# Economic Crime: Learning from Offender Methodologies, and Pathways into (and out of) Crime

Michael Levi, Mark Button and Monica Whitty

Cardiff University, University of Portsmouth and the University of Warwick

March 2017

# Contents

# 1. Introduction

In 2016, the City of London Police were awarded funding under the Police Innovation Fund to create an "Economic Crime Isomorphic Learning Centre" and in in partnership with Cardiff University, the University of Portsmouth and the University of Warwick, to pursue a project built upon police debriefs with convicted fraudsters and other knowledge generated from past incidents of economic crime. There were specific aims to fill the gaps in knowledge relating to:

- Criminal pathways; and
- Methodologies used by offenders.

This report provides the first output as a result of this partnership, and provides some insights on criminal pathways and the methodologies used by the offenders operating in this area. The report begins with a review of the literature relating to pathways into and out of online and offline economic crime. It then briefly sets out the methodology before exploring the results of research based upon prison debriefs undertaken by police officers in the City of London Police and a survey of police officers about fraudsters drawn from all over the United Kingdom.

## 2. Pathways into (and out of?) online economic crime and implications for control strategies

Much of the shift in thinking about crime and its management in recent decades has been provoked by former Home Office Research Unit Director Ron Clarke's promotion of 'proximal' (near) causes and downplaying the value of 'distal' (far) ones, via the commonsense mechanism of situational crime prevention theory whose Crime Triangle takes for granted the motivation to offend and concentrates analytical efforts on 'suitable targets' and (in our view, actually *or potentially*) 'capable guardians'.[1] It is a tautology that if guardians are capable, crime will be prevented. But especially in the context of cybercrimes, we suggest that it is mistaken to ignore the *concentration* and *number* of those willing to offend – which varies over their life cycle both as individuals and as 'connected communities' – and we need to examine variations in how 'suitable' targets are perceived as being and how capable *and motivated* the guardians are to protect against particular forms of crime. A large number of willing offenders can make it harder to stop all 'attackers', for example, for any given level of situational crime prevention efforts. In principle, capable guardianship can be motivated by criminal or regulatory legal obligations and/or by education and persuasion, as well as innovation. In other words, these constructs are not linear enough to adequately fit the constant reshaping or risk and protection in contemporary society. Taken literally, the Clarke typology has implications both for 'Prevent' and 'Pursue' strategies, rendering them both marginal as it focuses on the dimensions of crime that are covered by 'Prepare' and 'Protect'. The aim of this review is not to make assertions about the value of any particular approach but to reassess the range of them in the light of evidence that we have collected and what seems plausible to us.

It may be helpful to try to think through these issues from first principles. Most of the contemporary media (especially tabloid, technical and 'flash news' media) attention paid to economic crime is on the cyber aspects of this, unless celebrities are involved as suspects or victims, or the victims of offline fraud are visibly traumatised (Levi, 2006, 2008). The media, plus the correct perception by the College of Policing and others in authority that the police need to adjust significantly to the realities of digital crime and digital investigation, tend to drive social and institutional reactions in the direction of online fraud. But such a shift may be necessary without its being sufficient to deal with the full range of serious economic crimes, online and offline.

First, why should we focus particularly on cyber-enabled economic crimes rather than on economic crimes in general, whether online, offline or mixed? Three possibilities suggest themselves: the different *technical* requirements; relative harmfulness (including *perceived* harm) compared with offline crime; and the rate of *growth* of harmfulness. *Prima facie*, a reason for differentiation might

[1] See, e.g. Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, *19*, 91-150; Clarke and Cornish http://www.popcenter.org/library/reading/PDFs/ReasoningCriminal/01_introduction.pdf; http://www.popcenter.org/Responses/crime_prevention/PDFs/Cornish%26Clarke.pdf ; Wortley, R. (2012). Exploring the Person-Situation Interaction in Situational Crime Prevention (pp. 184-193). In N. Tilley and G. Farrell (eds) *The Reasoning Criminologist: Essays in Honour of Ronald V. Clarke*, London: Routledge. There is no need here to go into the many critiques of this perspective. Although it performed an important and valuable function in realigning criminology to focus more on the crimes themselves and their immediate context, and stimulating problem solving policing and citizen action, the casting aside of attractions and pressures to offend is unhelpful, whether for cybercrimes or for terrorism.

be expected to depend on the level of technological sophistication required, which might constitute different barriers to entry, depending also on whether the offender had to have that knowledge him/herself or whether social/financial ties to those with the knowledge (or insiders) were enough.[2] Fashion alone is a bad reason for focusing on hi-tech fraud, though it is reasonable for the police and government to be particularly concerned about the growth of a new set of potential career offenders, wherever situated, who could attack targets that they deemed suitable in the UK *and that would be seriously harmful in the UK*.[3] Is there any reason to suppose that the pathways into high technology crimes are different from those into low-tech serious or low level fraud?

The metrics of the harms of fraud are unevenly developed, but though social research shows high levels of anxiety and judgments about the seriousness of identity theft and suchlike frauds against individuals, cyber-enabled and cyber-dependent crimes may not be the most harmful or the most profitable/loss-generating economic crimes. Whether they be primarily offline or online, our understanding of how to aggregate fraud, IP and other losses depends on having a plausible attribution process with which to connect up the individual incidents, and this in turn depends on the traces of evidence searched for and detected, as well as on reporting and recording behaviour (improved in the UK because of Action Fraud, though this may not have changed the volume/ proportion of non-reporting). But it seems unlikely that many individual or even networked/ 'organised' cyber-enabled crimes will be as large as typical Serious Fraud Office fraud cases, either individually or in aggregate. Furthermore, there are many fraud cases against 'vulnerable adults' that are not committed by internet routes, not least because some vulnerable people do not use the internet. This 'age gap' of susceptibility to eCrimes may diminish in future generations,[4] but that is not presently relevant.

However, many such crimes – whether cyber-enabled or not in their main process - involve the victims or their innocent or scheming representatives going to the bank to transfer funds, either directly or by drawing the sums out in cash and then sending them to the criminals by some other route (e.g. Money Service Bureaux, most commonly Western Union because it is ubiquitous rather than because it is more negligent[5]). Since most funds transfers that are not physical cash hand-overs are sent electronically, this could make them cyber-enabled crimes, though such a classification risks discrediting the utility of 'cyber-enabled' or 'cyber-assisted' as meaningful terms. As Levi (2008) noted in *The Phantom Capitalists*, in terms of speed of funds transfer, the invention of the telegraph

[2] As in the crime-as-a-service model highlighted *inter alia* in the Europol iOCTA (2014 et seq.) as a trend that enables industrialisation of some cyber-crimes to those who otherwise would not have the capacity to offend.

[3] They may also plan to attack people, businesses and governments elsewhere, though that might not be of parochial concern. One might interpret the remit as a more global one rather than being focussed exclusively on UK victims. For example, as the Home Secretary observed to the Financial Conduct Authority's Financial Crime Conference 2016, "We must make the UK a hostile environment for fraudsters and those seeking to move, hide and use the proceeds of crime and corruption". In a later speech, during the Criminal Finances Bill's reading, Security Minister Ben Wallace said: "We need to make the UK a hostile environment for those seeking to move, hide and use the proceeds of crime and corruption. In an increasingly competitive international marketplace, the UK simply cannot afford to be seen as a haven for dirty money." (http://www.bbc.co.uk/news/uk-39047321). These all suggest a responsibility to victims outside the UK.

[4] There is a balance here between the extra risk posed by continuing access to the internet, and perhaps greater skill in handling such skills. The automatic immunity that comes from large segments of the present 'elder' generation not using the internet is arguably offset by their vulnerability to mail and telephone fraud offers, which latter may not diminish as their vulnerability to internet scams rises.

[5] We should always be careful to try to look at incidents as ratios of use volumes.

was more transformational than the Internet: but though packet ships were a slow time way of transfer compared with the telegraph, they were faster than methods of pursuit or sending letters to institutions or the police overseas before the invention of the telephone or fax! And it is the elapsed time between techniques of eCrimes and those of detection/pursuit/ asset freezing that is important here, whether these Pursue activities are conducted by the public or (at least initially) by the private sector.

