Journal of Economic Criminology 1 (2023) 100012

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Understanding the rise of fraud in England and Wales through field theory: Blip or flip?

Mark Button*, Branislav Hock, David Shepherd, Paul Gilmour

Centre for Cybercrime and Economic Crime, University of Portsmouth, UK

ARTICLE INFO

Keywords:
Fraud
Trends
Vulnerabilities
Enablers

ABSTRACT

There is a debate at the highest levels of government and civil society over whether the rise in fraud is a blip exacerbated by the pandemic or a more fundamental transformation (or flip) in the structure of crime. This paper examines this debate by exploring the social factors influencing the level of fraud. It does so by conceptualising these factors as a fraud field, offering a novel way to visualise and consider vulnerability through the broad categories of 'threats' and 'safeguards' which influence levels of fraud. In doing so it offers the first attempt to map the wide range of 'forces' that influence levels of fraud and produces a mathematical expression of this, which will provide a basis for further debate, refinement and research. The threats include the myriad of opportunities, the large population of fraudsters, and the range of human and technology enablers that support the fraudsters. The principal safeguards that resist the fraud threat are culture, the law and the defensive resilience of individuals and organisations. Using the fraud field and official crime statistics, the paper argues that the safeguards are so structurally weak that the fraud epidemic is not a blip, but an opportunistic flip from traditional acquisitive crimes. The forces influencing levels of fraud mean high volumes of fraud will continue at the current levels or even accelerate further, unless there is a collective national strategy to strengthen the safeguards.

Introduction

A recent report by the prestigious international relations think tank, the Royal United Services Institute, described fraud as an epidemic that threatens national security (Wood et al., 2021). In stark contrast, a senior official responsible for the counter-fraud policy in a large government agency expressed to one of this paper's authors their frustration in failing to secure greater interest and resources from colleagues and politicians because of the prevailing perception that the recent rise in fraud in the UK is a 'blip', exacerbated by the COVID pandemic. In another illustration of the sanguine view regarding fraud, one of the authors of this paper was contacted by an undergraduate student from another university, who asked what they thought of their lecturer's view that fraud was just another moral panic. These views attenuating the fraud problem might not be representative, but the fact of such views in 'informed' opinion in the face of the overwhelming evidence of the substantial fraud problem illustrated by the Crime Survey of England and Wales, illustrates the need for further exploration and exposure of the problem. Differential rationalisation theory suggests this sanguine view is dangerous because it justifies inaction (Shepherd and Button, 2018). The political perception is partly informed by a marked fall in traditional crimes since the early 1990 s in the UK and other Western nations (Tonry, 2014). It is also subject to the manipulative politicalisation of statistics. For example, former Prime Minister, Boris Johnson announced to the House of Commons in January 2022 that "we have been cutting crime by 14 %" (HC Deb, 2022). He was subsequently admonished by the head of the UK Statistics Authority for failing to explain that the fall excluded fraud and computer misuse (Norgrove, 2022). Had Johnson included fraud and computer misuse, he would have had to announce a 14 % increase in total crime. These political machinations do, nevertheless, point to a very important question. Can the fraud epidemic be ignored as just another cyclical change in crime that will eventually decline or is it a permanent feature of 21st century British society?

The most marked fall within police recorded crime statistics in England and Wales is theft. The recorded crime rate for theft has declined 63 % from 4.1 million in 1993–1.6 million in 2022 (ONS, 2022a). This downward trend in theft is mirrored in the adult victimisation survey, the Crime Survey of England and Wales (CSEW), which recorded an 76 % fall from 11.8 million victims in

* Corresponding author.
E-mail address: mark.button@port.ac.uk (M. Button).

https://doi.org/10.1016/j.jeconc.2023.100012
Received 12 May 2023; Received in revised form 27 June 2023; Accepted 28 June 2023

1993–2.8 million in 2022 (ONS, 2022a). This collapse in crime rates has confounded criminologists, disrupted traditional theories and stimulated debate about its causes. Studies have offered unconvincing explanations including vague notions of cultural change, reduced childhood exposure to lead, increased abortion rates, increased policing, and stronger economies (Farrell et al., 2010). A BBC journalist described it as the "riddle of peacefulness" (Easton, 2013).

Knepper (2015) looked for clues in the research conducted by Edwin Sutherland and SK Ruck into the dramatic decline in crime rates in England following the Great War that emptied the prisons. Their work identified the economy, welfare, policing policies and penal policies as the likely explanations. Farrell et al. (2011) used vehicle security as a case study of situational crime prevention to attribute the decline in theft to the proliferation of improved security measures. However, both Farrell et al. (2011) and Knepper (2015) warned that the crime drop could be an illusion due to the absence of unmeasured internet-related crime and called for more research.

Although the crime opportunities presented by the internet have been recognised since its emergence (Baker, 1999), the analysis of trends in fraud and cyber-enabled fraud has attracted limited scholarly attention. There have been attempts to assess the impact of crises and recessions on the levels of fraud, but with mixed results (Dionne and Wang, 2013; Gill, 2011; Kemp et al., 2021; Levi and Smith, 2021). However, recent improvements in measuring fraud crime in the UK enables more meaningful analysis of longer term fraud trends. Firstly, the measurement of recorded fraud incidents improved with the introduction of the Action Fraud call centre in 2009 along with data collected from the financial sector; secondly, fraud victimisation has been included in the CSEW survey since 2016 (ONS, 2022a).

This paper uses these official statistics to examine whether the rise in fraud in the UK is a blip or a fundamental switch from traditional theft. In the sciences and social sciences the concept of forces influencing the path of objects and behaviours is well developed. This paper deploys a novel conceptual analysis inspired by Kurt Lewin's field theory to explore the forces that influence fraud (Lewin, 1951). In doing so it provides the first comprehensive overview of the different factors influencing levels of fraud at a societal level. The paper first examines the trends in acquisitive crime in England and Wales to illustrate the transition from theft to fraud. It then introduces the novel 'fraud field' model, a method to visualise and differentiate between factors favourable to fraud and factors unfavourable to fraud. It subsequently analyses the elements of the fraud field to argue that the current level of fraud is not a blip and it will remain a sustained epidemic without substantial collective action. The paper provides a significant contribution to the sparse literature on factors that influence levels of fraud, setting the foundations for future studies to further build and develop more sophisticated models of analysis.

Fraud trends

Although the police recorded fraud and theft crime statistics underestimate the aggregate levels of the crimes, they do illustrate trends in the offences brought to the attention of the police by individuals and organisations (Ariel and Bland, 2019). The CSEW provides more accurate estimates of fraud and theft to enable more reliable trend curves, but it only considers the victimisation of individuals (Ariel and Bland, 2019). There are no equivalent victimisation statistics for organisations. From Fig. 1, the 50 % fall in police recorded theft and the concurrent 63 % fall in CSEW theft since 2001 indicates its declining popularity as an illicit means of acquisition. On the other hand, recorded fraud has doubled following the introduction of Action Fraud, whilst CSEW fraud has overtaken theft. The gap between the CSEW and recorded fraud indicates that millions of victims are not reporting fraud crimes to the police. The implication of these official statistics is that acquisitive criminality has evolved, shifting from theft to fraud. Farrell et al. (2011) and Knepper (2015) were right to be concerned about unmeasured crime.

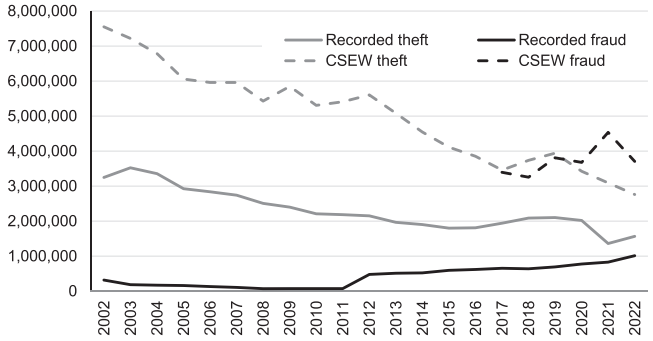

Fig. 1. Official fraud and theft statistics for England and Wales.

Although fraud against organisations continues to be a very significant gap in the official crime statistics, alternative research does provide strong clues. Regular surveys by the Association of Certified Fraud Examiners estimate the typical organisation loss at 5 % of turnover (ACFE, 2022), which is £224 billion/year based on the aggregate £4.5 trillion turnover of all organisations (BEIS, 2022). A sector analysis by the University of Portsmouth provides a similar result: it estimated the annual total loss by organisations in 2017 was £183 billion, 27 times the £6.8 billion loss suffered by individuals (University of Portsmouth, 2017). The implication is that even the new official statistics represent just a fraction of the amount of fraud perpetrated in the UK, which in turn means the unmeasured 'dark fraud' can be readily and conveniently ignored for administrative and political purposes.

The fraud field

Whilst the official statistics provide some insight into what is going on, they do not explain why. Research into fraud has considered a wide range of factors such as motivation, rationalisation and opportunity (Cressey, 1953), organisational climate (Greenberg, 1990), social learning in white-collar crime (Sutherland, 1940), vulnerabilities (Lee and Soberon-Ferrer, 1997), prevention (Tunley et al., 2018), law and policing (Button et al., 2022). These studies rightly focus on specific areas of interest, but they are rarely assembled into a coherent analysis. Button et al. (2018) pulled together several theories to attempt a more inclusive explanation for why people become corrupt. They listed seven factors which increase the likelihood of a person engaging in bribery, when a person:

is motivated by strains,
is at work,
is surrounded by noxious cultural messages,
is subject to weak external controls,
with a negligible chance of detection,
psychologically rationalises their actions,
and overcomes self-restraint controls.

