PERSPECTIVES ON POLICING: PAPER 10

THE ANATOMY OF ONLINE FRAUD

Michael Skidmore
The Police Foundation

April 2024

THE POLICE FOUNDATION
The UK's policing think tank

1. Introduction

In 2022-23 there were an estimated 3.5 million fraud offences in England and Wales, with members of the public now more likely to fall victim to fraud than any other type of crime (ONS, 2023a). And accordingly, the police are seeing an overwhelming rise in reported fraud, with levels of recorded crime exceeding one million offences, reflecting not only fraud against the public but also the considerable impact on businesses (ONS, 2023a). These patterns are largely the consequence of living in an increasingly digitised society in which the opportunities to perpetrate fraud have proliferated.

All this crime is reduced into one single offence category of 'fraud', which covers both a large volume and a wide variety of offenders, offending, victims, harm, and vulnerability. This paper focuses specifically on 'online fraud', forming part of a wider programme of work looking at fraud that is enabled by the internet and digital technology. The paper reviews the literature with the aim of unpacking the nature and particular characteristics of online fraud. It also examines how data and knowledge about fraud inform and direct the strategic and operational responses of the police and other organisations. The complexities of producing a 'true' picture of fraud are explored, including a discussion of the meaning and significance of fraud when it is 'online'. It highlights the gaps and challenges in our current understanding of online fraud that will be addressed in our ongoing research programme.

2. Starting from the beginning … what is fraud?

Fraud is a category of offence that binds together a very wide range of behaviours that include some form of deception or misrepresentation for personal gain. It commonly entails depriving a victim of money or other material goods and constitutes a specific type of property crime (ONS, 2016). It can also be perpetrated for non-monetary advantage, such as to gain access to information or documents that are otherwise of value to the offender (for example, fraudulent passport applications).

In the past, there was no single definition of fraud in law, and it encompassed multiple separate legal categories, which obstructed robust legal and strategic interpretations of the problem (Fraud Review, 2006). The introduction of the Fraud Act in 2006 was an important step in setting out a clear and comprehensive definition in law, consolidating fraud into a single legislative framework. The Fraud Act (2006) describes three principal ways in which a fraud can be perpetrated:[1]

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

Most frauds that are recorded as crime will fall under the Fraud Act (2006). Additional laws are used to address frauds that impact in certain areas of commercial business or public service; for example, consumer protection laws, false accounting, or benefit fraud.[2] Many incidents of fraud receive a civil regulatory response (for example, the Department for Work and Pension will respond to benefit fraud) or are progressed by victims through the civil courts (Button et al, 2016).

Importantly, fraud represents a continuum of deviant activity, not all of which would be classified as criminal, ranging from unethical business practices through to outright criminal fraud[3] (Button and Cross, 2017). Furthermore, phishing methods often employ deception to steal personal identity information, but these are not recordable offences in UK law. The term 'scam' is often used interchangeably with 'fraud' and encapsulates this broader continuum of fraudulent activity (Button and Cross, 2017). A criminal classification can depend on factors such as the underlying intentions, the nature and degree of dishonesty and the type of victim (Button et al, 2016). The focus of this paper is principally criminal fraud as defined by the Fraud Act (2006), although fraud that targets public sector institutions and is subject to internal regulatory responses is not in scope.

3. Tracking and measuring the problem of online fraud

The collection of recorded crime and survey data has for many years been integral to the design and delivery of an effective and efficient public service in response to crime in the UK, with the levels, patterns and trends in crime signalling to decision-makers the kinds of policies and resources that are needed and subsequently, their value in reducing crime.

[1] https://www.legislation.gov.uk/ukpga/2006/35/section/2

[2] Consumer Rights Act (2015), Theft Act (1968) and Social Security Administration Act, 1992.

[3] For example, see Skidmore (2020) which examines pension frauds that ranged from outright criminal deception, through to sharp practices which could be highly impactful on victims but did not constitute crimes.

However, there are a variety of methodological challenges to generating a 'true' picture of crime. These include shortcomings in police and government processes for capturing and presenting crime data; a tradition of counting units of crime as a discrete event instead of a process, which obscures serial offending and victimisation; the lack of a single accepted methodology to account for the seriousness and harm of crime; and the limited capacity for official data to capture hidden crime or its victims, or new and emerging types of criminal behaviour (Maguire and McVie, 2017). Static methodologies and data produce stable and comparable crime data year-on-year (for example, ONS, 2022a) but lack the agility to delve into nuance or explore the contemporary themes and issues of the day. This partly explains the lag between the growth in fraud and cybercrime and their introduction into the official data and public dialogue on crime,[4] bringing to light a picture of crime in the UK that is changing (i.e. migrating to online spaces) instead of reducing (Farrell and Birks, 2018).

A final point to note is the increasing diversity of information and perspectives on crime. Historically, public reporting was the business of the police, which provided a singular and authoritative picture of crime in the UK. However, official reports now constitute one version among multiple truths on crime, with a multitude of sectors and interested parties feeding into a 'kaleidoscope' of information and knowledge (Maguire and McVie, 2017). And nowhere is this hall of mirrors more apparent than in fraud and cybercrime for which data and knowledge emanate from a multitude of organisations (Button et al, 2016; Levi and Burrows, 2008). These include public and private sector organisations that are impacted by fraud and/or play a role in controlling or responding to fraud (HMRC, financial services, private security companies etc), and those who advocate for victim groups such as consumers or businesses.

How (and why) do we record different types of fraud?