Second, is there a reason for expecting that the pathways into cyber-dependent/enabled economic crime are different from those of economic crime generally? One factor might be that economic crime opportunities involving specialised *legitimate* access are often a function of age, education and experience. Thus, with the exception of some young dot.com entrepreneurs and gifted mathematicians developing formulae for financial services success, people with sufficient insider access to fraud and money laundering opportunities are likely to be in the 30-75 age range. Cyber frauds enable youthful outsiders to leapfrog these conventional routes. Felson (2002: p.95) comments that '[p]erhaps, then, "white-collar" offenses are best renamed crimes of specialized access. Occupations, professions, and organizations provide offenders practical routes to their targets. The central point is that *legitimate* features of the work role provide a chance to do misdeeds.' Many of the 'criminal career' aspects of economic crime generally are bound up with the need to gain specialised access either as insiders or as outsiders, or sometimes collusively. There is no reason why cyber-enabled and even cyber-dependent offenders should be expected to be young, especially in future generations when they may have grown up as digital natives. Furthermore, if we think of the networks involved in such crimes, these can include older as well as younger people, whether because the older/more experienced ones are extorting the younger or for more symbiotic reasons such as their wider networks of redistribution of stolen data, physical cards, 'drop houses' for the delivery of goods ordered on fraudulent identities, et cetera which constitute some of the 'social capital' of crime networks, whether we label them 'organised crime' or not.

Third, when we review pathways into cyber-enabled and cyber-dependent economic crime, do we focus on issues forming individual propensities, or do we also/instead include more proximal characteristics such as their social networks – which supply or refine knowledge of crime techniques - and the socio-cultural features that promote relaxed or even positive attitudes towards some or all cyber-offending? Research on a variety of crimes including genocide and on wartime activities such as dispatching bombs and drones discuss the disinhibition that occurs when the targets are far away and are not identified as persons like oneself.[6] But little is known about whether 'cybercriminals' – a far from homogenous or clearly defined category - are willing to target some victims/acts but not others, or about the extent to which they are also involved in other crimes. This may vary anyway between offenders in different jurisdictions: it is not evident why emotions, relationships and values that inhibit some offenders in the UK should apply in the same way to Nigerian or Ukrainian offenders, let alone to state-sponsored or state-tolerated cybercriminals in China and Russia.[7] Evidence from some Russians identified as responsible for hacking is that they may have been pressurised by the security services into hacking in exchange for not being prosecuted for criminal

[6] See contemporary films such as 'Eye in the Sky' as well as academic texts such as *States of Denial* (Cohen, 2000).

[7] We consider that 'state sponsored' means actually ordered by governments, whereas 'state tolerated' means allowed by government (including as a consequence of corruption). It is seldom possible to generate an account that all parties would accept as valid, because attribution chains are difficult to sustain.

offences: but equally, they may see their voluntary 'official' work as giving them protection for some private enterprises involving cyber-enabled crime for gain.[8] These accounts are compatible but are often deniable and a matter of interpretation.

## 2.1 Pathways into cyber-dependent crimes

The NCCU within the National Crime Agency has a remit for cyber-dependent crimes only, and its briefing and some very good case studies notes that the path is often via gaming and gaming sites which offer an avenue for experimentation, skills refinement, and the development of contacts (NCA, 2017; see also the less helpful because more generic report, NCA 2016). A more expansive study by Aiken et al. (2016) of *Youth Pathways into Cybercrime*, with some helpful illustrations, does not so clearly differentiate the crimes, but asserts that the combination of youthful stresses and the dopamine-release effects of stimulating games can generate addiction to cyber activities (though it is not clear why illicit activity should be the outlet). It uses expert interviews to support its recommendations for analysis and practice, but it is not clear how these relate to the general evidence base for cyber-offending. In both cases, the focus is on youthful offenders, and in keeping with their aims, crime for economic gain is not a central feature.

## 2.2 Pathways into cyber-enabled crimes

The evidence about how people get into cyber-related economic crime (and indeed fraud generally) is not strong. This is partly because of the low reporting, detection, prosecution and conviction rates, which means that few offenders are in jail and available for interview or analysis. [9] Like all profiling efforts, the analysis depends on how we are able to sample cybercrimes, individuals, and their networks over time. The dataset is not helped by classification problems, as offences of theft of computers have been classified as 'computer crimes'. Though there is dispute about whether anti-fraud policing resources in England and Wales have declined and by how much,[10] the universally attested low police priority traditionally given to fraud also contributes to our poor understanding of offenders. There are corporate investigations and scandals that are not dependent on police action, but the few criminologists and professional services firms who have looked at fraudster, organised crime and white-collar crime profiling have not focused specifically on cyber-enabled ones (Bethune, 2015; van der Geest et al., 2016; KPMG, 2013, 2016; Onna et al., 2014; Piquero and Weisburd, 2009; Piquero and Piquero, 2016; Piquero et al., 2016). Indeed, because of the attempt to look at offenders' development over a longer period, many of these studies start with offending careers in the 1970s, before online crime became a reality.

One of the problems in generalising from many such surveys is that there is an in-built bias arising from the fact that the mostly large corporate victims have chosen to pay professional services firms to investigate, and therefore we may assume that the frauds are at the high end financially and/or they involve staff in senior/sensitive positions that leads the victims to want to understand what

[8] New York Times and other newspapers, e.g. 'Reports of treason and CIA spies shed light on Russian hacking', 1 February 2017, https://www.ft.com/content/1b203b00-e7d7-11e6-967b-c88452263daf; 'Russia mobilises an elite band of cyber warriors', 23 February 2017, https://www.ft.com/content/f41e1dc4-ef83-11e6-ba01-119a44939bb6.

[9] An intelligence assessment by the NCA (2017) has offered some thoughtful profiles of pathways for cyber-dependent criminals which do not rely on conviction data: but cyber-enabled crimes may be expected to have more variable pathways and be less focused on earlier age groups.

[10] Button, M., Blackbourn, D., and Tunley, M. (2015); King, J. and Doig, A. (2016); Doig, A., and Levi, M. (2013).

happened.[11] Another problem is that they are very seldom prospective: they yield little insight into how legitimate and/or criminal careers evolve subsequently. This is important because it is quite plausible that as they get older, people move to a mixed legitimate/illegitimate role. This is not a criticism of those surveys that provide a snapshot in time: merely an observation. It is also difficult to track subsequent careers.

Weisburd and Waring (2001) identified three distinct criminal career patterns in their sample of offenders convicted in the late 1970s. Whereas some had very few or no convictions, the criminal career of others more closely mirrored that of the typical street-crime offender in length and diversity of offending. Substantial numbers also had 'punctuated offending' (analysed in greater sophistication by Piquero and Weisburd, 2009). Their typology identified:

(1) C*risis responders* - low-frequency offenders who commit white-collar offences typically in response to a crisis occurring in their personal or professional life. Few have multiple convictions for other offences and typically these offenders lead ordinary and law-abiding – though at times troubled – lives. They often own or manage small businesses that allow them to commit white-collar crime.

(2) *Opportunity takers*. For these, committing an offence is equally unusual. Unlike crisis responders, their key motivation to engage in white-collar crime is to take advantage of a specific opportunity that presents itself but is not always present.

(3) *Opportunity seekers*, who typically follow a more chronic – though intermittent – criminal career that spans multiple convictions.

(4) *Stereotypical criminals*, whose fraud offences are part of a mixed and high-frequent criminal career. Their profile is very similar to that commonly found in the general offender population: their personal lives reflect disadvantage, they often have experienced academic failure, and they show unstable employment careers.

Of these, the first two categories account for the great majority.

Van Onna et al. (2014) used official conviction data to reconstruct the criminal careers for a sample of recently prosecuted Dutch white-collar offenders again from their early teens up to age 50. Their four different developmental patterns and socio-demographic profiles matched those developed by Weisburd and Waring (2001) in the US, but these were retrospective and therefore not relevant to desistance, and additionally related only to complex and serious cases of white-collar crime brought by specialist prosecutors. They noted that the largest categories (accounting for over three quarters of offenders) turned to crime for the first time in adulthood. The rest had been largely active in white-collar crimes since they were juveniles. In short, Dutch research findings thus far indicate substantial variations in criminal development, reflected in large groups of sporadic offenders as well as distinct patterns of adult-onset offending. The more frequent the white-collar offending, the more likely the offenders were to engage in non-white collar crimes. One might expect this to be particularly true of offenders involved in payment card, insurance fraud, and social security fraud (most readily committed by outsiders with modest skill levels) but the data are not broken down in a way that would enable us to work this out.

[11] This may include being able to reassure the regulator that they are trying to understand what happened.

Van der Geest et al. (2016) reconstructed the criminal records of fraud offenders in the Netherlands (which is more likely than US data to be similar to the UK). One of the things that they did was to look at the age profile of offending and its relationship to how many convictions the offenders had (without controlling for offence seriousness or sub-type of fraud). The average time between the first and final fraud conviction during follow-up was 11.4 years (SD = 9.0).