However, this work focused on bribery in organisations, only briefly acknowledged wider cultural factors, and did not consider, for example, the law or law enforcement. The challenge in situating such research, including government statistics, within the broader scholarship has been the absence of a conceptual framework that facilitates a more holistic analysis. The model proposed for the present analysis is a substantial adaption of Kurt Lewin's field theory (Lewin, 1951). Lewin developed his theory as a way to analyse the range of personal and environmental interactions and forces that inhibit positive change, for example, in the relationship between partners (Burnes and Cooke, 2013). It has become known as the theory of change in analysing the forces within organisations that promote change and those that resist change (Swanson and Creed, 2014). Lewin was inspired by the rigour of mathematics to represent a person's life space by a field of forces and

their behaviour by a simple equation, which states that behaviour is a function of the person and their environment:

B = f(p,e)

Our fraud field theory borrows this mathematical idea to represent the quantity of fraud in any context as function of the forces in favour of fraud (threats, T) and the forces against fraud (safeguards, S). The quantity (F) can be any variable that conceptually characterises the scale of fraud: the number or rate of fraud incidents, offenders, victims, or financial value. As a percentage, it can represent the likelihood of victimisation or vulnerability to fraud. Thus, fraud is a function of the threat forces minus the safeguard forces:

F = f(T-S)

Presenting fraud as the outcome of two opposing force vectors helps to conceptually categorise factors based on their impact when they *increase*:

Threat field – *increasing* the threat force increases fraud

Safeguard field – *increasing* the safeguard force reduces fraud

Further, organising the fraud field in this way leads to an important hypothesis:

A change in a force causes the fraud quantity (or vulnerability) in a given context to shift over a period of time to a new steady state level.

The range (field) of threats and the range (field) of safeguards can be incorporated into the equation as required for the analysis. For example, the threat force increases fraud when the population of fraudsters (P), number of enablers (E), or the number of fraud opportunities (O) increase. On the other hand, the safeguard force reduces fraud when the strength of culture (C), law (L) or resilience (R) increase. Resilience refers to the defensive capabilities of potential fraud victims. Thus:

F = f(P,E,O – C,L,R)

Again borrowing from Lewin, these factors can be usefully visualised as sets of opposing forces within the fraud field (Fig. 2). The model is flexible in its application to any subject, which can be an individual, a community, an organisation, industry, government or nation. For instance, the model suggests that a business could reduce fraud by simply removing opportunities, for example, by withdrawing from a market. Alternatively, the business could increase the resilience force to overcome the opportunity force within that market, for example by introducing counter-fraud controls that close down the opportunities.

At the national level, the CSEW figures indicate that the current steady state level of fraud against just individuals is running at about 3.8 million incidents per year. Fraud field theory suggests this rate will not reduce without a change in the forces within the fraud field. The following sections consider each of the factors set out in Fig. 2 to assess whether there is any evidence of significant change in the fraud field to support the notion the UK is experiencing a blip in fraud.

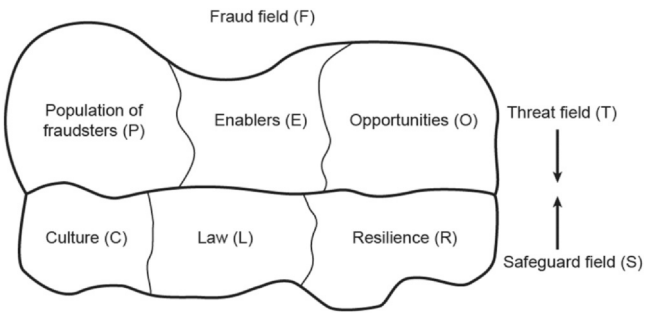

Fig. 2. The fraud field.

Threat field

Opportunities

The UK is a wealthy country with the sixth largest GDP at $3.1 trillion and is forecast to remain in sixth position for at least the next 15 years (Cebr, 2022). At £915 billion, the tax revenue is greater than the GDP of the Netherlands, ranked 17th in the GDP league table (House of Commons, 2023). The government's largest areas of annual expenditure are welfare at £260 billion and health at £168 billion (OBR, 2022). The adult population of the UK is 53 million (ONS, 2022b), of which 34 million are economically active employees earning wages (BEIS, 2022). There are 5.5 million businesses generating £4.2 trillion in sales (BEIS, 2022). 92 % of adults use the internet, rising to 99 % of those aged under 44 years (ONS, 2021), and 95 % use a mobile phone (Ofcom, 2022).

Just this sample of economic and social data illustrates the huge amount of money flowing through the economy, the high level of productive employment, high welfare expenditure and the saturation in technology engagement that all provide a vast number of opportunities for fraud. The UK's economic strength makes it an attractive target to both domestic and overseas fraudsters. Globalisation and the internet has made these opportunities accessible from anywhere in the world, thus significantly enlarging the population of fraudsters who target the UK. It also means UK businesses and travellers are exposed to opportunistic malefactors where cultures and laws are more tolerant to fraud.

Population of fraudsters

The most prevalent type of fraudster is the individual, the ordinary citizen who is motivated by need, greed or lure to exploit everyday opportunities (Karstedt, 2016). Karstedt and Farrall (2007) found that the majority (61 %) of people in the UK have at some time committed at least one minor 'everyday crime' against businesses, such as stealing something from work, falsely claiming refunds or padding an insurance claim. They further found that a significant minority of the public is willing to engage in such everyday crimes: for example, 22 % of the public in England and Wales would consider padding insurance claims (Karstedt and Farrall, 2006; Button et al., 2016). The public sector is also a very frequent target: the latest social security data indicates that 18 % of approved claims by individuals for the Universal Credit benefit are fraudulent (DWP, 2022). As the victims of all the above crimes are organisations, very few, if any, appear in the official crime statistics.

Occupational or insider fraud is an ever-present threat to organisations because trusted employees have routine access to organisational processes and assets (Cressey, 1953; Wall, 2013). It is also a high volume problem because most employee frauds are low in value and remain undetected: transactional frauds below scrutiny thresholds within the expense, payroll, purchasing and payment processes do not attract attention. Larger organisations are the most vulnerable simply because they employ more people and process very high volumes of transactions. The threat is most acute in the 10,550 large private, public and charity sector organisations (greater than 250 employees) which employ half the UK workforce, 17 million employees (BEIS, 2022). Employee fraud costs these organisations an estimated 5 % of their turnover (ACFE, 2022). Yet, very few occupational frauds appear in government statistics because most are invisible and even when high value incidents are detected, employers rarely report them to the authorities (Button et al., 2022).

Organised crime groups operating abroad and in the UK see fraud as a business opportunity. They are habitual, high volume fraudsters who actively seek victims. The National Crime Agency in the UK estimates there are 69,281 individuals involved in Serious Organised Crime, which is up from 50,000 in their previous assessment (NCA, 2020, 2021). Many of the groups are polycriminal, but research has found that up to 45 % of frauds reported by the public to the police are perpetrated

by OCGs (Garner et al., 2016). This indicates that they are a major contributor to the CSEW fraud rate. They are involved in boiler room, consumer, identity, mandate and welfare frauds, and they often recruit individuals from sections of society not traditionally associated with crime, such as students, graduates and the middle-classes (Copes and Vieraitis, 2009; Shover et al., 2003; Vedamanikam and Chethiyar, 2020).

Traditional crimes like burglary are predominantly the preserve of locally based criminals, but globalisation and cheap modern communication means a fraudster does not have to leave home in order to anonymously target victims anywhere in the world. The recent Home Office fraud plan estimated 70 % of frauds originated abroad or had an international element (Home Office, 2023a). Globally active fraudsters operate as individuals, as loose associations, or within organised crime groups (Levi, 2008). They include romance fraudsters in Nigeria (Lazarus, 2018; Lazarus and Button, 2022; Smith, 2010), pet scams fraudsters in Cameroon (Whittaker and Button, 2020), technology support scams in India (Sheckels and Farer, 2018), and cyber fraudsters in Russia and Eastern Europe (Hall et al., 2021; Levi, 2008; Timofeyev and Dremova, 2022). These offenders, who are effectively beyond the reach of the UK authorities, are major contributors to the victimisation rates registered in the CSEW.

As Sutherland (1940) explicated and more recently (Tombs and Whyte, 2015), the most egregious offenders are often respected/legitimate corporations. The harm caused by a single white-collar fraud scheme can be huge, yet these kinds of fraud are rarely represented in the official government statistics (Reiner, 2016). For example, when Madoff Investment Securities collapsed in 2008, it turned out to be a $65 billion Ponzi scheme that had fooled 4800 wealthy clients, including banks, investment firms and individuals (Quisenberry, 2017). A year later, Stanford Financial Group was also exposed as an $8 billion Ponzi scheme with 18,000 victims (Zweifach and Khan, 2010). The mis-selling by UK banks of worthless or overpriced Payment Protection Insurance (PPI) for over 20 years cost tens of millions of borrowers £ 38 billion, which the banks were forced to refund (FCA, 2020). Such mis-selling followed on from a comparable scandal where banking customers were mis-sold endowment mortgages (Fooks, 2003). The financial crisis of 2008 was caused by unethical and fraudulent practices in the financial sector. The crash resulted in a loss of $17 trillion in household wealth in the US alone (Financial Crisis Inquiry Commission, 2011), and it forced the UK government to inject £137 billion into the financial system (Mor, 2018).

