UNDERSTANDING THE CHARACTERISTICS OF SERIOUS FRAUD OFFENDING IN THE UK

THE POLICE FOUNDATION
The UK's policing think tank

MICHAEL SKIDMORE
AND BETH AITKENHEAD

MAY 2023

UNDERSTANDING THE CHARACTERISTICS OF SERIOUS FRAUD OFFENDING IN THE UK

Acknowledgements

We are very grateful to the Home Office for funding this research. The views expressed in this report are solely those of the authors. We would also like to express our gratitude to the police forces who gave their support to the work and facilitated access to data and personnel. And finally, we would like to thank all practitioners who gave up their valuable time to feed their knowledge and experiences into this study.

About the Police Foundation

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Its mission is to generate evidence and develop ideas which deliver better policing and a safer society. It does this by producing trusted, impartial research and by working with the police and their partners to create change.

Cover: iStockphoto

CONTENTS

EXECUTIVE SUMMARY

This study aims to improve our understanding of the most serious fraud offences perpetrated in the UK, specifically the diversity of methods for committing these crimes, the characteristics and pathways of offenders involved and where applicable, how the groups or networks of offenders operate. This is an exploratory study which used qualitative data taken from the documents compiled by police practitioners in 25 separate criminal investigations.

The cases included in this analysis do not constitute a representative sample of frauds in England and Wales during this period. The selection of cases reflects the choices made by the research team to incorporate a diversity of methods, offenders and settings to capture the breadth of fraud. Furthermore, the sampling frame is the product of practitioner choices over which crimes to assign investigation by specialist teams; these are a limited resource and due to the challenges of international investigation, will likely prioritise offending that has a footprint in the UK. Furthermore, in focusing on frauds that were perpetrated (at least in part) from within England and Wales it does not represent fraud offending that emanates from other countries.

The specific fraud cases were serious for different reasons; high financial losses (£100,000 or more), high volume offending (50 or more known victims) and high victim impact (assessed by the victim and/or police practitioner). These dimensions of harm reflect those used in practitioner assessments for deciding which frauds are high harm and a priority for intervention. Only three cases satisfied all three harm criteria, all of which involved the mis-selling of investments. Twelve cases satisfied only one criterion and those linked to each dimension of harm were associated with different methods and victims; all cases that fulfilled the high financial loss criterion had defrauded businesses, and two out of three that fulfilled the high-volume criterion involved taking advance payment from consumers.

In five cases the scale of victimisation and impact was hidden, but they were included because they involved high-risk offenders suspected of being engaged in serious and complex offending.

There was considerable diversity in the methods for perpetrating serious fraud and this study borrows from a typology of acquisitive crime developed in a previous study (Naylor, 2002). This model provided a good fit for distinguishing serious frauds on the basis of two overarching models of offending, and this delineation simultaneously revealed distinctions in the situational context, victim and offender profiles:

- **Commercial frauds**: perpetrated from within a legitimate or pseudo-legitimate business setting and included the sale of investments or the mis-selling of products or services online or face-to-face, and nearly all had victimised individual members of the public.
- **Predatory frauds**: involved theft by impersonating legitimate individuals or organisations, mostly by offenders operating from outside of a business setting and without the pretence of a legitimate commercial exchange. The victim profile was more varied, and over half had victimised businesses (for example, payment diversion fraud).

There was divergence in the types of fraud offence encompassed by each category of fraud. A full description can be found in Table 3.

THE METHODS FOR PERPETRATING SERIOUS FRAUD

The successful commission of these offences relied on gaining sufficient trust from victims. In commercial frauds the offenders concealed their activities behind a front that rendered them indistinct from legitimate operators within the relevant sector. A small number offended from within an otherwise legitimate organisation or occupation and counted among the most prolonged and high value frauds in this study. In other cases, the offenders fabricated an elaborate veneer by exploiting a range of business services to appear legitimate. Overseas financial services and products played a key role in evading regulators in the UK.

In predatory offences a range of methods were used to impersonate a legitimate individual or organisation to gain trust to deceive victims. This included the forcible infiltration of IT systems (e.g. hacking) to manipulate communications, the use of stolen or fake digital accounts or enlisting corrupted insiders from within the victim company. A small subset engaged in direct communication with victims to persuade them that they represented a legitimate organisation (e.g. the bank or police).

The common elements present in many of the cases included:

- Covering the financial trail: the success of many offences reflected the ability of offenders to manipulate business or finance systems so to access the criminal proceeds without being identified. The methods varied by context, with multiple commercial fraudsters exploiting global finance systems to launder money, and other (particularly predatory) offenders releasing stolen funds as cash or high value purchases. The recruitment of money mules for this purpose was evident in nine cases.
- The role of online crime and cybercrime:[1] the internet facilliatated most offences in at least one of the following ways – marketing and other communication to deceive existing and prospective victims; infiltration and manipulation of IT systems; evasion of detection through the use of anonymisation technology; or digital finance.
- Vulnerability: Many attempts to perpetrate fraud end in failure and so offenders sought to maximise the likelihood of success by targeting individuals or organisations that were considered most susceptible to the deception. In some cases, the offenders continued to exploit an identified vulnerability, leading to repeat victimisation.

The cases encompassed serious fraud that involved online and cybercrime, telemarketing and global finance systems, however taken overall these cases were strikingly local in their impact. Only six cases involved victims from overseas jurisdictions, and most offenders and offending were confined to the UK or in some cases, the region in which offenders lived.

THE PROFILE AND PATHWAYS OF SERIOUS FRAUD OFFENDERS

Of the 25 cases in this study, a total of 104 offenders were identified. In 12 cases two or more co-offenders had been identified in the investigation and there were suspected co-offenders involved in nine additional cases. Many offenders adopted a discrete role and function in the overall fraud, including sales, couriers (to collect the money or material goods) and money laundering.

Most offenders were male. Over half (52 per cent) of the offenders were aged 18-30, many of whom who adopted more peripheral roles in the fraud offence, and one in five were aged over 45. The majority of offenders (80 per cent) were British nationals. The ethnic backgrounds of the offenders were more mixed, with individuals from Black and minority ethnic groups over-represented. The offenders from minority ethnic groups were concentrated in a small number of cases, reflecting the prominence of co-offending that emanated from within the same local communities.

There were distinctive routes taken by different individuals into serious fraud, which varied not just by offence type, but also by the different roles that offenders took in the network:

- In at least ten cases there were offenders with prior links to serious criminality, commonly those with a central role in planning and coordinating the fraud and who received most of the illegal proceeds. These offenders had no legitimate source of income. Most had ties to a network of prospective co-offenders from which they could draw to facilitate the offence. In three cases the offenders had enduring ties to an urban street gang, two of which specialised in courier fraud offences. Other examples were in the commercial setting, including three cases in which the coordinating offenders had previously co-offended to perpetrate serious fraud and money laundering offences.
- There were eight cases that involved offenders for whom the opportunity to perpetrate fraud derived from an otherwise legitimate occupation. Two had

1. The nature and extent of the overlap with cybercrime showed considerable variation and in the sample there were cases that could be classified as cyber dependent, cyber enabled or cyber assisted (for example, see Levi et al, 2015; Maguire and Dowling, 2013)

abused their position as a director of a company to steal money from clients to fund a serious gambling addiction. Others used their occupation to defraud their employer or its clients: two frauds had been perpetrated in collaboration with offenders outside of the company. In at least three cases the offenders had used a frontline occupation in the informal economy – the building, care service or ticket sales sectors – to defraud local clients.

- A high proportion of the identified offenders took a peripheral or enabling role with the anticipation of modest financial gain, and as events unfolded, some received no recompense for the part they played in the fraud. Many offended for subsistence due to having little personal wealth and difficulties in earning a legitimate income, and some experienced significant financial hardship. Some frauds enlisted younger co-offenders with the promise of wealth or status that was put on display by other co-offenders; this included younger members of the urban street gang and those recruited to work in boiler rooms.

CO-OFFENDING AND COORDINATION

The recruitment of co-offenders was critical to many of the frauds in this study. This included individuals in possession of specialist skills or resources required in the commission of the fraud or to launder the illicit proceeds. However, many entered into the fraud with no specialist knowledge or resource, and often provided the interface with the victim and were the most exposed to detection; for example, the salesperson making unsolicited calls or the money mule who receives the victim's money into their account.

Much co-offending emanated from within an offender's established social network, such as those in the local community or neighbourhood. Some drew from networks of criminals with whom they had previously offended or in the case of commercial fraud, professionals in the business community. Larger networks provided the scope for offenders to draw flexibly from the resources of others, thereby enabling them to persist in and diversify their offending. Equally, there were clear examples of shared learning that appeared to set some peripheral offenders on to their own fraud offending pathway.

There were no cases in which the groups operated as a stable hierarchy. Much of the collaboration, especially among the more peripheral co-offenders, was restricted to the duration of the specific fraud, which represented time-limited project crimes. In each there was one or a small number of core individuals who planned and coordinated the activities of co-offenders who operated in isolation of one another; this included those who provided specialist skills or resources for a fee (for example, carding forums which supplied stolen credentials), specialist money launderers and more expendable frontline enablers such as money mules.

KEY IMPLICATIONS FOR POLICY AND PRACTICE

Fraud is an offence category that encompasses a wide range of methods and a broad spectrum of harm. This study draws attention to the limited conceptualisation and the challenge for delineating a subset of fraud offending that is 'serious', one that has significance for how law enforcement agencies rationalise their strategic and operational choices. This is especially relevant for fraud, a crime that has strained for prominence on the police agenda (HMICFRS, 2019). This research shows 'serious fraud' is an increasingly diverse construct within law enforcement, incorporating a diverse cohort of offenders and offending. It includes highly specialised fraudsters operating in particular occupational settings (e.g., financial services), and to a large extent, generalist offenders responding to the growth of opportunities to commit fraud online. Serious fraud is a diverse problem that requires diverse interventions and some key implications for policy and practice are listed below:

- **Pursuing offenders**: seriousness and complexity can sit behind ostensibly low harm fraud offences (e.g. an online shopping fraud), which highlights the limits to criminal investigation responding to a reported crime instead of pursuing the perpetrators. Moreover, the police need not be constrained to conventional criminal investigation. In some cases, the fraud was largely contingent on money laundering capability, a particularly exposed element of an otherwise hidden criminal process and so one that is more vulnerable to intervention. Incapacitating

those engaged in money laundering has the potential to constrain the capacity of the wider network to perpetrate serious fraud.

- **Diverting offenders**: not all those involved in serious fraud offending are serious offenders, especially those on the peripheries of the conspiracy and who are more expendable to the network. Effective intervention may need to be sensitive to the potential vulnerabilities of co-offenders so as to divert them from further offending. These offenders may also be a vital source of intelligence so there may be gains from a strategic approach to encourage individuals or vulnerable groups to approach the authorities with their concerns.

The rise of digital communications and finance means that serious fraud is borderless in scope. However, this research gives multiple illustrations of serious frauds which impacted in the UK and were perpetrated from within the UK. The requirement to appear credible to deceive victims and the various guardians in the private and public sector, and the pragmatic steps needed to gain access to the illicit proceeds, means that many opportunities to perpetrate fraud are domestic. In the context of crime control this introduces new considerations on how to configure policies and resources, specifically the appropriate balance between offender-oriented strategies such as disruption and diversion, and wider victim-oriented interventions.

1. INTRODUCTION AND BACKGROUND

Fraud is a high-volume crime that encompasses a wide diversity of offending methods, including complex and serious crimes (Levi, 2008; May and Bhardwa, 2018). Fraud is a recognised element of serious and organised crime in the government strategy (HM Government, 2018) however many serious frauds remain hidden due to widespread under-reporting and the barriers to effective criminal investigation (Blakeborough and Correia, 2018; Skidmore et al, 2018). The definitional boundaries for a serious fraud offence are unclear, but incorporate high value frauds, offences that exploit and target vulnerable people, fraud perpetrated by organised crime groups and those enabled by serious crimes such as money laundering and computer misuse crime (HM Government, 2018; Sentencing Council, 2014; Serious Crime Act, 2015).

