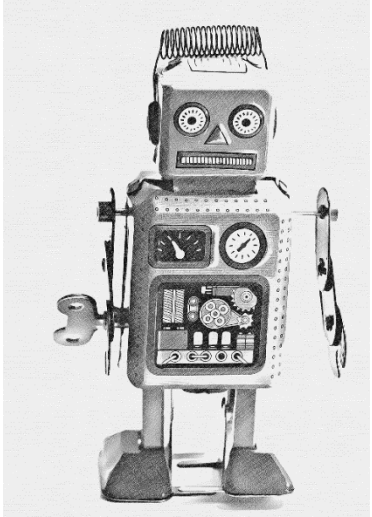
Challenging High-Volume, Automated Crime

- UK-SAFS prioritises the case and puts out a major alert which is carried on all major news channels. Information is shared with UN-GOPS who put out a global alert.
- The funds are traced to a company registered in Jakarta. UN-GOPS informs the Indonesian authorities and the Big Tech firms most involved which immediately take the advertisements down.
- Jahinda is kept informed of progress and she shares this with Imam and her friends.
- The Indonesian authorities arrest the company directors and confiscate their assets. These are used to refund, at least in part, Jahinda and all the other victims of the fraud.
- Details of all the financial institutions and ISPs the fraudsters have had dealings with are published. The most culpable ISP tips over a threshold that triggers a major consumer magazine to shame it nationally, hurting its business. It publishes a public apology and a reform programme.
- The machine-learning algorithm is hunted down by AI security agents and deleted.
- The Imam asks the women's group to hold a fraud awareness discussion in the near future where Jahinda can share her personal experience.

The Future Of UK Fraud Challenging High-Volume, Automated Crime

Future Narrative 5 - Ashley's Story

This narrative was submitted by the Centre For The Study Of Financial Innovation (CSFI) and occupies the border between the Big Tech Country and Island Kingdom scenarios.

	<p>Name: Ashley Burton</p> <p>Age: 38</p> <p>Details: Programmer and AI consultant</p> <p>Location: Burntvale, Staffordshire</p> <p>Background: Ashley, an AI consultant, has recently been made redundant by a multinational company that decided to replace its roughly 150 researchers with the now completed AI software that Ashley designed.</p> <p>It is a time of public sector erosion, implosion of the welfare system, and high labour market volatility due to technology disruption, where even those with the coding skills so much sought a few years ago, are now struggling to find well-paid jobs.</p>
<p>Attack Method: Disappointed with the decision of the company and needing to make ends meet, Ashley steals both the global bulletin subscriber's data and the information on past news sources the team of researchers and journalists compiled. The database includes photos and contact details, as well as specific comments and materials on the type of support provided.</p>	
<h4>Big Tech Country/Island Kingdom</h4>	
<ul style="list-style-type: none">• Using automated machine-learning, Ashley builds an AI system to defraud previous company's stakeholders, subscribers, and supporters.• The system is able to search for the social-media accounts of aforementioned people and collect information on their networks. It then produces high quality deepfakes that can even deceive facial recognition technology to defraud members of these networks using a range of behavioural strategies and mechanisms.• Ashley made sure that the AI system would make full use of automated self-learning continuously expanding the targeted networks, improving from its own success rates of different fraud strategies, detection rates and innovation in fraud schemes across the globe.• Proceeds of the fraud are also managed dynamically by the AI system, constantly learning and optimising finance channels to maximise risk-adjusted returns and minimise detection, using to full-advantage the increasing dislocation of capital markets, collapse of international coordination and mushrooming of crypto assets and private stable coins.• Ashley moves to the countryside to lead a discreet but financially secure life and continues improving his creation, accumulating wealth under the radar of the authorities. A few years later, he dies suddenly. His last thought is that his creation had one deep flaw: no self-destruction mechanism.• Ashley's system continues defrauding citizens around the globe, tailoring its strategies to societies 'vulnerabilities and fraud21 enforcement capabilities. Sometimes, the authorities	

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

succeed in dismantling some of its operations, but its deeply decentralised system makes it nearly impossible to fully eliminate it. As evil knotweed, cut it in one country, one social network and it re-emerges in another under a totally different disguise.

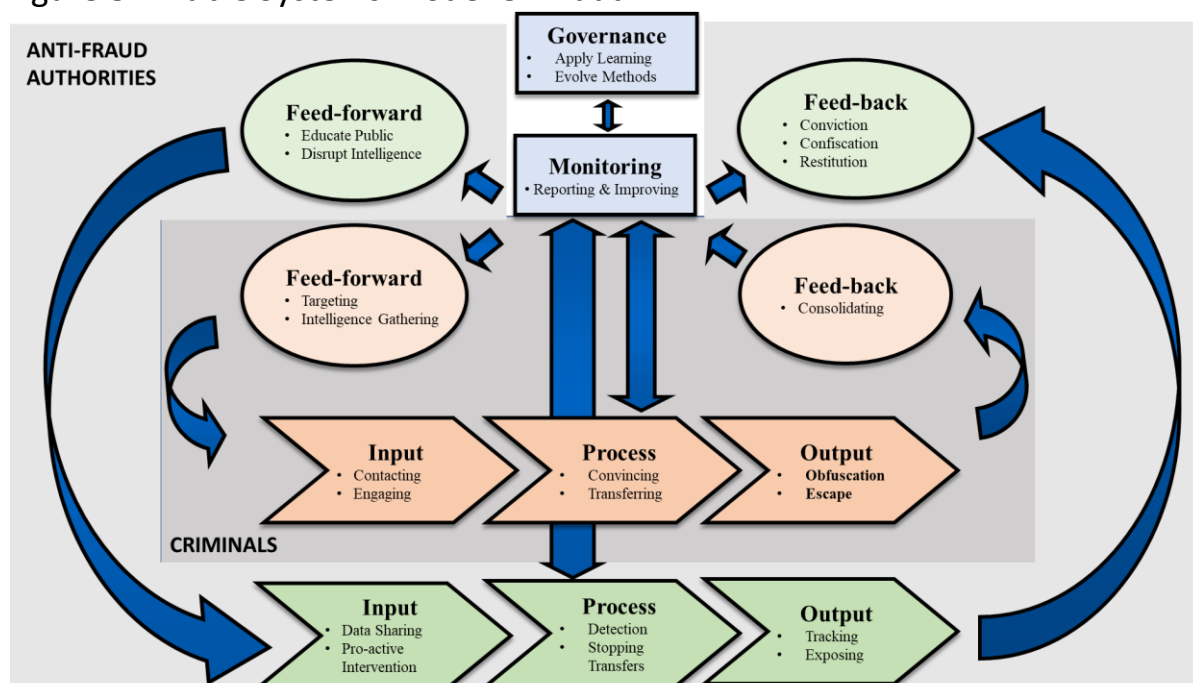
- Although the authorities also deploy AI as a predictive and fraud identification enforcement tool, it is difficult to predict future victims, due to the lack of discernible pattern among deepfakes recipients or to recognise the link between different fraud schemes which also appeared unconnected. The most sophisticated law enforcements authorities apply big data tools to identify unusual financial flows and unexplained wealth including in the metaverse, but Ashley's scheme proceeds have no longer an owner, and are never disbursed, removing another opportunity for law enforcers.
- His scheme continues to grow without him, fuelling social unrest and political instability, not only because the lack of recourse for its ever-increasing number of victims but because the proceeds grow sufficiently large to distort economies, with a myriad of unregulated investment instruments, solely maximising profit with no ethical dimension and designed to take advantage of every weakness in global governance.

6. Viable Systems Analysis & Exploration Generation

Individuals and criminal gangs seeking to defraud UK citizens must plan to accomplish a series of goals if they are to be successful in their enterprise. Similarly, anti-fraud authorities must effectively disrupt and interfere with criminals' ability to achieve those goals if they are to protect victims, prevent fraud, and bring perpetrators to justice.

One way of analysing these processes and interactions is the use of a viable systems model³⁶. A viable systems model approach states that all successful systems in complex environments have seven identifiable elements working together, viz: the implementation elements - input, process, output; the intelligence elements - feedforward, feedback; and the management elements - monitoring and governance. In fraud, there are two systems and thus two models, one for criminals and one for anti-fraud authorities. Criminal systems have inputs, processes, and outputs to select their victims, carry out the fraud, steal money or information, and make their escape. Anti-fraud authorities have systems to thwart, halt, and ameliorate the damage. Figure 8 shows the two viable systems and their interactions.