The police in the UK operate to the National Crime Recording Standards (NCRS), which set out a standard for recording crime in accordance with the law.[5] They are guided by two overarching principles which are to maintain consistency of recording across all police force areas, and for crime recording to be 'victim focused' – ie. ensure that crime recording accurately reflects the accounts given by victims. In addition to its administrative purposes,[6] recorded crime is described as having the following functions:[7]

- '[To provide] the police and partners with data, which informs the targeted use of resources and allows the effectiveness of crime reduction strategies to be established.
- [To assist the] public in making informed decisions about the risk of crime to themselves as individuals and to allow judgements on how effective government, police and partners are in tackling crime.
- [To assist the] government (both centrally and locally) to establish whether their policies are effective in driving down crime and to assess relative performance of the police and associated partners.'[8]

It is with these strategic aims in mind that the current approach to accounting for the problem of fraud needs to be considered. There are 48 separate categories of fraud captured in recorded crime statistics, an inordinately high number which is aimed to capture the considerable range of criminal activity that is encompassed by the Fraud Act (2006) (Home Office, 2021). These categories variously represent the different dimensions of fraud, with some categories focused on the specific techniques that are employed by offenders (e.g. 419 advance fee fraud), or the social, occupational or commercial environments in which the frauds occur (e.g. online shopping and auction fraud), or relatedly, a specific sector that is impacted (e.g. telecom industry fraud). These categories are not bound to a single conceptual framework, and more importantly, they do not express crucial human dimensions such as harm, seriousness, risk or vulnerability that are so important for informing the delivery of public services (Skidmore et al, 2018). This has implications for how we rationalise and account for the policies and interventions in place for tackling fraud; for example, if we can't identify the highest harm offending, how can the police be sure they are effective in reducing harm?

[4] The introduction of national reporting through Action Fraud in 2013 introduced more robust methods for recording and measuring crime that was reported to the police. And in 2017 the Crime Survey for England and Wales introduced questions pertaining to fraud and computer misuse crime.

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/116269/ncrs.pdf

[6] Systems for recording information all in one place and to ensure the collected data helps in guiding decisions on officer safety.

[7] The Home Office Counting Rules provide a framework that prescribes the specific processes for classifying and accounting for the crime events reported to the police — https://www.gov.uk/government/publications/counting-rules-for-recorded-crime

[8] Ibid

What are the key dimensions of police recorded fraud?

The UN developed a framework for classifying crime for statistical purposes and set out eight key attributes of a criminal event that the state should aim to capture, beyond just the 'type' of offence that has occurred (i.e. fraud) (UNODC/UNECE, 2012). A number of these attributes are discussed below in the context of fraud:[9]

The 'modus operandi' of the act/event

Fraud is property crime perpetrated by means of a deception (or false representation). The range of methods for deploying a deception is vast, with opportunities arising wherever there is a financial, commercial, or social exchange. And this landscape of opportunity has grown exponentially as more societal functions migrate to online spaces (Button and Cross, 2017). Furthermore, the methods for committing fraud continuously evolve, adapting to opportunities offered by new systems and technologies, as well as in response to new measures for controlling these crimes (Albanese, 2005). For this reason, categorising fraud modi operandi in a way that is both exhaustive and sufficiently descriptive is a challenge.

Despite the number of fraud categories used in police recorded crime, many methods remain unaccounted for – one study found up to 23 per cent of frauds recorded in UK were categorised as 'Other Fraud (Not covered elsewhere)'[10] (Correia, 2022). Furthermore, the relevance of very specific categories can diminish over time – for example, 'Pension Liberation Fraud' entailed persuading victims into evading their tax liabilities, and while at one time highly problematic, there has been a significant reduction in recent years because offending has adapted to changes in the consumer and regulatory landscape (Skidmore, 2020).

Fraud categories commonly represent the broad social, commercial or economic setting in which the deception occurs, indicating both the method of offending and the nature of the target. For example, Levi and Burrows (2008) developed a typology which included categories such as 'lending fraud', 'pension-type fraud' and 'embezzlement' and configured them according to different categories of victim – i.e. individuals or organisations in the public or private sector. Intuitively, orienting crime data in this way (alongside data on victims) provides opportunities for targeting control measures to where they are most likely to be impactive – for example, 'lending fraud' indicates fraud that occurs within a specific commercial sector.

A similar taxonomy of categories is based on the 'expected or promised reward, benefit or outcome from the fraudulent transaction' – for example, in investment fraud there is an expected investment return from the victim (Beals et al, 2015). In doing so, seven categories were designed to encompass all the variants of fraud against individuals:

- Consumer investment fraud
- Consumer products and services fraud
- Employment fraud
- Prize and grant fraud
- Phantom and debt collection fraud
- Charity fraud
- Relationship and trust fraud

A final point to note on modus operandi is that the use of online technology is not an organising principle in any of the typologies. Most are focused on categorising the specifics of the ruse (the investment, the romantic relationship etc) that is used by offenders. The significance of 'online' (or cyber) for understanding fraud will be discussed in more detail in the next section.

Non-official perspectives of modus operandi

As stated earlier, there are a multitude of organisations in the public and private sector that have a role in tackling online fraud, and in filling the gap left by the state they have taken a prominent role in defining the problem. However, these organisations do not have a public remit and so are guided by a different logic, one primarily oriented towards understanding threats to internal systems. This guides their approach to configuring information and knowledge on fraud (Cifas, 2023; UK Finance, 2022; Vasiu and Vasiu, 2004). To illustrate, in financial services the priority is to understand what products are being targeted and how; for example, 'unauthorised payment card' fraud involves external actors who exploit vulnerabilities in their systems (e.g. remote banking fraud) and are differentiated from 'first party' frauds that are perpetrated by their own customers (e.g. false insurance claims) (Cifas, 2019; UK Finance, 2022).

[9] Other categories not discussed here were the intent of the perpetrator in committing the offence and the sex and age of the victims.

[10] This may in part reflect errors in police recording.

The degree of completion of the offence (i.e. planned, attempted or completed)

Fraudsters that employ mass communication or marketing are in essence ‘playing the odds’, by making unsolicited contact with a high volume of people in the hope that some recipients will fall foul. Suspicious messages are ubiquitous, whether by phone, text, email, or postings or advertising online. One survey found that 8 in 10 adults in the UK had received ‘some form of suspicious messaging’ by text or phone within a period of three months, though most had not acted on the message (Ofcom, 2021).