Enablers

As the essence of fraud is a dishonest communication, any skill, tool or device that enables communication also enables fraud. One of the most significant enablers is competency in the English language as it opens up many opportunities for overseas fraudsters to communicate with and defraud UK citizens (and the many other English speaking countries). As the following list illustrates, the huge advance in communication technologies over the past two decades has leveraged language competency to enable the high volume of frauds originating from the UK and across the globe.

- Landlines and mobile phones for boiler room mass marketing investment frauds (Shover et al., 2004).
- Emails and text messaging for phishing and 419 frauds (Button and Cross, 2017).
- Websites for selling fraudulent online services and products (Fonseca et al., 2022; Whittaker and Button, 2020; Whittaker et al., 2022).
- Dating websites and social media for romance frauds (Carter, 2021; Cross and Holt, 2021; Cross and Lee, 2022).
- Social media for phishing-enabled frauds, consumer scams, and investment frauds (Lee, 2018).
- Social media influencers for investment frauds and fake goods (Matza, 2021; Shepherd et al., 2021)
- The Metaverse threatens both new opportunities and new enablers for fraud (Smaili and de de de Rancourt-Raymond, 2022).

Along with the huge expansion in means of communication, it has also become easier to create fake credentials and identity profiles. At its simplest, virtually anyone can set up fake email and social media accounts online. High quality printers can replicate numerous types of identity documents to a high standard. Software produced by Adobe and others can be used to alter or reproduce official documents, and websites can be easily cloned. A fraud industry has emerged to service fraudsters with equipment, software and fake documents (Gupta et al., 2007; Matchin, 2020; Wang et al., 2022; Zahedi et al., 2015).

The dark web is an anonymous marketplace for the fraud-as-a-service industry, where criminals peddle the technical infrastructure and tools to execute mass attacks. The resources and activities marketed include personal credentials and banking information, templates of official and branded documents (bank statements, letterheads), equipment, specialist software, techniques, discussion forums, and even training (Gee et al., 2018; UNODC, 2021; Upadhyaya and Jain, 2017). The Russia-based Genesis Market had 80 million credentials for sale before it was taken down in 2023 by the combined efforts of police agencies from 17 countries (BBC, 2023; NCA, 2023).

New types of fraud have emerged from the toxic nexus between cryptocurrencies, greed, irrationality, and the lack of regulation. Cryptocurrencies have become effective enablers of money laundering, obfuscating identities and hiding the proceeds of crime (Janze, 2017; Kethineni et al., 2018). Some are gigantic fraud schemes. Even if it was not originally intended, some cryptocurrencies have followed Bernie Madoff's illicit path, turning into global Ponzi-like scams. Luna and its sister cryptocoin, Terra USD, collapsed in 2022 wiping out $60 billion (Forbes, 2022). FTX also collapsed in 2022 owing its creditors at least £3.1 billion (BBC, 2022). The cryptocurrency industry has become the latest technology enabler of huge scams.

The affinity group is a powerful enabler of structured social engineering and mass victimisation of group members by the trusted insiders. The infamous Madoff scheme was rooted in an affinity group of the rich and famous (Reurink, 2019). Modern social media marketing and affinity groups enable fraudsters to efficiently victimise large numbers of similarly minded individuals, who in turn unwittingly market the pyramid or investment scam to further victims (Bosley and Knorr, 2018).

Professional enablers include the unscrupulous professionals who deliberately facilitate fraud, those that turn a blind eye to it, and those who are unwittingly involved (Duri, 2021). They typically work in the financial sector and associated professions, for example, banks, lawyers, accountants, banks, estate agents, mortgage brokers, investment advisors. They provide three types of enabling roles. Firstly, they organise and facilitate fraudulent transactions; secondly, they organise and facilitate subsequent money laundering transactions; thirdly, as gatekeepers to the financial sector, they provide the appearance of respectability and trust (FATF, 2011; Levi, 2021).

The law firm at the centre of the Panama Papers exposure, Mossack Fonseca, worked with more than 14,000 banks, law firms, company formation agents and other intermediaries to set up shell companies for secrecy, fraud and money laundering purposes (ICIJ, 2017). UK intermediaries were amongst the most active of Mossack Foinseca's clients. HSBC was the most active bank of 50 bank clients, creating more than 2300 shell companies.

One of the most prodigious, yet unwitting, enablers of trust in the UK is Companies House, which maintains a public register of companies. However, because Companies House does not verify the information provided to it, the register has long been a target of criminal activity (Chennells, 2022). It remains to be seen whether the Economic Crime Bill, which aims to transform Companies House into an active

regulator with verification, investigation and enforcement, solves the problem (HM Government, 2023).

Safeguard field

Resilience

There are a variety of psychological, attitude and demographic factors that make individuals less or more resilient to fraud. However, victimology research into the characteristics of victims is conflicting, partly as it is an immature field in the context of cyber-enabled fraud, and partly due to inconsistent methodologies. Weak resilience of individuals is associated with low technology competency, low self-control, weaker risk perception, higher risk behaviours, high susceptibility to persuasion, and excessive confidence in one's own judgment (Chen et al., 2017; Deliema et al., 2020; Fischer et al., 2013; Schoepfer and Piquero, 2009; Whitty, 2019). Lower risk awareness, higher risk tolerance and a propensity to engage in deviant behaviours online all increase the likelihood of victimisation amongst younger adults (Holt and Turner, 2012; Shepherd et al., 2021). Older adults suffering cognitive decline and those living alone are also at increased risk (Boyle et al., 2012; Judges et al., 2017). All these very human factors compromise individuals' security behaviours and increase their vulnerability to all types of telecoms-enabled or cyber-enabled fraud (Cain et al., 2018).

An important body of research has used statistical techniques to correlate organisational features and structures with fraud resilience. They have typically focused on specific types of fraud, for example financial statement fraud or occupational fraud. Some of the characteristics linked to increasing vulnerability to fraud include:

- Poor governance (Beasley et al., 2000; Huefner, 2010; Law, 2011; Taufik, 2019).
- The construction of rationalisations to justify not implementing anti-fraud measures (Shepherd and Button, 2018).
- Inadequate anti-fraud controls (ACFE, 2022; Button and Gee, 2013; Holtfreter, 2004).
- Inadequate risk management (Mohd-Sanusi et al., 2015; Norman et al., 2010).
- Poor cyber-hygiene of organisations and their staff (Buil-Gil et al., 2021; DCMS, 2020; FSB, 2019; Kearney and Kruger, 2014; Kumaraguru et al., 2007).
- Organisational complexity which makes it easier to hide fraud and harder to detect (Arnold et al., 2012; Rispel et al., 2016; Suh et al., 2020; Toms, 2019).

Culture is a particularly difficult concept to analyse because it is a dynamic accumulation of many social factors and forces. For our purposes, culture represents the normative values and attitudes of a group towards fraud. The unit of analysis in the fraud field can be any social group: a community, organisation, industry sector, region or nation. Indifference is perhaps the most powerful cultural problem that permeates through all these areas of British society. Britons view fraud as one of the least serious crimes, less serious than anti-social behaviour and other non-criminal delinquency (Ipsos Mori, 2022). This collective tolerance helps to explain the discomfiting finding that the majority of UK adults are willing at some point in their lives to commit small frauds (Karstedt and Farrall, 2006, 2007), and why employee fraud aggregates to such a pervasive problem (ACFE, 2022). Attitudes in some countries are even more permissive (Ibrahim, 2016; Institute of Business Ethics, 2018; Lazarus et al., 2022), creating yet more space for everyday fraud to flourish. It also means that businesses and consumers are unprepared for different risks when dealing with overseas entities.

Similarly, the ethical climates of organisations vary from resolute intolerance of fraud to embracing it in their business models (Shepherd and Button, 2018). The strength of leadership, organisational structures, institutional attitudes, ethical values, and the treatment of staff all influence levels of fraud (Greenberg, 1990; Kumar et al., 2018; Law, 2011; Mars, 2019; Shepherd and Button, 2018). The failure of Enron shows how some organisational cultures facilitate fraud by ignoring it or actively encouraging it (Sims and Brinkmann, 2003). Siemens, for example, used fraud to fund 4283 bribes worth $1.4 billion (Berghoff, 2017). Volkswagen were able to manufacture and sell 11 million cars in the "dieselgate" scandal because, like Siemens, the company's compliance culture obliged employees to blindly comply with corrupt rules (Blackwelder et al., 2016; Mansouri, 2016). The collapse of the banking sector in 2008 due to endemic fraud in the mortgage market illustrates how low moral climates can become normalised across an entire industry (Financial Crisis Inquiry Commission, 2011). These examples of profit-motivated white-collar crime demonstrate the potential for catastrophe when a weak cultural force fails to resist the threat forces.

The law

Relative to the agile, innovative capabilities of fraudsters, the evolution of the law is glacially slow. Consequently, new threat forces appear unopposed by the force of existing legal frameworks. This is especially apposite with respect to the digital technologies. Unlike the traditional manufacturing industries, the digital industry habitually launches unsafe products (devices, applications, and platforms) without adequate consideration of the risk consequences. The behaviour of these new technology companies mirrors the dangerous practices of the old technology firms in the late 19th century and early 20th century that so concerned Sutherland (1949).

For example, the lack of industry regulation means that social media is awash with postings that promote fraudulent trading and investment schemes involving foreign exchange, binary options, and cryptocurrencies (Jones, 2021a). The Federal Trade Commission (2019) in the USA reported a tripling of reports of scams emanating from social media. The Financial Conduct Authority in the UK issued over 1200 warnings to Google and other social media platforms about fraudulent advertising of financial products (Makortoff, 2021b).