Figure 8 - Viable Systems Model Of Fraud

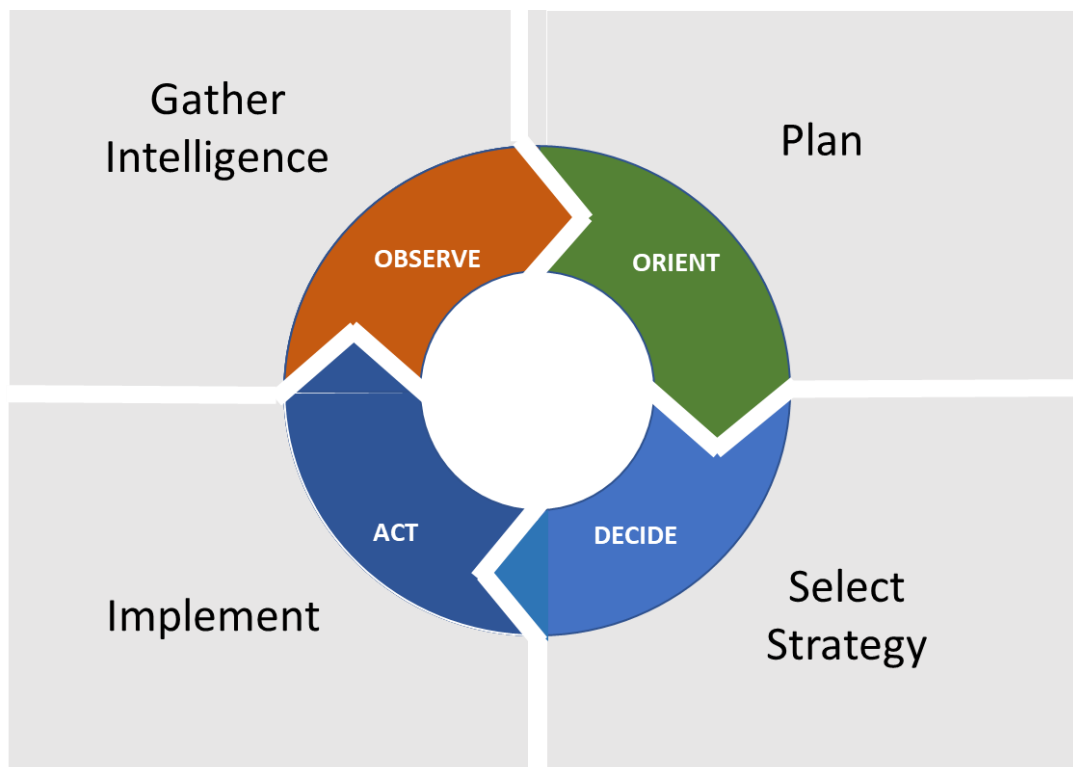


³⁶ Beer S 1989 *The Viable System Model, its provenance, development, methodology and pathology*
https://www.kybernetik.ch/dwn/Viable_System_Model.pdf .

Observe-Orient-Decide-Act (OODA) is a tactical air combat doctrine that was developed by US Air Force Colonel John Boyd during the Korean war³⁷, see Figure 9:

- **Observe:** The first step is to identify the problem or threat and gain an overall understanding of the internal and external environment.
- **Orient:** The orientation phase involves reflecting on what has been found during observations and considering what should be done next.
- **Decide:** The decision phase makes suggestions towards an action or response plan, taking into consideration all of the potential outcomes.
- **Act:** Action pertains to carrying out the decision and related changes that need to be made in response to the decision. This step may also include any testing that is required before fully committing to an action.

Figure 9 - The OODA Loop



Although OODA is a simple ‘counter-attack’ approach, each of the seven viable systems elements for the anti-fraud authorities can be examined using OODA to identify potential actions that could be taken by the anti-fraud authorities. The OODA counter-attack approach was stretched to consider societal, technical,

³⁷ Luft A 2020 *The OODA Loop And The Half Beat*, <https://thestrategybridge.org/the-bridge/2020/3/17/the-ooda-loop-and-the-half-beat>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

economic, and political means of counter-attack. The results of this analysis are summarised in Table 6 as a series of possible

Table 6 – Exploration Suggestions Arising From Viable Systems Theory Combined With OODA Loops

Viable Systems Model – Perpetrators	Viable Systems Model – Authorities	Potential Responses By Policy Makers
Feedforward - Targeting	Feedforward – Pre-bunking & Inoculation	<p><i>Societal</i></p> <ul style="list-style-type: none"> • Heighten authority trust levels through more frequent, less ‘messed’, contact with reliable facts and figures. <ul style="list-style-type: none"> ○ Ensure that the public is alert to the dangers of fraud: ○ Raise awareness of the rising threat; ○ Raise awareness of its origins - frame the threat as an attack by invaders; ○ Pre-bunk harmful memes; ○ Reduce and control digital footprints on social media. • Increase cooperation with various NGOs, e.g. Age UK or Friends of the Elderly (good example here with City of London Police - https://www.citybridgetrust.org.uk/what-we-do/strategic-initiatives/age-uk/), or mental health charities.
		<p><i>Technical</i></p> <ul style="list-style-type: none"> • Attack dark web marketplaces to stop email, card number, and other illegal data sales. • Mandate the tagging of emails emanating from highly suspicious regions abroad. The metadata in email headers allows Internet Service Providers (ISPs) to identify the origins of email traffic, or to flag traffic where this data is missing.
		<p><i>Economic</i></p> <ul style="list-style-type: none"> • Reduce target attractiveness - make British citizens less attractive targets for fraudsters by increasing the ‘cost of doing business’ in the UK: <ul style="list-style-type: none"> ○ Reduce the range of opportunities for fraud; ○ Reduce the potential rewards; ○ Increase the probability of being caught; ○ Increase the probability of conviction; ○ Increase the penalties including confiscation; of assets and long custodial sentences.

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<ul style="list-style-type: none"> • Mandate data breach insurance so that breaches are an integral part of corporate risk manage <p><i>Political</i></p> <ul style="list-style-type: none"> • Record direct usage of government registers, e.g., electoral roll or Companies House for collecting information. • Revive the idea of registered and audited sets of Uniform Resource Locator (URL) suffixes. Nominet enforces the registration of .ltd.uk URLs to private limited companies (which would assumed to be registered at Companies House) and would let consumers know whether the firm they are interacting with is British and is subject to UK law. Wider promotion of .uk style domain approaches and registrations should tie organisations to government-validated registers, e.g., Her Majesty’s Revenue & Customs (HMRC) for customs documentation, Driver & Vehicle Licensing Agency (DVLA) for vehicles, Department of Work & Pensions (DWP) for pensions, etc.
<p>Input – Contacting & Engaging</p>	<p>Input – Detection & Blocking</p>	<p><i>Societal</i></p> <ul style="list-style-type: none"> • Promote two-way identity proof as the norm for all transactions. • Create fraud ‘weather reports’ using predictive engines, identifying the types of fraud that are likely to increase and their countries of origin. This information should be shared internationally and used in public information campaigns. • Create proactive defences such as ‘white hat’ ‘spear phishing’ attacks. <p><i>Technical</i></p> <ul style="list-style-type: none"> • Zero-tolerance for phone call non-identification, (with exceptions for legitimate uses such as the Police, GPs, etc.) and abuse of mass marketing registries - if they can’t contact them by phone fraudsters may fall short of victims. • Enforce current systems such as The Telephone Preference Service (TPS) effectively – mandate ‘opt in’ clause for customers for all service providers, so that customers are automatically added to TPS unless they ask not to be. • Block mass marketing calls from non-UK numbers. Impose performance reporting on service providers and penalise under-performance. • Consider adding a call sequence service on phones, e.g. “*1” that reports a spam or fraud call. This can be used in real-time to close down calls emanating

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<p>from the spam or fraud callers. This would need consideration of side effects, e.g., reporting by accident or maliciously to harass people or to mislead providers. Something similar exists for text messaging - forwarding the text to 7726 works across providers.</p> <ul style="list-style-type: none"> • Consider adding an automatic URL reporting services for fraudulent sites. URL-Vigilante.com? Such crowdsourcing approaches would rapidly build databases. Browsers could be configured to block reported sites using levels of reporting to determine risk tolerances. OSINT can use the reporting database for analysis and prosecution. Email systems could use this service in their spam blockers. There would be issues with false reporting, as occurs on Amazon with competitors giving false ratings to each other. • Work to reduce advertising fraud, another mechanism for recruiting victims. Consider requiring the identification of all online marketing ads traced to the company paying for them.
		<p><i>Economic</i></p> <ul style="list-style-type: none"> • 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, and providing a validation link back to their certificates. • Consider a ‘reverse phone charge’ system. An individual can trigger a reverse phone charge with a call sequence service on phones, e.g. “*2”, and an amount would be charged. Spammers would have to seriously curtail random calls or wind up paying significantly for them. In a richer system, individuals might be able set a sum, e.g. between £0.01 and £10.00 for the charge, which would be available in advance to systems. In a very rich system, people might publish the sum they would expect to be paid to take a call from any new number.
		<p><i>Political</i></p> <ul style="list-style-type: none"> • Government identity ‘infrastructure’ system (not necessarily ‘government identity cards’). Digital ID infrastructure – while seen to be a ‘third rail’ in the UK after the 2006 ID card debacle,³⁸ as well as many subsequent attempts, virtually everyone looks to

³⁸ https://en.wikipedia.org/wiki/Identity_Cards_Act_2006

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<p>government infrastructure support for personal and business identity. Infrastructure support does not necessarily mean the government actually providing personal or business identity, rather setting out standards for inter-operability and using the infrastructure itself.</p> <ul style="list-style-type: none"> Smart ledger ID systems exist, Estonia is one example, as well as numerous other ‘infrastructures’ where identity is verified, secure, and controlled by the owner, who can choose which elements of their identity they wish to share (e.g., address, nationality, qualifications, health record, bank accounts details, etc), and even set one-time use parameters for authorised users.^{39 40}
Process – Convincing & Transferring	Process – Interference & Trapping	<p>Societal</p> <ul style="list-style-type: none"> ‘Nudging’ two-factor and biometric authentication. Encouraging people to warn others when they themselves have been defrauded. Call five friends, go onto social media, to reduce the ‘embarrassment’ factor. On authorised push payment fraud, adding the 36 banks that are Direct Connect (DC) to the Faster Payments Scheme, 100% banks using instant payments will be covered as they use DCs as agents, for example, Pay Pal uses Barclays.
		<p><i>Technical</i></p> <ul style="list-style-type: none"> Metaverse ‘officers’, human and AI. Mandate full compliance by payment providers with Confirmation of Payee. Promote widespread use of e-signatures to encourage less paper and more process standardisation.
		<p>Economic</p> <ul style="list-style-type: none"> Implement a scale of cooling off periods for financial transmissions, e.g., two day minimum holding time plus one day per £x,000. These should be easily reset by consumers to levels and times appropriate to them. Timing and limit restrictions on overseas credit card usage.
		<p><i>Political</i></p> <ul style="list-style-type: none"> Create supra-national ‘closing down’ teams.