There remain considerable gaps in the evidence for understanding the behaviour of serious fraud offenders including the pathways taken into offending, the characteristics of offenders and groups and the methods and techniques used in the commission of these crimes. Studies in the past have focused on those who offend within a white collar setting, including offenders who react to opportunities that arise in their legitimate occupation and others who more actively exploit their role to persistently offend (Shover et al, 2004; Van Onna et al, 2014; Weisburd and Waring, 2001).The rise in the volume of fraud offending dovetails with the change in the nature of these crimes, most significantly in response to the widespread adoption of online communications and finance which has diversified and expanded opportunities to perpetrate fraud (Ablon et al, 2014; Levi et al, 2015). In addition to online fraud that emanates from overseas (Lusthaus and Varese, 2017; Whitty, 2018) there is emerging evidence that offending within the UK is changing, drawing in a greater diversity of offenders from different backgrounds (Roks et al 2020).

1.1 RESEARCH AIMS AND OBJECTIVES

There has been little previous research into fraud offending in England and Wales. The sheer scale of fraud and the diversity of methods in use (for example, see Home Office, 2021) suggests a problem that is wide-ranging in complexity and impact, with a high volume targeted at public and private sector agencies that engage in internal counter-fraud and enforcement measures (Button et al, 2016). The focus of this study will be on the most serious frauds investigated by the police forces included in this study, specifically those which impact on the local public and businesses (though acknowledging the inevitable overlap with corporate victims in cases such as identity fraud). This more restricted perspective focuses the analyses on offenders that are comparable in terms of harm and/or complexity.

In addition to the diversity of methods for perpetrating serious frauds, this study will examine the characteristics of the different offenders, identifying commonalities and distinctions, the pathways taken into perpetrating these crimes and in cases linked to co-offenders, the structures and processes for coordinating the offending.

The key research questions that this work aimed to address are:

- What are the different models of offending linked to serious fraud?
- What are the key contexts, opportunities and enablers of serious fraud?
- Who are the perpetrators of serious fraud?
- What are the individual pathways and opportunities for involvement in these crimes?
- What are the characteristics of co-offending in groups linked to serious fraud?

1.2 METHODOLOGY

The research approach was divided into three parts:

- Literature review: We completed a review of the existing research evidence. Key themes included fraud offenders (including where relevant, white collar and cybercrime offenders), criminal pathways theory for fraud and organised crime and the methods used in serious fraud offending. This review informed the development of subsequent methodologies including the framework for collecting the data from police documents and interviews.
- Case-file analysis: We examined the documents collected and compiled by the police in 25 separate criminal investigations. The information was extracted from these documents into a data collection framework which arranged information into key themes: the nature of serious fraud, the methods used by offenders, the roles and pathways of individual offenders, and group structure and cooperation. The data collection framework was initially based on the literature review and was further developed during the process of data collection.
- Semi-structured interviews: We conducted a total of 17 interviews with lead investigators for each case file included in the study; in four interviews, the same investigator discussed multiple cases.[2] These interviews were structured under the same key themes used in the data collection framework, and the focus was to supplement and fill any gaps in the information available in the police documents and test the validity of our initial findings. The interviews were recorded and the relevant information manually integrated into the data collection framework. Each interviewee was asked to provide answers based only on the facts of the case, avoiding speculative or generalised comments.

Once the information from the police documents and interviews had been collected, the data was analysed to identify patterns and themes relevant to the objectives of the study.

1.2.1 Case selection

Serious fraud cases were identified as those which had been assigned by police to specialist fraud, economic or cybercrime investigation units, under the assumption that because these units constitute such a limited resource (for example, see Skidmore et al, 2018) they are assigned to tackle only the most serious fraud cases. This was a pragmatic step to identify fraud and/or fraudsters that had been pre-defined by law enforcement as serious, as well as cases for which sufficient information had been collected during proactive investigation.

From a total of 25 cases, 21 were selected from the caseloads of specialist economic or cybercrime teams in five local police force areas and four from the caseload of a national investigation unit. A purposive sampling strategy was used to capture the diversity of fraud offenders and methods, including:

- fraud cases with two or more co-offenders;
- cases with links to other criminality (for example money laundering)
- cases that targeted individual victims and / or businesses
- cases that represented the diversity of fraud offence categories including those perpetrated in high volumes and those that cause high harm to victims.

In total there were 104 offenders linked to the 25 cases, with 12 cases that involved multiple offenders. All cases involved at least one perpetrator who had offended from within the UK and targeted members of the public or small to medium-sized business. Corporate and insider frauds and fraud targeting organisations in the public, third or corporate sector were broadly excluded, though in some cases the impact was shared between local individuals or businesses and corporate bodies (for example, some identity frauds impacted on account holders and corporate financial services).

The number of cases from each police force ranged from two to seven, partly reflecting their capacity to provide cases with sufficient detail. All cases related to investigations initiated within three years prior to data collection[3] and had undergone a comprehensive police investigation; in 12 cases the offenders had been convicted, seven had been charged and awaited trial, four had reached the stage of charging the offender and two had not been successfully progressed to a charge.

2. In one case, the lead investigator had provided a written response to questions in the interview template and in another, it had not been possible to contact the investigator to conduct an interview.
3. The data for the 25 cases studies was collected from the various police agencies between September 2020 and January 2021.

1.2.2 Key limitations

The cases selected for this study do not represent the distribution of serious fraud in the UK during this period. Cases were not selected at random but rather to capture the full breadth of serious fraud offending. Furthermore, these cases represent only fraud offences that were detected and selected for investigation by the five law enforcement agencies. It is known that a significant proportion of fraud is not reported to the police or otherwise identified, and the extent to which the cases in this study are representative of all serious fraud offending is not known.

The information provided by the different law enforcement partners varied in format but most shared police intelligence logs, case management notes and court summaries. The majority of the information incorporated into this analysis was extracted from these documents, and data to verify and supplement this information was collected in interviews. There was some variability in the completeness of the information for each case, reflecting in part the resources available to each investigation team, their specific objectives and the ability to collect the accounts of victims or suspects. Some investigations were targeted to the money laundering network, not the individuals central to the commission of the fraud. Moreover, criminal investigations are primarily focused on deconstructing the offending for the purposes of gathering evidence therefore information on offenders – who they are, their pathways into offending and how they collaborate – was often not complete. In general, the more specialist investigation teams collected the most contextual information through the use of proactive investigative techniques. That said, the frauds investigated by local police forces involved methods or group structures that were less complex.

2. CHARACTERISTICS AND METHODS OF FRAUD

SUMMARY

There is a bewildering range of scenarios in which offenders can employ deception to perpetrate serious fraud, however closer analysis revealed a number of common elements and themes across the different methods employed in each case. Particularly prominent were the distinctions between commercial and predatory frauds which revealed distinctions in the offence model, setting and the characteristics of the victims. In both categories, success for offenders relied on the ability to appear legitimate and credible to gain the trust of victims. In the context of commercial fraud, many offences required elaborate business structures and systems to appear as legitimate organisations within financial or commercial markets. In predatory offences various techniques included the use of insiders or technology to infiltrate IT systems or access data, to disguise themselves as a legitimate individual or organisation.

However, common themes across all cases included strategies to target people or entities most vulnerable to the deception, and the adoption of techniques to cover the financial trail. In most cases, the offence represented a complex, multi-staged process that established a veil of legitimacy and enabled the fraudsters to repeat offend. However, many frauds were time-limited, lasting only as long as the deception could be sustained. In this regard many could be considered project crimes. Predatory offence methods were particularly time-constrained because of the more explicit nature of the theft which was more quickly identified and reported by the victim or bank. Those who offended from legitimate occupations were able to engage in continuous offending over prolong periods of time.

2.1 THE CHARACTERISTICS OF SERIOUSNESS

Cases were included in this study on the basis that the offenders had perpetrated a serious crime. Offence seriousness can be defined using multiple criteria to reflect the scale of offending by the fraudsters and the actual or intended impact on victims (Sentencing Council, 2014). Impact can be measured by the value of the financial losses but must also take account of key contextual elements that include victims who are vulnerable, groomed over time, repeat victimised or otherwise exploited, and also the subjective impact on their physical, mental and financial wellbeing (Kerr et al, 2013; Skidmore et al, 2020). These factors are not mutually dependent and therefore different offences can be 'serious' for different reasons.

The case selection primarily reflects practitioner decision-making about which of the fraud cases that came to their attention should be treated as serious and prioritised for investigation. The seriousness of each case was examined using the following dimensions of victimisation and impact (see Table 1 below).

Table 1: The dimensions of seriousness

Type of victimisation and impact	
High volume of victims	For the purposes of analysis, high volume fraud was defined as a case that involved the victimisation of 50 or more known victims.
High harm to individual victims	This criterion reflects the subjective impact on the victims, based either on their own account or the assessment of the investigator. Cases that were high-harm included those assessed by officers to have caused a significant detriment to a victim's lifestyle or wellbeing, targeted the same victim on multiple occasions or in which a victim was otherwise flagged as vulnerable (for example, due to a mental health difficulty).
Intended aggregate losses to victims	Collective financial losses to known victims that amounted to £100,000 or more. This included not only actual losses to victims but also the intended loss (or attempted gains), thereby reflecting both victim impact as well as the intent and capabilities of the offenders.
Type of offender	
Hidden and complex	This dimension is included to represent cases for which the scale of victimisation and impact was not known, but the offenders were assessed by practitioners to be involved in serious fraud. It acknowledges the importance of offender characteristics as an additional factor in determining the seriousness, with repeat offending, complex modus operandi and links to co-offenders indicative of greater culpability, risk and the presence of organised crime (HM Government, 2018; Sentencing Council, 2014).

Table 2 shows the characteristics of seriousness in the fraud cases included in this study. In 13 cases the intended aggregate victim losses exceeded £100,000, ranging from a victim who lost £130,000 in an authorised push payment fraud to a £39 million investment fraud. In eight cases the volume of known victims exceeded 50. This included one outlier impacting over 27,000 online consumers and the remainder ranged from 55 to 900 victims. Ten frauds were assessed to have caused high victim harm, though in some cases the impact was variable between different victims.

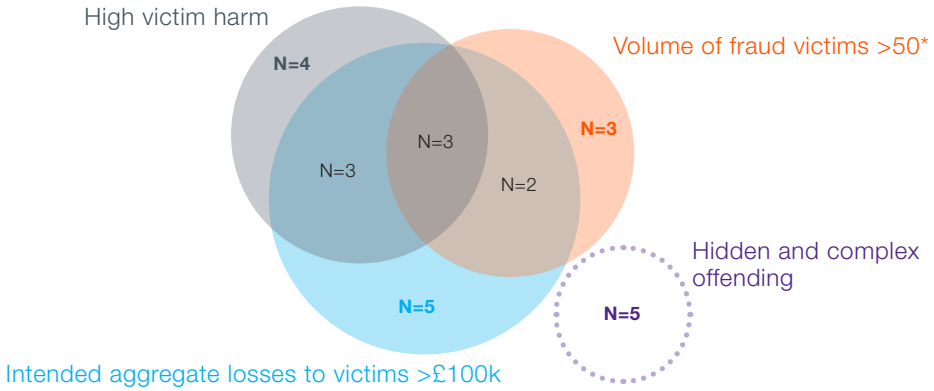
These characteristics are the sum of knowledge developed by police investigators in each case and may underestimate the true scope or impact of offending particularly in the case of five 'hidden and complex' cases that are included on the basis of the offenders' characteristics.

Table 2: The characteristics of seriousness in the fraud cases

Dimensions of seriousness	No. of cases	Range
>£100,000 intended aggregate losses	13	£130,000 to £39 million
50 victims	8	55 to 27,361
High harm to an individual victim	10	N/A
Hidden and complex offending	5	N/A

Figure 1 shows the variable composition of seriousness in the different cases. Eight cases contained two or more of the criteria for seriousness but only three cases satisfied all three (high volume, aggregate loss and victim harm), all of which pertained to the sale of fraudulent investment schemes. 12 cases satisfied just one of the three seriousness criteria and involved distinctive methods; for example, the five cases in which the intended aggregate losses exceeded £100,000 had all targeted local businesses, and two of the three which impacted on 50 or more victims involved taking advance payment from consumers for items not provided.

Figure 1: The composition of seriousness in the fraud cases



* This includes all known victims including those compensated for their losses but excludes fraud offending that was suspected but not confirmed by the investigators.

The scale of victimisation and impact was more hidden in five cases, but each had involved 'hidden and complex offending' in which the offenders had suspected links to wider criminal networks and criminality, including money laundering and computer misuse crimes; four out of the five were linked to payment diversion fraud that involved a precursor computer misuse offence.[4] To illustrate, in one case the offenders had hacked into company IT systems and while only two specific victims had been identified, the central suspect was connected to multiple co-offenders and was observed to regularly facilitate money laundering.