Telecommunication companies have been repeatedly criticised for not doing enough to tackle fraud against their customers. The Director General of the National Economic Crime Centre has called for phone companies to do more to prevent number spoofing (Whitworth, 2021). There is also concern about how easy it is to legitimately purchase SIM cards and SIM boxes to send scam texts (Matza, 2021). Cavaglierie (2020) further highlighted the lack of controls over SIM swapping, where a fraudster tricks the telecoms carrier into transferring a victim's number to their SIM card in order to capture credentials and access the target's online bank accounts.

Law enforcement

However good a law is, it is toothless without meaningful enforcement. Unfortunately, fraud is not a high priority for the police in the UK (Button, 2021; Her Majesty's Inspectorate of Police, Fire and Rescue Services [HMICFRS], 2019; Skidmore et al., 2018). It is poorly resourced with just 896 officers, equivalent to 0.6 % of all officers, and an additional 876 civilian staff dedicated to a crime which accounts for 40 % of all offences experienced by individuals (Home Office, 2023b). The politicians' own House of Commons Home Affairs Committee (2018, p. 26) concluded:

> "The proportion of fraud cases being investigated is shockingly low."

Consequently, the force of law enforcement currently offers lacklustre resistance to the forces of fraud, even less than it did 20 years ago. In 2002, 18,126 fraud offenders were convicted by the courts in 2002 including 3754 incarcerations (MOJ, 2007). In 2022, whilst 3.7 million frauds were experienced by individuals, just 3449 offenders were convicted and a mere 1152 offenders were sentenced to custody (MOJ, 2023). Thus, despite the observable rise in fraud, enforcement of the fraud laws has plummeted a full 80 % over two decades. In contrast, theft remains a high priority for the Criminal Justice System: 2.8

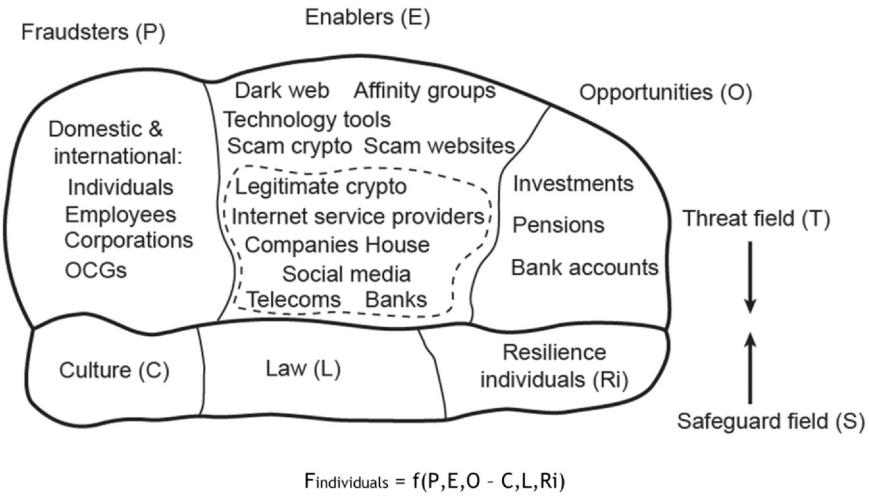

Fig. 3. Fraud field for individuals, Findividuals = f(P,E,O – C,L,Ri).

million individuals were victimised in 2022, 77,347 offenders were convicted, and 25,425 were imprisoned (MOJ, 2023). The current unprecedented attrition rate means that fraudsters are less likely than ever before to be apprehended or prosecuted, which partly explains why fraud is a rational alternative to theft and, more importantly, why the deterrence force of the law is so weak.

The fraud field in flux

From both conceptual and practical perspectives, an important feature of the fraud field is that it is in flux. Whenever innovative policies or technologies come along, new threat forces are loaded onto the existing, and typically inadequate, safeguards. Globalisation, the internet, novel communications and new transaction technologies are the most obvious disrupters, enabling both the scale and reach of fraud. At the local level, new opportunities for fraud appear whenever an organisation launches new products or services, enters new markets, or expands its workforce.

Businesses, for instance, have always been challenged by the threats of cheating employees, competitors, suppliers and customers. Indeed, in the absence of adequate safeguarding obstacles, employees still remain the most prevalent threat to organisations. However, the advent of online shopping brought new, unforeseen threat forces such as fraudulent consumer returns, which boosted the steady state level of fraud against US retailers by nearly $8 billion per year (Zhang et al., 2023). The retailers had failed to understand that new opportunities enabled by the policy shift from in-person to online returns would stimulate an increase in abuse by ordinary people living in a culture that tolerates everyday fraud. Had the retail industry considered the dimensions of the fraud field prior to implementing the new procedures, they could have anticipated the foreseeable threat forces and reinforced their resilience safeguards.

The public sector also fails to adequately consider the fraud field when implementing new policies. The full roll out of the Universal Credit (UC) social security system in the UK began in 2016. With simplification and efficiency in mind, UC replaces six different types of benefit and claims are submitted through an online system. Like the retailers, the government did not appreciate that online transaction systems are powerful stimulators and enablers of fraud because ordinary people are more likely to lie to a computer than to a person (Button and Cross, 2017). As a result, 18 % of UC claims are fraudulent and the roll out of the benefit to 5.7 million claimants has nearly quadrupled the overall rate of welfare fraud from 0.8 % in 2015 to a new steady state level of 3 % in 2022 (DWP, 2022). Annual losses have risen from £1.3 billion to £6.5 billion, the highest on record, 80 % of which is from UC (£5.25 billion). Having failed to design resilience into its systems, the DWP is now hiring thousands of additional counter-fraud staff to strengthen its resilience force (Markson, 2022).

Responsibilisation and collective action

The fraud field paints a distressing picture of an array of forces in favour of fraud which far outweigh those in opposition. The culmination of these forces suggests fraud is far from a 'blip', it is a 'flip' with the preponderance of forces pushing fraud. The attitude of those that see fraud as a 'blip' is symbolic of the collective failure to recognise the strength of the threat field and the weakness of the safeguard field. This communal myopia is the corollary of a cultural indifference that normalises everyday fraud by ordinary people (Karstedt, 2016). Fraud field theory states that the strength of the threat forces will not mysteriously atrophy, and that shifting the level of fraud in a given context to a reduced steady state level can only be achieved by action that strengthens the safeguard forces.

The fall in theft provides important clues to the type of action required. The decline is attributed to a securitisation strategy based on situational crime prevention techniques (Farrell et al., 2011). Vehicle manufacturers produced enhanced security systems; windows, doors, locks and alarm systems for premises now conform to higher standards. Stimulated by policy and regulation, this strategy involved collective action by industry actors for the public good (Hock, 2020; OECD, 2020): standards organisations, insurance companies and manufacturers. As a result, both organisations and individuals are more protected. Although an unintended consequence of the collective action against theft is the substantial displacement of acquisitive crime to fraud, the lessons can be applied to fraud.

Consider the idealised fraud field with regards to individuals in Fig. 3. Although education and enhancing skills is important in developing the resilience of individuals, it is not feasible to expect 53 million adults to reliably safeguard their investments, pensions and bank accounts against the global population of cunning, innovative, technology-enabled fraudsters, who are supported by an industry of malicious, indifferent or unwitting enablers. It is not reasonable to expect 53 million people to reliably discern between dishonest and legitimate communications. Although law enforcement should be far more active in deterring serious, habitual and organised fraudsters, it is also wholly unreasonable to expect the police to arrest the problem away. Like the anti-theft securitisation strategy, the fraud safeguard field needs collective action by large organisations, entities with substantial resources and capacity. It especially needs the technology and transactional organisations which enable fraud to take responsibility for the resilience vacuum. This approach would exploit a distinctive feature of fraud, that most frauds at some point touch organisations: welfare, tax, customer,

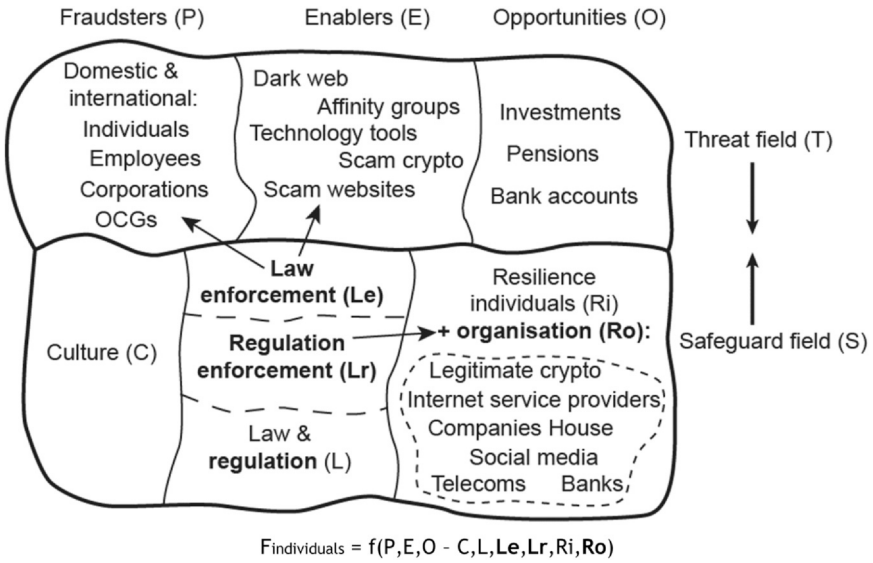

Fig. 4. Collective action impact on the fraud field for individuals. Findividuals = f(P,E,O – C,L,**Le**,**Lr**,Ri,**Ro**).

supplier and employee frauds victimise organisations; the telecoms, technology and banking industries enable frauds.