³⁹ Shumsky P 2019 *How to Enhance KYC Systems With Blockchain*
<https://www.finextra.com/blogposting/18914/how-to-enhance-kyc-systems-with-blockchain>

⁴⁰ example only - Z/Yen IDChainZ, <https://www.chainzy.com/products/idchainz/>,
<https://www.zyen.com/publications/public-reports/be-have-know-smart-ledgers-identity-authentication/>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<ul style="list-style-type: none"> Work out how recovery proceeds should be apportioned to agencies and back to victims.
Output – Obfuscation & Escape	Output – Prosecution & Recovery	<i>Societal</i> <ul style="list-style-type: none"> Encourage more active use of transaction-by-transaction notification.
		<i>Technical</i> <ul style="list-style-type: none"> Target finding large-scale activity and/or energy-consuming hot spots in the UK, e.g., large scale emails, large quantities of suspicious processing.
		<i>Economic</i> <ul style="list-style-type: none"> Slow banks down on multi-account transfers between institutions. Encourage discussion with regulators about ‘fixed fines’ – in line with indemnities, getting regulators to provide a pre-determined scale of fines, e.g., £1,500 per poorly on-boarded client, would encourage better information sharing and also permit robust cost-benefit analysis. Adjusting the fines over time would be a more subtle regulatory tool in line with risk-based compliance. Work with the insurance industry on ‘restitution’ insurance, especially terms & conditions and information sharing. Restitution insurance conditions would aid in spreading best practices, help industry work together, and alleviate some of the monetary damage from fraud.
		<i>Political</i> <ul style="list-style-type: none"> Government and/or ISP automatic tagging, e.g., banners, of emails emanating from highly suspicious regions or URLs abroad. Consider working with HMRC on targeting tax inspections on people who have large numbers of personal transfers to their personal accounts, i.e., a higher probability they might be large-scale fraudsters or connected to them (e.g. their mules) taking monies directly. Consider requiring financial institutions to report application details of all those whom they reject accounts.
Feedback – Consolidating	Feedback – Sharing lessons	<i>Societal</i> <ul style="list-style-type: none"> Encourage reporting of frauds. Provide timely and transparent reporting to victims.
		<i>Technical</i> <ul style="list-style-type: none"> Provide private sector with OSINT tools such as inbound internet traffic analysis for the UK as a

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

		<p>whole, or cryptocurrency tracing services to follow payment trails.</p> <ul style="list-style-type: none">• Consider cooperating with OSINT community for national anti-spam AI systems, even competing AI systems. Of note is the US Treasury Financial Crimes Enforcement Network using hackathon/Sprint techniques on anti-money laundering (AML) - FinCEN's TechSprints and Events FinCEN.gov. <p><i>Economic</i></p> <ul style="list-style-type: none">• Shift the balance of liability for fraud from the consumer to shared liability with financial services institutions. 2017 research by Beker et al found that when a customer reports fraud, “a common approach of the bank is to request that the customer answers a checklist of whether they complied with security recommendations taken from the bank T&Cs [Terms & Conditions]. This advice includes recommendations that never appear in bank publicity, and even contradict advice from banking trade bodies... This creates a climate of expectation in which a court or Ombudsman will be tempted to run through the checklist, in effect asking the customer to prove they were not careless... The exceedingly onerous UK bank T&Cs are particularly worrisome in this context.” Possible actions to rectify this imbalance and encourage action include:<ul style="list-style-type: none">○ A judicial review of banking T&Cs relating to fraud and the development of consumer-oriented standards would encourage banks to take a more proactive approach to reviewing their customer protection security systems and educating their customers on the dangers of fraud.○ Creating a duty of care in law for social media platforms could allow consumers to take civil action against platforms that fail to discharge that duty by taking prompt action against fraudulent adverts.• Remove obstacles to private sector information sharing, particularly liability.• Examine closely fiat-to-crypto and crypto-to-fiat conversion zones, especially regulation of exchanges. Note that TSB refuses customer interaction with exchanges.⁴¹ <p><i>Political</i></p>
--	--	--

⁴¹ <https://www.tsb.co.uk/fraud-prevention-centre/>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<ul style="list-style-type: none"> Working with multi-lateral institutions, e.g., OECD, BIS, publish very regular, e.g., monthly, international fraud comparisons. Implement ‘ultimate beneficial ownership’ register (UK government policy), zero tolerance for Londongrad, e.g., eliminating Scottish Limited Partnerships, enforcing AML to reduce British profile, enforcing ‘unexplained wealth orders’.
<p>Monitoring – Reporting & Improving</p>	<p>Monitoring – Reporting & Improving</p>	<p><i>Societal</i></p> <ul style="list-style-type: none"> 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. Publish statistics on nation-by-nation originated internet traffic to the UK, highlighting anomalies.
		<p><i>Technical</i></p> <ul style="list-style-type: none"> 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? Using accreditation – International Standards Organisation (ISO) approaches and kitemark(s) such as those accredited by the United Kingdom Accreditation Service could be an aspiration for firms want to meet account opening and service standards. This approach was taken by www.fairbanking.org.uk on bank accounts that were fair and trustworthy. A more basic offer might be to encourage the sharing of ‘how to’ processes to move towards a better understanding of good practices;
		<p><i>Economic</i></p> <ul style="list-style-type: none"> Work with insurers on setting notification times for claims beyond which fraud is not covered, speed up reporting times. Work with the ONS, and OECD, to create a set of reliable national fraud statistics, incorporating for the UK at least NFIB, Action Fraud, UK Finance, and Cifas. Consider extending the Financial Fraud Research Center at Stanford taxonomy of fraud across all UK reporting and work to develop yet stronger international taxonomies and reporting standards. Enhance information sharing between anti-fraud authorities and financial service providers, particularly anonymising information sharing and reducing liability issues for firms reporting data.

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<ul style="list-style-type: none"> Suspicious Activity Report (SARs) feedback – encouraging law enforcement officials to provide more feedback on which SARs help and which don't, including perhaps a testset of 'good SARs' and 'bad SARs'. In August 2019, Jim Richards, former global head of financial crimes risk management for Wells Fargo usefully asked – “Can we produce fewer alerts and have it cost less and investigate fewer cases and file better SARs? The answer to that is maybe — but we don't know what a better SAR is”.
<p>Governance - Evolve</p>	<p>Governance - Evolve</p>	<p><i>Political</i></p> <ul style="list-style-type: none"> Developing further the NFIB Cybercrime and Fraud Dashboard to expand functionality and enhance the range of queries that it can deal with.⁴² Daily publication of the national fraud situation, hot scams this week, recovery rates, recovery times, heat maps of failing financial institutions, failing retailers, etc. A 'Fraud Stoppers' show equivalent to 'Crime Stoppers'.
		<p><i>Societal</i></p> <ul style="list-style-type: none"> Consider support and encouragement for OSINT 'digital vigilantes' and/or 'bounty hunters'. Clearly a large number of issues implementing such schemes, but would increase resources and has been made to work on software bug bounties. <p><i>Technical</i></p> <ul style="list-style-type: none"> Set out a national approach to quantum-resistant encryption.⁴³ Anti-fraud 'meme machines' – dynamic anomaly & pattern response (DAPR) software can identify successful meme patterns and emerging anomalies, and then automatically craft responses to harmful memes countering them and reducing their impact on society. Set up automated genetic-algorithm AI penetration testers against fraudsters. Conduct technical challenges, <i>a la</i> DARPA or perhaps ARIA, where teams are given financial rewards for techniques that stop fraud. Consider integrating these approaches into an 'anti-fraud regulatory sandbox'.

⁴² https://cambridgeshireinsight.org.uk/communitysafety/topics/scams/nfib-fraud-and-cyber-crime-dashboard/#/view-report/ccbc9a17fb634ec7a831edc16acf2f4f/___iaFirstFeature

⁴³ <https://www.zyen.com/publications/public-reports/the-quantum-countdown-quantum-computing-and-the-future-of-smart-ledger-encryption/>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

		<ul style="list-style-type: none">Improving technical capabilities – As technology evolves, fraudsters find new ways to subvert it and turn it to their advantage. Particularly important jumps are indicated by X-Gen or trend terms, e.g., 5G, 6G, IR4.0, The Metaverse, IoT, AI (machine-learning), Big Data, quantum computing, cryptocurrencies, or NFTs may all become increasingly important over the coming decade. Anti-fraud authorities must enhance their capabilities and understanding to encompass new threats as part of their daily remit.
		<p><i>Economic</i></p> <ul style="list-style-type: none">Create a marketplace for the prosecution of frauds by independent, licensed firms.Encouraging discussion about ‘indemnity’ among certifiers – “If I use your certification documents and they turn out to be incorrect, how much obligation do you have towards me?” This could lead to discussions about mutual fault insurance;
		<p><i>Political</i></p> <ul style="list-style-type: none">Government timestamping services.Going further, perhaps a government messaging service with timestamping. The original Open Banking architecture had something similar, designed to be used so data was controlled by the user and handed across institutions with appropriate logging.All government documents issued electronically with government PKI certificates for checking, thus eliminating need for paper certification and reducing wasted bureaucracy.