‘Attempted’ frauds have become an ambient part of everyday life, as much public nuisance as criminal endeavour. These ‘tripping hazards’ are avoided by most but for those who fall there are direct and sometimes severe consequences. For a crime to be recorded by police there needs to be a ‘specific intended victim’, which as a minimum requires a victim to have responded to the initial communication (e.g. clicking on an online link) (Home Office, 2021). Therefore, most attempted frauds, including precursor events such as phishing, are not treated as victim-based crimes. These particularities in crime recording create some inconsistency between fraud as counted by the police, and that which is self- reported by the public; for example, not all frauds reported in the Crime Survey for England and Wales would necessarily meet the criteria for recorded crime (ONS, 2023b).

The intended ‘target’

A ‘victim-centric’ approach to developing a typology acknowledges which sectors of society are reporting crime and relatedly, where demand on the criminal justice system and/or protective services is coming from (Levi and Burrows, 2008). At its most straightforward, a typology can distinguish between fraud committed against individuals and fraud committed against organisations (Beal et al, 2015), however even this brings complications because ‘the victim’ of a fraud can simultaneously be an individual, corporation and other business (Correia, 2022). For example, an individual who is the victim of a card-not-present fraud needs to report to their financial service provider, which will ultimately bear the financial cost of the crime and be recorded as the victim on police systems,[11] and there may also be a merchant who provided the goods or services who suffers a loss. Crime statistics show that industry bodies Cifas and UK Finance accounted for 62 per cent of all fraud reported to the police in 2021-22 (ONS, 2022b), though many of these crimes will have been experienced initially by individual service users.

The ‘seriousness’ of the act/event:

The seriousness of an event is largely a representation of the harm that has been caused (or is intended) (Adriaenssen et al, 2020) and performs an important function in both the justice system for determining judicial outcomes, but also for assigning resources and interventions in law enforcement to the most important crimes (Hales and Higgins, 2016; Sentencing Council, 2014). However, in the past law enforcement agencies failed to recognise and register the significant impact that that fraud can have on its victims (Button et al, 2014; Cross, 2015). These blind spots are the result of an occupational culture in the police and wider public sector that does not prioritise fraud, and structural gaps across policing, including a lack of robust data and systems for identifying the most important fraud offences (Correia, 2022; Skidmore et al, 2018).

The Crime Survey for England and Wales (CSEW) indicates that the experience of fraud is likely to be trivial for many; over half (52 per cent) who experienced fraud in 2019-20 did not consider the incident to have been serious, a quarter (26 per cent) had not lost any money and 30 per cent reported losses of less than £100.[12] However, a significant minority (20 per cent) of victims did perceive the incident as serious.[13] The experience of harm is subjective and cannot be calculated only in terms of financial losses and is dependent on other contextual factors (Button et al, 2014; Kerr et al, 2013).

Importantly, in cases that involve a series of crime, ‘seriousness’ is not necessarily determined by the characteristics of a single criminal event, but rather the volume and pattern of offending or victimisation over time (Correia, 2021; Skidmore and Aitkenhead, 2023; Skidmore et al., 2020a). These characteristics are not systematically assigned to recorded crimes and instead reflect post-hoc assessments and resourcing decisions guided by policy frameworks related to serious and organised crime or vulnerability (Skidmore et al, 2020a; Skidmore et al, 2020b).

[11] This is to avoid double-counting the same criminal event.

[12] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

[13] ibid

The 'degree of co-responsibility' of other persons involved in the act/event

Enlisting co-offenders is common for the most serious and complex frauds. This includes the involvement of individuals who occupy certain positions or have certain capabilities (legitimate or criminal) or others who adopt more general roles to facilitate the fraud (May and Bhardwa, 2018; Shover et al, 2004). Complex frauds can involve a long chain of events in which a range of disconnected actors perform different functions. Not all co-offenders in a fraudulent scheme are fully aware or complicit, with some content to play their role and take payment without asking too many questions (for example, professional enablers or money mules). Furthermore, at various points along the chain of events different offenders can perpetrate a range of crimes, such as computer misuse crime, money laundering and corruption (Yip et al, 2013; Leukfeldt, 2014; Levi, 2008; Skidmore and Aitkenhead, 2023). Co-offenders can be vital in determining a fraudster's scope of offending however the police are limited in their capacity to capture this information. This is because the underlying processes are often hidden from the victims who report the crime, there are limited resources to proactively uncover this information, and the considerable number of suspects can mean that many are not subject to a criminal investigation (for example, see Skidmore, 2020).

The 'policy area' of the act/event

Online fraud has become the predominant form of crime experienced in the UK and has risen high on the national policy agenda (Fraud Act 2006 and Digital Fraud Committee, 2023; Home Affairs Committee, 2018; Skidmore et al, 2018). However, problems that ascend the social and political agenda are not always clearly codified in legislation or crime recording, and such is the case with online fraud. Moreover, no single organisation owns the online fraud agenda nor can lay claim to a single authoritative viewpoint because it is dispersed across a wide policy and regulatory horizon. Different stakeholders in the public and private sector are responsible for different aspects of the problem (for example, see Button et al, 2016). This diffusion is evident in the array of legal and policy frameworks for online fraud in the UK, which include a multitude of stakeholders in the public and private sector:

- Online Safety Act (2023): a proposal to regulate the private sector response to fraudulent content such as scam advertisements, on social media platforms and internet search engines.[14]
- Economic Crime and Corporate Transparency Act (2023): a proposal to impose a duty on large companies to prevent fraud against the public or other companies by an employee or other internal agent.[15]
- National Cyber Strategy: a government strategy to enhance cyber security across the UK, which includes disrupting 'cyber criminals' and strengthening protections against fraud (HM Government, 2022).
- Economic crime plan: a government strategy to deliver a multi-agency response coordinated by the National Crime Agency to reduce money laundering and fraud (including regulation to stem the abuse of crypto-assets) (HM Government, 2023c).
- Fraud and Serious and Organised Crime Strategy: two government strategies for directing law enforcement and partner organisations in pursuing offenders and protecting victims and the wider public from fraud (HM Government, 2023a; HM Government, 2023b).