**Table 1.** Fraud-offending career characteristics by accumulated number of offences.

| Total no. of fraud offences | *N* | Av. age of onset in fraud offending | Duration of fraud-offending career |
|---|---|---|---|
| 1 | 645 | 32.7 | – |
| 2 | 257 | 29.1 | 8.3 |
| 3 | 91 | 27.0 | 12.8 |
| 4 | 53 | 25.7 | 15.0 |
| 5 or more | 114 | 26.3 | 15.4 |
| Total | 1160 | 30.5 | 11.4 |

The age– crime curve for fraud is less steep than that commonly found for general offending and reaches its maximum between ages 23 and 35. The average conviction frequencies are low at any given age, with less than one conviction in every 10 or more years, suggesting that – even among those who are reconvicted – fraud convictions are highly intermittent. Of course, the 'real' rate of criminality may be higher due to the attrition between commission, detection, prosecution and conviction: but we cannot speculate what that would look like or how it would vary. Judged from the convictions, offenders appear to commit fraud offences at a steady rate throughout their fraud-offending career. Thus, age differences in participation – rather than active offenders becoming less active over time – seem to contribute to the slowly declining age–crime curve. This makes sense because age does not inhibit the ability to commit fraud: if anything, it enhances it because older offenders look less suspicious.

The authors note (p.11) that "High-frequency fraudsters (who commit five fraud offences or more) are disproportionately involved in swindling. Constituting less than 10 per cent of the sample (9.8 percent), they commit more than half of all offences of swindling (52.4 percent). These convictions involve a variety of fraud offences, such as identity fraud, mortgage fraud and – less often – internet fraud." Only high-frequency fraud offenders have a high degree of specialization: for the majority of the sample, those convicted of fraud also have significant criminal records for serious non-fraud. The authors raise the question of to what extent fraud offenders share personal and social background characteristics with the common offender population, and to what extent these characteristics can also explain fraud.

**Table 3.** Offending versatility within fraud-offending careers.

| No. of fraud offences | Percentage of crimes within the individual criminal careers | | | | | |
|---|---|---|---|---|---|---|
| | Forgery | Embezzlement | Swindling | Bankruptcy fraud | Tax fraud | Customs fraud |
| 1 | 52.1 | 30.7 | 15.0 | 0.3 | 0.8 | 1.1 |
| 2 | 51.8 | 27.8 | 17.9 | 1.0 | 0.8 | 0.8 |
| 3 | 54.9 | 28.2 | 16.1 | 0.0 | 0.4 | 0.4 |
| 4 | 50.0 | 29.2 | 20.8 | 0.0 | 0.0 | 0.0 |
| 5 or more | 40.6 | 23.5 | 34.0 | 0.3 | 0.9 | 0.7 |
| Total | 48.1 | 27.2 | 22.9 | 0.4 | 0.7 | 0.7 |

In discussion, van der Geest et al. note that more than two-fifths of the sample follow a pattern that is consistent with that of *crisis responders* and *opportunity takers* in the Weisburd and Waring American study: they commit very few offences and may do so in response to specific life-course circumstances or specific opportunities for committing fraud (or other forms of white-collar crime). Another two-fifths bear a resemblance to *opportunity seekers*, who display an intermittent but nevertheless persistent pattern of criminal behaviour. Especially for Young Adult offenders, who stop serious non-fraud offending in their late thirties while still committing a few fraud offences, the shift in offending may reflect changes in the opportunity structure of offending (though it is not obvious to us what these are). Finally, one in six offenders are like *stereotypical criminals*, showing large numbers of street crimes – for example, theft and fencing – both before and at the same time as committing fraud. They suggest that fraud offenders respond to or create opportunities for crime in general, rather than for fraud exclusively. The authors do not mention or explore the possibility that their involvement with other crimes is what may have drawn these fraud offenders to the attention of the authorities.

They note (p.20) that their sample consisted of offenders brought to court in the late 1970s. "For some of these offenders a substantial part of their criminal careers materialized in an era without the internet. With the introduction and subsequent blooming of the internet, access to opportunities for fraud have equally sky rocketed, reducing traditional barriers to white-collar offences even further. The consequences for the typology of white-collar crime offenders, in terms of both offender types and their distribution across the offender population, will require additional research based on more contemporary samples." We agree.

Van Koppen and De Poot (2013) note that among Dutch organised criminals, important life-course transitions, such as marriage or employment, that are generally thought to deter individuals from offending can also give rise to changes in the offenders' opportunity structure, making crime more instead of less likely. Whether this is also true of fraud and money laundering, for example among 'professional enablers' (Middleton, 2008; Middleton and Levi, 2005, 2015) is unknown at present.

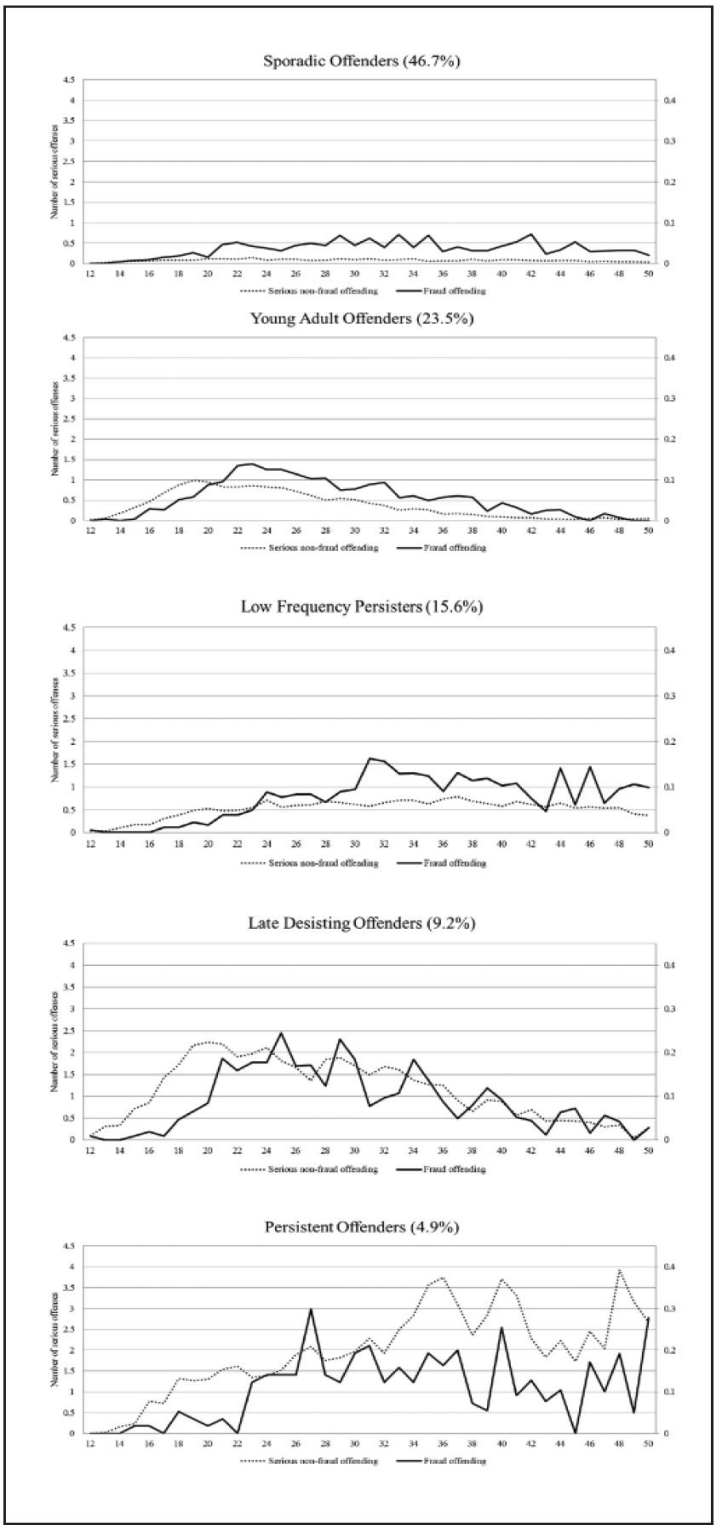


Figure 2.1. Observed patterns of serious non-fraud and fraud offences by trajectory group.