A core cultural and utilitarian debate sits at the heart of the resilience vacuum. For example, American technology, telecommunications and financial firms argue that they are not responsible for how people use their products, and increased regulation would choke the economic and social good their innovations provide (Economist, 2012; Kaal and Vermeulen, 2017; Smith and Van Alstyne, 2021). This Silicon Valley attitude is supported by US law, Section 230 of the 1996 Communications Decency Act (CDA), which provides online services with 'safe harbour' immunity against liability for material published by users, and is regarded as the pillar of free online speech that enabled the internet (Morrison, 2023). Prompted by regulation, the manufacturing sector has long since crossed this cultural barrier with respect to security and safety. For example, the United Nations first introduced harmonised vehicle safety regulations in 1958 (ECE/TRANS/WP.29/2016/2) and the ubiquitous 'CE' safety mark regulation was implemented in the European Union in 1993 (Council Decision 93/465/EEC). As a consequence, it is now well-established practice for manufacturers to conduct risk assessments and design safety features into their products in *anticipation* of consumers using them badly. They embrace the commercial imperative of increasing the resilience of their products by designing out the risk of abuse, a design philosophy the technology firms have yet to learn.

However, the responsibilisation agenda is moving in a positive direction with respect to economic crimes. Recent laws in the UK oblige corporations to engage in private policing in order to prevent bribery (Bribery Act 2010), to prevent money laundering (Proceeds of Crime Act 2002 and subsequent Money Laundering Regulations) and to prevent tax evasion (Criminal Finances Act 2017), whilst the Online Safety Bill currently passing through parliament aims to 'force social media platforms to remove all illegal content' covering a range of behaviours including fraud (HM Government, 2022), and the Economic Crime Bill will empower Companies House to be an active regulator (HM Government, 2023). Furthermore, the banking sector in the UK has recently introduced the Contingent Reimbursement Model (CRM), a voluntary code for reimbursing victims of authorised push payment (APP) fraud (Payment Systems Regulator, 2023). It is akin to insurance in that the cost of victimisation is shifted from individuals to the banks, thus incentivising the banks to invest in the resilience force of their products, which then leads to stronger protections for both themselves and their customers. The CRM policy in effect relocates the banks from the enabler field to the resilience field, from enabler to disabler. Similarly, encouraging industries as well as passive regulators like Companies House to change their mindsets and migrate from bystanders in the enabling field to disablers in the resilience field would have a significant impact (Fig. 4).

Discussion

Fraud field theory suggests the UK needs to further embrace collective action with a substantial expansion of the private policing capacity that strengthens the resilience forces of 10,550 large organisations, especially the telecoms, technology and transactional organisations that enable fraud. Such a strategy would require considerable political courage to enact legislation that obliges these organisations to build their resilience. Extending the failure-to-prevent doctrine to fraud would substantially amplify the impact of the law (L) as regulators (Lr) would focus on the resilience compliance of a small number of entities (Ro) (Fig. 4). The irresponsible decline in the capacity and competency of the police and the criminal justice system would need to be reversed to support the organisations and to reembrace their deterrence purpose with a concerted focus on the most egregious fraudsters and enablers (Le). The strategy would strengthen the protections for both the organisations and the 53 million adults in the UK, and it has the potential to directly and positively influence the cultural attitudes of the organisations' 17 million employees (C). Only then might politicians and senior civil servants be able to look back and say that the fraud *epidemic* was just a blip.

Tackling the Silicon Valley attitude in the USA as well as the permissive cultures in other places is challenging. However, the appetite for change in America is evident with the responsibilisation debate regarding Section 230 of the CDA reaching both the White House and the Supreme Court (Morrison, 2023). Greater responsibilisation in the USA, however, will not cure fraud alone. The significant amount of fraud that involves an international element, at 70 %, illustrates fraud cannot be tackled one country (Home Office, 2023a). There are nations with large pools of active fraudsters who see little wrong with targeting other, particularly rich, Western countries (Lazarus et al., 2022). Combined with modern communications and banking there is very little friction to international offending, but by contrast there are huge barriers to law enforcement and other relavent bodies working together to disrupt and bring to justice offenders (Button, 2012; Cross, 2020). Reducing fraud will require not just actions that improve the resilience of individuals and organisations and the enforcement in the home country alone. There will also need to be a law enforcement response that

crosses borders and causes significant disruption to the overseas based fraudsters, that requires more than just co-operation, but new institutional structures or bodies to facilitate it (Button, 2012). Once fraudsters in one country are regularly disrupted, brought to justice and even extradited, this will add an important deterrence dimension to the fraud field. China has shown cross-border action is possible, by regularly extraditing dozens of fraudsters targeting Chinese citizens from abroad (See, CNN, 2019). Policy-makers must also grapple with the challenge of trying to change attitudes and cultures, particularly in developing countries and how aid and government actions can be utilised to divert offenders to more positive activities. This international dimension to fraud will prove the most challenging part of the fraud field to address.

At the time of writing of this article the UK Home Office has published its plan to reduce fraud (Home Office, 2023a). The plan sets out a wide range of measures including a new national fraud squad of 400 staff, numerous measures to tackle telecoms fraud, making tech companies more responsible for preventing fraud, the replacement of Action Fraud, among others. Some of the actions noted above in this article are clearly in the plan. It is welcome, in at last indicating serious attention from highest levels of government. But to just put the 400 staff in context, even if they are new posts (which is not clear), there would still be at least five times as many counter fraud staff in the Department for Work and Pensions tackling social security fraud – one of dozens of fraud types, than tackling the many more frauds and victims the police deal with. The ambition of the plan is realistic in recognising the limitations of the proposed actions, by only setting a modest target of reducing fraud from 2019 levels by 10 %, by the end of 2024. Even if this is achieved – which is quite feasible - there will still be almost 4 million individual fraud victims per year without even considering organisational victims, particularly SMEs, which are largely absent from the strategy. The plan clearly accepts fraud is not a blip, but a high volume crime that is here to stay.

Conclusion

Galvanised by the dismissive attitudes of some senior leaders in the UK, this paper challenges the notion that the fraud epidemic in the UK could be described as blip. The examination of the official crime statistics shows that acquisitive crime has switched from theft to fraud because fraud has become a more accessible offence and, from the offender's perspective, it is lower risk. Using the novel fraud field concept to visualise fraud threats and safeguards, the paper has noted the significant forces influencing fraud levels and developed a novel mathematical expression of this. From this assessment the paper argues that the threat forces in favour of fraud currently overwhelm the safeguard forces. The array of threat forces has been hugely amplified by the disruptive impact of new technologies. In particular, because the essence of fraud is a false communication, the digital communication and transaction technologies are powerful enablers that provide a whole generation of fraudsters across the world with access to victims anywhere in the world. Indifference is the essential cause of the weakness of the safeguard forces: an indifferent public, marginal interests within law enforcement, irresponsible organisations, and dismissive politicians. Consequently, it is naïve and reckless to regard the current level of fraud in the UK as a blip, and it will continue at the current levels or accelerate without strategic intervention. The fraud field analysis suggests that the threat field can be tackled by collective action: strengthening law enforcement, obliging large organisations to transition from enablers to disablers by investing in resilience that protects both themselves and the public, and by greater international efforts to tackle the international dimension of fraud.

Declaration of Competing Interest

The authors have no declarations to declare in relation to this paper.

References

ACFE. (2022). Occupational fraud 2022: a report to the nations. ⟨https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf⟩.

Ariel, B., Bland, M., 2019. Is crime rising or falling? A comparison of police-recorded crime and victimization surveys. In: Deflem, M., Silva, D. (Eds.), Methods of Criminology and Criminal Justice Research, vol. 24. Emerald Publishing Limited, pp. 7–31 https://doi.org/10.1108/S1521-613620190000024004/full/html.

Arnold, U., Neubauer, J., Schoenherr, T., 2012. Explicating factors for companies' inclination towards corruption in operations and supply chain management: an exploratory study in Germany. International Journal of Production Economics 138. pp. 136–147. https://doi.org/10.1016/j.ijpe.2012.03.011

Baker, C., 1999. An analysis of fraud on the internet. Internet Res. 9 (5), 348–359. https://doi.org/10.1108/10662249910297750

BBC. (2022, November 20). FTX crypto exchange owes biggest creditors $3.1bn. ⟨https://www.bbc.co.uk/news/business-63697459⟩.

BBC. (2023, April 4). Genesis Market: Popular cybercrime website shut down by police. ⟨https://www.bbc.co.uk/news/uk-65180488⟩.

Beasley, M., Carcello, J., Hermanson, D., Lapides, P., 2000. Fraudulent financial reporting: consideration of industry traits and corporate governance mechanisms. Account. Horiz. 14 (4), 441–454. https://doi.org/10.2308/acch.2000.14.4.441

BEIS. (2022). Business population estimates 2021. ⟨https://www.gov.uk/government/statistics/business-population-estimates-2022⟩.

Berghoff, H., 2017. "Organised irresponsibility"? The Siemens corruption scandal of the 1990s and 2000s. Bus. Hist. 29 (3), 423–445. https://doi.org/10.1080/00076791.2017.1330332

Blackwelder, B., Coleman, K., Colunga-Santoyo, S., Harrison, J.S., Wozniak, D., 2016. The Volkswagen scandal. University of Richmond. ⟨https://scholarship.richmond.edu/robins-case-network/17/⟩.