In total, twelve cases involved multiple offenders[5] but only five were formally recognised as an organised crime group (OCG) by police, reflecting to some extent the limited priority afforded to fraud compared to other forms of organised crime (Skidmore et al, 2018).

2.2 THE CHARACTERISTICS OF THE OFFENCES

The literature has shown that fraud can arise in a variety of business and market settings that lay the ground for highly distinctive offending opportunities, social contexts, offender characteristics and victims (Levi, 2008). And further, it shows that serious fraud takes a different shape depending on the social and economic context from which it emerges, and the internet has played a significant role in expanding and diversifying these contexts as new opportunities to perpetrate fraud increase in line with a growing number of social, commercial and financial activities that have moved online (Leukfeldt and Yar, 2016; Van der Geest et al, 2017).

The cases in this study were selected to represent the breadth and variety of offending that is part of serious fraud. The identification of discrete typologies is important for refining our understanding of this complex area of crime and helping to inform and focus public strategies and interventions to the problem. Previous research identified two overarching typologies of acquisitive crime (Naylor, 2002):

- *Commercial crime:* perpetrated from within a 'normal' business setting, these crimes involve the production or provision of products or services through illegal means (for example, financial services or online commerce). Superficially, there is a voluntary exchange with a victim, though with an involuntary aspect, such as the underlying deception in a sales pitch or unfair market value. The income that is 'earned' or generated is unmerited due to the illegal methods used by the offender.
- *Predatory crime:* perpetrated outside of a 'normal' business setting or relationship, and without the pretence of an exchange with the victim. These crimes represent the redistribution of wealth (e.g. money taken from one account and placed

4. These crimes and associated offenders were among the least visible to police investigators.
5. This excludes peripheral actors in the wider business sector, criminal markets or local community (including money mules) who enabled fraud offending.

into another), often through involuntary transfers either by force or through a process of deception. Victimisation and losses are straightforward to determine.

For each serious fraud case, the characteristics of the 'inclusion' offence were analysed and Table 3 below divides the cases into the commercial and predatory fraud categories; 10 were classified as commercial and 15 as predatory fraud. These two categories do not differentiate fraud offences by seriousness or complexity, but several distinctions are revealed:

- *Fraud offence methods*: Commercial frauds were predominantly comprised of investment, online or face-to-face sales, and predatory frauds included payment diversion, identity and authorised push payment fraud.
- *The role of online crime and cybercrime:* Only two commercial fraud cases involved online crime in the commission of the offence, principally the use of online marketing and sales. Four predatory fraud cases had involved computer misuse crimes to infiltrate IT systems using computer misuse crime and two others had links to online networks selling stolen identity data.
- *The impact of the offence*: Nearly all (10) commercial offences had impacted on an individual victim.[6] While some predatory frauds impacted on individuals, many targeted businesses; in eight cases the offenders had directly (e.g. payment diversion fraud) or indirectly (e.g. identity fraud) victimised a business.
- *The offenders:* There was limited crossover between commercial and predatory offending, most likely reflecting the distinctive settings in which the different offenders operated. Most commercial frauds were perpetrated from within a more conventional white-collar business setting. In contrast, most predatory fraudsters did not operate from behind a commercial front, but instead manipulated people or systems from without, commonly by impersonating a legitimate person or organisation online, over the phone or face-to-face. However, there were four cases in which offenders used an occupation in the informal economy to facilitate their offending, two had involved the mis-selling of tickets or building services (i.e. commercial) and another two, stealing money from vulnerable customers (i.e. predatory).

The majority of offenders had perpetrated fraud that was exclusively predatory or commercial in nature. Fraud encompasses such a wide range of offending behaviours and the classification taken from Naylor (2002) was adopted as a good fit for articulating an overarching distinction in the methods of offending observed across the cases. This also distinguished some of the situational opportunities within different social or other situational contexts – for example, the opportunities to mis-sell investment schemes requires knowledge and the resources and means to access these markets that many predatory offenders were unlikely to possess.

The cases were classified as predatory or commercial frauds based on the characteristics of the inclusion offence for this study, and each was classified according to the offence that was foremost in the investigation.[7] While the distinctions between commercial and predatory fraud offences and offenders (noted throughout the report) represent the predominant pattern, some overlap was evident in a minority of cases:

Patterns in offending: the characteristics of 'recovery'[8] fraud mean it is predatory in nature, but it can dovetail with commercial fraud by falsely promising to return a victim's money after they have been mis-sold an investment scheme. In one case, the investigator suspected that the same individual who had mis-sold the investment to a victim, following a hiatus, had made contact to claim he could recover this money for a fee. In addition, offenders in an enabling role, particularly in relation to money laundering, can be linked to multiple offenders perpetrating different types of fraud. One offender was suspected to have laundered the proceeds of investment, payment diversion and loan application frauds.

6. In two cases the legitimate service provider had provided some of the victims with compensation.
7. A small number of cases had involved fraud offending that was concurrent or consecutive to the inclusion offence; for example, in one payment diversion fraud an offender had concurrently perpetrated identity fraud.
8. This fraud method involved an offender contacting a previous fraud victim (commonly a victim of investment fraud) posing as a legitimate company that is able to recover the money the victim has lost or assist in apprehending the offender. The victim is asked to pay a fee upfront for this service and in this way, they are re-victimised (Home Office, 2022).

Table 3: The distribution of fraud offence types included in this study

Fraud method	Description	Home Office offence category	No. of cases
Commercial fraud			
Investment	The marketing and sale of investment schemes to the public.	Share sales or boiler room	2
		Pyramid or ponzi scheme	2
Consumer and retail	The mis-selling of various goods and services including gift items, foreign currency, event tickets and building services. These were marketed online or in-person	Online shopping and auction	2
		Ticket fraud	1
		Door to door sales and bogus tradesmen	1
Other	Frauds perpetrated from within a business setting. One involved the abuse of a position at a firm of solicitors to defraud clients, and in the other, the owner of an online retail business enabled and perpetrated various types of fraud.	Abuse of position of trust	1
		Other fraud (not covered elsewhere)	1
Predatory fraud			
Payment diversion	The infiltration and manipulation of a company's IT systems for communications / finance, to divert payments or transfers to an account controlled by the offender	Mandate fraud	5
Identity fraud	The use of stolen personal / financial information or materials (e.g. bank cards) to gain access to money or financial products or purchase goods / services. Transactions were online or in-person, and some used falsified identity documents.	Cheque, plastic card and online bank accounts	2
		Application fraud	1
		Abuse of position of trust	1
Authorised push payment	Unsolicited phone calls from offenders impersonating an official from the police or a private company to persuade the victim to provide access to their money or financial accounts. Three cases involved the distinctive method that is categorised by police as courier fraud.	Other fraud (not covered elsewhere)	4
		Recovery fraud	1
Other	One case in which the offenders defrauded the local branches of a company in the leisure industry by exploiting their financial systems.	Other fraud (not covered elsewhere)	1

Characteristics of the inclusion offence: all frauds represented a process rather than isolated incident, but there was only one example in which the methods of predatory and commercial fraud coincided; the offender liquidated the goods acquired through identity fraud (predatory fraud) by selling them on an online shopping platform (i.e. a commercial fraud). In all cases of commercial fraud, the offenders (through various means) had infiltrated legitimate markets to create opportunities to perpetrate fraud. However, each deception lay on a spectrum, with variation in the nature and extent of the overlap with legitimate commerce. The indication was that most had provided a product or service to some of their customers; for example, in the early stages of each investment fraud, most had tried to satisfy the terms of service by paying the money due to clients (though this was likely to be motivated by the need to avert suspicion). In five of the commercial fraud cases the offenders had operated through a company that had previously and/or concurrently engaged in legitimate commercial activity.

There could be a thin line separating an investment fraud from a predatory crime and it was not always possible to ascertain whether the product or service that was linked to the fraud was 'real'; in one case, the investigators had a challenge

to determine if the suspect's legal entitlement to develop an overseas industrial facility was genuine. In some cases, the deception was less about the product and more about business practices; for example, charging exorbitant fees for managing the investment or redirecting money to inappropriate investment products without the investor's knowledge.

2.3 THE METHODS FOR PERPETRATING SERIOUS FRAUD

In this section we first examine the distinctive nature of the methods and deceptions that were in use to perpetrate commercial frauds, that require effective sales and marketing strategies to sell misrepresented products or services, and predatory frauds, which commonly require the impersonation of a legitimate individual or organisation. We then discuss the common themes that were present in both categories of fraud.

2.3.1 Commercial fraud

Communications

Communication was a central component of the methods used in many commercial frauds because of the requirement to reach prospective victims and persuade them of their legitimacy. Some offenders were able to use the established sales and marketing activities of the legitimate company from which they offended. Others needed to proactively engage in mass-marketing strategies, commonly with the offer of something unavailable or in short supply in the legitimate sector; examples include high demand goods, high investment returns and in one case, a card facility that allowed clients to readily access money from their investment.

The more targeted the marketing, the more efficient the process of identifying a prospective victim, and fraudsters adopted various strategies to reach the people most likely to be receptive to the product and/or those most susceptible to unsolicited contact and fraud (individuals on the so-called 'suckers lists'). One online shopping fraud used website 'optimisation' techniques to help direct users making relevant internet searches to their web page. In three investment frauds there was indication of a vibrant industry in developing and trading in 'leads' – i.e. contact details for people who would receive a marketing phone call. In one case, a co-offender generated thousands of leads, one method being the collection of information from an online questionnaire on investments (i.e. phishing). Once the fraud had run its course, offenders extracted more value from victims by selling their information to other fraudsters.

Establishing trust

The deceptions were commonly multi-layered, to create a veil of legitimacy and go undetected by victims or the governing authorities and regulators, and enable them to operate for as long as possible. Different fraudsters needed to adopt different methods depending on their starting points. Some offended from within an established legitimate company whereas others needed to invest a great deal of time into creating an organisation that had the illusion of legitimacy, requiring in-depth knowledge of the sector and the gaps open to exploitation.

The ability to establish and maintain trust was critical to be able to avoid detection during initial and ongoing contact with customers or clients, thereby allowing them to perpetrate fraud undetected and uninterrupted for months or years.

There were a number of techniques adopted in commercial frauds to garner trust from prospective consumers:

- **Credibility:** Most gave the appearance of a functioning business with staff and operating costs, which were in part necessary for undertaking the daily business of marketing and sales but also represented a cost in generating the façade. The offenders were able to tap into a range of legitimate services-for-hire in the UK or overseas which helped them to operate in plain sight; these included payment service providers, trading platforms, website developers and property companies that provided virtual spaces or desks-for-hire in prestigious financial districts. While some frauds were concealed behind an established legitimate business, some adopted brands so close to that

of another legitimate and successful business they became erroneously conflated in the minds of consumers. One group exploited a small online retail company which was already established as a legitimate and credible retailer.

- **Regulatory gaps:** There can be challenges for individuals in verifying the legitimacy of products, services or providers, and public and private sector bodies and registers have a role in monitoring and regulating against bad actors. Fraudsters found various ways to circumvent these trust mechanisms, usually by deceiving or bypassing the relevant authority. In two cases the offenders sold binary investment options to individuals in the UK but operated from a trading platform or company registered in an overseas jurisdiction, putting them beyond the influence of the UK regulator (the UK Gambling Commission). In one case the fraudsters had made claims that they fell into the jurisdiction of the overseas regulator, but this was found to be untrue following checks with the overseas authorities. Another case involved the sale of investments into an overseas facility that fell outside of UK regulation (see the example below). In all these cases, a sales team operated from within the UK, but was divorced from the investment service or instrument that was located overseas and thereby eluded a regulatory response. One group of commercial and retail fraudsters bypassed the internal regulation of a payment service provider in the private sector in order to gain access to an online payment facility that was necessary for receiving the money from victims; this involved verifying that the distribution company could legitimately provide the marketed products, most of which the offenders claimed were supplied by an overseas company.
- **Service delivery:** Consumer and client expectations of the product or service to be delivered were established at the point of a sale, and it was often the eventual failure to meet this agreement which led to a fraud unravelling. In the investment frauds clients signed up to contracts lasting a year or more, giving offenders the time and space to cultivate the deception. All investment frauds had been 'Ponzi' schemes where little or none of the investor's money was actually invested but fraudsters ostensibly met their obligations to clients by paying previous victims with money received from the most recent victims. Victims commonly had no direct means to monitor their investment, and their view was limited to company activity seen through periodic statements or their accounts on the company website, which could be readily manipulated by offenders. The information seen through this filter provided a false impression of high returns and encouraged some to invest more and so become repeat victims.
- **Cultivating relationships and trust:** High value investments call for considerable trust from an investor and while some relied solely on mass marketing (exploiting those least vigilant), in three cases the offender gave considerable effort to cultivating relationships with clients, not only to encourage them to invest themselves, but to also tap into a client's own social network by encouraging them to endorse the scheme to their family and friends. One group attended social events with clients and offered financial incentives for referring friends to their scheme. Another had drawn from people within established social circles, including his family and members of his local religious community.