KPMG fraudster profile (KPMG, 2016)

Consistently over time, the perpetrator of fraud tends to be male between the ages of 36 and 55, working with the victim organization for more than six years, and holding an executive position in operations, finance or general management. Only one percent were under 26, and a further 14 percent were under 36. In almost two thirds of cases, the offender colluded with others: collusion

involving more than five people increased from 9 percent in 2010 to 20 percent in 2015.[12] Technology was a significant enabler for 24 percent of the fraudsters, and the 2016 survey included for the first time 31 cyber fraudsters (out of 750 profiled). It is not stated what qualifies them to be cyber-fraudsters. 44 percent of perpetrators have unlimited authority in their company and are able to override controls, and 61 percent were able to exploit weak controls: unfortunately the latter amounts to a tautology since if controls were not weak, how could they have been overridden? 66 percent of frauds were perpetrated over one to five years (72 percent in 2013) and 27 percent cost the company US$1 million or more, little changed from 2013: the corresponding figures for cyber-enabled frauds are not given. Collusion is particularly common in Latin America and Africa and the Middle East (76 percent and 74 percent respectively); In contrast, in North America and Oceania, KPMG found a disproportionately high number of fraudsters working by themselves (58 percent and 65 percent respectively). Fraudsters who collude tend to be more-senior employees and to have worked longer at the company than the solo fraudsters.

The proportion of technology-enabled frauds was lowest in Europe (18 percent) and highest in Oceania (30 percent) and North America (29 percent), followed by Africa and the Middle East (28 percent). The mechanisms are set out below (KPMG, 2016: 20).

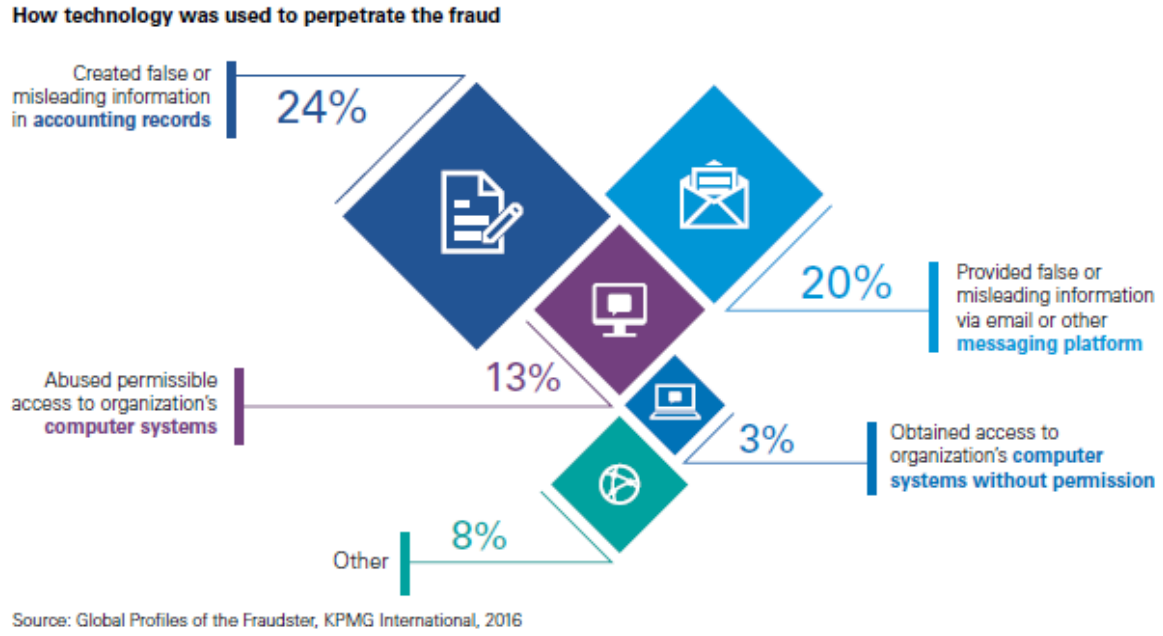


Figure 2.2. How technology was used to perpetrate the fraud

16 percent of the frauds were cyber-dependent; 8 percent cyber-enabled; and 24 percent cyber-assisted. The report notes that proactive data analytics, searching for fraud amid anomalies and suspicious business activity, accounts for only 3 percent of frauds detected. In technology-enabled frauds, the fraudster tends to be younger (60 percent are aged between 26 and 45 years old), though we note that this is still older than those examined in the NCA (2017) and Aiken et al. (2016) studies. The KPMG survey notes (2016, p.22) that "the single largest portion (13 people) consisted of employees of the victim's organization, often working with outside syndicates. Nine were associated with organized criminal groups and seven were individual criminals, hacking from outside. The main objectives of cyber fraud are the theft of

[12] This comfortably meets the criteria for 'organised crime', but may not fit the stereotypical view of mafia-type organised crime.

personal data and intellectual property, senior executives' emails, strategic access to company data, and denial of services."

Finally, though the *proportion* of cyber-enabled and other frauds they account for is unknown, many fraud and cyber-dependent crime suspects are overseas, often unreachable by mutual legal assistance (either in principle or in practice): so a rational approach to explaining criminal careers in cyber would have to take account of the backgrounds, networks and other features that make cyber-enabled fraud attractive to willing offenders, in places as varied as Brazil, China, Nigeria, Romania, Russia, Spain and Ukraine. This is compatible with the governmental (and NCA) objective of making the UK a hostile place for serious and organised criminals, a goal that often includes action abroad 'upstream' and 'downstream' of locally delivered crime, whether in interventions against drugs, fraud, modern slavery, et cetera.

It is against this background that we need to see the contribution made by the offender debriefs – which will be explored later in this report - conducted by the City of London police, with the authors' assistance in framing the questions. The debrief team selected the offenders – not apparently using involvement in cyber-enabled or cyber-dependent crime as a key selection criterion - and for legitimate reasons of protecting the offenders' identity, we have fewer details of their offences than would be ideal. Many of the interviews conducted suggest internal 'conversion' to crime, and others outside social engineering: these are discussed in detail in the next section. However with some exceptions, including insider data theft, the focus of *cyber-enabled* and certainly *cyber-dependent* economic crimes has been on external attacks against businesses and individuals and, depending on whether the motivation is excitement, political and/or financial, against government departments.

## 2.3 Leaving cybercrimes

Before we turn to these, however, it is important to consider the relative absence of information about *exiting* economic crime, especially about cyber-enabled crimes. It is not the objective of this study to review life course criminology, but much delinquency literature discusses the natural 'maturing out' of juvenile crimes as offenders grow older and develop attachments to conventional life. These typically arise in the context of Anglophone Western OECD countries rather than those countries in which concentrations of cyber-fraudsters typically are known to reside. One of the problems of comparative work often ignored by criminology is whether our models 'work' elsewhere, and we content ourselves here with the *a priori* argument that there is no reason why we should expect such a maturation out of crime in poor countries where there are few legitimate opportunities for affluence *and* no serious stigmatisation of fraud against outsiders in local cultures. Without pushing too far into an often simplistic rational choice model, 'maturation out' of cyber-enabled fraud is an open empirical question that merits investigation but on which the data are too weak even to speculate. In earlier work, Levi (2002, 2016) and Levi and Suddle (2009) were sceptical about the impact of shaming on those white-collar offenders who were not embedded in 'conventional' lives, especially those who lived Nomadic lifestyles among others who were incurious or ignorant of their backgrounds or activities. In a non-criminal context, the controversy over how much Sir Philip Green was prepared to pay to avoid commercial as well as elite and popular social opprobrium, and to retain his knighthood in the aftermath of the BHS pensions scandal illustrates this. The level of social censure or approval and its constraining effect on behaviour needs to be taken in a fine-grained way by age and social context, and we lack sufficient information about peer group reactions for many forms of cyber-dependent and cyber-enabled crime.