Bosley, S., Knorr, M., 2018. Pyramids, Ponzis and fraud prevention: lessons from a case study. J. Financ. Crime. 25 (1), 81–94. https://doi.org/10.1108/JFC-10-2016-0062

Boyle, P., Yu, L., Wilson, R., Gamble, K., Buchman, A., Bennett, D., 2012. Poor decision making is a consequence of cognitive decline among older persons without alzheimer's disease or mild cognitive impairment. PLoS One 7 (8). https://doi.org/10.1371/journal.pone.0043647

Buil-Gil, D., Lord, N., Barrett, E., 2021. The dynamics of business, cybersecurity and cyber-victimization: foregrounding the internal guardian in prevention. Vict. Offenders 16 (3), 286–315. https://doi.org/10.1080/15564886.2020.1814468

Burnes, B., Cooke, B., 2013. Kurt Lewin's field theory: a review and re-evaluation. Int. J. Manag. Rev. 15, 408–425. https://doi.org/10.1111/j.1468-2370.2012.00348.x

Button, M., 2012. Cross-border fraud and the case for an "Interfraud". Polic.: Int. J. Police Strateg. Manag. 35 (2), 285–303.

Button, M., 2021. Hiding behind the veil of action fraud: the police response to economic crime in England and Wales and evaluating the case for regionalization or a National Economic Crime Agency. Polic.: A J. Policy Pract. 15 (3), 1758–1772. https://doi.org/10.1093/police/paab022

Button, M., Gee, J., 2013. Countering Fraud for Competitive Advantage: the Professional Approach to Reducing the Last Great Hidden Cost. John Wiley & Sons.

Button, M., Cross, C., 2017. Cyber Frauds, Scams and Their Victims. Taylor & Francis.

Button, M., Pakes, F., Blackbourn, D., 2016. 'All walks of life': a profile of household insurance fraudsters in the United Kingdom. Secur. J. 29 (3), 501–519. https://doi.org/10.1057/sj.2013.43

Button, M., Shepherd, D., Blackbourn, D., 2018. Co-offending, bribery and the recruitment of participants to corrupt schemes and the implications for prevention. Secur. J. 31 (4), 882–900. https://doi.org/10.1057/s41284-018-0139-0

Button, M., Hock, B., Shepherd, D., 2022. Economic Crime: from Conception to Response. Routledge.

Cain, A., Edwards, M., Still, J., 2018. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. 42, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Carter, E., 2021. Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. Br. J. Criminol. 61 (2), 283–302. https://doi.org/10.1093/bjc/azaa072

Cavaglierie, C. (2020, April 6). Sim-swap fraud: how criminals hijack your number to get into your bank accounts. Which? ⟨https://www.which.co.uk/news/2020/04/sim-swap-fraud-how-criminals-hijack-your-number-to-get-into-your-bank-accounts/⟩.

Cebr. (2022). World Economic League Table 2023. ⟨https://cebr.com/reports/world-economic-league-table-2023/⟩.

Chen, H., Beaudoin, C., Hong, T., 2017. Securing online privacy: an empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. Comput. Hum. Behav. 70, 291–302. https://doi.org/10.1016/j.chb.2017.01.003

Chennells, L. (2022, November 29). Fraud is causing Companies House to crumble. It needs a stonger footing. Finextra. ⟨https://www.finextra.com/blogposting/23311/fraud-is-causing-companies-house-to-crumble-it-needs-a-stronger-footing⟩.

CNN (2019) 94 Taiwanese criminal suspects extradited from Spain to Beijing. ⟨https://edition.cnn.com/2019/06/07/asia/taiwan-extradition-beijing-intl/index.html⟩.

Copes, H., Vieraitis, L., 2009. Understanding identity theft: offenders' accounts of their lives and crimes. Crim. Justice Rev. 34 (3), 329–349. https://doi.org/10.1177/0734016808330589

Cressey, D., 1953. Other People's Money; a Study of the Social Psychology of Embezzlement. The Free Press.

Cross, C., 2020. 'Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims. Criminol. Crim. Justice 20 (3), 358–375.

Cross, C., Holt, T., 2021. The use of military profiles in romance fraud schemes. Vict. Offenders 16 (3), 385–406. https://doi.org/10.1080/15564886.2020.1850582