Fraud encompasses huge diversity, incorporating crime that is highly variable in terms of the way it is committed, who is targeted, and the experiences and perspectives of victims and wider public. Levi and Burrows (2008) made the point that a "true picture of fraud is a chimera", one requiring the collection of perspectives and data from a range of stakeholders in business, the public, public sector and the police. Many dimensions of fraud that are discussed in this section elude the current systems for recording and assessing fraud, either because they are hidden from the data, hidden within it, or dispersed across a fragmented assemblage of public and private sector organisations that play a role in controlling fraud. This is problematic because effective and accountable policies are contingent on having clear and transparent assessments of the problem.

4. What is 'online' fraud?

Online fraud is a key component of 'cybercrime due to the especially profound effect that online technology has had on this offending (Albanese, 2005; , 2001 Fried). The term 'cybercrime' has entered the public consciousness and language to describe any offending that in some way makes use of information and communication technology. However, there is no single authoritative definition of what it means, and no consensus on where 'crime' ends and 'cybercrime' begins (Phillips et al, 2022; Yar and

[14] https://www.legislation.gov.uk/ukpga/2023/50/enacted

[15] https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-failure-to-prevent-fraud-offence

Steinmetz, 2019). It is a flexible construct used to depict the various transformative effects of the internet on either offending, victimisation or the methods for controlling or responding to crime (Brown, 2015; Gordon and Ford, 2006; Levi et al, 2015; Wall, 2007a; Wall, 2007b).

Just as online technologies have permeated much of modern life, they have also permeated many areas of crime, but articulating their key implications for crime in modern-day society is not straightforward. A common approach is to focus on the extent to which offending has been transformed by online technology by assigning individual crimes to one of three categories:

- **Cyber-dependent crimes** are offences that can only be committed by using a computer, computer networks, or other form of information and communications technology (ICT) (for example, hacking).
- **Cyber-enabled crimes** are traditional crimes that use computers, computer networks or other information and communications technology to increase their scale or reach.
- **Cyber-assisted crimes** use networked digital technologies in the course of criminal activity which would take place anyway. The nature and volume of criminal activity are essentially unaffected by its involvement.

(Maguire and Dowling, 2013; Levi et al, 2015)

In legal terms, 'online' fraud, just like offline fraud, involves a perpetrator that has intended or caused a harm that has been specified in law (i.e. fraud), and who is thereby criminally liable (Brenner, 2001). Online fraud is still fraud, the crime is the same, but the medium has changed to take advantage of online technologies; just as previously there was no specified 'telephone fraud' offence in UK law, there is no 'online fraud' offence in UK legislation. Accordingly, online fraud is often viewed as old crime that has taken on new forms – the proverbial 'old wine in a new bottle' (Grabosky, 2001) – and so is broadly classified as cyber-enabled crime (Maguire and Dowling, 2013). This means that whatever the role played by online technology, it is treated as somewhat incidental to the core fraud offence in the official data:

- In 2020-21 the City of London Police estimated that 80 per cent of reported fraud is 'cyber-enabled' in some unspecified way.[16]
- In 2021-22, the Crime Survey for England and Wales showed that 61 per cent of fraud offences experienced by the public had in some way involved "the internet or any type of online activity".[17]

These statistics provide a window onto crimes as they were experienced and perceived by the victims, however victims do not always know how a fraud has occurred (Button et al, 2014). There can be a multitude of stages in the process of commissioning a fraud and multiple crimes can be perpetrated along the way, some of which may occur online and out of sight of the victim. For example, the deployment of malware to steal personal data is a precursor offence for some identity frauds, and then further along the sequence of events, there may be a need to exploit digital finance to launder the criminal proceeds (Skidmore and Aitkenhead, 2023).

In this regard, whether a fraud was 'online' or not might depend on the perspective that is taken. An examination from the perspective of the perpetrators can provide a more holistic perspective on the different stages in commissioning the offence (i.e. the 'crime script') and the role of online technology along that sequence of events (for example, see Ekblom and Gill, 2016). That said, victims can provide a window onto the more publicly visible stages of an offence, such as the initial method for communicating with the victim. A defining characteristic of fraud offending is the use of deception to trick victims into voluntarily parting with their money (as opposed to using force); the victim plays a central role in the 'script' (Tun and Birks, 2023). So, while the victim's perspective is partial, it can provide critical insights into the victim-offender interaction, the vulnerabilities, and how these are exploited.

Pinning the tail onto 'online' fraud

A binary classification of online and offline fraud is misleading (Levi, 2022). 'Online' crime is perhaps more accurately represented as a continuum (Gordon and Ford, 2006; Phillips et al, 2022) and fraud, in all its diversity, traverses the whole continuum. There are examples where the locus of a fraud is primarily technological or online, but there are others in which online technology plays a more marginal role. Most fraud is somewhere in the middle; a hybrid where different mediums are woven into the criminal process as and when required to deceive the victims and steal the money. To illustrate, the example below is taken from Leukfeldt (2014) and breaks down the sequence of events involved in commissioning a banking fraud:

[16] https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf

[17] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

Steps for committing the banking fraud	Medium
A multitude of co-offenders who met, or were recruited from within the local community, including insiders in the bank and the postal service who provided information on the bank systems and customers.	Physical
Phishing emails sent to victims that appeared to be from their bank.	Online
Victims are asked to fill out and submit their details by email or click a link which took them to a website that was a copy of the legitimate website and under the control of offenders.	Online
Equipped with the victim's online banking details, the victim receives a phone call from the offenders posing as employees of the bank, to trick the victim into providing the transaction code that is needed to transfer money from their account.	Telephone
A series of transfers are made from the victims' online bank account.	Online
Money mules were recruited from local contacts, some were met in person and others approached through social media communications. The money was received into the money mule account and quickly withdrawn from cashpoints.	Physical/online

An alternative to examining the use of online technology through the lens of fraud methodologies, is to look at fraud methodologies (and any other crime) through the lens of online technology. So, while fraud is 'old wine', there may be value in switching focus to examine the particularities of technology that provide the various gateways into offending (i.e. 'the new bottles').