7. Challenge Themes For The Next Decade (2023-2032)

Pulling together the scenarios, the narratives, the viable systems model, and the OODA action, this study would suggest the following set of challenge themes to guide the next decade's agenda. The challenges are best contextualised by viewing 'fraud as a service' that must be disrupted.

1. Measure & Manage Fraud Systematically

This study was unable to find evidence of the benefit-cost approach to fraud being applied rigorously in the UK. Such evidence would have provided for enhanced alignment between the anti-fraud expenditure and comparable anti-terrorism or anti-crime expenditures. Rigorous benefit-cost studies need to be conducted, in order for anti-fraud spending to be compelling and convincing. Establishing strong benefit-cost evidence would provide policy-makers and consumers with essential information in developing responses to reducing fraud. The clear assumption here is that fraud can be managed in ways similar to those of other crimes and other social problems, e.g., speeding offences, pandemics, or pollution.

This report is not a critique of current anti-fraud activity, but it is apparent that the scale of high-volume fraud against individuals has been growing outside the control of the anti-fraud authorities. Properly equipping such authorities with the staff, resources and tools to combat the increased scale of fraud should be considered a priority. The full specification of such management approaches is outside the scope of this report, but clearly mimics viable systems theory, i.e., setting out feedforward (targets and expectations), input (detection & blocking), processes (particularly multi-agency clarity), output (prosecution & recovery), feedback (data, intelligence, knowledge, and sharing lessons), and governance (ensuring progress towards zero-tolerance of fraud).

2. Automate Offensive & Defensive Tools For All Of Society

There are probably three stages to this challenge. The first is data, information, and knowledge sharing. Currently, the systems used to collect and collate data on fraud in the UK are inadequate. Data is subject to double or triple counting, has incompatible time series, and lacks a standardised taxonomy. Reported fraud only makes up a small fraction of fraud attempts. There is currently no attempt to record unsuccessful fraud. Recording and analysing patterns in these attempts are important as it enables real-time understanding of how the global

fraud landscape is evolving. The profiling of criminals engaged in large-scale mass-market fraud is in its infancy, and research should be commissioned to analyse these criminals, their organisations, their economics, and their motivations. Private sector financial institutions are reluctant to share detailed information on fraud, citing commercial confidentiality and data protection regulations.

The second is the use of OSINT in the area of fraud. OSINT has already proven its value in real warfare, so why not the war on fraud? There are many lessons to learn from the Open Source community, not least recognising that secure ICT systems, e.g., Linux, can be provided via open source techniques. There is a need to distinguish open-source tools from open-source intelligence, i.e. intelligence derived from open sources which may well be processed and analysed using proprietary tools

The third is a recognition that the anti-fraud authorities will have to commission and use large-scale, automated systems for offence and for defence. High-volume, real-time crime executed by machines will not be thwarted by detectives and paperwork after the fact. The scale of anti-fraud automation needed, as well as tips and techniques, are likely to be found in the Big Tech firms themselves.

3. Nurture Global, Grassroots Coalitions

It is clear that, in common with other areas of crime, e.g., domestic violence, a wider community of support is needed for victims, but also for intelligence and counter-intelligence, as well as action. A few areas for purposeful cooperation stand out:

- NGOs, national and international, and health authorities – who can help develop victim-oriented approaches, as well as provide vital intelligence;
- International bodies – time and again, high-volume consumer fraud is international. International cooperation is the cornerstone of the ability of UK anti-fraud authorities to pursue criminals across borders, stop them, and recover assets. Obviously, cooperation via international bodies such as Europol and Interpol is essential, but bi-lateral arrangements with regulatory and police authorities of high-fraud countries might make a difference. Countries that are not cooperating in international efforts to tackle fraud could be named and shamed, and sanctions, such as withholding aid, should be considered.

- International payment providers – the vast bulk of frauds are worthless without being able to remit the proceeds. Relationships with the payment and financial services industries are strained, not least as cooperation comes with an undertone of possible prosecution. Less capricious enforcement and fines of responsible organisations might make a very positive difference and inspire a culture of mutual benefit. After all, it is the interests of payment providers and financial services firms to have safe and trusted markets.
- Big Tech firms – as with payment and financial services firms, the Big Tech community too has safe and trusted online markets as a key enabler of doing business. Moreover, Big Tech firms have the skills and resources, if properly motivated and supported, to deliver many anti-fraud technologies as a ‘matter of course’ and globally.
- High-fraud nations – building cooperation and local capacity to reduce fraud ‘on the ground’ before it comes to UK shores.

4. Actively Provide A National Identity Infrastructure

There is a need to review and modernise the identity systems operating in the UK. The plethora of identity approaches leads to confusion about ‘normal’ processes for the public. Government identity systems, especially when associated with national ID cards, can be highly contentious. However, several uncontroversial steps could be taken which could remove anonymity from fraudsters and make it harder for them to operate. Equally, if norms of identity are established, then the public will come to be suspicious of those operating outside them. ISO standards and accreditation might play a large role here in encouraging take up and commercial evolution, as well as reducing the need for direct regulation.

Incentivising the development of common identity systems infrastructure for use by the general public and by government in relations with citizens. Further encouragement of social media platforms and others to require their use for full-service access would reduce identity theft and make the creation of aliases more difficult. One approach might be for government departments to lead in using an identity infrastructure. Further, although a great deal of media attention is focused on the sale of stolen information on the dark web, a great deal of personal information on citizens is held in state records that are freely accessible to criminals.

5. Grow A Victim-Oriented, Zero-Tolerance, Anti-Fraud Culture

At first, such a challenge theme might seem to be about public awareness campaigns. Campaigns are unlikely to be of much help, and more likely to be lost among the deluge of other campaigns. However, a longer-term goal can be to change the views of victims from being 'greedy idiots' to being genuine victims, harmed neighbours. A good example of such a change over time was the US gay community shifting from 'marriage as a right' to 'marriage denied separating true lovers'.

A crucial part of this culture change is having the anti-fraud authorities treating victims as they themselves would wish to be treated, in a compassionate and open manner. Feedback on the progress of prosecution and recovery needs to be improved drastically. Successes need to be celebrated. The public needs to be involved in helping anti-fraud activities. OSINT may well have a role here too in empowering people with the information they need to help make a difference themselves.

6. Evaluate & Evolve

During this study, it became apparent that some people believed fraud could be eliminated, though were unclear on the means. This study was conducted under the assumption that fraud is endemic. An analogy can be drawn with the cyber-community. Some still await a technical silver bullet. Others assume cyber-crime is with us forever. Those who think cyber-crime is endemic look to other endemic risks for solutions. For example, insurance has played a major role in the past in helping the nation to manage risk. Recall that: the development of fire insurance led to much better assessment and high standards leading to enormously reduced fire incidents; universal automotive coverage led to many fewer accidents and automotive thefts; workers' compensation cover led to many fewer injuries; and non-compulsory home and contents insurance led to many fewer burglaries. An assumption that seeking elimination is possible might not have led to these solutions.

In fact, there is a case that fraud is a necessary condition for improvement. Striving for improvement has led to increasingly intertwined and complex societal systems. Societal systems are messy, and some of that messiness makes us more vulnerable to fraud in the interstices. Yet, if societal systems were faultless, they might become unable to evolve or be creative when faced with novel problems. 'Peccadilloes that pay' do motivate some people to alter or bend the system. These people are rational agents breaking down information asymmetries and getting other people to reveal preferences that lead to

resource reallocation, albeit theft and other illegal acts. Still, perhaps there is a grey area between corruption and faultless sterility.

Economists, central bankers, and the public fear hyperinflation. Note that the current UK inflation target is 2% based on the Consumer Prices Index (CPI), not zero. Our fraud targets could be set similarly. Very low, but not zero. An anti-fraud culture though is wider than targets and law. The law firm Dickinson Dees once advertised, troublingly, "If it's legal - we'll do it!", implying that the ethical framework is identical to the legal system. Persaud and Plender disagree, "The nub of it is that much of finance is about promises whose fulfilment takes place over time. Those promises need to be sustained by trust, which cannot exist without an ethical framework."⁴⁴ Hyper-corruption and hyper-fraud lie on a far slipperier slope than hyper-inflation. The development of an ethical society lies far outside the scope of this study, but it is worth noting its importance.

In conclusion, some low-level fraud may serve a purpose of helping to inoculate our systems and make them more resilient. Recognising that fact is not inconsistent with zero-tolerance revulsion in hope of a better future. 'Fraud is good' only if it helps us to figure out what needs fixing, i.e., that we learn from it and strengthen our defences.

"The time to guard against corruption and tyranny is before they shall have gotten hold on us. It is better to keep the wolf out of the fold, than to trust to drawing his teeth and talons after he shall have entered."

[Thomas Jefferson, Notes on the State of Virginia (1787)]

⁴⁴ Persaud, Avinash D and Plender, John, Ethics and Finance, Longtail Publishing Limited, 2007, page 18.