# 3. Methods

The researchers used two principal methods in partnership with the COLP. The first was an online survey of police officers, using Survey Monkey. The survey sought data on fraudsters the officers had recently dealt with covering the fraudsters' profile, background, motivation, methods and attitudes amongst others. This type of research is used regularly by the US-dominated but global Association of Certified Fraud Examiners (ACFE)[13] in their *Reports to the Nation*, where an annual survey of fraud examiners produces data on the frauds they deal with. The respondents for this research were drawn from the COLP police contact list (those who had signed up to receive alerts on fraud and cyber-crime), which had 841 entries, who were all sent an invitation to respond by e-mail. 126 usable responses were received from this group. Respondents were able to provide more than one response if they wished, so the actual response rate by respondent is not possible to determine. Responses came from at least (not all identified) 27 different police forces/bodies, with the largest number of responses from Cleveland, City of London Police and Derbyshire, all at 4 each. Though this generated a reasonable geographic spread, as a piece of exploratory research drawn from such a sample it is not possible to generalise these findings against all fraudsters or all fraud investigators. It does, however, represent the largest set of data on fraudsters and their frauds, drawn from the police officers who investigated them, to date in the UK. The high value and seriousness of the frauds that will be shown in this report also make it valuable. It is also nevertheless important to note the following caveats:

- The survey collated the police officers' knowledge and views of the fraudster. But they may not be in possession of all the facts and as the investigators, they are not independent observers of the fraudster's conduct in the round.
- The data represents the fraudsters the police want to talk about, and those whom they have actually pursued. Attrition in fraud cases is large and the police are known to prioritise certain frauds. The data are unlikely to be representative of fraudsters in general.

The second area of data gathering used were the de-brief reports of 16 fraudsters interviewed by City of London Police Officers in prison, using a semi-structured interview schedule developed in partnership with the authors. Interviews took place on the basis that no identifying factors could be linked to the prisoners and as a consequence, there was no data on the actual fraud they participated in, their personal details or the sentence. We note the following caveats with this method.

- The debriefs represent the fraudsters the police were able to talk to in prison. The selection is therefore biased by first, the fraudsters in prison represent those the policing agencies seek and succeed to catch and prosecute; second the study is limited to the type of fraudsters who are actually sent to prison and who happened to be there at the time of the interviews; and third, it is limited to those that are willing to be interviewed, which might represent a particular type of fraudster.

[13] See http://www.acfe.com/rttn-archive.aspx for the past reports produced.

- Second, the interviews were conducted by police officers in prisons. The officers were not those who investigated the case, but might not have been viewed as independent researchers and prisoner perceptions of them may have affected fraudsters' responses.
- Third, limitations have been noted as prisons as context for interviews with offenders by independent researchers. These criticisms have been noted to include prisoners eager to please, limited time with prisoners and an inability to record interviews (Copes and Hochstetler, 2010; and Dan and Dietz, 2008).[14]

In the absence of extensive research on fraudsters, however, despite these limitations the data offers some interesting insights on fraudsters and some promising areas which could be developed into preventative action and with further research and development.

Given the dearth of research on this crime, grounded theory was deemed an appropriate methodology for this research (Glaser & Strauss, 1967).[15] Grounded theory allows researchers to keep an open mind to newly emerging theories from the data. It is an inductive, theory discovery methodology that allows the researcher to develop theory, while at the same time, grounding the theory in data collected in empirical research. As Willig[16] (2001) has pointed out ''grounded theory involves the progressive identification and integration of categories of meaning from data. Grounded theory is both the process of category identification and integration (as method) and its product (as theory)'' (p. 33). It is a method of investigation that is based in raw data gathered systematically, usually via interview using a semi-structured schedule, and analysed by the "method of constant comparative analysis" (Glaser & Strauss, 1967, p. vii). Grounded theory allows a researcher to listen to the data without necessarily imposing preconceived ideas on the data; however, it does not mean that previous theories cannot be brought to light in the analysis (Glaser & Strauss, 1967). The questions asked derived from grounded theory, but to do this optimally more time and access would have been needed.

# 4. Findings from the debriefs and survey

The report will now examine the findings from the debriefs and survey using a number of themes.

## 4.1 Types of fraud

To protect the identity of the fraudsters interviewed in prison, the type of fraud they were engaged in was not provided to the researchers. The data, however, did suggest many of the fraudsters were investment or banking related fraudsters, which was similar to the survey. For this the respondents used an open question to write in their description of the fraud. A variety of different names were

[14] See Copes, H. and Hochstetler, A. (2010) Interviewing the Incarcerated: Pitfalls and promises. In W. Bernasco (Ed.), *Offenders on Offending*. Cullompton: Willan; and Kalof, L., Dan, A. and Dietz, T. (2008). *Essentials of social research*. Maidenhead: Open University Press. Though see for a less critical perspective, Levi, M. (2015) 'Qualitative Research on Elite Frauds, Ordinary Frauds and "Organized Crime"', in M. Miller and H. Copes (eds.) *Handbook of Qualitative Criminology*, New York: Routledge (pp.215-235).

[15] Glaser, B., & Strauss, A. (1967). The discovery of grounded theory: strategies for qualitative research, Chicago: Aldin Pub.

[16] Willig, C. (2001). Qualitative research in psychology: A practical guide to theory and method. *Buckingham: OUP*.

used and the researchers codified these and once they did, just over 20 types of fraud were identified. The most common frauds with more than 10 responses were:

- Boiler room/investment fraud = 38
- Identity fraud = 16
- Occupational fraud = 14
- Online shopping fraud = 11

The most common fraud types are listed in figure 4.1 below:


Figure 4.1. Types of fraud covered in the survey

A lack of clear classifications which are used by all, and published statistics by Action Fraud of the different types of fraud by volume and loss makes it difficult to determine to what extent these represent the totality of recorded frauds. Identity related frauds are the most common type of fraud, but after that it is more difficult to determine with the added dimension of non-reporting.[17] However, what these do broadly represent are the frauds that the police in economic crime units pursue.

## 4.2 £ Value of fraud and number of victims

Officers were asked the value of the fraud. Whether unconsciously or not, the responses are weighted towards high value frauds, with almost 2/3 of the responses valued at £250,000 or more, and over four fifths at £50,000 or more. These figures and further findings to be discussed later suggest more organised and sophisticated fraudsters in this sample.

Table 4.1. Total loss to victims

| Total Loss to Victims | Responses | Percentage |
|---|---|---|
| **Under £1000** | 1 | 0.8 |
| **£1001-£3000** | 2 | 1.6 |
| **£3001-£5000** | 2 | 1.6 |
| **£5001-£10,000** | 2 | 1.6 |

[17] ONS (2017) Crime in England and Wales: Year Ending Sept 2016. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

| | | |
|---|---|---|
| **£10,001-£50,000** | 15 | 12 |
| **£50,001-£250,000** | 23 | 18.4 |
| **£250,001-£1m** | 24 | 19.2 |
| **£1m+** | 56 | 44.8 |
| | | |
| **Total** | 125 | 100 |

The number of victims targeted by the fraudsters in the survey ranged from 1 to 1001 +. The most common group were 2-20 victims, accounting for 32.8% of the cases. If the single victim fraudsters are added, as well as the 21-50 range, these account for almost 2/3 of responses. Frauds involving 1001 or more victims were rare, only accounting for 4% of cases.

Table 4.2. Number of victims targeted by fraudsters

| **Number of Victims** | **Responses** | **Percentage** |
|---|---|---|
| **1** | 25 | 20 |
| **2-20** | 41 | 32.8 |
| **21-50** | 16 | 12.8 |
| **51-100** | 16 | 12.8 |
| **101-500** | 21 | 16.8 |
| **501-1000** | 1 | 0.8 |
| **1001+** | 5 | 4 |
| | | |
| **Total** | 125 | 100 |

The original aspirations of this project were to provide more data on the growing variety of frauds perpetrated via cyber-enabled or cyber-dependent means. The profile of the types of frauds in the survey would already suggest a dominance of cyber-enabled and assisted and more traditional means of conducting fraud. Indeed, there was only one response which could be identified as clearly a cyber-dependent fraud using malware.

The police officers were asked how the fraudsters perpetrated the frauds. They could use more than one answer. The most common tool was e-mail, accounting for 63 of the cases, followed by face-to-face at 41. Websites (other than social networking) were used in 27 cases and the postal mail was used in 20. Unfortunately we were unable to determine which combinations were in play, but other research suggests that 'pure' cyber-enabled crime without any offline interaction is not as common as popular imagery suggests.

Table 4.3. Method of perpetration

| Method of perpetration | Responses |
|---|---|
| **Face-to-face** | 41 |
| **Over the telephone (landline or mobile)** | 13 |
| **By E-mail** | 63 |
| **VoIP** | 8 |
| **Instant Messaging Programme** | 7 |
| **Social networking website** | 13 |
| **Website other than a social networking site** | 27 |
| **Postal Mail** | 20 |
| **Other** | 1 |

## 4.3 Profile of the fraudsters

Offender profiling has gained a high profile as a potential method to detect potential offenders for a variety of crimes.[18] The data gathered for this project is unlikely to offer the basis for the profiling of fraudsters for the purposes of detection. It does, however, offer some insights that deserve further research on the types of persons who have become involved in fraud and how they differ from other profiles of fraudsters and other types of criminal. There has been extensive research of varying quality on the profile of fraudsters by professional services companies and some academics, as was noted earlier in this report. These studies are predominantly about occupational fraudsters.[19] The Bussmann and Werle (2006) study identified 87% male, 71% aged 31 to 50 and the dominance of men and the middle aged is prevalent in most profiles of occupational fraudsters. Button et al's (2016) study of household insurance fraudsters, however, found near gender balance: 54% male, 46% female and only 57% in the 31-50 age category. The findings from this COLP research, however, show some similarities, but also some differences.