One study identified five core categories in a taxonomy of cybercrime; social engineering and trickery; identity-related crime; hacking; online harassment; and denial of service and information (Nurse, 2018). It identifies several behaviours that when mediated by online technology can provide key entry-points for committing fraud:

- Social engineering and online trickery: methods to 'exploit human psychology' though the application of online technology, to appear to be someone or something they are not. Key examples are phishing scams and romance fraud.
- Identity-related crime: methods that capitalise on the volume of information available online about individuals that can be exploited for monetary gain. Key examples include card-not-present and application fraud.
- Hacking: methods that include hacking of personal accounts or the deployment of malware to compromise computing systems or digital information. This can be used to acquire personal data, manipulate communications, and provides another entry-point for committing identity fraud.

None of these cybercrime categories pertain exclusively to fraud, but using this wider framework may produce meaningful interpretations of fraud when it is 'online'.

5. Does being 'online' matter?

There are some who dispute the significance of the 'online' component of fraud. This is in part due to the ubiquity of online technology, but also the limited significance of being 'online' for the person who has fallen victim; for them, online fraud is 'just fraud', and harm is harm (Cross, 2019). Furthermore, the 'online' classification potentially distracts the police from the job of delivering a service, because the police have been slow to adapt their capabilities to the demands from cybercrime, and slow to embrace their role in tackling it (Bossler and Holt, 2012; Cross, 2019).

The question is perhaps less whether the 'online' element is significant or not, but rather in what ways is it significant in terms of controlling and responding to fraud. It is the configuration of policies, structures and resources to a problem that is increasingly 'online', that is of key concern to policymakers who are tasked to deliver effective law enforcement, public protection or crime prevention strategies.[18] The online nature of fraud impacts on a number of different public policy objectives:

Law enforcement

Online technology has expanded the frontiers of offending, enabling a fraudster to communicate and transact with high volumes of prospective victims located anywhere on the globe, at speed and at little cost (Levi et al, 2015). Furthermore, online anonymisation and related technologies (e.g. encryption) facilitate the concealment of identities and criminal activities, and the capacity to co-offend and share criminal resources has been radically

[18] For example, the Serious and Organised Crime Strategy (HM Government, 2018) adopts the so-called 4 Ps – Pursue, Prevent, Protect and Prepare – which delineate law enforcement from other interventions that tackle structural causes such as vulnerability in communities.

transformed by the availability of online communications (for example, see Ablon et al, 2014; Leukfeldt et al, 2016; UNODC, 2015). The police have struggled to configure law enforcement activity to tackle crime in this context. Reasons include the fragmented structure of the police in the UK and internationally, with each separate jurisdiction focused on a localised rather than cross-border agenda; operating models that are primarily focused on responding to reported crime rather than on proactively uncovering hidden crime; and the difficulties of embedding digital investigation capability across the workforce (NPCC and APCC, 2020; Nagyfejeo, 2018; Skidmore et al, 2020b).

The different ways in which offenders make use of technology might influence how they are treated by law enforcement. Firstly, in establishing which offenders ought to be prioritised for a police response; for example, the police may choose to prioritise those who use automated technologies or engage with online criminal communities, because these technological enablers increase their capacity to repeat offend and so they present the greatest risk of harm (Brenner, 2004; Odinot et al, 2017).[19] Secondly, the role of technology will have a bearing on the types of police resources and capabilities that are assigned to respond. The complexity of a crime and the commensurate investigation can vary depending on how an offender exploits technology; for example, an effective criminal investigation of fraud that uses malware may require investigators with sufficient technical expertise (Gordon and Ford, 2006).

Finally, a significant proportion of online fraud emanates from overseas (for example, see Lusthaus and Varese (2017); Whitty, 2018). This external threat to internal order presents a fundamental challenge to the role and capacity of our domestic institutions to maintain law and order (Brenner, 2004). Furthermore, fraud and cybercrime can extend beyond the territory of criminal justice, with offending that is tied to national security matters such as terrorism, information warfare and interference by hostile states (Brenner, 2004; Wood et al., 2021).

Managing offenders

In addition to the widespread availability of criminal opportunities, research shows that people behave differently when online due to factors such as anonymity and the disassociation of the 'real' self from their online 'self' (Suler, 2004). This so-called 'disinhibition' effect fosters a propensity to commit crime that might not otherwise arise in the 'real' world.[20] And the same has been observed with fraud, with some individuals more readily engaging in harmful behaviour and able to rationalise crime and the harm that they cause if it involves faceless victims (Duffield and Grabosky, 2001; Hutchings, 2010).

A key implication is that people who would not otherwise commit crime can be drawn into fraud offending, creating new and more diverse pathways and offender profiles (for example, see Hutchings, 2013). This may include opportunistic and less determined offenders for whom prevention and diversionary interventions could prove to be a more effective, efficient or proportionate response. For example, there is growing concern over the rise in the number of young people being drawn into cybercrime offending, and the need for a more diverse set of responses such as education (Aiken et al, 2016; Davidson et al, 2022).[21]

Supporting and protecting victims

Public policy and the provision of resources and interventions are commonly informed by assessments of harm, or relatedly, risk of harm. In the past, public services had failed to acknowledge the impact and needs of fraud victims (Button et al, 2009; Cross, 2015). This issue is potentially compounded by the challenges in identifying and accounting for 'online harms' in ways that are comparable to traditional offline crime (DCMS, 2021). Frontline service providers in the police and other public services have limited capacity to assess and interpret online harms, and deliver support to address the impact, risk and needs of the victims (HMIC, 2015). Consequently, victims of online crime have tended to receive less robust responses than victims of offline crime.

Crime prevention

The ability to prevent crime relies on having a sufficient understanding of the patterns of crime and the underlying causal factors for how, where and why crime manifests in the way that it does. Many established techniques and strategies for preventing crime are rooted in opportunity theory, whereby crime results from a motivated offender converging with a suitable target, in an environment where a guardian is either absent or ineffective (Cohen and Felson, 1979).

Traditionally, analyses have focused on convergences in the physical world (for example, Tilley, 2008). However,

[19] For example, see also - https://www.darkreading.com/dr-tech/are-ai-engineered-threats-fud-or-reality-

[20] As an active participant in the fraud 'script', the same principles might apply to victims who behave online in ways they would not in other contexts (for example, see Williams et al, 2017).