Cross, C., Lee, M., 2022. Exploring fear of crime for those targeted by romance fraud. Vict. Offenders 17 (5), 735–755.
DCMS. (2020). Cyber Security Breaches Survey 2020. ⟨https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020⟩.
Deliema, M., Shadel, D., Pak, K., 2020. Profiling victims of investment fraud: mindsets and risky behaviors. J. Consum. Res. 46 (5), 904–914. https://doi.org/10.1093/jcr/ucz020
Dionne, G., Wang, K., 2013. Does insurance fraud in automobile theft insurance fluctuate with the business cycle? J. Risk Uncertain. 47 (1), 67–92. https://doi.org/10.1007/s11166-013-9171-y
Duri, J. (2021). Corruption and economic crime. Transparency International. ⟨https://knowledgehub.transparency.org/assets/uploads/kproducts/2021-Corruption-and-economic-crime_final.pdf⟩.
DWP. (2022). Fraud and error in the benefits system 2022. ⟨https://www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-financial-year-2021-to-2022-estimates⟩.
Easton, M. (2013). The riddle of peacefulness. BBC. ⟨https://www.bbc.co.uk/news/uk-22268015⟩.
Economist. (2012). You, robot? ⟨https://www.economist.com/technology-quarterly/2012/08/30/you-robot⟩.
Farrell, G., Tilley, N., Tseloni, A., Mailley, J., 2010. Explaining and sustaining the crime drop: clarifying the role of opportunity-related theories. Crime. Prev. Community Saf. 12, 25–41. https://doi.org/10.1057/cpcs.2009.20
Farrell, G., Tseloni, A., Mailley, J., Tilley, N., 2011. The crime drop and the security hypothesis. J. Res. Crime. Delinquency 48 (2), 147–175. https://doi.org/10.1177/0022427810391539
FATF. (2011). Laundering the proceeds of crime. ⟨https://www.fatf-gafi.org/documents/documents/launderingtheproceedsofcorruption.html⟩.
FCA. (2020). Payment protection insurance complaints deadline – final report. ⟨https://www.fca.org.uk/ppi-complaints-deadline-final-report⟩.
Federal Trade Commission. (2019). Mass market consumer fraud in the United States: a 2017 update. ⟨https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf⟩.
Financial Crisis Inquiry Commission. (2011). The financial crisis inquiry report: The final report of the National Commission on the causes of the financial and economic crisis in the United States. ⟨https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf⟩.
Fischer, P., Lea, S., Evans, K., 2013. Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. J. Appl. Soc. Psychol. 43 (10), 2060–2072. https://doi.org/10.1111/jasp.12158
Fonseca, C., Moreira, S., Guedes, I., 2022. Online consumer fraud victimization and reporting: a quantitative study of the predictors and motives. Vict. Offenders 17 (5), 756–780. https://doi.org/10.1080/15564886.2021.2015031
Fooks, G., 2003. In the valley of the blind the one eyes man is king: corporate crime and the myopia of financial regulation. In: Tombs, S., Whyte, D. (Eds.), Unmasking the Crimes of the Powerful. Peter Lang.
Forbes. (2022, December 13). What really happened to LUNA Crypto? ⟨https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/⟩.
FSB. (2019). Calling time on business crime. ⟨https://www.fsb.org.uk/resource-report/calling-time-on-business-crime.html⟩.
Garner, S., Crocker, R., Skidmore, M., Webb, S., Graham, J., & Gill, M. (2016). Organised fraud in local communities. ⟨https://perpetuityresearch.com/wp-content/uploads/2016/08/org_fraud_in_local_communities_final.pdf⟩.
Gee, J., Hall, L., Wang, V., Button, M., & Joseph, E. (2018). The dark web-bad for business. ⟨https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/Dark-Web-Report.ashx?la=en-GB&hash=BFCB10939528D385EE7E3AD763EC329BB46EAD90&hash=BFCB10939528D385EE7E3AD763EC329BB46EAD90⟩.
Gill, M., 2011. Fraud and recessions: views from fraudsters and fraud managers. Int. J. Law, Crime. Justice 39 (3), 204–214. https://doi.org/10.1016/j.ijlcj.2011.05.008
Greenberg, J., 1990. Employee theft as a reaction to underpayment inequity: the hidden cost of pay cuts. J. Appl. Psychol. 75 (5), 561–568 https://psycnet.apa.org/doi/10.1037/0021-9010.75.5.561.
Gupta, G., Saha, S., Chakraborty, S., Mazumdar, C., 2007. Document frauds: identification and linking fake document to scanners and printers. International Conference on Computing: Theory and Applications. IEEE, pp. 497–501 https://doi.org/10.1109/ICCTA.2007.55.
Hall, T., Sanders, B., Bah, M., King, O., Wigley, E., 2021. Economic geographies of the illegal: the multiscalar production of cybercrime. Trends Organ. Crime. 24, 282–307.
HC Deb (31 Jan. 2022) (708) col. 23. ⟨https://hansard.parliament.uk/Commons/2022-01-31/debates/6B412B49-AB7D-4FE3-9F82-B9EAE93FB6AC/SueGrayReport⟩.
HM Government. (2022). A guide to the Online Safety Bill. ⟨https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill⟩.
HM Government. (2023). *Factsheet: Economic Crime and Corporate Transparency Bill.* ⟨https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-economic-crime-and-corporate-transparency-bill-overarching⟩.
HMICFRS. (2019). Fraud: time to choose. ⟨https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf⟩.
Hock, B., 2020. Extraterritoriality and International Bribery: a Collective Action Perspective. Routledge.
Holt, T., Turner, M., 2012. Examining risks and protective factors of on-line identity theft. Deviant Behav. 33 (4), 308–323. https://doi.org/10.1080/01639625.2011.584050
Holtfreter, K., 2004. Fraud in US organisations: an examination of control mechanisms. J. Financ. Crime. 12 (1), 88–96. https://doi.org/10.1108/13590790510625070
Home Office (2023a) Fraud Strategy: Stopping Scams and Protecting the Public. ⟨https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154660/Fraud_Strategy_2023.pdf⟩.
Home Office. (2023b). Police workforce, England and Wales, 31 March 2022. ⟨https://www.gov.uk/government/statistics/police-workforce-england-and-wales-31-march-2022⟩.
House of Commons Home Affairs Committee. (2018). Policing for the future. ⟨https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/515.pdf⟩.
House of Commons. (2023). Tax statistics: an overview. ⟨https://commonslibrary.parliament.uk/research-briefings/cbp-8513/⟩.
Huefner, R., 2010. Local government fraud: the Roslyn School district case. Manag. Res. Rev. 33 (3), 198–209. https://doi.org/10.1108/01409171011030363
Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. Int. J. Law Crime. Justice 47, 44–57.
ICIJ. (2017). Explore the Panama Papers key figures. ⟨https://www.icij.org/investigations/panama-papers/explore-panama-papers-key-figures/⟩.
Institute of Business Ethics. (2018). Ethics at work. 2018 survey of employees: *Europe*. ⟨https://www.ibe.org.uk/uploads/assets/ba9cd14a-a195–4c79-b12c68f7b06fd203/IBESurveyReportEthicsatWork2018surveyofemployeesEuropeINT.pdf⟩.
Ipsos Mori. (2022). Public perceptions of local policing and the police. ⟨https://www.ipsos.com/sites/default/files/ct/news/documents/2022–05/uk-public-perceptions-of-local-policing-and-the-police-ipsos-april-2022.pdf⟩.
Janze, C. (2017). Are cryptocurrencies criminals best friends? Examining the co-evolution of bitcoin and darknet markets. In America's Conference on Information Systems. AMCIS. ⟨https://cointhinktank.com/upload/academic%20Are%20Cryptocurrencies%20Criminals%20Best%20Friends_%20Bitcoin%20and%20Darknet%20Markets%202017.pdf⟩.
Jones, R. ({C}2021a{C}). Social media sites warned over risky investment offers. Guardian. ⟨https://www.theguardian.com/business/2021/apr/20/city-watchdog-warns-social-media-over-investment-offers⟩.
Judges, R., Gallant, S., Yang, L., Lee, K., 2017. The role of cognition, personality, and trust in fraud victimization in older adults. Front. Psychol. *8*. https://doi.org/10.3389/fpsyg.2017.00588
Kaal, W.A., Vermeulen, E.P., 2017. How to regulate disruptive innovation - from facts to data. Jurimetrics 57 (2), 169–209. ⟨https://www.jstor.org/stable/26322665⟩.
Karstedt, S., 2016. Middle-class crime: moral economies between crime in the streets and crime in the suites. In: Van Slyke, S., Benson, M., Cullen, F. (Eds.), The Oxford Handbook of White-collar Crime. Oxford University Press.
Karstedt, S., Farrall, S., 2006. The moral economy of everyday crime: markets, consumers and citizens. Br. J. Criminol. 46 (6), 1011–1036. https://doi.org/10.1093/bjc/azl082
Karstedt, S. and Farrall, S. (2007*). Law abiding majority? The everyday crimes of the middle classes* . Centre for Crime and Justice Studies. ⟨http://www.crimeandjustice.org.uk/opus45/Law_abiding_Majority_FINAL_VERSION.pdf⟩.
Kearney, W., Kruger, H., 2014. Considering the influence of human trust in practical social engineering exercises. Information Security for South Africa. ISSAhttps://doi.org/10.1109/ISSA.2014.6950509
Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., Díaz-Castaño, N., 2021. Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during COVID-19. J. Contemp. Crim. Justice 37 (4), 480–501. https://doi.org/10.1177/10439862211027986
Kethineni, S., Cao, Y., Dodge, C., 2018. Use of bitcoin in darknet markets: examining facilitative factors on bitcoin-related crimes. Am. J. Crim. Justice 43 (2), 141–157. https://doi.org/10.1007/s12103-017-9394-6
Knepper, P., 2015. Falling crime rates: what happened last time. Theor. Criminol. 19 (1), 59–76. https://doi.org/10.1177/1362480614541290
Kumar, K., Bhattacharya, S., Hicks, R., 2018. Employee perceptions of organization culture with respect to fraud – where to look and what to look for. Pac. Account. Rev. 30 (2), 187–198. https://doi.org/10.1108/PAR-05-2017-0033
Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L., & Hong, J. (2007, October). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In Proceedings of the Anti-phishing Working Groups (pp. 70–81). eCrime. https://doi.org/10.1145/1299015.1299022.
Law, P., 2011. Corporate governance and no fraud occurrence in organizations: Hong Kong evidence. Manag. Audit. J. 26 (6), 501–518. https://doi.org/10.1108/02686901111142558
Lazarus, S., 2018. Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. Criminol. Crim. Justice Law Soc. 19 (63), 63–80. ⟨https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/wescrim19&section=17⟩.
Lazarus, S., Button, M., 2022. Tweets and reactions: revealing the geographies of cybercrime perpetrators and the North-South divide. Cyber, Behav. Soc. Netw. 25 (8), 504–511. https://doi.org/10.1089/cyber.2021.0332
Lazarus, S., Button, M., Adogame, A., 2022. Advantageous comparison: using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians ("Yahoo men"). Heliyon 8 (11), e11142.
Lee, J., Soberon-Ferrer, H., 1997. Consumer vulnerability to fraud: influencing factors. J. Consum. Aff. 31 (1), 70–89. https://doi.org/10.1111/j.1745-6606.1997.tb00827.x
Lee, N., 2018. Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. Commun. Educ. 67 (4), 460–466. https://doi.org/10.1080/03634523.2018.1503313
Levi, M., 2008. Organized fraud and organizing frauds: unpacking research on networks and organization. Criminol. Crim. Justice 8 (4), 389–419. https://doi.org/10.1177/1748895808096470
Levi, M., 2021. Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation. Trends Organ. Crime. 24 (96–110). https://doi.org/10.1007/s12117-020-09401-y

Levi, M., Smith, R., 2021. Fraud and its relationship to pandemics and economic crises: from Spanish flu to COVID-19. Australian Institute of Criminology. 〈https://www.aic.gov.au/publications/rr/rr19〉.

Lewin, K., 1951. Field Theory in Social Science. Harper & Row.

Makortoff, K. ({C}2021b{C}). UK regulator warns Google about accepting scam adverts. Guardian. 〈https://www.theguardian.com/business/2021/jun/14/uk-regulator-warns-google-about-accepting-scam-adverts〉.

Mansouri, N., 2016. A case study of Volkswagen unethical practice in diesel emission test. Int. J. Sci. Eng. Appl. 5 (4), 211–216. https://doi.org/10.7753/IJSEA0504.1004

Markson, T. (2022, November 17). DWP and HMRC get cash boost for 6,000 new staff to tackle fraud, error and tax dodging. Civil Service World. 〈https://www.civilserviceworld.com/professions/article/autumn-statement-hmrc-dwp-fraud-6000-new-staff-tax-compliance-cash-boost〉.

Mars, G., 2019. Cheats at Work: An Anthropology of Workplace Crime. Routledge.

Matchin, T. (2020). A summary of fake identity document trends in 2019 – Right to Work checks. 〈https://www.trustid.co.uk/a-summary-of-fake-identity-document-trends-in-2019-right-to-work-checks/〉.

Matza, M. (2021, December 14). Social media influencers charged with $100m stock scheme. BBC. 〈https://www.bbc.co.uk/news/world-us-canada-63981003〉.

Mohd-Sanusi, Z., Rameli, M., Omar, N., Ozawa, M., 2015. Governance mechanisms in the Malaysian banking sector: mitigation of fraud occurrence. Asian J. Criminol. 10 (3), 231–249. https://doi.org/10.1007/s11417-015-9211-4

MOJ. (2007). Sentencing statistics 2006. 〈http://data.parliament.uk/DepositedPapers/Files/DEP2007–0350/DEP2007–0350.pdf〉.

MOJ. (2023). Criminal Justice System statistics quarterly: September 2022. 〈https://www.gov.uk/government/statistics/criminal-justice-statistics-quarterly-september-2022〉.

Mor, F. (2018). Bank rescues of 2007–09: outcomes and cost. House of Commons Library. 〈https://commonslibrary.parliament.uk/research-briefings/sn05748/〉.

Morrison, S. (2023, February 23). Section 230, the internet law that's under threat, explained. Vox Media. 〈https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-supreme-court-social-media〉.

NCA. (2020). National Strategic Assessment of Serious and Organised Crime 2020. 〈https://nationalcrimeagency.gov.uk/component/finder/search?q=%22National+Strategic+Assessment%22&Itemid=101&Itemid=101〉.

NCA. (2021). National Strategic Assessment of Serious and Organised Crime 2021. 〈https://nationalcrimeagency.gov.uk/component/finder/search?q=%22National+Strategic+Assessment%22&Itemid=101&Itemid=101〉.

NCA. (2023). Notorious criminal marketplace selling victim identities taken down in international operation. 〈https://www.nationalcrimeagency.gov.uk/news/notorious-criminal-marketplace-selling-victim-identities-taken-down-in-international-operation〉.