### 4.31 Gender of fraudsters

The sample was dominated by male fraudsters, accounting for 86.1% of the sample, with only 13.9% females.

Table 4.4. Gender of fraudsters

| Gender | Responses | Percentage |
|---|---|---|
| **Male** | 93 | 86.1 |
| **Female** | 15 | 13.9 |
| | | |
| **Total** | 108 | 100.0 |

### 4.32 Age of fraudsters

Officers identified the exact or approximate age of the offender in the survey and in doing so, some noted a range as they were not aware of the exact age. In these latter cases, the mid-point of the range was used. There was a total of 91 responses with a range from 18 to 76. The median was 40 and mean 42.1.

[18] Canter, D. (1994) Criminal Shadows: Inside the Mind of the Serial Killer. London: Harper Collins; Jackson, J. and Bekerian, D. (1997) Offender Profiling: Theory, Research and Practice. Chichester, UK: Wiley.

[19] See Bussmann, K., D. and Werle, M., M. (2006) Addressing Crime in Companies First Findings from a Global Survey of Economic Crime. *British Journal of Criminology*, 46, 1128-1144; ACFE (2016) *Report to the Nation on Occupational Fraud and Abuse*. Austin: ACFE; KPMG (2011) *Who is the Typical Fraudster*. London: KPMG. There has also been a profile of household insurance fraudsters by Button, M., Pakes, F. and Blackbourn, D. (2016) 'All Walks of Life': A Profile of Household Insurance Fraudsters in the United Kingdom. *Security Journal.* 29 (3). pp. 501-519.

Table 4.5. Age of fraudsters

| Age of Offenders | Responses | Percentage |
|---|---|---|
| **18-21** | 3 | 3.3 |
| **22-30** | 20 | 22.0 |
| **31-40** | 25 | 27.5 |
| **41-50** | 16 | 17.6 |
| **51-65** | 22 | 24.2 |
| **66+** | 5 | 5.5 |
| | | |
| **Total** | 91 | 100.0 |

## 4.33 Education of fraudsters

The police officers were also asked to state the highest level of educational achievement reached by the offender. Of 52 responses, the largest group were those that left school at 16 (36.5%). However, just over 30% were educated to at least degree level and over 60% had been educated to at least 18.

Table 4.6. Educational background of fraudsters

| Highest Level of Education | Responses | Percentage |
|---|---|---|
| **Left school at 16** | 19 | 36.5 |
| **Educated to 18** | 17 | 32.7 |
| **Educated to degree** | 15 | 28.8 |
| **Postgraduate** | 1 | 1.9 |
| **Total** | 52 | 100.0 |

## 4.34 Nationality of fraudsters

The vast majority of the fraudsters in the sample (80%) were British citizens. The other 20% included: Ghana (1), Irish (3), Iraninan (1), New Zealand (1), Indian (1), Lithuanian (1), Malaysian (1),

Nigerian (5), Pakistan (2), Romanian (3), Sri Lanka (1) and Zimbabwe (1) (1 entry Romanian and Pakistani). The debriefs included two offenders from abroad, neither of whom claimed to have come to the UK to commit crime, but that after arrival, their particular circumstances led them into crime.

Table 4.7. Nationality of fraudsters

| Nationality | Responses | Percentage |
|---|---|---|
| **British** | 82 | 80.4 |
| **Non-British** | 20 | 19.6 |
| **Total** | 102 | 100.0 |

## 4.4 'Breaking Bad': Newcomers to fraud

The profile of occupational fraudsters often shows no prior criminal involvement. Indeed the ACFE Report to the Nation notes 88.3% of fraudsters in their survey had no prior conviction or arrest.[20] The frauds covered in the survey were much wider than occupational. This survey suggested a much more significant number of the fraudsters in the survey did have prior convictions. The responses revealed a 50/50 split in the sample of those with any previous criminal convictions. Of those that did have convictions, 62% had a prior fraud related conviction. Only 14% had prior violent convictions.

Table 4.8. Any previous convictions

| Past Conviction | Responses | Percentage |
|---|---|---|
| **Yes** | 51 | 50 |
| **No** | 51 | 50 |
| **Total** | 102 | 100 |

Table 4.9. Type of previous conviction

[20] ACFE, op. cit., p 66.

| Type of Conviction | Response | Percentage |
|---|---|---|
| **Fraud** | 15 | 30 |
| **Fraud and other** | 15 | 30 |
| **Fraud and violence** | 1 | 2 |
| **Volume property** | 8 | 16 |
| **Traffic** | 3 | 6 |
| **Violent crime** | 7 | 14 |
| **Multiple** | 1 | 2 |
| **Total** | 50 | 100 |

The police officers in the survey were also asked about the social background of the offenders. Officers who responded noted that 84% came from a law abiding family background, attributing the backgrounds to be 36.8% working class, 41.4% middle class and 5.7% upper middle class (accepting that such classifications are approximate). Only 16% of offenders were thought to come from families associated with crime, with the biggest group of those (13.8% of the total) coming from families associated with petty crime. This along with several other questions later in this analysis suggests that they were mainly new entrants to crime.

Table 4.10. Social background of fraudsters

| Social Background | Responses | Percentage |
|---|---|---|
| **Comes from law abiding wc family** | 32 | 36.8 |
| **Comes from law abiding mc family** | 36 | 41.4 |
| **Comes from law abiding upper mc family** | 5 | 5.7 |
| **Comes from family associated with petty crime** | 12 | 13.8 |
| **Comes from family associated with serious crime** | 2 | 2.3 |
| **Total** | 87 | 100.0 |

The police officers were asked to identify the last known occupation of the fraudster. Occupations from all sections of the labour market were revealed, as the word diagram below illustrates.


Figure 4.2. Previous occupations of fraudsters in the survey

The occupations were also rated according to the National Occupational Coding Tool.[21] This rates occupations from 1 to 9, with the former the highest status, 9 the lowest status. Student and unemployed were also added as categories, as they are not included in the tool. The median code was 3 (classing students and unemployed as 9). The table reveals that a third of the fraudsters came from the top two occupational codes and almost half from the top three. Excluding students and the unemployed, just over 20% came from the bottom three. However, perhaps the most striking finding is that all sections of society seem to be engaged in fraud.

Table 4.11. Occupational code of fraudster's last known job

| Occupational Code | Responses | Percentage |
|---|---|---|
| **1** | 16 | 20.5 |
| **2** | 13 | 16.7 |
| **3** | 10 | 12.8 |
| **4** | 9 | 11.5 |
| **5** | 6 | 7.7 |
| **6** | 1 | 1.3 |
| **7** | 13 | 16.7 |
| **8** | 1 | 1.3 |
| **9** | 3 | 3.8 |
| **Unemployed** | 3 | 3.8 |

[21] See, http://www.neighbourhood.statistics.gov.uk/HTMLDocs/dev3/ONS_SOC_occupation_coding_tool.html . This tool is built upon the research of Hollingshead, A. (2011). Four factor index of social status. *Yale Journal of Sociology, 8*, 21-53.

| | | |
|---|---|---|
| **Student** | 3 | 3.8 |
| **Total** | 78 | 100.0 |

The first important finding from this data is that there are a substantial group of fraudsters with prior convictions, particularly involving fraud and property crime. This would seem to highlight the importance of organisations adequately vetting persons who are in positions, whether employees, contractors, clients etc where there are significant opportunities for frauds to take place. Such controls will be returned to later in this report.

On the other hand, the data also suggests a very large number of fraudsters coming from law abiding backgrounds, as well as the generally high status of their last job or at least holding a job previously. Combined with 50% with no prior convictions, it suggests an interesting group of offenders who are 'breaking bad' from non-crime backgrounds. This raises important questions about why individuals who belong to groups not traditionally associated with offending are turning to fraud. This is an issue that requires more research.