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

APPENDIX 1 - Additional Sources

Author/Year	Title	Publisher
Levi M & Smith R	2021 <i>Fraud And Its Relationship To Pandemics And Economic Crises: From Spanish Flu To Covid-19</i>	Australian Institute of Criminology
NFIB	2021 <i>Fraud Crime Trends 2021</i>	NFIB
Davies G	2020 <i>Shining A Light On Policing Of The Dark Web: An Analysis Of UK Investigatory Powers</i>	The Journal of Criminal Law 2020, Vol. 84(5) 407–426
Lewis C	2009 <i>A Cross-Cultural Comparison Of Computer-Mediated Deceptive Communication.</i>	Pacific Asia Conference on Information Systems 2009
Boer A	2021 <i>No AI Risk If You Don't Use AI? Think Again!</i>	KPMG IT Advisory
HMICFRS	2020 <i>Spotlight Report A Review Of Fraud: Time To Choose</i>	HMICFRS
Buhring J & Koskinen	2019 <i>Beyond Forecasting: A Design-Inspired Foresight Approach For Preferable Futures</i>	Intellect ISBN 978-1-78938-136-8
Holkar M & Lees C	2020 <i>Caught In The Web - Online Scams And Mental Health</i>	Money & Mental Health Institute
Signifyd	2021 <i>State of Ecommerce Fraud in Europe How New Trends — Good and Bad — Will Shape 2022</i>	Signifyd
HMG	2021 <i>Economic Crime Plan, 2019 to 2022</i>	HMG
Experian	2019 <i>Helping Identify And Pre-Empt Financial Vulnerability</i>	Experian
Kemp S et al	2021 <i>Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During Covid-19</i>	Journal of Contemporary Criminal Justice 2021, Vol. 37(4) 480– 501
UK Finance	2019 <i>Fraud The Facts 2019 - The definitive overview of payment industry fraud</i>	UK Finance
UK Finance	2021 <i>Fraud The Facts 2021 - The definitive overview of payment industry fraud</i>	UK Finance
City Of London Police	2020 <i>Fraud Crime Trends 2019-20</i>	City Of London Police
College of Policing	2020 <i>Policing in England and Wales Future Operating Environment 2040</i>	College of Policing
Yaşar R	2022 <i>A Critical Overview of the Geometry of Fraud and a Model Proposal within the Framework of Situational Action Theory</i>	Muhasebe ve Finansman Dergisi – Ocak 2022 (93): 93-116
MOD	2018 <i>Global strategic trends - the future starts today 6th edition</i>	MOD
HOC	2021 <i>Banking fraud</i>	Briefing Paper Number 8545, 23 February 2021
Ringland G	2011 <i>In Safe Hands? The Future of Financial Services</i>	Long Finance

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

Becker I et al	2017	<i>International comparison of bank fraud reimbursement: customer perceptions and contractual terms</i>	Journal of Cybersecurity, 3(2), 2017, 109–125
Yang V	1998	<i>International Cooperation in Combating Fraud: Beyond the Treaties and Conventions</i>	International Symposium on the Prevention and Control of Financial Fraud Beijing, 19-22 October 1998
OECD	2012	<i>International Co-operation against Tax Crimes and Other Financial Crimes A Catalogue Of The Main Instruments</i>	OECD
ONS	2019	<i>Living longer: caring in later working life</i>	ONS
Levi M	2008	<i>Organized fraud and organizing frauds: Unpacking research on networks and organization</i>	Criminology and Criminal Justice December 2008
Adams J	1995	<i>Risk</i>	Routledge ISBN 0-203-49896-8
Home Office	2018	<i>The scale and nature of fraud: a review of the evidence</i>	HMG
Ringland G	1985	<i>Scenario Planning Managing For The Future</i>	Wiley ISBN 0-471-97790-X
Curry A	2008	<i>Seeing in Multiple Horizons: Connecting Futures to Strategy</i>	Journal of Futures Studies, August 2008, 13(1): 1 - 20
Beale M et al	2015	<i>Framework For A Taxonomy Of Fraud</i>	Stanford Center on Longevity
Wood H et al	2021	<i>The Silent Threat The Impact of Fraud on UK National Security</i>	RUSI
Fields L	2021	<i>The Penrose Review: Power to the Consumer?</i>	Oxera
Poppleton S et al	2021	<i>Who suffers fraud? Understanding the fraud victim landscape</i>	Victims' Commissioner
Beer S	1989	<i>The Viable System Model: its provenance, development, methodology and pathology</i>	Cwarel Isaf Institute
Nemr C & Gangware W	2019	<i>Weapons Of Mass Distraction: Foreign State-Sponsored Disinformation In The Digital Age</i>	Park Advisors
World Economic Forum	2021	<i>The Global Risks Report 2021 16th Edition</i>	WEF
Saleem W	2020	<i>Tackling Fraud In The UK - Successes, Shortfalls And Strategies For Improvement</i>	Birmingham University

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

APPENDIX 2 - Trend Analysis

Trend	Notes
I. Reduction In International Cooperation	The increasingly transnational nature of fraud means criminal gangs located overseas are increasingly involved in UK fraud. Without strong international cooperation ⁴⁵ and data sharing combatting these gangs becomes increasingly difficult and action against marketplaces becomes impossible.
II. Increased Volume Of Misinformation By State And Non-State Actors	The use of so-called “ <i>weapons of mass distraction</i> ” ⁴⁶ has become a feature of the information age. Aided by the algorithms of social media companies ⁴⁷ , certain state actors, adopt a “ <i>firehose of misinformation</i> ” ⁴⁸ strategy with little internal coherence or narrative. Extremist ideologies and conspiracy theories have proliferated, leading individuals down the rabbit hole of paranoia, isolation and distrust of ‘mainstream media’ and authority which makes them vulnerable to fraud.
III. Increasing Social Fragmentation And Tribalism	Globalisation, the decline of traditional industries and skill-biased growth have generated income disparities, that have resulted in social fragmentation (the adoption of increasingly incompatible social identities and values), which in turn have generated political fragmentation (the adoption of increasingly incompatible economic policies). The result of this fragmentation, when combined with the rise of social media, is the spread of mistrust in authority ⁴⁹ and the isolation of groups of the population in self-affirming echo chambers, all of which makes them vulnerable to social engineering and fraud.
IV. Inflation In Cost Of Basic Goods And Services	Financial difficulties increase the likelihood of mental health problems. People who have experienced mental health problems are three times more likely than the rest of the population (23% versus 8%) to have been a victim of an online scam. ⁵⁰
V. Global Recession	A global recession will act as an amplifier ⁵¹ for the majority of trends in this analysis, adding to economic hardship, driving evolutionary

⁴⁵ **UN 2003** *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>

⁴⁶ **Nemr C & Gangware W 2019** *Weapons of Mass Distraction* <https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf>

⁴⁷ **Wall Street Journal 2021** *Social-Media Algorithms Rule How We See the World. Good Luck Trying to Stop Them.* <https://www.wsj.com/articles/social-media-algorithms-rule-how-we-see-the-world-good-luck-trying-to-stop-them-11610884800>

⁴⁸ **Rand 2016** *The Russian "Firehose of Falsehood" Propaganda Model* <https://doi.org/10.7249/PE198>

⁴⁹ **Bright J 2018** *Explaining the Emergence of Political Fragmentation on social media: The Role of Ideology and Extremism* <https://doi.org/10.1093/jcmc/zmx002>

⁵⁰ **Money & Mental Health Policy Institute 2020** *Caught in The Web* <https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf>

⁵¹ **University of Portsmouth 2020** *With a coronavirus economic recession approaching, are we doing enough to deal with a new high in cybercrime and fraud?* <https://www.port.ac.uk/news-events-and-blogs/news/coronavirus-economic-recession-approaching>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

	pressure for fraudsters and exacerbating societal isolation and fragmentation.
VI. Continued Migration Of Retail Online	The continued migration of retail activity online may result in the creation of retail deserts ⁵² for certain communities, where traditional high-street retail outlets are scarce or absent. This will disproportionately affect poorer and older people, who will be forced online and may not have the knowledge, skills or technology to do this safely.
VII. Disruption To Employment, Redundancy Of Certain Skills And Business Models	Changes to traditional employment patterns, the rise of the gig economy and zero-hours contracts, technological disruption to skills and business models (e.g., retail) can result in increased uncertainty, financial pressure and mental health issues, all of which increase vulnerability to fraud. ⁵³
VIII. A Cashless Society	The pandemic saw a watershed in society's move to a cashless economy. UK Finance recorded a 35% drop in cash transactions in 2020 and according to research by Link ⁵⁴ Cash payments are likely to fall to as little as 10 per cent of all UK transactions within the next 15 years. The increase in the value of contactless payments to £100, may increase skimming fraud, and the lack of technical skills in older people, who may be uncomfortable with online banking, combined with branch closures may increase their vulnerability to fraudsters.
IX. Ageing Population	Statistics and projections produced by Office for National Statistics (ONS) have long shown that the UK's population is ageing. ⁵⁵ Older people are more vulnerable to fraud. ⁵⁶
X. Increasing Inequality	The UK is seeing a rise in debt and levels of arrears ⁵⁷ , caused by a range of economic and social factors including stagnating wages, rising household bills and an ageing population. Income disparities, as well as perceived racial and religious inequality can increase financial pressure and mental health issues and increase individuals' vulnerability to fraud. ⁵⁸
XI. Increase In Economic, Conflict And Environmental Induced Migration	Economic, environmental and political global events can drive population migration. Migrants, who may be unfamiliar with their host country's laws and have an experiential distrust of authority are

⁵² Schwuetz et al 2011 *Are Poor Neighborhoods "Retail Deserts"?*

<https://www.sciencedirect.com/science/article/abs/pii/S0166046211001128?via%3Dihub>

⁵³ Brooke C 2020 *Cybercriminals Take Advantage of Mass Unemployment in Phishing Scams*

<https://www.tessian.com/blog/cybercriminals-take-advantage-of-mass-unemployment-in-phishing-scams/>

⁵⁴ Ceeney N 2019 *Access To Cash Review* <https://www.accesstocash.org.uk/media/1087/final-report-final-web.pdf>

⁵⁵ ONS 2018 *Living longer: how our population is changing and why it matters*

<https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/ageing/articles/livinglongerhowourpopulationischangingandwhyitmatters/2018-08-13>