[21] https://www.nationalcrimeagency.gov.uk/cyber-choices

cybercrime challenges these established theories for explaining crime (Leukfeldt and Yar, 2016; Yar, 2005). An online fraudster can just as easily target a bank in another country as they can in the local area, and the account holder may be somewhere else entirely. Geographic, demographic, social and economic patterns in fraud victimisation have been changed by online technology (Home Office, 2015). Furthermore, these patterns need to be considered alongside the ways in which fraud is distributed across online technologies and online spaces, for example, the ways in which different technologies are used to exploit the human vulnerability to social engineering (Nurse, 2018). Understanding the significance of 'online' to the patterns in fraud would seem to be a critical underpinning for any crime control strategy.

6. Conclusion

Fraud is daunting in terms of its scale and variety; the methods adopted by fraudsters, the criminal opportunities that are exploited, and the array of victims and victim experiences. Furthermore, the landscape is continuously changing as fraud methodologies adapt to new technological, social, commercial and economic contexts. In this context, official counts of total fraud are currently limited by their capacity to describe or explain the problem. Moreover, key data is dispersed among a wide range of stakeholders in the public and private sector, not only in relation to the occurrence of fraud, but also to instances of criminality and deviance that occur below the surface in an expansive digital ecology (e.g. data breaches or suspicious business entities).

Despite these challenges, effective use of the data is particularly important when responding to fraud for several reasons; the volume far exceeds the capacity of police and other public services to respond, so limited resources ought to be directed to where they are most needed; robust assessments help to direct the attention of practitioners that habitually do not prioritise fraud; and human assessments of victims and cases are increasingly being replaced by data analytics[22] (HMICFRS, 2019; Skidmore et al, 2018). Questions remain over whether existing data (particularly crime data) can be used to represent the demand for public services in meaningful terms, though it seems undeniable that data analytics have a vital part to play to ensure that resources and interventions are assigned in ways that are rationalised, effective, and accountable.

This paper has described the different ways we can understand the concept of online fraud. It has not developed a new taxonomy of online fraud, although the paper suggests that there might be better ways of organising our understanding of the problem. We will be looking at whether a better typology of online fraud might be developed as part of our wider programme of work undertaken in partnership with Crest Advisory and Birkbeck University.

Our aim is to develop a better understanding of the characteristics of online fraud, its effect on victims, how online fraud offenders operate and the effectiveness of the policy framework. The focus of that work will be on fraud that meets the following definition of cybercrime:

> *"… any [criminal fraud] that is facilitated or committed using a computer, network, or hardware device."*
> *(Gordon and Ford, 2006)*

This inclusive definition introduces the scope to explore the variable role and significance of online technologies to fraud offending.[23] It will encompass ancillary crimes such as hacking, corruption and money laundering but only when linked to fraud offending, because many of these offences are perpetrated for reasons other than fraud.

This programme of research[24] into online fraud will look at:

- How we organise our knowledge and data on online fraud, particularly ways to meaningfully show that online fraud is a source of demand for public services.
- Our understanding of victimisation and the impact of fraud, including the risk, needs and experiences of victims and the wider public.
- Our understanding of online fraud offending perpetrated in the UK, including the different methods, criminal opportunities and pathways into offending.
- Future trends in online fraud offending.
- The effectiveness of organisations with a role in tackling online fraud from the local to national level.
- The role that online anonymity plays in vulnerability to fraud and the key considerations for public policy.

A series of reports and outputs from this programme will be published over the course of 2023 and 2024.

[22] In the UK the national centralised systems for collecting and analysing crime are housed by Action Fraud and the National Fraud Investigation Bureau (NFIB).

[23] As noted in a previous section, frauds that target public sector bodies and that are addressed through internal regulatory enforcement (for example, tax or benefits fraud) are out of scope for this study.

[24] https://www.police-foundation.org.uk/project/improving-the-police-response-to-fraud-2-2/

7. References[25]

Ablon, L., Libicki, M. and Golay, A. (2014) *Markets for Cybercrime Tools and Stolen Data*: *Hackers' Bazaar*. RAND Corporation.

Adriaenssen, A., Paoli, L., Karstedt, S., Visschers, J., Greenfield, V.A., and Pleysier, S. (2020) Public perceptions of the seriousness of crime: Weighing the harm and the wrong. *European Journal of Criminology*, 17(2) pp.127–150.

Aiken, M., Davidson, J. and Amann, P. (2016) *Youth pathways into cybercrime*. Europol.

Albanese, J.S. (2005) Fraud: The characteristics crime of the twenty-first century.*Trends in Organized Crime* 8(4) pp.6-14.

Beals, M., DeLiema, M. and Deevy, M. (2015) *Framework for a Taxonomy of fraud*. Standford Center for Longevity/Investor Education Foundation.

Bossler A. M. and Holt T. J. (2012) 'Patrol officers' perceived role in responding to cybercrime'. *Policing: An international Journal of Police Strategies and Management* 35(1), pp.165-181.

Brown, C. (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology* 9(1) pp.55-119.

Brenner, S.W. (2001) Is There Such a Thing as "Virtual Crime"? *Criminal Law Review* 4(1).

Brenner, S.W. (2004) Cybercrime Metrics: Old Wine, New Bottles? Virginia Journal of Law and Technology, 9(13), pp.1-52.

Button, M., Blackbourn, D. and Shepherd, D. (2016) *The Fraud 'Justice Systems': A Scoping Study on the Civil, Regulatory and Private Paths to 'Justice' for Fraudsters*. University of Portsmouth.

Button, M. and Cross, C. (2017) *Cyber frauds, scams and their victims*. London: Routledge.

Button, M., Lewis, C., and Tapley, J. (2009). *Support for the victims of fraud: an assessment of the current infrastructure in England and Wales*. London: National Fraud Authority.

Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. (2014) Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, 47(3) pp.391–408.

Cifas (2019) Tackling first-party fraud: How industry and government can reduce the cost to consumers and businesses. London: Cifas.