## 4.5 Motivation of fraudsters

The police officers were asked to identify the motivation of the offenders to engage in the fraud. They were able to identify more than one and below and the table illustrates that the overwhelming factor was to secure money for a materialistic lifestyle. This was identified in 94 cases and accounted for 61.8% of explanations. The next most significant answer was to secure money to pay for an addiction (drugs, gambling, sex etc), but this was only identified in 15 cases. This was followed by securing money to save at 11 and then funding other crimes and having been pressured to engage at 9.

Table 4.12. Ascribed motivations of fraudsters

| Motivation for offending | Responses |
|---|---|
| **To secure money to save** | 11 |
| **To secure money for a materialistic life** | 94 |
| **To secure money to pay for addiction (drugs, gambling, sex, etc.)** | 15 |
| **To fund other crimes** | 9 |

| | |
|---|---|
| **They were pressured to engage in the offending by friends/associates/loved ones, etc.** | 9 |
| **For the excitement** | 6 |
| **Fund terrorism** | 1 |
| **Engage in a hedonistic lifestyle** | 5 |
| **Finance business** | 1 |
| **Unknown** | 1 |

The debriefs offered some more insights in words of the reasons some of the fraudsters use to explain why they had committed fraud, echoing some of the data from the survey.

*Materialistic and hedonistic lifestyle*

Money for clothes, cars, watches. Status. **Always for pleasure**. Debrief 4.

The **only thing the person hoped to get from this was money**, in order to live & give them a better standard of life. They stated that they didn't know whether it was fun. As an alternative, the interviewee said they could have instead tried to find a job. Debrief 14.

*Depression*

I was approached and my head was turned, I was tempted. Told lots of people doing this. Not money motivated. Was the buzz. Shit time at work, clients leaving, **borderline depressed. Should have seen a shrink. Home life not going well. Not uncommon in the City**. Debrief 8.

*Narcissistic and sensation seeking*

Not money. Everything but money. Not much fun. **Doing something I shouldn't have done. Feeling untouchable, getting around a rule.** Could have done it with much more money. Debrief 8.

The interviewee said **"It was fun till I got caught"** and that when doing it they did get an adrenalin rush. Debrief 10

Their aim from the start was to make a living out of it. **They enjoyed the betting side of it and when it worked mathematically it gave them a real buzz**. They had no alternatives once into this scheme. Debrief 16.

*Financial pressure*

They had **always had financial problems and used the money they made to pay their debts** off. Debrief 10.

More research needs to be done on why such individuals become fraudsters. The strong theme that does emerge is materialistic and hedonistic lifestyles. Clearly many of the fraudsters in the survey and debriefs came from the City where such lifestyles are common, so it is not suggested that the lifestyle per se would enable them to be identified as 'deviant'. Nevertheless the findings suggests that assessing whether the person is living within their means would help to identify fraudsters sooner.

## 4.6 Length of time involved before getting caught

The survey found that in over three quarters of responses noted it took at least one year of offending before getting caught and almost half took three years.

Table 4.13. Length of time involved before getting caught

| How long before caught | Responses | Percentage |
|---|---|---|
| **Less than month** | 1 | 1.1 |
| **1 month to 6 months** | 9 | 9.8 |
| **6 months to 1 year** | 10 | 10.9 |
| **1 to 3 years** | 30 | 32.6 |
| **3 years or more** | 42 | 45.7 |
| **Total** | 92 | 100.0 |

If these findings are then juxtaposed against the most common means of getting caught, which was a victim reporting the offender – accounting for 60% of cases – this illustrates the importance of victims coming forward as early as possible to report fraud. The inclusion of individual fraud victims in the England and Wales Crime Survey, which suggests 3.6 million fraud offences, set against around 232,000 frauds recorded by Action Fraud (which also showed a small decline on the previous year) and 623,000 in total (Cifas and Financial Fraud Action UK added) illustrates the huge gap and potential for more frauds to be reported (and plausibly to do so earlier), even if the logistics of police

resources in times of austerity constrain turning many more of these reports into early arrests (ONS, 2017).[22]

These findings suggest the importance of more efforts, particularly high profile campaigns to encourage victims to report frauds as early as possible. This could possibly lead to fraudsters being identified, disrupted and detected earlier. This, however, must be balanced against giving those victims who do come forward unrealistic expectations that their individual case will be successfully investigated through to prosecution. There is a tension between overloading the system with reports and maximising the data that enable intelligent prioritisation decisions to be made.

Table 4.14. Getting caught

| Getting Caught | Responses | Percentage |
|---|---|---|
| **CHIS** | 3 | 3.5 |
| **Audit** | 2 | 2.4 |
| **Company Insolvency** | 2 | 2.4 |
| **Investigation** | 9 | 10.6 |
| **Other crime investigation** | 3 | 3.5 |
| **Other agency referral** | 2 | 2.4 |
| **Safeguarding referral** | 2 | 2.4 |
| **Whistleblower** | 1 | 1.2 |
| **Victim report** | 51 | 60.0 |
| **SARS** | 10 | 11.8 |
| | | |
| **Total** | 85 | 100.0 |

## 4.7 Co-offending and organised crime

Co-offending has been under-researched by criminologists, outside the arena of organised and networked crime (ONS, 2017).[23] The findings from the survey and the debriefs, however, suggest

[22] ONS (2017) op. cit.

extensive co-offending and the involvement of organised crime groups. Almost three quarters of survey responses involved two or more offenders and only a quarter a lone fraudster. Almost half involved teams of 3 to 10 offenders and 13.8% involved 11 or more.

Table 4.15. Total Number of Offenders Involved

| Total Number of Offenders | | Percentage |
|---|---|---|
| **1** | 32 | 26.0 |
| **2** | 17 | 13.8 |
| **3 to 5** | 29 | 23.6 |
| **6 to 10** | 28 | 22.8 |
| **11+** | 17 | 13.8 |
| **Total** | 123 | 100.0 |

The extent of co-offending was further illustrated with the finding 57% of respondents considered the fraudster to be part of an organised crime group. These findings support recent research by the Police Foundation which found between 31% to 45% of frauds occurring locally were linked to an organised crime group (Perpetuity Research and Police Foundation, 2016).[24]

Table 4.16. Part of organised crime group

| Part of Organised Crime Group | Responses | Percentage |
|---|---|---|
| **Yes** | 55 | 57.3 |
| **No** | 41 | 42.7 |

The debriefs suggested a mix of coercion, trickery, incentives and wider social networks as the means other criminals enticed the interviewees into fraud. Some of the quotes from the debriefs illustrate this, though the authors are not in a position to test the claims, all of which involve mitigating their own culpability.

[23] Van Mastrigt, S. and Farrington, D. (2009). Co-offending, age, gender and crime type: Implications for criminal justice policy. *British Journal of Criminology, 49*(4), 552-573.

[24] Perpetuity Research and Police Foundation (2016) *Organised Fraud in Local Communities*. London: Police Foundation.

*Coercion*

They operated a legitimate company when **a business partner put a large sum of money into the business bank account.** When the **interviewee questioned this, they were told the money was from a notorious crime family and they wanted a 10% return.** The interviewee paid this from their own money and told the partner to tell them they didn't want any more involvement. Unfortunately the money kept on appearing and under duress the interviewee set up a Ponzi scheme as they felt this was the only way they could keep paying the money and protect their family. They knew it was a serious crime and would be viewed as such but felt they had no alternative. **Quote "100% knew it was wrong and serious. Either got caught by paying money or killed. Threats to family made me do it."** Debrief 3.

*Trickery*

The interviewee did not believe they were getting involved in a scam and **thought they were investing in a genuine business.** They had never been in trouble before this offence. They had a successful company and had been making a good living before they got involved with this one. They were approached by a friend who asked for investment into his business and produced paperwork and documents to support the claim that it was a good company. **They made an investment and had been seeing returns for over 4 years before becoming aware it was a fraudulent scheme.** Debrief 9.

*Incentives*

The interviewee had been employed in their industry for over 12 years and had moved onto a different shift. It was at this point they were told about the 'scam' and how easy it was and that everyone else was involved. **They became involved and did so because they saw it as easy money.** Yes they believed other people would view it as a serious crime. Debrief 10.

*Social Networks*

**I was surrounded by them. Don't think anything would stop the people I knew.** They are still doing it so it hasn't put them off! Debrief 5.

The police, fraud policing agencies and the National Fraud Intelligence Bureau already do extensive analysis of known or suspected fraudsters using network analysis. These findings if typical of fraud highlight extensive co-offending and the involvement of organised crime networks. These point to the importance of these and other relevant bodies continuing to invest in staff and tools which enable network analysis to be conducted.