⁵⁶ AgeUK 2018 *Applying the brakes: Slowing and stopping fraud against older people*

https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf

⁵⁷ JRF 2019 *Dragged down by debt: Millions of low-income households pulled under by arrears while living*

costs rise <https://www.jrf.org.uk/file/58812/download?token=5uqtUprf&filetype=briefing>

⁵⁸ Experian 2019 *Helping Identify And Pre-Empt Financial Vulnerability*

<https://www.experian.co.uk/assets/ebook/financial-vulnerability-v2.pdf>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

	vulnerable to fraud and exploitation, and research in the US shows they may be less likely to report it or seek help. ⁵⁹
XII. Pressure On Social Care And Public Services	Pressure on public finances is increasing pressure on social care and public services which in turn can increase the vulnerability of individuals to fraud and reduce the range of assistance that they can seek if they have been a victim of fraud. ⁶⁰
XIII. Pandemics	Criminals turned to online and technology-enabled scams to exploit people’s fears about the Covid-19 pandemic. Although the probability of another pandemic within the next 10 years is low, it is not impossible. ⁶¹
XIV. Advances In Quantum Computing	Advances in quantum computing over the last ten years may compromise the security of public-key encryption algorithms if attackers have access to large quantum computers. ⁶² However, the technology still has a long way to go before it becomes a common consumer product, and techniques are already available to reduce public-key encryption algorithms vulnerability. Standards have already been developed to counter this threat (IEEE Std 1363.1 and OASIS KMIP)
XV. Advances In Technology And Interactions Between Technology And Society	<p>Current technological trends indicate that virtual reality, augmented reality and the metaverse are likely to become more widespread in their use and applications. VR headsets and the associated consumer electronics present a new attack surface⁶³ for hackers seeking to steal personal data and socially engineer frauds.</p> <p>There are two particular components to technological advances that pose potential threats. The first is consumer electronics, such as wearables, smart speakers, doorbell cameras, smart fridges and other IoT devices,⁶⁴ where design and smart features are given more consideration than security.</p> <p>The second is the continued advance of AI Fraudsters are already using AI to commit e-commerce fraud,⁶⁵ and have used AI to socially engineer the fraudulent transfer of funds.⁶⁶ A hidden threat may be evolutionary or “black box” algorithms - AI programs that ‘learn’ and re-write themselves to improve their efficiency. Without strictly</p>

⁵⁹ **UCSC 2022** *First nationwide study of scams targeting immigrants shows local social context may help or hinder reporting* <https://news.ucsc.edu/2022/02/immigration-scam-reporting.html>

⁶⁰ **Action For Carers Surrey** *Avoiding fraud and scams* <https://www.actionforcarers.org.uk/how-we-help/money-matters/managing-debt-and-avoiding-fraud/>

⁶¹ **Marini M et al 2021** *Intensity and frequency of extreme novel epidemics* <https://doi.org/10.1073/pnas.2105482118>

⁶² **Martin L 2022** *Is quantum computing the end of security as we know it?* <https://techbeacon.com/security/quantum-computing-end-security-we-know-it>

⁶³ **Mainelli M & Mills S 2022** *The Metaverse & Insurance - Pixel Perfect?* <https://www.longfinance.net/publications/long-finance-reports/metaverse-insurance-pixel-perfect/>

⁶⁴ **Norton 2019** *12 tips to help secure your smart home and IoT devices* <https://us.norton.com/internetsecurity-iot-smart-home-security-core.html#smart>

⁶⁵ **Bradley 2019** *How Fraudsters Use AI to Commit Ecommerce Fraud* <https://www.merchantfraudjournal.com/ai-ecommerce-fraud/>

⁶⁶ **WSJ 2019** *Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case* <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

The Future Of UK Fraud

Challenging High-Volume, Automated Crime

	defined ethical parameters, these algorithms may ‘learn’ that fraud is an effective way of meeting their objectives. The owners of these algorithms may be unaware that fraud is taking place, ⁶⁷ and may have no idea how to prevent it from taking place. ⁶⁸
XVI. Growing Digital Footprints	The growth of social media and online shopping means that almost every individual in the UK has a growing digital footprint. If a fraudster gains access to one element of our online identity, they may be able to hack multiple platforms to harvest data. ⁶⁹
XVII. Aging Security Systems	“Guess Attacks”, occur where an organised criminal gang works out a credit or debit card number and the expiry date. They don’t need to have stolen the card number in a hack or physical theft but use a bank card’s 16-digit card number and four-digit expiry date. This is possible as the first six digits of a credit card number signify the card network and the issuing bank, while the final digit is the Luhn algorithm checksum. ⁷⁰ That means they only have to guess seven numbers, while the final Luhn digit helps verify whether the rest of the card number is valid. The card verification value (CVV) usually printed on the back of the card can complicate matters, but there are websites (mostly outside the UK) which accept payment without a CVV, and some small businesses such as takeaway restaurants don’t always ask for the CVV. As a result this type of fraud is increasing in frequency ⁷¹ and is a good example of an aging security system being outpaced by fraudsters.
XVIII. Increase In Climate Change And Environmental Disruption (Flood, Drought, Storms And Wildfires)	The impacts of climate change are increasingly being felt in the UK through the increased frequency of storms, flooding, and other extreme weather events . As public uncertainty and anxiety grow fraudsters are likely to use this, coupled with rising energy prices, as a means to socially engineer opportunities for fraud.
XIX. Growth In The Power And Influence Of Big Tech Companies	Tech companies derive their power and influence from three sources and three spheres: economic power, technological power, and political power ⁷² – their economic power is well documented, growing from a cottage industry to dominance of the world’s stock exchanges in a matter of decades. Their technological power and political power are intertwined and are rooted in the algorithms that determine the worldview of participants in digital platforms.

⁶⁷ Coldewey D 2018 *This clever AI hid data from its creators to cheat at its appointed task* https://techcrunch.com/2018/12/31/this-clever-ai-hid-data-from-its-creators-to-cheat-at-its-appointed-task/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLnNvbS8&guce_referrer_sig=AQAAALUBLcV3BsJ6ccZCplih8gD6kb0_mqRwY7SJoHYCpiqN1Tk_aciigtWCY-hPIC_EsE6GkWdQQcTPnn_IBnYUpWwE0hBJNjrXDlqllqvprLTviiYdkOjx7KryqMMgxldk4D2WESO3PshBNuaKXaIlVhKukK_V7QwImxwEwAZ953gK

⁶⁸ McDowall B 2020 *Explaining The Inexplicable? Explaining Decisions Using Artificial Intelligence* <https://www.longfinance.net/news/pamphleteers/explaining-inexplicable-explaining-decisions-using-artificial-intelligence-machine-learning/>

⁶⁹ Cifas 2019 *Digital footprints online – what we leave behind* <https://www.cifas.org.uk/insight/fraud-risk-focus-blog/digital-footprints-online-what-we-leave-behind>

⁷⁰ Decode.fr *Luhn Number Checksum* <https://www.dcode.fr/luhn-algorithm>

⁷¹ <https://www.theguardian.com/money/2022/feb/26/credit-card-fraud-scammers-guess-attacks>

⁷² Swabey P & Harracá M 2021 *Digital power: How Big Tech draws its influence* <https://techmonitor.ai/boardroom/power-of-tech-companies>

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

	Increasingly, western democracies are viewing this stranglehold on information with alarm as the legal framework ⁷³ that enabled this growth has given tech companies power without responsibility and enabled the growth of misinformation and increased individuals' vulnerability to fraud.
XX. Divergence Between International Laws And Standards	Multijurisdictional regulations and standards and the increase in fraud within payments have created a difficult environment for payments providers ⁷⁴ . These issues may increase if regulation and standards continue to diverge.
XXI. Industrialisation Of Fraud	The anonymity the internet provides – and the speed at which criminals can adapt, has enabled organised crime rings methodically and systematically to leverage vast amounts of breached data to perpetrate financial crimes. There is some evidence that some of these gangs have the backing of rogue states or terrorist organisations ⁷⁵ .

⁷³ EFF Section 230 of the Communications Decency Act <https://www.eff.org/issues/cda230>

⁷⁴ McCaw M 2019 Regulatory divergence and presence of fraud causing pain within payments <https://www.paymenteye.com/2019/01/07/regulatory-divergence-and-presence-of-fraud-causing-pain-within-payments/>

⁷⁵ RUSI 2021 The Silent Threat - The Impact of Fraud on UK National Security https://static.rusi.org/the_silent_threat_web_version.pdf