Cifas (2023) *This is Fraudscape 2023*. Available at: <https://www.fraudscape.co.uk/>

Cohen, L., and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4) pp.588-608.

Correia, S. (2021) *Cybercrime victims: victim policy through a vulnerability lens*. SSRN Working Paper.

Correia, S. (2022) Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud. *International Journal of Population Data Science* 7(1) pp.1:09.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology.* 21(2) pp.187-204.

Cross, C. (2019) Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Ccriminological Research, Policy and Practice* 5(2), pp.120-131.

Davidson, J., Aiken, M., Phillips, K. and Farr, R. (2022) *Researching cybercriminality to design new methods to prevent, investigate and mitigate cybercriminal behaviour: 2022 Research Report.* London: Institute for Connected Communities, University of East London.

Department for Culture, Media and Sport (DCMS) (2021) *Online harms feasibility study*. London: DCMS.

Duffield, G. and Grabosky, P. (2001) *Psychology of fraud*. Canberra: Australian Institute of Criminology.

Ekblom, P., and Gill, M. (2016) Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime. *European Journal of Criminal Policy and Research*, 22(2), pp.319–339.

Farrell, G. and Birks, D. (2018) Did cybercrime cause the crime drop? *Crime Science* 7(8).

Fraud Act 2006 and Digital Fraud Committee (2023) *Fighting Fraud: Breaking the Chain*. Available at: <https://committees.parliament.uk/publications/31584/documents/177260/default/>

Fried, R. (2001) *Cyber Scam Artists: A New Kind of .con*. Available at: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6dcbfeb9fd78c14e3af7e051d435b88c98d38e37>

[25] Accessed 16.02.24

Gordon, S. and Ford, R. (2006) On the definition and classification of cybercrime. *Journal in Computer Virology* 2(1), pp.13-20.

Grabosky, P.N. (2001) *Virtual criminality: Old wine in new bottles? Social and Legal Studies* 10(2), pp.243-249.

Hales, G. and Higgins, A. (2016) *Prioritisation in a changing world: seven challenges for policing*. London: The Police Foundation.

HM Government (2018) *Serious and Organised Crime Strategy.* (Cmnd 9718). London: HMSO

HM Government (2022) *National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK*. London: Cabinet Office.

HM Government (2023a) *Fraud strategy: Stopping scams and protecting the public*. (Cmnd CP 839). London: HMSO.

HM Government (2023b) *No Place to Hide: Serious and Organised Crime Strategy 2023-2028*. London: The Stationery Office.

HM Government (2023c) *Economic Crime Plan 2, 2023-2026*. London: HM Goverment.

Her Majesty's Inspectorate of Constabulary (HMIC) (2015) *Real lives, real crimes: A study of digital crime and policing*. London: HMIC.

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) (2019) Fraud: Time to Choose. An inspection of the police response to fraud. London: HMICFRS.

Home Office (2015) *Serious and Organised Crime Protection: Public Interventions Model.* Available at: <https://assets.publishing.service.gov.uk/media/5a805fbe40f0b6230269320e/Gov.uk_Serious_Organised_Crime_deck_vF.pdf>

Home Office (2021) *Home Office Counting Rules for Recorded Crime: Fraud.* Available at: <https://assets.publishing.service.gov.uk/media/645b7b87479612000fc29318/nfib-fraud-april-2023.pdf>

Home Affairs Committee (2018) *Policing for the future: Tenth Report of Session 2017–19. HC 515.*

Hutchings, A. (2010) Cybercrime trajectories: An integrated theory of initiation, maintenance and desistance. In T. J. Holt (ed), *Crime Online: Correlates, Causes, and Context* (pp. 117-140). Durham: Carolina Academic Press.

Hutchings A (2013) Hacking and fraud: Qualitative analysis of online offending and victimization. K. Jaishankar and N. Ronel (eds), *Global Criminology: Crime and Victimization in the Globalized Era* (pp. 93-114).

Kennedy, L.W., Caplan, J. M. and Piza, E.L. (2018) *Risk-Based Policing: Evidence-Based Crime Prevention with Big Data and Spatial Analytics*. Oakland: University of California Press.

Kerr, J., Owen, R., Nicholls, C.M. and Button, M. (2013) *Research on sentencing online fraud offences*. London: Sentencing Council.

Leukfeldt, E.R. (2014) Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime*. 17(4) pp.231-249.

Leukfeldt, E.R., Kleemans, E. and Stol, W. (2016) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change* 67(1 pp.:39-53.

Leukfeldt, E. R. and Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behaviour 37(3), pp.263-280.

Levi, M. (2008) Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, 8(4), pp.389-419.

Levi, M. (2022) Frauds in Digital Society Housley W. Edwards A., Benito-Motagut R. an*d* Fitzgerald R. (eds) *in the Sage Handbook of Digital Society. Sage: London.*

Levi, M. and Burrows, J. (2008) Measuring the impact of fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology.* 48(3), pp.293–318.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. (2015) *The Implications of Economic Cybercrime for Policing*. London: City of London Corporation.

Lusthaus, J. and Varese, F. (2017) *Offline and Local: The Hidden Face of Cybercrime. Policing: A Journal of Policy and Practice* 15(3), pp.4-14.

Maguire, M. and Dowling, S. (2013) *Cyber crime: A review of the evidence. Research Report 75: Summary of key findings and implications*. Home Office.

Maguire, M. and McVie, S. (2017) Crime data and criminal statistics: A critical reflection. In Liebling, A., Maruna, S. & McAra, L. (ed) *The Oxford Handbook of Criminology*. Oxford University Press.

May, T., and Bhardwa, B. (2018) *Organised crime groups involved in fraud. Crime Prevention and Security Management.* London: Palgrave Macmillan.

Nagyfejeo, E. (2018) EU's Emerging Strategic Cyber Culture(s). *Policing: A Journal of Policy and Practice* 51(1), pp.79-102.