Two commercial frauds were perpetrated by offenders working in frontline occupations who initiated contact with victims face-to-face in the local community (through selling tickets and a building repairs service). They operated on the fringes and/or outside of consumer regulations, and engaged in some of the least complex deceptions, requiring neither co-offenders nor a great deal of artifice to give the illusion of legitimacy. It was not clear to what extent the offenders actively targeted prospective victims or acted in response to offending opportunities that arose in the context of their work, but both were known or suspected to have engaged in similar offences with more than one victim.

Case example: *The offenders set up a UK-based trading company which claimed to have purchased a fixed-term lease for an overseas industrial facility and a 50 per cent share was being sold to private investors. The principle being to use the money to improve its operation and that it would yield a return over time. They produced marketing material that show-cased their connection to a celebrity, insinuated an affiliation to a successful UK-based company and investors were told to expect up to 300 per cent in profits. They contracted the services of multiple marketing (or 'broker') companies to make unsolicited calls to potential investors. Over the course of two years, shares were sold to 340 victims, many of whom were elderly and had previously fallen victim to similar frauds. They were promised two dividend payments each year (which were fulfilled in the early stages) and they*

maintained contact through 'compliance calls' and a newsletter that on a number of occasions announced profits. The nature of the investment scheme meant that it fell outside of UK regulation. Furthermore, the legal entitlement to the facility came under the jurisdiction of the country in which it was based. It transpired that the company had no legal rights to the facility and so the investment was not real, and much of the money invested by victims had gone to paying the exorbitant commission fees of offenders.

2.3.2 Predatory frauds

These fifteen crimes were perpetrated by fraudsters who did not operate from within a legitimate or pseudo-legitimate business setting, and often did not enter into a commercial arrangement with the victim and were in many cases unknown to them. Instead, the offenders commonly disguised themselves as another person or organisation with whom there is a legitimate relationship. Many frauds in this setting impacted on businesses and involved offenders who were able to infiltrate and manipulate an organisation's internal IT system, financial system or personnel. In three cases the offenders had the cooperation of someone legitimately employed by the organisation who helped them to bypass internal security measures.

Case example: *The offenders defrauded a company in the UK by sending multiple fake invoices over a period of two months. Using software freely available on the open web, they sent multiple 'spoofed' emails purporting to be from the personal assistant of the company CEO, requesting payment of invoices that were included as attachments. Each invoice gave the details of accounts under the control of the offenders. One co-offender was temporarily employed in the finance department and intercepted each fake email, falsely verified the company, and arranged for them to be entered on to their system for payment. The external fraudster received the money into multiple bank accounts under his control, several of which belonged to his associates, and others that had been opened fraudulently in someone else's name. He had intercepted post received at a vacant address near to where he lived and used this personal information to fraudulently purchase goods and apply for financial products.*

Technology

In six cases the offenders used technology to infiltrate IT systems, most commonly a precursor computer misuse offence (i.e. hacking) to forcibly gain access to information on systems which they could use to exploit the trust that already existed between two parties. Computer misuse crime was apparent in nearly all payment diversion frauds, in which offenders monitored communications and business activity on hacked systems and used this information to manipulate communications and trick recipients into sending money to accounts under their control. The frauds were directed principally by the precursor hacking offence and to IT systems that were vulnerable, and in this way, victimisation could arbitrarily fall to any business or individual transacting with the infiltrated company. In some cases, the fraud seamlessly crossed international borders. To illustrate, the same offenders hacked into the systems of both a private school in the UK and a company located in Asia, leading to fraud directed to both a parent paying tuition fees and an overseas business paying a large sum to a service provider.

The use of digital identifiers to authenticate people or organisations in digital transactions (such as account numbers) made it possible for offenders to readily impersonate others in payment diversion frauds. And similarly, identity fraud was made possible by stealing or manipulating personal and financial information to appear legitimate to financial service providers and vendors, to gain access to finance, goods or services. In four cases offenders had accessed personal data or bank cards to impersonate a legitimate account holder and make purchases, apply for financial products, or withdraw cash. In three cases this information was supplied to offenders by a third party, two of which involved online criminal markets in which this information was sold by identity thieves.

Social engineering

Finally, the authorised push payment offences entailed more elaborate social engineering, in which offenders communicated directly with the victims on the phone, to persuade them that they were representatives of a legitimate organisation. One distinctive method involved offenders making

direct phone contact with individuals to engage in a relatively low-tech deception, requiring little more than a phone book and a simple phone dialling trick[9] (i.e. 'courier' fraud). In two cases this was done by purporting to represent the police or the bank, claiming the individual was at risk of fraud and encouraging them to provide access to their accounts or money for protection. These frauds mostly impacted on a cohort of elderly victims who appeared more susceptible to being misled in this way.

Case example: *A single elderly victim lived with his wife who was in poor health, and practitioners suspected he was suffering from dementia based on the difficulties he had recalling information and events. He had building work completed at his home by a single trader and had been satisfied with the work (though the police assessed the work had been over-priced). Several weeks later he received a call, which he believed was based on a referral by the trader, from someone claiming to be able to supply equipment to repair a problem identified from the previous work. He was asked to pay an initial deposit, but the equipment failed to arrive. Instead, he received periodic contact over several months from individuals requesting additional payments for various reasons that included difficulties arranging delivery or tax due on the equipment. Over the course of multiple online transfers, the individual went on to spend most of his life savings.*

2.4 THE COMMON CHARACTERISTICS OF SERIOUS FRAUD OPERATING MODELS

There were a number of common elements in the methods in use in commercial and predatory frauds, notably the central and enabling role of the internet, money laundering, and resources for identifying and targeting vulnerability. However there was variation in how these elements manifested, reflecting the discrete contexts and opportunities afforded to offenders in different settings.

2.4.1 Covering the financial trail

Fraudsters went to varying lengths to conceal their criminal gains, depending on their method of fraud offending , their sophistication or the settings in which they operated. Some who offended in commercial fraud settings established business structures that not only put distance between the money and the crime but also themselves and the crime, giving them licence to operate in plain sight. In three cases offenders had positioned themselves as employees or a third-party service contracted by the offending company, deflecting criminal liability from themselves despite being in receipt of the proceeds. Distance can also be inserted by processes of misdirection, such as periodically winding down one fraudulent company before resuming as a newly established company or registering a company under someone else's name or a fake identity. The stronger an offender's legitimate veneer, the less effort is required to legitimise the income; this is most clearly illustrated by two conventional white-collar offenders who perpetrated fraud from within an otherwise legitimate organisation and offended for many years without any attempt to conceal the illicit origins of their income.

Money laundering is defined in the Proceeds of Crime Act (2002) as the process in which criminal proceeds are 'sanitised' to disguise their illicit origins, principally to evade the suspicion of the authorities while moving and accessing criminal funds. One of the most effective ways is to move the money out of the UK. In five commercial frauds the offenders had access to business entities and accounts overseas through which they funnelled the criminal proceeds, putting the money outside of UK money laundering regulations and obfuscating the financial trail. For example, in one investment fraud the funds were passed (or 'layered') through multiple accounts across several jurisdictions, some of which were registered to fake identities, including an 'escrow' agent in Ireland. In a small number of cases the criminal proceeds were physically transported overseas as cash or high value items.

9. The offenders used a vulnerability in the telephone system, specifically landlines, which allowed the line to stay open for 10 seconds after one party has hung up, and on redialling the victim was unknowingly still speaking to the offenders.

Some who engaged in identity or authorised push payment frauds were provided with direct access to cash or purchases from the victims, leaving no digital trace or requirement to engage in money laundering processes at the time of the offence. However, offenders who received the money through bank transfers (such as payment diversion fraud) were challenged because it left a digital trail and no ostensible legal basis for receiving the money. They needed strategies to disperse and quickly release the funds before the offence could be identified and reported by the victim, while at the same time bypassing the security checks of banks and covering the financial trail to prevent the fraud leading back to them. In nine cases, offenders had recruited 'money mules' who allowed them use of their accounts. This enabled offenders to receive, disperse and release funds from the accounts of people not connected to the fraud, most of whom either would or could not lead back to the fraudsters. In these cases, the offender's capacity to perpetrate fraud was aligned to their capacity to launder the money, principally to access and exploit a sufficient number of bank accounts. To illustrate, in one case over £1.5 million was dispersed into 14 separate bank accounts, all linked to contacts from their local community, including a group of older women who appeared to have had no other role in the fraud. From the mule accounts the money was transferred to other accounts, withdrawn as cash or spent on high value purchases.

2.5 THE ROLE OF ONLINE CRIME AND CYBERCRIME

The internet and online technologies provided some offenders with capabilities and opportunities that would not otherwise have existed, particularly those who perpetrated predatory frauds and who would be unable to access and exploit financial or company systems without networked technology. In other contexts, the online elements enhanced the scope and speed of offending. Rather than requiring specialist criminal methodologies the modus operandi in some cases extended from mainstream practices in relevant online sectors, and in mirroring licit practices they were better able to mask the fraud while at the same time reap the same commercial benefits (such as the use of online sales platforms or online advertising services). Four principal enabling functions of online technology were identified:

- **Marketing and communication:** online spaces provided the means to target marketing and sales to individuals most likely to spend money on a product or service, either by tapping into the functions available on mainstream shopping or communications platforms or diverting search engine users to their own websites. One offender linked to an investment fraud used online advertising to phish for the contact details of individuals susceptible to their scheme. These online mass-marketing techniques enabled offenders to reach high volumes of people with minimal resources. Instead of providing first-contact with prospective consumers, in three investment fraud cases the company websites provided a continuous interface for their clients and helped to maintain the deception.

- **Infiltration:** there were six predatory frauds in which offenders had hacked into company systems, as a precursor to accessing information that would enable them to socially engineer online communications to the victim or their associates. This stage of offending was in most cases the least exposed and the identities and methods of hackers were often unknown to the victim or police.

- **Financial transfer:** Digital finance, in the form of bank account transfers or online payment services, was integral to accessing the victim's money in both commercial and predatory fraud cases.

- **Evade detection:** mainstream anonymisation technologies were employed in at least four cases to prevent attribution to their offline identity. In three cases unsolicited calls were made using untraceable Voice Over Internet Protocols (VOIP) and two used proxy servers or Virtual Private Network (VPN) connections to hide their online activities and prevent investigators sourcing their real location. In two other cases offenders used cloud computing and cryptocurrency which obstructed evidence-gathering.

There were seven cases in which online communications, systems or finance played little or no role in the commission of the fraud, relying instead on face-to-face or phone communication to establish and sustain contact; these included offenders who manipulated individuals with a personal vulnerability into accessing and supplying the money themselves, such as in authorised push payment frauds.

2.6 VULNERABILITY

There are many people and organisations who are vigilant and resistant to approaches by fraudsters, meaning that many attempts end in failure. In most cases where offenders made unsolicited calls to prospective victims, high volumes of calls were made before someone would fall victim; for example, one group of courier fraudsters were making up to 400 calls a day. To be successful many frauds required the prospective victim to engage and take active steps, and the more substantive and significant the amounts at stake, the more likely a person will show caution. Offenders employed various strategies to maximise their hit rate which intrinsically involved targeting vulnerability, commonly rooted in gaps in an individual's understanding of either the risk or product, or a lack of vigilance. There were multiple cases in which fraudsters targeted individuals on the basis of a personal vulnerability. In a small number of cases this was inferred by the police investigator based on the victims' demographics (for example, in one courier fraud all victims were described as elderly) or the experience of individual victims who had been repeatedly targeted. In at least four cases the police uncovered preparatory materials to indicate they had targeted unsolicited phone calls at individuals who were assumed to be vulnerable. Some offenders made crude attempts to interpret environmental cues that signalled the likelihood of vulnerability; for example, in several cases offenders targeted people who were elderly based on personal information (including age) that was provided on open web directory sites. Others were able to profile vulnerability from previous behaviour, such as engagement with the relevant market, product or service; in one investment fraud unsolicited calls were made to individuals known to engage with unregulated investments.