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

APPENDIX 3 – Synopsis Of Common Frauds

Type	Description	Targets	Victims
Advance fee and lottery scams	With this type of scam, victims are asked to make a payment as ‘administration fees’ in return for a much larger sum of money or a lottery win.	Individual	Preys on all age groups
CNP Fraud	Fraudsters obtain debit or credit card details either through dark web marketplaces or using ‘guess attack’ (see trend XVII in Appendix 2) and use them to make unauthorised purchases from overseas websites or small traders, such as takeaways, that do not require CVV verification,.	Individuals	Preys on all age groups
Courier scam	This is a rarer scam as it is high risk and high investment for the fraudster. The victim receives a call from someone pretending to be from the bank or the police. They’ll pretend that they’ve spotted suspicious activity and claim your card needs to be replaced. They’ll convince the victim to call back on the bank or police’s real number. However, they’ll stay on the line, so the victim is still speaking to them. The victim will be asked for PIN or details of their accounts. Then the fraudster will send a courier to pick up their card, which they’ll be able to use because they’ve now got all the necessary personal information they need.	Individual	Preys on all age groups but most likely to affect older victims
Investment scams	Fraudsters comb shareholder registers of listed companies, which are publicly available and contact individuals to convince them to invest in bogus shares or assets boasting above market rates of return. Often firms running this type of scam operate from overseas but will have a UK business address to convince victims they are legitimate. The focus of the fraudulent investments varies, but recently many have focussed on cryptocurrencies and NFTs	Individual	Preys on all age groups but more likely to affect older and more wealthy victims
Invoice or mandate scam	This can take a number of forms. A common scam aimed at the catering sector is for a fraudster claiming to be a customer who has had red wine spilt on an expensive coat or handbag and is seeking redress for cleaning or repairs. The fraudster may impersonate a solicitor and have ‘evidence’ in the form of cleaning or repair invoices, purporting to be claiming redress for a client in an attempt to frighten the business owner in to paying a small sum, generally less than £500, rather than facing court action. When aimed at individuals or organisations, the scammer may intercept emails between a victim and the legitimate payee, such as a utility company or service provider and send an email	Individual, Sole Trader, Small company, Large Company, Public Sector	Preys on all age groups

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

	advising the victim details of changes to payment the account, these details belong to a fraudster, not the genuine company.		
Pension scams	These involve cold-calling and asking the victim whether they'd like to release cash from their pension or retirement savings before the age of 55. The fraudster transfer the funds to their account.	Individual	Preys on all age groups but more likely to affect older and more wealthy victims
Phishing, vishing and smishing	Phishing fraud , which occurs when a criminal attempts to get hold of personal information by sending out e-mails containing a link to a bogus website, which emulates a bank, utility company, or service provider. A victim who attempts to log onto the fake account has their information stolen and used by the fraudsters to empty their bank accounts or lock them out of the service. Vishing is used by fraudsters who phone their victims in an attempt to convince them that they are an agent of their bank, insurance company, utility company or other service provider. They extract information such and bank account details and pin numbers in order to illegally transfer funds. Smishing follows a similar pattern to vishing, but involves an SMS text message either asking you to respond with personal information, or directing you to a fraudulent website. During the pandemic fraudsters used a version of smishing known as parcel fraud, asking victims to pay excess postage or 'customs charges' on fictitious packages.	Individual, Sole Trader, Small Company	Preys on all age groups
Premium rate and telephone prize scams	Victims receive a letter, text or automated phone call telling them they have won a prize, but they need to telephone a premium rate phone line to claim it. The number to call is a premium rate overseas number the call lasts several minutes and costs tens of pounds. There is no prize.	Individuals	Likely to affect older victims
Property Scams	Although relatively rare, this type of crime is on the rise. They can take two forms – either as interception fraud, whereby the fees for a house sale are intercepted and diverted to a fraudsters account, or title fraud. Title frauds are mostly perpetrated on unmortgaged property - scammers obtain the title of the victim's property by stealing the victim's identity and changing ownership on the property title into their name. They will then typically take out loans secured against the property or even sell it. In 2020 the	Individuals	Likely to affect older and more wealthy victims

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

	Land Registry paid out a total of £3.5 million in compensation for fraud.		
Romance fraud	This often involves an individual encountering the fraudster online. A relationship is formed, which may be entirely virtual. Over many months the victim is slowly groomed by their supposed new partner. The scammer will gradually start to request money, often starting with small sums and then requesting larger and larger sums as time goes on.	Individual	Preys on isolated and lonely individuals
Safe account scam	This is similar to the courier scam, in so far as the victim is contacted by someone saying they are from the bank or the police. They'll tell the victim that their local bank branch is being investigated and will ask them to transfer your money to a "safe account" they have set up on the victim's behalf. The account will belong to a fraudster.	Individual, Sole Trader, Small company	Preys on all age groups but likely to affect older victims
Ticket scams	These work in a similar way to holiday or tour operator scams. Criminals set up fake websites selling tickets for popular events, such as concerts, plays and sporting events. Once a victim pays for a ticket, they're either sent fakes, or they never turn up at all.	Individual	Preys on all age groups but highly likely to impact younger, tech savvy individuals
Tour operator and holiday scams	Most holiday and tour operator scams take place online, with criminals setting up fake websites selling flights and breaks in the UK and overseas. Often these mimic the sites of well-known airlines or holiday companies, and it's only once the victim has paid that they discover their tickets never arrive, or that they are imitations. Other holiday scams involve fraudsters posting advertisements on trusted booking sites and then encouraging people to pay them directly rather than via the site for a holiday or accommodation that doesn't exist.	Individual	Preys on all age groups but highly likely to impact younger, tech savvy individuals and families
Work at home and business opportunity scams	Fraudsters advertise work opportunities that require few skills/qualifications but claim to provide above average financial rewards. The fraudsters secure monies through up-front fees to enable the victim to become involved, but, in reality, there is no paid work. Common jobs include stuffing envelopes, home assembly kits and home directories.	Individuals	Preys on all age groups, but most likely to affect those facing financial difficulties

APPENDIX 4 – Questionnaire & Webclave Synopsis

Questionnaire

A ‘sighting’ questionnaire was sent to an expert community and two think tanks⁷⁶ on 2 March. Three responses were received that helped inform setting the impact and likelihood of trends. A number of trend suggestions were also contributed. Among those that were not used was one exploring a dystopian UK, with a break-up of the four nations. This response highlighted a potential trend of lack of trust in the police, law enforcement, and rule of law which was not specifically included:

- Growing corruption in official circles and the power of influencers - reduction in satisfaction of those seeking remedies;
- Failure of policing at strategic national, regional and local levels - policing will not have the capability nor the numbers to offer a service that protects citizens in general and vulnerable sectors in particular;
- Likelihood of the continuation of a stuttering approach among the agencies in criminal justice - justice delayed, justice not done and citizen dissatisfaction. Unless organisations offering services recompense voluntarily or are forced to do so;
- Weakening of organisations like INTERPOL (questionable appointments) and EUROPOL (after Brexit) - quality of reputation of international policing agencies is in decline with serious implications for those defrauded

Other responses worth noting were sometimes stronger than those expressed in the scenarios:

- Wealth Distribution - gaps between the richest and the poorest cause increased friction leading to dysfunctional behaviours;
- Shortages of food and water - opportunities for scams in threat areas vital for life
- CBDCs - Cashless society - At what point in the future does the use of cash become an indicator of fraud in its own right? When do people stop trusting cash?
- CBDCs – Cashless society - The pandemic saw a watershed in society’s move to a cashless economy. UK Finance recorded a 35% drop in cash transactions in 2020 and according to research by Link cash payments are likely to fall to as little as 10 per cent of all UK transactions within the next 15 years. The increase in the value of contactless payments to £100, may increase skimming fraud, and the lack of technical skills in older people, who may be

⁷⁶ [CSFI](#) and [Cityforum](#)

uncomfortable with online banking, combined with branch closures may increase their vulnerability to fraudsters.

- Mental health - Financial difficulties increase the likelihood of mental health problems. People who have experienced mental health problems are three times more likely than the rest of the population (23% versus 8%) to have been a victim of an online scam.⁷⁷
- Underage computer users - Data shows an increasing use of technology by those under the age of 18. The vast majority of teenagers already have mobile phones and spend significant time on social media. There are rising rates of various types of mental health issues in children relating to the use of technology. Technology providers are not taking sufficient responsibility to address this issue and there is widespread evidence of children using systems 'underage' and the potential for children to be exposed to inappropriate or dangerous content. This create an environment in which children could increasingly become subject to financial exploitation.

Some longer responses worth setting out provide some colour:

- *On policing - "If a fraud victim in one of the 43 Police and Crime Commissioner jurisdictions in the UK reports a complaint at a local police station, he or she will generally find the service ill qualified to respond and the suggestion to report to Action Fraud made instead. When the claimant finds Action Fraud to be In-Action Fraud and goes back to the local police, he or she is likely to find that their concerns are not a priority to the local force because, for the most part, Police and Crime Commissioner's crime plans prioritise threats that are much more local and physical than those that are wider and digital. The reason for this is that the PCC prioritises the elements that help with re-election. To help in the future combatting of fraud and prevent damage to the citizen it would be worth examining what might alter such prioritization. What could be done to influence PCCs locally and make fraud a priority for them as a national group would provide an area worth study."*
- *On "Multiple Me" Synthetic Fraud At Scale - A world of quantum-enabled synthetic fraud, that is AI enhanced and Deep Fake supported: where virtual word equities (such as the Metaverse) are treated much like real world equities absent legal, regulatory, policing, cultural or policy/governance guardrails. Humans are encouraged to explore their interests by creating virtual versions of themselves and living alternative existence in different virtual worlds. Fraudsters exploit these various virtual worlds by faking identities faster than enforcement tools can monitor and take action.*

⁷⁷ <https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf>

Fraudsters exploit, steal and convert the currency created for these virtual worlds into various crypto currencies⁷⁸ and at times ransom entire worlds. Legally the metaverse becomes a wild west, short on legal frameworks and devoid of enforcement mechanisms.⁷⁹ Conflict in these worlds play out in the human world as grievance transfers to the human daily lives of advanced metaverse participants. Aggrieved people seek out supporting technology to create multiple synthetic personae in the real world targeting those that inflicted real or virtual harm onto them in other worlds.