Norgrove, D. (2022). Response from Sir David Norgrove to Alistair Carmichael MP – Use of official crime statistics by Prime Minister, Home Secretary and Home Office. UK Statistics Authority. 〈https://uksa.statisticsauthority.gov.uk/correspondence/response-from-sir-david-norgrove-to-alistair-carmichael-mp-misuse-of-official-crime-statistics-by-prime-minister-home-secretary-and-home-office/〉.

Norman, C., Rose, A., Rose, J., 2010. Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk. Account. Organ. Soc. 35 (5), 546–557. https://doi.org/10.1016/j.aos.2009.12.003

OBR. (2022). A brief guide to the public finances. 〈https://obr.uk/forecasts-in-depth/brief-guides-and-explainers/public-finances/〉.

OECD. (2020). Collective action and the fight against corruption. www.oecd.org/south-east-europe/programme/Collective-Action-and-Fight-Against-Corruption-Policy-Briefing-Note-May2020.pdf.

Ofcom. (2022). Adults' media use and attitudes 2022: interactive report. 〈https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes/interactive-tool〉.

ONS. (2021). Internet users, UK: 2020. 〈https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020〉.

ONS. (2022a). Crime in England and Wales: year ending September 2022. 〈https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2022〉.

ONS. (2022b). Mid-Year Population Estimates, UK, June 2021. 〈https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland〉.

Payment Systems Regulator. (2023). What are authorised push payment scams?. 〈https://www.psr.org.uk/our-work/app-scams/〉.

Quisenberry, W.L., 2017. Ponzi of all Ponzis: critical analysis of the Bernie Madoff scheme. Int. J. Econ. Financ. Manag. 5 (1), 1–6. https://doi.org/10.12691/ijefm-5-1-1

Reiner, R., 2016. Crime, the Mystery of the Common-sense Concept. John Wiley & Sons.

Reurink, A., 2019. Financial fraud: a literature review. Contemporary Topics in Finance: a Collection of Literature Surveys. In: Claus, I., Krippner, L. (Eds.), Financial fraud: a literature review. John Wiley & Sons, pp. 79–115.

Rispel, L., Jager, P., Fonn, S., 2016. Exploring corruption in the South African Health sector. Health Policy Plan. 31 (2), 239–249. https://doi.org/10.1093/heapol/czv047

Schoepfer, A., Piquero, N., 2009. Studying the correlates of fraud victimization and reporting. J. Crim. Justice 37 (2), 209–215. https://doi.org/10.1016/j.jcrimjus.2009.02.003

Sheckels, J., Farer, J., 2018. Investigating and prosecuting transnational telefraud schemes: the India-based call center scam and Costa Rica telemarketing fraud cases. Dep. Justice J. Fed. Law Pract. 66 (7), 213–262. 〈https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/usab66&section=126〉.

Shepherd, D., Button, M., 2018. Organizational inhibitions to addressing occupational fraud: a theory of differential rationalization. Deviant Behav. 40 (8), 971–991. https://doi.org/10.1080/01639625.2018.1453009

Shepherd, D., Whitman, K., & Button, M. (2021). Influencer report: the impact of complicit social media influencers on the consumption of counterfeit goods in the UK. Intellectual Property Office. 〈https://www.gov.uk/government/publications/social-media-influencers-and-counterfeit-goods〉.

Shover, N., Coffey, G., Hobbs, D., 2003. Crime on the line. Telemarketing and the changing nature of professional crime. Br. J. Criminol. 43 (3), 489–505. https://doi.org/10.1093/bjc/43.3.489

Shover, N., Coffey, G., Sanders, C.R., 2004. Dialing for dollars: opportunities, justifications, and telemarketing fraud. Qual. Sociol. 27 (1), 59–75. https://doi.org/10.1023/B:QUAS.0000015544.69646.f1

Sims, R., Brinkmann, J., 2003. Enron ethics (or: culture matters more than codes). J. Bus. Ethics 45 (3), 243–256. https://doi.org/10.1023/A:1024194519384

Skidmore, M., Ramm, J., Goldstraw-White, J., Barrett, C., Braleaza, S., Muir, R., & Gill, M. (2018). Improving the police response to fraud. The Police Foundation. 〈https://www.police-foundation.org.uk/project/improving-the-police-response-to-fraud-2/〉.

Smaili, N., de Rancourt-Raymond, A., 2022. Metaverse: welcome to the new fraud marketplace. J. Financ. Crime. https://doi.org/10.1108/JFC-06-2022-0124

Smith, D., 2010. A Culture of Corruption. Princeton University Press.

Smith, M., & Van Alstyne, M. (2021, August 12). It's time to update Section 230. Harvard Business Review. 〈https://hbr.org/2021/08/its-time-to-update-section-230〉.

Suh, I., Sweeney, J., Linke, K., Wall, J., 2020. Boiling the frog slowly: the immersion of C-suite financial executives into fraud. J. Bus. Ethics 162 (3), 645–673. https://doi.org/10.1007/s10551-018-3982-3

Sutherland, E., 1940. White-collar criminality. Am. Sociol. Rev. 5 (1), 1–12.

Sutherland, E. (1949). White collar crime. Dryden.

Swanson, D.J., Creed, A.S., 2014. Sharpening the focus of force field analysis. J. Chang. Manag. 14 (1), 28–47.

Taufik, T., 2019. The effect of internal control system implementation in realizing good governance and its impact on fraud prevention. Int. J. Sci. Technol. Res. 8 (9), 2159–2165. 〈http://www.ijstr.org/final-print/sep2019/The-Effect-Of-Internal-Control-System-Implementation-In-Realizing-Good-Governance-And-Its-Impact-On-Fraud-Prevention.pdf〉.

Timofeyev, Y., Dremova, O., 2022. Insurers' responses to cyber crime: evidence from Russia. Int. J. Law Crime. Justice 68, 100520.

Tombs, S., Whyte, D., 2015. The Corporate Criminal: Why Corporations must be Abolished. Routledge.

Toms, S., 2019. Financial scandals: a historical overview. Account. Bus. Res. 49 (5), 477–499. https://doi.org/10.1080/00014788.2019.1610591

Tonry, M., 2014. Why crime rates are falling throughout the Western world. Crime. Justice 43 (1), 1–63 https://www.journals.uchicago.edu/doi/epdf/10.1086/678181.

Tunley, M., Button, M., Shepherd, D., Blackbourn, D., 2018. Preventing occupational corruption: utilising situational crime prevention techniques and theory to enhance organisational resilience. Secur. J. 31 (1), 21–52. https://doi.org/10.1057/s41284-016-0087-5

University of Portsmouth (2017). Annual Fraud Indicator. Experian and Crowe Clark Whitehill. 〈https://researchportal.port.ac.uk/files/18878333/Annual_Fraud_Indicator_report_1_2017.pdf〉.

UNODC. (2021). Darknet cybercrime threats to Southeast Asia. 〈https://www.unodc.org/southeastasiaandpacific/en/2021/02/darknet-cybercrime-southeast-asia/story.html〉.

Upadhyaya, R., & Jain, A. (2017). Cyber ethics and cyber crime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In International Conference on Computing, Communication and Automation 2016 (pp. 143–148). IEEE. https://doi.org/10.1109/CCAA.2016.7813706.

Vedamanikam, M., Chethiyar, S., 2020. Money mule recruitment among university students in Malaysia: awareness perspective. Pupil.: Int. J. Teach. Educ. Learn. 4 (1), 19–37. https://doi.org/10.20319/pijtel.2020.41.1937

Wall, D., 2013. Enemies within: Redefining the insider threat in organizational security policy. Secur. J. 26 (2), 107–124. https://doi.org/10.1057/sj.2012.1

Wang, V., Gee, J., Button, M., 2022. Crime on the Darknet: the case of brand abuse. In: Gill, M. (Ed.), The Handbook of Security. Palgrave Macmillan, pp. 447–467.

Whittaker, J., Button, M., 2020. Understanding pet scams: a case study of advance fee and non-delivery fraud using victims' accounts. Aust. N. Z. J. Criminol. 53 (4), 497–514. https://doi.org/10.1177/0004865820957077

Whittaker, J., Edwards, M., Cross, C., Button, M., 2022. "I have only checked after the event": consumer approaches to safe online shopping. Vict. Offenders 1–23. https://doi.org/10.1080/15564886.2022.2130486

Whitty, M., 2019. Predicting susceptibility to cyber-fraud victimhood. J. Financ. Crime. 26 (1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Whitworth, D. (2021, March 27). Phone companies 'must do more' to stop fraud calls. BBC. 〈https://www.bbc.co.uk/news/business-56521518〉.

Wood, H., Keatinge, T., Ditcham, K., & Janjeva, A. (2021). The silent threat: the impact of fraud on UK national security. RUSI. 〈https://rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security〉.

Zahedi, F.M., Abbasi, A., Chen, Y., 2015. Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. J. Assoc. Inf. Syst. 16 (6), 448–484. https://doi.org/10.17705/1jais.00399

Zhang, D., Frei, R., Senyo, P.K., Bayer, S., Gerding, E., Wills, G., Beck, A., 2023. Understanding fraudulent returns and mitigation strategies in multichannel retailing. J. Retail. Consum. Serv. 70. https://doi.org/10.1016/j.jretconser.2022.103145

Zweifach, L.J., Khan, S.N., 2010. Recent developments in Ponzi scheme litigation. In: Carroll, M., Morvillo, R. (Eds.), Auditor Liability in Current Environment: How to Protect Yourself. Practising Law Institute, pp. 99–132.