In seven cases, vulnerability from prior victimisation was further exploited by the same or other offenders. In three investments frauds the offenders were indicated to have sold or bought the personal details of victims (i.e. 'suckers' lists), with some victims receiving high volumes of calls from multiple fraudsters that had access to their personal information. To illustrate, a victim in his 80s who had already lost much of his personal wealth to an investment fraud, was contacted the following year by the same suspect purporting to be from another finance organisation that had located the stolen money, and that they could release it back to him for a fee (i.e. recovery fraud). This attempt was not successful, but the victim went on to experience a high volume of calls and emails from different fraudsters.

Targeting vulnerability was central to the offending method across the range of fraud categories included in this study, though not all offenders were able to exploit and repeat victimise the same individuals or entities. Vulnerability to payment diversion fraud was in part determined by the strength of a company's IT security; one company claimed to have had no security such as firewalls or password protected access for employees. And in the offline context companies were targeted for gaps in their systems and procedures; in one case, a group targeted the local branches of a company, having recognised the vulnerabilities in their system that were not apparent in other companies in the industry. It stands to reason, that offenders exploit the paths that provide the least resistance.

Case example: *A group of offenders from the same neighbourhood in a large city made thousands of unsolicited landline calls claiming to represent either the police or the bank. Typically, they claimed the person was a victim or at risk of becoming a victim of fraud and advised them to withdraw the money from the account and hand it over to them for protection. Multiple suspects could be involved in the phone exchange, each taking the part of a different police officer or other role. Once the victim had consented a courier would attend their address to collect the money, travelling by taxi. 36 victims were identified (though it was suspected many went unidentified) and all had been aged between 65 and 95, with most in their 80s or early 90s. The losses ranged from £1,000 to £12,000 and a small number were targeted on repeat occasions following a successful fraud attempt. The suspects interpreted the information available in online phone directories to target elderly residents in affluent locations in neighbouring police force areas. Many victims had complex health problems, and some had passed away or became too unwell to engage with the police investigation.*

2.7 THE GEOGRAPHIC DISTRIBUTION OF FRAUD

The basis for inclusion into this study was that the serious fraudsters had operated (at least in part) from a police force area in England and Wales, and the majority lived and offended in the UK. However, their impact was also strikingly local, even in cases linked to cyber criminals, with most offending confined to victims based in the UK or even in the regions close to where the offenders lived. Only six cases involved offending that impacted on overseas victims, though each had concurrently targeted local victims. For example, there were two cases that involved hacking and payment diversion fraud that victimised both overseas and UK-based organisations.[10] In two investment frauds, the central offenders (who were UK nationals) had operated from overseas but established companies in multiple countries, including the UK, and local victims were contacted by co-offenders operating from local companies.

The nature of cyber space and global finance means there is the practical scope for offending to be borderless. However, many frauds continue to rely on communication that engenders trust from the victim, and with it a requirement to appear credible and legitimate. This is most apparent in investment frauds in which some offenders took great pains to set up London offices to create a veneer of legitimacy and credibility, and others who established trust through extensive personal engagement with victims. And similarly, offenders linked to payment diversion and identity frauds had to credibly impersonate a legitimate person or organisation, which is more easily achieved when they can readily engage in behaviour or use language that is familiar to the victim. To illustrate, offenders in possession of the stolen financial credentials of US citizens chose to travel to the US to make purchases without raising the suspicions of financial service providers.

The methods of some frauds introduced a practical requirement for direct access to victims and/the stolen money or material goods, and so the selection of targets could be determined by locations that were readily accessible to the offender or their available co-offenders. The nature of fraud perpetrated by those in frontline occupations (for example, builders or carers) meant targeting individuals they came into direct face-to-face contact with; therefore, all victims had lived in the same area or close to where the offender lived. Several predatory frauds had required the use of couriers to physically collect the money or item from the victim and were targeted so they could travel to neighbouring suburban areas using local public transport. To illustrate, one offender made use of associates in the local area to collect the cars he had acquired fraudulently, and so targeted dealerships in or around the city in which he lived.

10. It is not possible to know the degree to which this reflects the operational decisions of the police to prioritise offenders impacting in the UK for criminal investigation.

3. THE PROFILE OF SERIOUS FRAUD OFFENDERS

SUMMARY

The cases in this study involved a high volume of offenders due to the prominence of co-offending in 12 of the cases analysed. A large proportion of offenders were British nationals, though a small number of cases involved high concentrations of co-offenders from the same foreign national or minority ethnic group. Many offenders had a prior offence history, most commonly linked to fraud and forgery, though offenders linked to predatory frauds revealed a more diverse history than the offenders of commercial fraud, including links to violence or drug offences. These serious frauds encompassed offenders who displayed a wide range of motivations, including a substantive cohort of non-serious peripheral offenders.

There were three overarching offender typologies that reflected both their entry point and their role in the fraud offence. A category of career criminals had a central role in a number of cases, typically made considerable financial gains from the offence and had prior links to serious criminality (most commonly fraud or other economic crime). Other offenders abused their occupation within an otherwise legitimate business to defraud victims. In a small number of cases, an offender abused their employment at the victimised organisation to facilitate the fraud. A final category had engaged in offending for subsistence, though in some cases they were motivated by aspirations of status and wealth. These offenders commonly took peripheral roles in the fraud and received little recompense for their involvement.

3.1 DEMOGRAPHIC PROFILES OF OFFENDERS

There was a total of 104 offenders identified across the 25 cases, 52 were linked to commerical fraud offences and 52 to predatory frauds. These were concentrated in 12 cases for which multiple offenders had been identified in the investigation.[11] This incorporates offenders from diverse backgrounds who adopted a variety of roles in commissioning the frauds. This section starts with an analysis of the demographic profiles of offenders, followed by an analysis of their offence histories and then a more qualitative discussion of the distinctive motivations and pathways into perpetrating serious fraud.

There were only 11 identified offenders who were female, linked to seven cases. Two had been lone offenders who perpetrated fraud from within the informal economy; one had abused her position as a carer for a vulnerable victim and another had been involved in fraudulent ticket sales over several years. In other cases, female co-offenders were recruited into more peripheral roles from within family or social networks; some had been in a romantic relationship with a co-offender. To illustrate, one case had involved multiple female co-offenders and the coordinating offenders, who were male, had used the bank accounts of older female family members to receive the stolen money,[12] and one had been in a relationship with a female co-offender who used her position at the victimised company to enable the fraud.

Table 4 shows the distribution of ages in the different offending contexts and compares coordinating offenders with those in all other roles. Coordinators were those who initiated and planned the fraud; this classification is based on the information collected during the police investigation including witness accounts,

11. At least nine additional cases were suspected to have involved co-offenders who had not been identified.

12. These individual co-offenders were not identified in the data.

Table 4: The age distribution of the known fraud offenders, by offending context

Age*	Commercial Fraud		Predatory fraud	
	Co-ordinators	Other	Co-ordinators	Other
18-30	2	14	3	19
31-45	5	12	3	8
Over 45	5	7	2	4
Total	45		49	

* These were the ages of offenders at the time of the first known fraud offence linked to each investigation. In 13 cases this was approximated for offenders based on the individual's year of birth. For 10 known offenders linked to five cases (three predatory and two commercial fraud cases), there was missing data for the offender's age.

observations on the flow of criminal finances and where relevant, the structure of the business.[13] The 'other' roles varied according to the specific modus operandi but included sales, couriers or offenders who facilitated money laundering and within this cohort, there was wide variation in the understanding and complicity of each co-offender. Overall, a high proportion of offenders were in 'other' roles, signalling the need in some offences to enlist a multitude of co-offenders; for example, three quarters of commercial fraudsters were in 'other' roles.

The age of offenders ranged from 19 to a maximum of 76 years of age. Forty-eight offenders were aged 18 to 30 and offenders in this age group were especially prevalent among those who had an 'other' role in the offence. Just under one in five (18) offenders in the sample were aged over 45, though offenders in this age category were more prominent in the commercial fraud offences.

Nationality and ethnicity data were not available for many offenders (30 and 40 respectively). Where nationality was known, most were British nationals (59, 80 per cent).[14] Even in the small number of cases that had involved co-offenders who operated from overseas, nearly all were indicated to be British. Other nationalities included seven who were Romanian, though all but one was linked to the same criminal group, and four from Nigeria who were linked to two fraud cases.

The ethnic background of offenders showed more variation; 15 offenders were recorded as White British and eight as White other. The remaining 41 were from a Black or other minority ethnic group background.[15] However, a minority of cases involved groups comprised of co-offenders from the same or similar background. Most notably, 25 Asian offenders were linked to just four cases and in three payment diversion fraud cases, all co-offenders were from a Black British or Nigerian background. As will be discussed in the later section on co-offending and coordination, this distribution of nationality and ethnicity will in part reflect the significance of social networks and local community settings in the recruitment of co-offenders.

Importantly, this analysis reflects only the cases that were identified and selected for investigation by the six police units and furthermore, selected for inclusion into this study. They cannot be assumed to represent all offenders who perpetrated serious fraud in this time period.

3.2 PATHWAYS INTO SERIOUS FRAUD OFFENDING

3.2.1 Offence history

Table 5 provides an outline of the known offence histories for each offender prior to their involvement in the serious fraud;[16] some fraud cases involved methods that targeted multiple victims over a number of years and these were

13. There were six cases in which the suspected coordinator was not identified and for which all known co-offenders were assigned to the 'Other' category; all were predatory fraud offences.
14. There was missing nationality data for 30 (29 per cent) identified offenders.
15. There was missing ethnicity data for 40 (38 per cent) identified offenders.
16. The offence histories include both convictions and other suspected offending compiled from the information included in court and police intelligence documents and that provided by investigators in interviews.

Table 5: The offence histories of fraud offenders linked to fraud perpetrated in different contexts*

Offence category**	Commercial fraud offenders (n=24)	Predatory fraud offenders (n=37)
Fraud and forgery	13	18
Other acquisitive	6	12
Violence	7	20
Drugs	2	15
Other	11	18

* This is not a count of all prior offending but rather the distribution of offence categories linked to each offender - for example, an offender may have perpetrated multiple frauds but this will only be counted as one, to represent a prior involvment in fraud offending. A single offender may be linked to more than one offence-type.

** 'Other crime' includes diverse offence-types, some of which may have been ancillary to fraud offending, such as money laundering, but also a range of unrelated offences such as public order offences, driving offences, anti-social behaviour and fly-tipping.

counted under the inclusion offence for this study and so are not included in the table. There were 61 offenders (59 per cent) who were known or suspected to have a history of prior offending; 37 predatory and 24 commercial fraud offenders. Notably, there were only four cases where an offender in a co-ordinator role in the fraud had no known prior criminal history, two of whom had offended from within their established profession (a financial services director and a solicitor).[17]

Offenders with a prior offence were linked to a diversity of offending, though most commonly they had links to at least one prior fraud and forgery offence. This was the case for over half of the commercial fraud offenders (13), and just under half of the predatory fraud offenders (18) There was a more even distribution in the types of prior offences linked to predatory fraud offenders, indicating they are a group with a more diverse offending profile; over half were linked to a least one prior violence offence (20) and four in ten (15) to a prior drugs offence'.

3.2.2 Individual pathways

The different offenders showed a diverse range of pathways into their involvement in the serious fraud offence, which broadly varied by the different offending methods and in some cases the role of different offenders operating as part of a group or network. Three groups, with distinctive pathways, were observed: offenders who had abused their occupation to perpetrate fraud; career criminals who were more prolific and versatile in their offending, and those who offended for subsistence who had limited financial means and made minimal gains from the fraud.

Career criminals

In at least ten cases there were offenders who had historical links to serious criminality, had enduring ties to a wider criminal network, and in some cases displayed versatility in their offending behaviour. Typically, these offenders had no legitimate source of income, were central to initiating and planning the fraud and their criminal gains could be considerable (the destination of stolen funds could not be traced in all cases), especially those operating in the context of a commercial fraud who were able to tap into high value markets.

There were six predatory fraud cases perpetrated by individuals who were mostly in their early to mid-20s and were prolific in their offending behaviour. At least three of these were affiliated to a larger urban street gang; these were associated with a specific local area, had all involved at least three offenders, two were described as large groups with a leadership structure, and in all three cases there were offenders with links to drugs or violent offences.[18] Many of these offenders had links to wider criminality associated with the activity of the criminal network, and some were persistent and systematic in their perpetration of courier fraud. Some displayed highly versatile offending but for most, their involvement in street-based crime (such as drug offending)

17. There was no information on prior offending for 43 offenders (41 per cent), and this includes offenders for whom the police have no knowledge of prior offending but also some where there is missing data.