- *On Big Tech – “Tech companies derive their power and influence from three sources and three spheres: economic power, technological power, and political power – their economic power is well documented, growing from a cottage industry to dominance of the world’s stock exchanges in a matter of decades. Their technological power and political power are intertwined and are rooted in the algorithms that determine the worldview of participants in digital platforms. Increasingly western democracies are viewing this stranglehold on information with alarm as the legal framework that enabled this growth has given tech companies power without responsibility and enabled the growth of misinformation and increased individuals' vulnerability to fraud.”*
- *On Big Tech and Island Kingdoms – “Economic and political tensions between nations drive a divergence in technology systems used. Nations in the East such as Russia and China already limit access to many technology platforms used by the West and choose in various areas to ignore international policy or law. As these nations look to develop their own solutions to avoid ‘technology sanctions’ being used as a disincentive there is the potential for global ‘alliances of nations’ to emerge each of which relies on a set of polarised technologies developed within the group. At the same time large technology companies simultaneously create painful ‘exit costs’ for those wishing to move to a competitor driving the trend towards large oligopolies with ‘captured markets’. The individual citizen becomes ‘held hostage’ to their nation or technology provider, limiting their options/choice and or rendering them powerless. Individuals report issues such as fraud but nothing happens either because it is a “high-volume issue, small value” case or because those in charge wish to bury it (e.g., minor issue that is result of a*

⁷⁸ *Fraud Risk in a Cryptocurrency World.* <https://www.fraud-magazine.com/article.aspx?id=4295016816>. Accessed 9 Mar. 2022.

⁷⁹ *“Akin to the Wild West’: Attorneys Warn of Cybersecurity Concerns for Firms in the Metaverse.”* *Legaltech News*, <https://www.law.com/legaltechnews/2022/02/24/akin-to-the-wild-west-attorneys-warn-of-cybersecurity-concerns-for-firms-in-the-metaverse/>. Accessed 10 Mar. 2022.

The Future Of UK Fraud
Challenging High-Volume, Automated Crime

much bigger underlying issue) for the sake of their own (organisation or individual) interests.”

- *On climate change and energy demand – “As the world increasingly moves online the demand for computing power and IT hosting capability grows exponentially. The amount of electricity required to run the background IT infrastructure increases substantially as does the amount of emissions (heat and environmental) generated. Significant progression in alternative technologies for both energy generation and network hosting have not progressed fast enough and as the effects of climate change become increasingly felt by individuals, social pressure to limit and reduce the contribution made by IT infrastructure and data processing grows. Government, technology companies and other organisations are then forced to limit activity or usage compromising the ability to prevent, monitor and respond to fraud; in contrast organised crime continue to operate now illicit technology.*

Webclave

A webclave (an online interactive discussion) was held on 10 March to test the preliminary findings. Invitations were issued to an expert community and to selected individuals from Z/Yen’s, CSFI’s, and Cityforum’s networks of senior individuals with expertise and interests in fraud. Invitations were also issued to public sector stakeholders engaged economic crime programmes. 88 individuals registered. 51 attended.

Webinar ID	Date/Time	Duration	Attended
548-309-611	03/10/2022 04:00 PM GMT	1 hour 15 minutes	51
Attendee Details			
Organization		Job Title	
Withheld		Strategic Leadership Engagement	
Withheld		Head of Product	
Withheld		Product Analyst	
Withheld		London Angel Club Manager	
Withheld		Senior Policy Manager	
Withheld		Consultant	
Withheld		Director	
Withheld		MD	
Withheld		Generalist Adviser	
Withheld		Professor	
Withheld		CISI member	
Withheld		Senior Executive Assistant	
Withheld		Director	

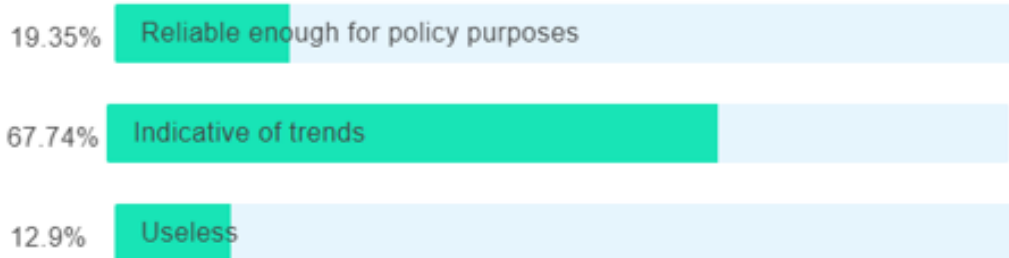
The Future Of UK Fraud
Challenging High-Volume, Automated Crime

Withheld	Director, Strategic Delivery Unit
Withheld	Content Manager
Withheld	Head of Marketing
Withheld	Professor in law
Withheld	CEO
Withheld	Risk Management Director (Financial Crime)
Withheld	Administrator
Withheld	Consultant
Withheld	Subject Matter Expert
Withheld	CEO
Withheld	Senior Lecturer
Withheld	CEO
Withheld	President
Withheld	Independent
Withheld	Manager
Withheld	Director
Withheld	Director-General, UK & Europe
Withheld	Group Head Of Secretariat
Withheld	Head of Press
Withheld	Director
Withheld	Director
Withheld	Investor
Withheld	CEO
Withheld	Senior Manager
Withheld	Director
Withheld	Dist. Prof & President CIA
Withheld	Head of Fraud Operations
Withheld	Director of Security
Withheld	Web Engineer
Withheld	Fraud lead
Withheld	Senior Financial Officer
Withheld	Director
Withheld	Researcher
Withheld	CEO
Withheld	External Affairs Consultant
Withheld	CEO
Withheld	Managing Director
Withheld	Director
Withheld	Past Master

Poll Responses During Webclave

1 of 3. How reliable are our fraud statistics?

Multiple choice with single answer



2 of 3. Which scenario best reflects your view of where we are headed?

Multiple choice with single answer



3 of 3. Please rate the challenge that resonates most:

Multiple choice with single answer



The Future Of UK Fraud

Challenging High-Volume, Automated Crime

Selected Comments

Police recorded crime data is of (very) limited value. Banks all work in silos and nobody is joining up the dots to provide information for action so the number victims continues to grow

If we record attempted (or other inchoate) frauds then surely we'd be swamped by highly ineffective 419s and such like, as with AML SARs. Surely proactive investigation against would be a more effective route (alongside international cooperation etcetera)

On Identity - the way identity (physical, virtual, digital) is being brokered is at the very core of many of these. Also, perhaps US has some slightly different categories that are more prevalent (e.g., Synthetic ID Fraud)

We've been doing our own counter fraud research at Clue, particularly around how technology is providing a solution to pressing pain-points in 2022, including proactive prevention and collaborative data sharing. We'll be releasing our findings in a whitepaper soon. If you're interested in receiving a copy, you can read more here: <https://clue.co.uk/counterfraud-panel/>

Reporting - the John Hopkins University Covid-19 dashboard shot to global fame. it pulled together data from across the world in a way that anyone could interrogate. Something similar for fraud could be helpful?

Does fraud correlate with economic cycles - e.g., downturns and recessions fraud rises, and vice versa?

It can seem to take forever with lots of hurdles for most people to open a new bank account. But fraudsters seem to be able to move money through accounts at will, and presumably have many to choose from. Why is that allowed to happen. Am not sure Susan's loneliness is able to be addressed easily, but surely this payment problem can be addressed more consistently.

Try the Danish solution where banks have liability for man in the middle attacks. A way forward? Recognises who has the capability and resources here.

About The Principal Authors

The authors would like to thank the many people who provided time and advice in interviews, on the webinar, and via email, as well as the Centre for the Study of Financial Innovation community.



Professor Michael Mainelli MStJ FCCA FCSI(Hon) FBCS, Chairman, Z/Yen Group

Michael is a qualified accountant, securities professional, computer specialist, and management consultant, educated at Harvard University and Trinity College Dublin with his PhD from LSE. Originally a research scientist in aerospace (rocket science) and computing (architecture & cartography), he became a senior partner of accountants BDO Binder Hamlyn and a director of UK Ministry of Defence research. During a mergers & acquisitions spell in merchant banking with Deutsche Morgan Grenfell, he co-founded Z/Yen, the City of London's leading think-tank, promoting societal advance through better finance and technology. Z/Yen is renowned for its Global Financial, Green Finance, and Smart Centres indices. Michael is a Fellow of Goodenough College, Honorary Fellow of King's College London, Visiting Professor at UCL's Bartlett School, and Alderman of the City of London for Broad Street. He was Sheriff of the City of London 2019-2021. His third book, written with Ian Harris, *The Price Of Fish: A New Approach To Wicked Economics And Better Decisions*, won the Independent Publisher Book Awards Finance, Investment & Economics Gold Prize.



Simon Mills BSc (Hons) MSc MPA, Senior Associate, Z/Yen Group

Simon began his working life as a field botanist in the Cloud Forests of Northern Costa Rica. His subsequent career encompassed minerals & highway planning and environmental management systems before he joined the City of London Corporation where he became Corporate Policy Manager and Head of Sustainable Development. Whilst at the Corporation, Simon worked extensively with the financial services sector on carbon trading, ESG, Smart Cities and Infrastructure Finance. In 2010 he was seconded to Defra where he was responsible for establishing the Local and Regional Adaptation Partnership before returning to the City. In 2016 Simon joined Z/Yen where he has worked with a range of domestic and international clients on mutual distributed ledgers, blockchain governance, standards, and green finance.



Z/Yen is the City of London's leading commercial think-tank, founded to promote societal advance through better finance and technology. Z/Yen 'asks, solves, and acts' on strategy, finance, systems, marketing, science, and intelligence projects in a wide variety of fields.

www.zyen.com

Z/Yen Group Limited
1 King William Street
London EC4N 7AF
United Kingdom

+44 (20) 7562-9562 (telephone)
hub@zyen.com (email)