National Police Chiefs' Council (NPCC) and Association of Police and Crime Commissioners (APCC) (2020) National policing digital strategy: Digital, data and technology strategy 2020-2030. Available at: <https://pds.police.uk/wp-content/uploads/2020/01/National-Policing-Digital-Strategy-2020-2030.pdf>

Nurse, J. (2018) "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit" in *The Oxford Handbook of Cyberpsychology* (2018/19), Attrill-Smith, A., Fullwood, C. Keep, C. and Kuss, D.J. Oxford University Press.

Odinot, G., Verhoeven, M.A., Pool, R. and de Poot, C.J. (2017) *Organised Cybercrime in the Netherlands: Empirical findings and implications for law enforcement*. The Hague: WODC, Ministry of Security and Justice.

Ofcom (2021) *Scams research 2021: Chart pack.* Available at:<https://www.ofcom.org.uk/__data/assets/pdf_file/0029/232877/2021-ofcom-scams-survey.pdf>

Office for National Statistics (ONS) (2016) *Focus on property crime: year ending March 2016* Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/focusonpropertycrime/yearendingmarch2016#:~:text=In%20the%20survey%20year%20ending,compared%20with%20the%20previous%20year>

Office for National Statistics (ONS) (2022a) *Crime in England and Wales: year ending March 2022*. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022#:~:text=Police%20recorded%20crime%20in%20England,2020%20(6.1%20million%20offences)>

Office for National Statistics (ONS) (2022b) *Nature of fraud and computer misuse in England and Wales: year ending March 2022.* Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022#:~:text=Estimates%20showed%20there%20were%204.5,%E2%80%9Cconsumer%20and%20retail%20fraud%E2%80%9D>

Office for National Statistics (ONS) (2023a) *Crime in England and Wales: year ending March 2023*. Available: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023>

Office for National Statistics (ONS) (2023b) *Transformation of the Crime Survey for England and Wales: Discovery research on the redesign of multi-mode questions Discovery phase research into the feasibility of a multi-mode design for the Crime Survey for England and Wales (CSEW)*. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/transformationofthecrimesurveyforenglandandwalesdiscoveryresearchontheredesignofmultimodequestions>

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S. and Aiken, M.P. (2022) Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences* 2(2), pp. 379-398.

Sentencing Council (2014) *Fraud, Bribery and Money Laundering Offences: Definitive Guideline*. Available at: <https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud-Bribery-and-Money-Laundering-offences-definitive-guideline-Web.pdf>

Shover, N., Coffey, G. and Sanders, C. (2004) Dialing for Dollars: Opportunities, Justifications, and Telemarketing Fraud. *Qualitative Sociology* 27(1), pp.59-75.

Skidmore, M. and Aitkenhead, E. (2023) *Understanding the characteristics of serious fraud offending in the UK*. Available at: <https://www.police-foundation.org.uk/wp-content/uploads/2023/05/serious_fraud_FINAL.pdf>

Skidmore, M., Goldstraw-White, J., and Gill, M. (2020a). Vulnerability as a driver of the police response to fraud. *Journal of Criminological Research, Policy and Practice* 6(1), pp.49-64.

Skidmore, M., Goldstraw-White, J., and Gill, M. (2020b). Understanding the police response to fraud: the challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management,* 40(5) pp1-11.

Skidmore, M. (2020). *Protecting people's pensions: Understanding and preventing scams.* The Police Foundation. Available at: <https://www.police-foundation.org.uk/publication/protecting-peoples-pensions-understanding-and-preventing-scams/>

Skidmore, M., Ramm, J., Goldstraw-White, J., Barrett, C., Barleaza, S., Muir, R., and Gill, M. (2018). *More than just a number: Improving the police response to victims of fraud.* The Police Foundation. Available at: <https://www.police-foundation.org.uk/publication/more-than-just-a-number-improving-the-police-response-to-victims-of-fraud/>

Suler, J. (2004) The Online Disinhibition Effect. *CyberPsychology & Behavior*. 7(3), pp.321-6.

Tilley, N. (2008) Modern approaches to policing: community, problem-oriented and intelligence-led in Newburn. T. (ed) Handbook of policing. Cullopton: Willan, pp.401-431.

Tun, L. and Birks, Z.. (2023) Supporting crime script analyses of scams with natural language processing. *Crime Science* 12(1).

UK Finance (2022) 2022 *Half year fraud update.* Available at: <https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf>

UNODC/UNECE (2012) Principles and Framework for an International Classification of Crimes for Statistical Purpose: Report of the UNODC/UNECE Task Force on Crime Classification to the Conference of European Statisticians.

United Nations Office on Drugs and Crime (UNODC) (2015) Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children. New York: UNODC.

Vasiu, L. and Vasiu, I. (2004) *Dissecting Computer Fraud: From Definitional Issues to a Taxonomy. Proceedings of the 37th Annual Hawaii International Conference on System Sciences (2004)* Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2578514>

Wall, D. (2007a) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research: *An International Journal* 8(2) pp.183 205.

Wall, D. (2007b) *Cybercrime:The transformation of Crime in the Information Age.* Cambridge: Polity Press.

Whitty, M. (2018) 419 – It's just a Game: Pathways to CyberFraud: Criminality emanating from West Africa. *International Journal of Cyber Criminology* 12(1), pp.97-114.

Williams, E.J., Beardmore, A. and Joinson, A.N. (2017) Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior* , 72(2017), pp.412-421.

Wood, H., Keatinge, T., Ditcham, K., and Janjeva, A. (2021) *The silent threat: The impact of fraud on UK national security*. Royal United Services Institute. Available at: <https://rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security>

Yar, M. (2005) The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* 2(4), pp.407-427.

Yar, M. and Steinmetz, K.F. (2019) *Cybercrime and Society* (Third Edition). Sage.

Yip, M., Shadbolt, N. and Webber, C. (2013) *Why Forums? An Empirical Analysis into the Facilitating Factors of Carding Forums. ACM Web Science*. Proceedings of the 5th Annual ACM Web Science Conference. Available at: <https://www.researchgate.net/publication/266653699_Why_forums_An_Empirical_Analysis_into_the_Facilitating_Factors_of_Carding_Forums>

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE
POLICE
FOUNDATION
The UK's policing think tank