18. In two cases, the police used the term 'street gang' and we also referenced the definition in the Serious Crime Act 2015 - https://www.legislation.gov.uk/ukpga/2015/9/notes/division/3/3/2/7.

appeared to pre-date their involvement in fraud which seemed to represent a diversification in their offending. To illustrate, in addition to identity fraud one individual was serving a prison sentence for a firearms offence and had prior involvement in drug supply and ransomware crimes. Courier fraud appeared to be a gateway to fraud offending for some, especially those linked to networks engaged in these crimes. Other frauds in this context included identity and payment diversion fraud. The illicit gains in at least three cases were indicated to have been fed back into the criminal network; the criminal gains from one courier fraud had been transferred to overseas accounts and one family-based network of highly specialist fraud offenders laundered the money back to their home country overseas. A number of individual offenders indulged in luxury spending on disposable goods and services that included cars, holidays and designer fashion.

There were four cases in which the offenders operated from within more conventional business settings, but from companies that were established for the express purpose of facilitating fraud offending; primarily front companies in the investment or e-commerce markets. These offenders commonly coordinated the frauds and specialised in perpetrating economic crime (including the use of international business and finance sectors). In three cases, the same two co-ordinating offenders had previously co-offended to perpetrate a serious fraud. In commissioning the fraud these offenders were able to draw from a loose network of co-offenders with whom they had previously offended or had contact. Examples included a group that commissioned individuals in a known boiler room to market their fraudulent investment, another that commissioned a known 'leads supplier' (providing details of potential victims to receive calls) and one offender was providing specialist money laundering services to multiple criminal groups. A minority displayed links to wider criminality; an investment fraud was indicated to have close links to a well-known local crime family.

Case example: *A company was established to mass market what transpired to be a 'classic Ponzi scheme'; instead of being invested, most of the money was paid directly to the offenders, and the dividends for existing investors were paid using the money from new investors. There were 15 suspects and most had no prior involvement in fraud. There was one suspect considered to have been in charge; he coordinated the set-up of the scheme and the work of the sales team and received a substantive share of the illicit funds. He was a UK national but operated from various overseas locations. He had multiple links to previous investment frauds, including a case several years earlier when he had worked in the sales teams of a company run by another suspected 'conman'. It was in this previous role where he had met two co-offenders in the current case who assisted in setting up the company in the UK and in funnelling the money overseas using offshore accounts opened in their name. There was also a 'lead generator' who provided the call lists for this scheme and other separate fraudulent investment schemes. Once this investment scheme began to unravel, a new business entity was established, and they made contact with the victims claiming to have taken over their accounts. The main offender had no legitimate employment and was suspected to have concurrently been setting up similar fraudulent schemes overseas.*

Abuse of an occupation

There were at least eight cases in which the opportunity to perpetrate fraud derived from an otherwise legitimate occupation. In concealing criminality behind a legitimate role these offenders were able to readily gain the trust of victims, facilitating some of the highest value and/or longest running frauds in the study. Two cases had involved lone offenders who abused their position as the director of a company. Both cases accorded to a pattern observed in previous studies of white-collar crime in which otherwise law-abiding individuals exploited an opportunity in their legitimate occupation to gain money by illicit means to address a personal or financial difficulty (for example, see Levi et al, 2017; Smith, 2003). Both offenders claimed to be suffering from gambling addiction. One had been the only example of what in the previous literature was described as a 'one-shot' offender (Van Der Geest et al, 2017). He had no history of offending but in a single month exploited the opportunity to steal money from online customers to resolve a pressing gambling debt.

Three offenders had abused a position of employment at a legitimate company. In all cases the employer was the victim, though one had also targeted clients. Two cases involved insiders that were recruited to facilitate offending planned and coordinated by external co-offenders, and none had any known history of offending prior to the current offence. One payment diversion fraud was coordinated by a prolific fraudster operating from outside of the organisation and involved a co-offender in his early 20s who had worked for the victim organisation for just a few months.

Case example: *An investment fraud was perpetrated by an individual who owned and was the self-appointed director of a global wealth management company. He was an established finance professional, regulated by the Financial Conduct Authority, and he and his wife (also established in her occupation) had considerable personal wealth. His company was predominantly involved in legitimate financial services which provided a front (or 'conduit') for the fraud. Most victims were at retirement age and had been persuaded to invest in a fictitious financial product (purportedly offered by a high street bank), whereupon their money was 'locked in' for a period of up to five years. None of the money was invested and the money received from each new investor was used either to pay the money that was due to previous investors or transferred to his own personal accounts. The frauds were perpetrated over a period of 14 years and losses exceeded £14 million. Most victims were sourced from within his local community, and such was the trust, none had suspected fraud prior to being approached by police investigators. This trust and his position at the company, with full control of the company accounts, negated the necessity for co-offenders or complex processes to conceal his illicit gains. He claimed to have a long-standing gambling habit and financial records showed millions of pounds paid to online gambling sites.*

An implicit element of fraud perpetrated in the informal economy is an offender who uses their frontline occupation to identify opportunities to offend. None were linked to a formal or registered business entity, but most appeared to offer a genuine service while exploiting opportunities to commit fraud when they arose. Over approximately five years one lone female offender had been active in the black market for selling tickets to forthcoming live events in the area, taking advance payment from people within the community; she was known to fulfil some orders where possible, but regularly failed to provide the tickets following payment.

Offending for subsistence

There were many co-offenders who appeared to have no personal wealth gained by either legitimate or illegitimate means. These co-offenders were commonly (but not exclusively) involved in predatory fraud offending, and many were peripheral to the fraud and offending network and received little recompense for their role in the fraud.

Employment status was recorded for 39 of the 52 predatory fraud offenders, and 16 were unemployed and/or on benefits. In three cases there was evidence of co-offenders experienced significant hardship. Two were foreign national offenders; one coordinated money laundering for cyber criminals (linked to payment diversion fraud), was unemployed and had 'sofa-surfed' at various friends' addresses following a relationship breakdown, and the other was prevented from gaining legitimate employment due to his unsettled immigration status. One perpetrator of multiple high value identity frauds, lived in shared accommodation that was in a poor condition, and was believed to suffer from class A drug addiction. He claimed all criminal gains had gone to an OCG to which he was affiliated.

There were at least three cases in which money mules were recruited from outside of the offender's established social network. These were commonly young people with limited financial means, and so willing to accept relatively little for the use of their account to help meet everyday living expenses such as rent. Where employment status was known, money mules tended to have unsecure jobs such as delivery drivers, retail and security roles, and some were university students.

In at least three cases, younger co-offenders were drawn into a visible hierarchy of offenders and while many received relatively little recompense, some were motivated to climb the ladder and achieve the observed status of other co-offenders.

One group of investment fraudsters set up a pseudo-legitimate company structure formed principally of a telemarketing team (i.e. a 'boiler room'), half of which was comprised of young inexperienced males in their late teens or early 20s who took up 'junior broker' roles. There was an initial pretence of legitimacy and while some left on realising the dubious nature of the business, others remained. They were paid very modest basic salaries (ranging for £500 to £1,000 each month) and spurred on by the promise of a luxury lifestyle put on display by the core offender. In the street gangs perpetrating courier frauds more senior members central to the fraud were able to make use of younger affiliates who were paid modest amounts to take the role of courier. It was suggested that younger affiliates were motivated to make a name for themselves in the gang.

There was limited evidence of offenders in this group crossing over into the other pathways described above. While some may progress from the proving grounds of a marginal offender to become a career criminal, the available data was unable to demonstrate any such transition. What is clear, is that a considerable proportion of serious fraud offending, especially that linked to predatory frauds, involved offenders who were commonly marginal to the conspiracy and made relatively little financial gain from the commission of these crimes.

Case example: *An identity fraud involved multiple incidents over an 18-month period in which the offender used the legitimate bank cards for 13 customers of a single bank. In each incident he entered a different branch, all located in the same city, to withdraw sums ranging from several hundred to several thousand pounds (i.e. account takeovers). Multiple cash withdrawals could be made from a single account. In total he stole over £45,000 and there were further attempts that had failed. For each withdrawal he presented the bank card and a fake driving licence or passport with the customers information and his photo. The offender was middle-aged and had a history of offending going as far back as the 80s that included low level acquisitive crime and fraud (at least one had involved a similar method). He was living at a friend's address that was described to be in a poor state, along with six others, all of whom (including the offender) were suspected to have a substance misuse problem. The offender had ostensibly perpetrated the fraud alone however he claimed to have been recruited because of his links to a criminal group and previous experience of fraud. It was suspected that he had been provided with bank cards, identity documents and explicit instructions, and his role was to collect the money from the bank branches. The money could not be traced following his arrest, and he claimed all of it had gone to the criminal group which had supplied him with drugs as payment.*

4. CO-OFFENDING AND COORDINATION

SUMMARY

The ability to enlist co-offenders was central to the success of the fraud in many cases. In predatory frauds, co-offenders were especially critical to overcoming the various obstacles to accessing and laundering the stolen money. Co-offenders were particularly important in providing a front to interface with the victims, and offenders in more peripheral roles could be the most exposed and added a layer of protection for the coordinating offenders. In most cases, co-offending was based on social ties rooted in the offenders' local communities. The links between more central co-offenders who planned and coordinated the frauds were commonly borne out of long-standing and close relationships.

The involvement of co-offenders ranged from complicit agreement, deception or manipulation, or a willingness to look the other way. Many of the fraud offences constituted project crimes, meaning a specific method (involving a specific set of processes and criminal enablers such as a front organisation or stolen identity data) was used to perpetrate multiple frauds within a fixed period of time. The involvement of many co-offenders was transient or intermittent and they were restricted to a role in this specific project crime; these were often young adults who were themselves at risk of being exploited. In this way, the groups or networks seldom represented stable hierarchies. Those in coordinator roles were often involved in continuous offending, in some cases establishing multiple fraudulent schemes concurrently, and were able to flexibly draw on prospective co-offenders and related criminal resources from their social, criminal or business networks.

4.1 THE ROLE OF CO-OFFENDERS

Most of the frauds were perpetrated online or over a phoneline but regardless, co-offenders were involved in 19 out of the 25 cases (including cases that drew in individuals who played marginal roles). The reason being that co-offenders had a critical role in creating the veneer to help persuade each prospective victim they were legitimate. Notably, none who abused a legitimate occupation to defraud consumers had required co-offenders, as they were able to conceal their criminality behind business entities or activities that had been otherwise legitimate. The specific functions of co-offenders varied depending on the offending method in each case. Some were enlisted to provide a specific capability, and for others their recruitment was less targeted, but they gave the fraudsters an adequate base from which to offend; for example, the success of two investment frauds relied to a large extent on having the manpower to make the unsolicited sales calls.

Many fraudsters relied on co-offenders to provide the interface with victims, providing the necessary front for the underlying fraud. Offenders in these roles commonly required little or no specialist knowledge, and in many cases, they were peripheral and had only a partial knowledge of the overall fraud method. In three of the investment frauds the offenders operated within a conventional business structure, which included employing or contracting the services of unregulated salespeople or 'brokers' to engage in high volume telemarketing or business networking activity. The ability to be persuasive and sell the product was the most important skill and most did not have formal qualifications or experience of work in investments or finance prior to recruitment. This lack of expertise enabled the core offenders to more easily manipulate and deceive them (in

two cases the offenders provided training or a script for telemarketers to follow). In at least one case, the indication was that these recruits were not aware from the outset that the scheme was fraudulent.

Many predatory fraud offences involved enlisting co-offenders to interface with victims, including the 'money mules' whose account details were shared in the interactions with victims (to receive the money) or the use of couriers to physically collect items or money. While not adding a specific capability, the people in these roles were integral to establishing or upholding the deception. Furthermore, in occupying these more front-facing roles they were the most exposed, which provided a protective layer that put distance between the core offenders and the crime. For example, in a case of payment diversion fraud the stolen money was transferred to the bank accounts of students who were quickly chaperoned to the bank or foreign exchange bureau to withdraw the money. When the victim eventually identified and reported the crime the investigation strained to reach further than these account holders who had only known the co-offender by an alias.

Other co-offenders possessed more specific capabilities, some of which represented highly specialised criminal resources that were essential to the commission of the offence. While some had a stable role in the groups' offending, others possessed valued resources that they made available to multiple different offenders. An explicit example was an individual known for his capability to 'con' people and who for a fee, made himself available to different groups engaged in courier fraud. Other key capabilities included that of cyber criminals to steal large volumes of personal and financial credentials (this was integral in two cases), offenders with the ability to forge or falsify hard-copy identity documents and in one case, an offender was contracted by an investment fraudster to supply thousands of customer 'leads' to their brokers.

In five cases, investigators identified an individual with a specific role in coordinating money laundering activity.[19] One offender had opened up multiple shell companies linked to over 100 bank accounts, and it was suspected that he allowed other offenders engaged in investment, payment diversion and loan fraud to make use of them. Two of his co-offenders had recruited at least 12 young adults to provide their identity details and documents for a small fee, allowing him to register companies using their details. Other money launderers were described as 'herders' because of their central role in recruiting and coordinating the activity of money mules. These offenders required continuous access to communities or social networks from which to enlist new 'mules' and needed the forensic awareness to be able to quickly mobilise them and release funds from their accounts without leaving a trace. The need to control the money mules meant that this was one of the few elements of fraud where the ability to physically threaten or intimidate could prove valuable.

> ***Case example:*** *In an identity fraud case the offender had contacted other offenders on an online forum on the dark web, from whom he was able to purchase stolen identity information for victims in the UK. He contacted car dealerships across the region and used the personal details to purchase a car by making a vehicle finance application. He recruited at least three co-offenders to travel to the dealerships and pick up each vehicle. The dealerships required those collecting the cars to verify their identities and so he commissioned a third party to produce counterfeit hard-copy identity documents (including driving licences), which placed the stolen identity information alongside the co-offender's photo. In this way the offender successfully defrauded around 20 separate dealerships.*

In a handful of cases, the capabilities of co-offenders were linked to their legitimate position at an organisation, two of whom had been employed at the company being defrauded. One offender visited local branches of a company in the leisure industry to get to know the cashiers because the fraud was contingent on recruiting a complicit insider to enter falsified details on to company IT systems.

19. There had been nothing to indicate these offenders had a direct involvement in commissioning the fraud.

4.2 THE FORMATION OF FRAUD OFFENDING NETWORKS

The serious and organised crime literature has highlighted the central role that personal relationships and trust have in the formation and growth of OCGs, specifically within the context of social, professional or criminal networks (Kleemans and Van De Bunt, 1999). This ability to form the requisite relationships is influenced by social and environmental conditions in the community, specifically locations in which prospective co-offenders converge to form new networks (Felson, 2006). There is evidence of similar patterns in serious fraud, with many criminal networks emerging from within established social networks, and evidence to show the importance of relationships forged within the local community. There were several distinct social contexts in which fraud offending could emerge, categorised below as community, criminal, and business networks. These different social contexts could represent different places, people and relationships but they were not mutually exclusive, with some offenders drawing co-offenders from multiple settings.

4.2.1 Community-based networks

There was a pattern in which fraud offending concentrated within established family, friendship or other community-based networks, especially in the cases of predatory fraud. These trusted relationships were of particular significance to those operating at the more stable core of the group; for example, three frauds had revolved around offenders who were brothers and in three others, at least two of the core offenders had been old school friends. In some cases, co-offenders had mainly emanated from the same or neighbouring communities where they continued to live, which enabled offenders to engage in fluid collaborative arrangements, especially for those who took more peripheral roles. For example, in one courier fraud an offender's girlfriend was suspected to have communicated with the victim as part of the deception. Several groups were ethnically homogenous in their composition; one group was comprised mostly of offenders from the same Eastern European country (many of whom were family members) and three groups had involved British nationals from the same minority ethnic background. This highlights the importance of relationships rooted in an offender's established community to the formation of criminal groups.

Individuals who gave access to their accounts (i.e. money mules) or personal details had a more marginal role in the fraud, but social networks could still be important in the recruitment of these co-offenders. In two cases the offenders had taken control of bank accounts linked to individuals from their own personal friendships or relationships. Three other offenders were able to tap into the recruited person's own social network; one offender had targeted students attending the local university, one of whom was active in recruiting other students on his behalf.

4.2.2 Criminal networks

In the context of serious fraud in this study, the term 'criminal networks' refers to identified co-offenders who had perpetrated the same or similar fraud together in the past, but also includes a wider criminal network that could be drawn upon in the commission of the fraud. In the context of some commercial frauds the criminal collaborations could span global jurisdictions, but trusted relationships remained significant. In one investment fraud, the primary suspect coordinated the fraud from overseas and enlisted a number of UK-based individuals with whom he had worked in the past, including one he had met while working at another fraudulent company and who helped establish the companies used to commission the fraud. In another, the main offender maintained his links to a member of a known crime family with whom he had previously perpetrated serious fraud (his specific role was uncertain). Further, in order to sell the investment, he contracted the services of 'boiler rooms' known to him from previous offending.

In a similar vein, in the context of predatory fraud offences there were offenders who retained criminal affiliations from prior offending to facilitate the fraud, four of whom had ties to 'conventional' OCGs or urban street gangs that were also involved in drug supply and/or serious violence. These offenders were able to flexibly exchange knowledge and resources with others in these

established criminal networks. This enabled them to repeat offend and evolve their methods, and at the same time exposed and drew other members into fraud offending. To illustrate, the members of a street gang who were perpetrating courier fraud were able to enlist others who were lower down in the gang hierarchy (and looking to prove themselves) to take the role of a courier to collect money or cards from victims.

Some criminal affiliations extended from the offenders' social network however there were also those that appeared to be grounded in more transactional relationships, particularly where specific capabilities and resources were supplied to a group. The most apparent example of this was in two cases in which offenders accessed online markets to purchase stolen personal or financial details from anonymous actors on the internet.

Case example: *One case involved two co-offenders who had grown up in the same area in the UK and gone to the same school. They were both suspected to have links to the supply of drugs that spanned multiple regions in the UK, money laundering and serious violence. One had been convicted of a firearms offence and was in custody at the time of the inclusion fraud offence but remained involved using a mobile phone. They displayed versatility in their offending, with links to payment diversion and identity frauds, and a denial of telephony service ransomware attack that was targeted to a company in the local area. They were not especially technical but were 'very adept at money laundering' and their methods included pressurising money mules to receive stolen money or goods and using cryptocurrencies or online gambling sites to launder illicit proceeds. They were suspected to have links to a network of individuals (none of whom were identified) in the local area who were able to facilitate the more 'technical aspects' of the fraud; for example, the precursor hacking offence to perpetrate the payment diversion fraud. The offender in prison was considered to have the greater standing and more connections with people in the network. The co-offenders perpetrated 'identity' frauds by accessing fake or stolen credentials from online carding forums. It is suspected these credentials were purchased and supplied by other unidentified offenders in the network.*

4.2.3 Business networks

These networks primarily pertained to offenders operating in the commercial fraud context, because predatory fraud offenders had fewer requirements for legitimate or ostensibly legitimate business services (with the exception of those who used insider employees to offend). The line separating a business and criminal network was in some cases thin, depending on the degree of complicity from the facilitators in the business network and the extent to which they provided otherwise legitimate services. One offender recruited a small number of unregulated salespeople through informal channels (one had been referred by an investor) who were paid a commission for the sale of the investments, and only some indicated a partial knowledge of the underlying deception. While operating behind a legitimate veneer, the core offenders could recruit others on this basis, but informal channels and personal contacts continued to be important, in part to draw in the least discerning recruits. In an investment fraud case, a number of the 'brokers' described having met the main offender at a social event and others joined through a more formal application process after responding to an advert on social media; they were mostly young males lured by an aspirational lifestyle exhibited by the main offender. Commercial fraud offenders could therefore draw in known criminals actors who were already active within the relevant markets (for example, prior co-offenders in 'boiler rooms'), as well as legitimate actors from within business networks.

Case example: *An online shopping and auction fraud involved individuals occupying three points along a purported supply chain; the retailer who operated a website for selling the items, the distribution centre that sourced and delivered the goods to customers and a product supplier based overseas. There were ten identified co-offenders linked to the different companies, many from the same minority ethnic background. The two core offenders operated from the distribution centre and the supplier, with the former receiving consumer funds from the retailer and transferring this to the overseas supplier as payment for the imported goods. These two individuals were known organised criminals linked to serious fraud and international money laundering and had*

previously co-offended in a high value tax fraud. In the year prior to the fraud the two brothers who ran the online retailer, had sought to expand their business and were referred by a friend to a distribution centre in another area of the country. And in the first year all customers' orders had been fulfilled. The next year, the individuals at the distribution centre provided the link to the core offenders, who used the online retailer to provide a credible front for the fraud. It was indicated that the retailer was not wholly complicit in the commission of the fraud. Over a period of a few months the group had taken thousands of orders, the majority of which were not fulfilled, and much of the money was transferred overseas to the fictitious supplier and withdrawn as cash.

4.3 SHARED LEARNING AND RESOURCES IN SOCIAL NETWORKS

It was social opportunities that arose from community, criminal or business networks that enabled many to engage in fraud offending, and some were able to continuously draw on the resources and knowledge available in these networks to sustain their offending. There were some clear examples of knowledge exchanges which equipped co-offenders with the capabilities to perpetrate the same or similar frauds, thereby feeding into the stock and flow of fraud offenders and increasing the criminal capital available to these criminal networks. In one case the co-offenders were seen to have discussed methods for managing investigations by a state regulator. The central offender in an investment fraud was known to have engaged in similar frauds for several years prior to the current fraud, and at one time had worked in the sales team of another known investment fraud 'con man'. Furthermore, those in his own sales team received training and on proving themselves capable, were promoted to the position of 'senior broker'. At least one had moved to another company that was also suspected of fraud and linked to some of the same victims.

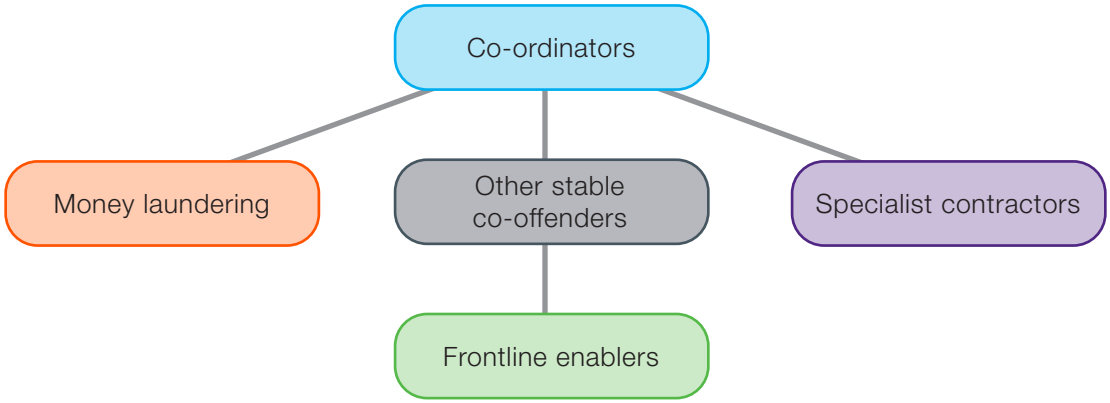
This process of social learning was also evident in the predatory fraud context. In two cases, courier fraud offenders operated within a wider social hierarchy rooted in gang culture, in which knowledge was exchanged and those most capable could progress to more serious offending; one fraudster had prior links to an OCG involved in courier fraud and had since progressed to other forms of fraud offending. Another identity fraudster had a history of fraud offending and claimed to have perpetrated the current offence on behalf of a criminal group to which he was affiliated and had provided him with the requisite resources (including stolen cards and fake identity documents). Criminal networks offline and online were able to provide a range of resources that facilitated more persistent and versatile offending by fraudsters, which for some included fraud and computer misuse crime.

4.4 THE STRUCTURE OF THE NETWORKS

In all cases that involved multiple offenders there was one or a small number of individuals who had initiated the fraud and coordinated the activities of co-offenders. Offenders in these roles tended to be among the most persistent fraud offenders and were often those in the network who had the closest social ties (for example, family members, friendships and/or prior criminal association). Offenders varied in the extent to which they enlisted additional offenders – ranging from two coordinators who drew in a small number of money mules from their own social network, to another that formally recruited office staff and contracted the services of various criminal enablers. However, none of the groups represented a stable hierarchy,[20] with coordinators drawing flexibly on individuals from networks, as was needed, in the commission of a given fraud 'project'. As a result, many co-offenders were transient and only partially aware of the overall modus operandi. Moreover, the illicit profits would often concentrate in the accounts of coordinating offenders.

20. There were a small number of cases in the predatory fraud offending context in which the fraud offenders themselves operated within a wider and more stable hierarchy linked to identity-based street gangs.

Figure 2: The structure and functions of co-offenders linked to the criminal networks*



* This depicts the maximum distribution of roles/functions across co-offenders, but individuals with specific money laundering, specialist contractor or frontline enabler roles were not present in all cases.

Figure 2 provides an illustration of the key roles and structure in which the offenders operated. It differentiates coordinators from others with a relatively stable co-offending role in the specific fraud (for example, sales teams selling investments). It also delineates the outsourced providers with specialist capabilities (for example, an offender contracted to supply 200,000 potential sales leads), the offenders with a specific role in coordinating money laundering and a lower tier of commonly more expendable co-offenders (such as money mules and couriers). While there was often a clear division of labour, the group structure seldom extended beyond the three layers and in some cases the structure was even flatter, especially when the coordinating offenders had the requisite resources themselves (see the example case study below).

The control over the fraud conspiracy accorded those in coordinator roles with a higher standing; they were often the only co-offenders with full sight of the fraud modus operandi, were less exposed to detection and often received a large proportion of the stolen money. Those in other roles would often play their part in isolation of one another, and their value to the network was variable and most likely dependent on the value of the resource or capability they possessed. The capability to launder money could determine a group's ability to perpetrate serious fraud, and individuals with the ability to coordinate money laundering had considerable value to some fraudsters; one individual specialised in fraudulently opening companies and business accounts and provided money laundering services to multiple groups. There were a variety of other roles that were important to sustaining fraud offending (for example, the scope to perpetrate identity fraud could be determined by the ability to access stolen credentials) and those most able to continuously provide or draw the requisite resources from the various networks brought considerable value. This was especially apparent in urban street gangs which operated to a structured social hierarchy (the most senior referred to as 'elders') which was mirrored in the standing of each co-offender in the fraud offending network.

Case example: *To illustrate a case that involved a small number of co-offenders, one investment fraudster had set up a binary investment scheme in 2004 which operated from overseas. He had set up an office with at least six staff and employed the services of a legal representative, all of whom had been deceived by the fraudster and believed the company to be legitimate. He did not employ special measures to launder the illicit proceeds because the deception was established at the point of sale and he maintained a legitimate appearance to his existing clients (for example, making the scheduled payments). His main requirement of co-offenders was marketing and sales. He contracted the services of three UK-based sales representatives who organised high profile networking events attended by affluent individuals with the means to invest in the scheme. The culpability of the sales agents was not clear however the investigators suspected some dishonesty and awareness that the scheme was not legitimate.*

Case example: *A large group of at least 16 co-offenders were involved in defrauding two local branches of a business in the leisure industry. Most co-offenders were family members or friends with a shared foreign national background. Two brothers were responsible for coordinating the fraud and both had a suspected history of perpetrating similar frauds in other parts of the UK. Co-offenders were necessary to attend the branches (posing as customers) to commission the fraud, and then subsequently to launder the money. Furthermore, in each of the branches a female employee was recruited; one was in a relationship with a co-offender in the network and the other had been promised payment for facilitating the fraud. A process was needed to receive the stolen money without raising the suspicion of the banks and so the money was transferred to 14 separate bank accounts. These included the accounts of core co-offenders (though not the brothers coordinating the offence) but also elderly women linked to the family acting as money mules but who appeared to have limited knowledge of the fraud. The money was then laundered through a process of cash withdrawals and high value purchases, and two co-offenders were involved in purchasing vehicles and taking them overseas along with large amounts of cash.*

4.5 THE ROLE OF EXPLOITATION

The partial nature of the roles played by many co-offenders creates a challenge in determining the extent of their complicity (with each motivated to deny full complicity). However, across the different frauds there was a pattern in which individuals were recruited as expendable offenders into the lower tier (see Figure 2 above), meaning they often had limited knowledge or understanding of the wider fraud, received little or no recompense, and helped provide a buffer between the victim and the core offenders. Many exploited close personal relationships or those in their wider social network, including individuals with limited financial means or those with a personal vulnerability. To illustrate, one identity fraudster had a drug misuse problem and claimed to have been paid in drugs by an OCG that commissioned him to perpetrate the fraud.

This exploitation was particularly evident in the predatory fraud cases, by offenders with less access to resources in business networks (most notably financial instruments in the UK or overseas) and who instead harnessed the resources available to them in their community and criminal networks. A particular challenge to overcome was releasing stolen funds from financial accounts while evading detection, and in nine cases the offenders recruited 'money mules' for this purpose. These were individuals who typically received minimal information from offenders about the underlying fraud and were offered small payments to provide access to their personal bank accounts. Their involvement was in some cases short-lived by design because on identifying a potential fraud their account was frozen by the bank or an investigation would lead directly to them. Recruitment took various forms, with some using individuals from within their own social or criminal network (sometimes by means of deception), and at least three were more systematic in recruiting mostly young people from the wider community. While dubious, some were lured by the modest financial reward and once they agreed it could be difficult to reconsider and withdraw, with fraudsters, or those who coordinated the money laundering, sometimes using intimidation and coercion.

Fraud offenders with established links to urban street gangs operated in a social hierarchy which enabled fraud offenders to enlist younger and more junior affiliates to take the frontline roles and thereby carry the greater risk. This is a pattern observed in the commission of other serious criminality such as local drug supply. An example of this was a young person in a street gang who took the role of courier in a fraud perpetrated by senior gang affiliates to prove himself in the wider gang. The use of social status to motivate co-offenders was also evident in an investment fraud, wherein young and inexperienced brokers were sold an aspirational lifestyle by the coordinating offender but were paid low salaries under the promise of high commission that some never received. In commercial fraud settings, the line separating co-offenders and frontline enablers could be more difficult to draw. There were a

number of actors who played an important role to sustain the veneer of legitimacy but whose understanding was partial and who had not made any significant financial gains; examples included a trader suspected to have mental health difficulties who was paid a low monthly salary to engage in a notional amount of trading to reassure investors, and the owners of an online retailer used to provide a front for a large-scale consumer and retail fraud.

Case example: *One offender and several associates were suspected to have had regular involvement in money laundering activities but the precise relationship of the associates to the cyber fraudsters remained unclear. The offender was proactive in targeting members of the local student population. One student had been recruited after meeting the offender at a local takeaway and had recruited several of his own friends to provide the use of their accounts for a small fee (several hundred pounds). The offender was only known to the money mules by an alias. None had any knowledge of the fraud and while some expressed having doubts over the legality they chose to proceed regardless; one was experiencing financial difficulty. Some reported beginning to reconsider but were fearful of repercussions if they did not follow through. The money received into their accounts was linked to a payment diversion fraud and once suspicious activity on their account was detected by the bank, the offender ceased all contact. Few received any payment for their involvement. The high turnover created pressure for the offender to continuously source new money mules and at one stage he approached two friends from his own social network. They claimed he had asked if they would allow him to use their bank accounts for what he purported to be a legitimate reason. These two individuals were identified as suspects in the police investigation.*

CONCLUSION

The findings of this study represent serious fraud perpetrated by offenders in the UK. They provide an in-depth analysis of 25 discrete cases but do not represent the full nature and distribution of serious fraud during this period, but rather those that came to the attention and were selected for investigation by law enforcement teams in England and Wales. The documentation shared by the different investigators varied, and in some cases, there remained gaps in the information on certain offenders or elements of offending. The cross-sectional study of cases helped to profile the roles, backgrounds and offending of offenders known to police during this period of time. Analysis of changes in serious fraud and individual progression in offending would require a study that uses longitudinal methodologies.

The serious frauds included in this study comprised offending that is remarkably diverse in method, complexity and impact. There was an overarching requirement for offenders to appear credible and legitimate to gain the trust of victims, and there were offenders operating in different settings exploiting a range of opportunities available to them. In the context of commercial frauds such as selling misrepresented investments or other products and services, offenders exploited legitimate markets and systems to allow them to offend in plain sight. In predatory frauds such as identity and payment diversion fraud, offenders used technology or stolen identity information to infiltrate and disguise themselves as legitimate individuals or organisations. Unsolicited calls to pressurise and persuade victims to provide access to their money was a prominent feature in multiple cases, with success contingent on being able to target activity to individuals who were susceptible to the deception. Despite the diversity, there were a number of common themes that spanned the different types of fraud in the sample; the significance of online enablers in commissioning many of the frauds, the necessity to identify and target vulnerability in its various guises and a requirement to cover the financial trail to evade detection.

The offenders themselves had emanated from diverse social and economic backgrounds; a small number had exploited opportunities from within a legitimate occupation and others had no legitimate occupation but continuously occupied conventional white-collar settings to perpetrate commercial frauds. Others abused a frontline occupation in the informal economy. Predatory frauds mostly targeted victims in the public or business community from outside of a legitimate setting.

Serious fraud in most cases is an offending process rather than an isolated event and which involves multiple activities over a period of time. In general, offenders who operated further from a legitimate setting were required to develop the most complex methods, with a particular imperative to enlist co-offenders to facilitate the deception, launder the proceeds and evade detection. Those who coordinated the fraud often drew co-offenders from within their established social networks, many of whom had no specific skills or knowledge, however some engaged individuals with access to specialist criminal knowledge or resources to enable them to commission the fraud or money laundering. The co-offending arrangements were commonly flexible, with durable co-offending most common between a small number of offenders who were central to planning the fraud. Importantly, serious fraud cases encompassed many individuals who did not fit the profile of a serious offender, especially those peripheral to the overall conspiracy and vulnerable to criminal exploitation.

REFERENCES[21]

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

Blakeborough, L. and Correia, S. (2018) *The scale and nature of fraud: A review of the evidence*. London: Home Office. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf>

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.

Felson, M. (2006) *The ecosystem for organised crime*. Heuni paper 26.

HM Government (2018) *Serious and Organised Crime Strategy*. London: The Stationery Office.

HMICFRS (2019) *Fraud: Time to choose – An inspection of the police response to fraud.* HMICFRS.

Home Office (2021) *Home Office Counting Rules for Recorded Crime: Fraud*. Available at: <https://www.gov.uk/government/publications/counting-rules-for-recorded-crime#full-publication-update-history>

Home Office (2022) *Home Office Counting Rules for Recorded Crime*: *Fraud.* Available at: <https://www.gov.uk/government/publications/counting-rules-for-recorded-crime>

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

Kleemans, E.R. and van de Bunt, H. (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(1), pp.19-36.

Leukfeldt, E.R. and Yar, M. (2016) Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 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., Button, M. and Whitty, M. (2017) *Economic Crime: Learning from Offender Methodologies, and Pathways into (and out of) Crime*. London: Home Office.

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(1), pp.4-14.

May, T., and Bhardwa, B. (2018) *Organised Crime Groups involved in Fraud*. Palgrave: London.

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

Naylor, T. (2002) *A typology of profit-driven crimes*. Canada: Department of Justice Canada.

Proceeds of Crime Act (2002) (c.29). [online] Available at: <https://www.legislation.gov.uk/ukpga/2002/29/contents>

Roks, R.A., Leukfeldt, E.R. and Densley, J.A. (2020) The hybridization of street offending in the Netherlands. *British Journal of Criminology*. 16(4), pp.926-945.

Sentencing Council (2014) *Fraud, bribery and money laundering offences: Definitive guideline*. Available at:<https://www.sentencingcouncil.org.uk/sentencing-and-the-council/about-sentencing-guidelines/about-published-guidelines/fraud-bribery-and-money-laundering>

Serious Crime Act (2015) (c.9). [online]. Available at: <https://www.legislation.gov.uk/ukpga/2015/9/contents/enacted>

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

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*. London: The Police Foundation/Perpetuity Research.

Van Der Geest, V., Weisburd, D. and Blokland, A. (2017) Developmental trajectories of offenders convicted of fraud: A follow-up to age 50 in a Dutch conviction cohort. *European Journal of Criminology* 14(5) pp.543–565.

Van Onna, J. H. R., Van der Geest, V. R., Huisman, W., and Denkers, A.J.M. (2014) Criminal trajectories of white-collar offenders. *Journal of Research in Crime and Delinquency* 51(6), pp.759-784.

Weisburd D., and Waring, E. (2001) *White-collar Crime and Criminal Careers*. New York: Cambridge University Press.

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

21. Accessed 30 November 2022.

Email: info@police-foundation.org.uk

www.police-foundation.org.uk

Charity Registration Number: 278257

THE POLICE FOUNDATION

The UK's policing think tank