## 4.8 Sentencing and the aftermath of conviction

In the survey the most common sentence for the fraudsters was one to five years imprisonment accounting for 25 cases, followed by five years or more at 20 cases. In 2004 Levi (2010)[25] found the average length of a custodial sentence for fraud cases tried in a Magistrates' courts was 3 months, for more serious cases of fraud tried in the Crown Courts, the average sentence was 15.4 months. For cases involving conspiracy to defraud the length was 25.6 months, for those in excess of £1m, and investigated by the SFO, between 2000-2005 the average sentences were 31.7 months, with the

[25] Levi, M. (2010). Hitting the suite spot: sentencing frauds. *Journal of Financial Crime*, *17*(1), 116-132.

most severe sentences being 4-5 years. None of the responses to the survey indicated they were from the SFO (although some did not declare which policing body they were from). The sentencing profile could suggest two key findings. First that the average sentencing for fraud cases involving conspiracy and large sums of money has increased since 2004. Second, that the sample of responses is focused at the much more serious end of fraud cases. There were also some cases where the police officer indicated the case was not complete yet or the sentence was unknown.

Table 4.17. Sentence of fraudsters in the survey

| Sentence | Responses |
|---|---|
| **Custody more than five years** | 20 |
| **Custody one to five years** | 25 |
| **Custody under one year** | 1 |
| **Suspended** | 6 |
| **Community order/fine** | 2 |

In terms of loss of assets, 15 responses indicated the offender lost assets, 25 indicated no and 38 noted this was still pending. All the fraudsters in the debriefs had experienced prison. The outlined mixed views: some were surprised to be sent to jail or by the severity of their sentence.

> **Much too long.** Really unfair for my part in the fraud. The bigger guys never got caught. Confiscation is still ongoing. Debrief 4.
>
> When asked this they said "How can it be a fair sentence? For losing my own money? I put more in than I took out." They also couldn't understand how others involved got off completely or got lesser sentences. **They don't think prison will have any effect on their future and will get some form of work on leaving.** The confiscation hearings are still on-going but they stated they have lost everything already so what can they do. Debrief 10.
>
> In response to this question the reply was **"I got a big sentence for a small fraud. I'm in prison for nothing".** Others who were more involved didn't get caught which they felt was unfairly reflected on them in sentencing. On release from prison the interviewee intends on returning to their country of origin and is unsure what effect this sentence will have on them. As for confiscation they are still going through the process and said no one was listening to them in regards the money they made from the fraud. Debrief 13.

One prisoner did indicate they got less than what they had been briefed to expect.

> Once charged the indication from the solicitor was to **expect 7 years and in the end they got less than that**. Debrief 16.

Several of the prisoners interviewed pointed towards the ineffectiveness of prison.

> Before prison they didn't know any other criminals. They felt that the problem with being inside prison is **you meet other people with skills that can be used and you have plenty of time when you can plan and think. It's a University of crime!** Debrief 2.

> The interviewee admits they did wrong but feels **locking him up is not the best way to punish him. He has other skills that could be used to pay his debt to society** back and this would save the cost of keeping him inside. Debrief 16.

Some of the fraudsters expressed frustrations surrounding confiscation.

> They went onto explain that **confiscation could be better when selling goods for example an item worth thousands of pounds is only sold for hundreds**. They feel more research is required when selling goods and essentially list items correctly for better returns on confiscation. Debrief 11.

> Although they have the offer of work on leaving prison he feels opportunities will be limited because of being inside. Along with the sentence they have also **had a POCA put on them for a substantial amount which will be with them for a number of years. They understand the principal behind POCA but felt in a lot of cases all the moving around of prisoners and court time outweighs the returns.** When asked if they knew all this before the crime would they have done anything different the short answer was "Wouldn't have done it". Debrief 16.

> Got an £100,000 benefit on my **Confiscation. Had to pay £500. Not sure how I feel about that**. Default sentence is really scary and people need to know about that. **Bank was frozen. Confiscation is serious**. Debrief 16.

One of the most significant impacts noted by the fraudsters was the media coverage of them and the impact upon their relationships, their family and friends. This seemed to be the most significant impact upon the fraudsters taking part in the debriefs noted, although not all received coverage nor was it an issue for some. The researchers did not know who the offenders were and therefore it was not possible to view the coverage they received and come to any judgement on that. Levi (2006)[26] has noted the interest of the media in a certain genre of fraud cases that have the potential to pursue sensational coverage, noting the concept of 'infotainment'. Negative media coverage has also been noted in a small number of studies of offenders, including white collar offenders.[27] The

[26] Levi, M. (2006). The media construction of financial white-collar crimes. *British Journal of Criminology*, *46*(6), 1037-1057.

[27] There is a body of American research led by Benson which has identified the negative impact of the media on white collar criminals, see Benson, M. (1990). Emotions and adjudication: Status degradation among white-collar criminals. *Justice Quarterly*, 7, 515-528; Benson, M. (1984). The Fall from Grace. *Criminology*, 22, 573-593; Benson, M. and Cullen, F. (1988). The special sensitivity of white collar-offenders to prison: A critique and research agenda. *Journal of Criminal Justice*, 16, 207–215. In the UK, Condry has noted the impact of media

observations below do offer insights for more research as well as some areas policing bodies could build upon to develop some preventative and deterrence tools.

The debriefs noted a number of different themes in this negative coverage. This first debrief illustrates the offender never thought about the potential coverage and it was the hardest thing they had had to deal with. They also reflected that if they had known what coverage was likely it might have deterred them, something prison wouldn't do.

> **Had they known then the reputational damage that would be caused by the press that would have helped deter them.** Once the interviewee had committed themselves they couldn't turn back. 6 months into it they started to Google potential punishments but don't feel that the prison sentence acted as a deterrent to them. They think for white collar criminals community service, tags or some form of work would be better alternative but having said that if someone spent few months in certain prisons would be enough to put you off!... When the interviewee was asked this question they said the **media reporting was probably the hardest thing and if it was just prison that would have been ok.** It was **all sensationalised by the press and the spin the investigating agency** put on it. They said when you know truth and read articles it makes you sick and causes stress. When they moved prisons the new inmates somehow found out about them and suddenly befriended them. **Their partners' family attitude towards them changed after seeing articles** which has proved difficult. They are considering changing their name because it's so difficult to get away from the internet and press articles. It has also had a negative effect on their child's mother's relationship with them. Debrief 2.

Debrief 15 also noted if they had known the coverage they would have received they would have thought again about getting involved.

> **Media destroyed us. Saying a lot of lies.** Blame on me and my co-defendant. **I felt embarrassed, humiliated. If I had known it would be on the news I wouldn't have got involved.** Good friends won't treat you differently. Being portrayed as a different character was really distressing. The media had their fun. Because of my race and culture they tried and accused us of terrorist finance which wasn't the case. For family to see this was gutting. On the internet so always there. Debrief 15.

Several of the debriefs illustrated the fraudsters felt they secured negative and unfair media coverage with implications for them and their family.

> The interviewee answered this by stating 'Who ever believes the media'. The person's objection was they thought that what **the media portrayed them as must have come from**

---

coverage of the families of serious offenders Condry, R. (2007). *Families Shamed: The Consequences of Crime for Relatives of Serious Offenders*. Cullompton: Willan; and Robbers has noted similar impacts on sex offenders? Robbers, M. L. (2009). Lifers on the Outside Sex Offenders and Disintegrative Shaming. *International Journal of Offender Therapy and Comparative Criminology*, *53*(1), 5-28.

> **the Police.** They also stated that they were portrayed as preying on certain types of people, which wasn't correct. Debrief 5.
>
> The interviewee stated they **don't think they've read one accurate press report on their case** & that there was no press in court for the sentencing. It made headline news & was on social media before they were even charged. Very little of it has been reported correctly. Debrief 6.
>
> The interviewee explained that now they have been inside prison the media have a blinkered view of any crime including many fraud cases. They stated that the media are not interested in truth because their job is to sell newspapers/stories. They commented that a small article came out in national press about them and they felt embarrassed. **The interviewee said the quote in paper was incorrect about the purchase of high end goods.** They explained they was referring to a friend who had purchased items and not them self. They said the context was incorrect. That the journalist was selective by changing the story and giving the impression it was them that had the expensive items when not correct. The interviewee said they created what they wanted. Debrief 11.

The worst impact was noted in debrief 16 where the offender's family had to move house, posters were displayed of him in the village and his wife was physically attacked.

> The interviewee said the **local newspaper ran a number of stories on his case and made him and his family out to be the worst people in town who went around fleecing people.** He was approached by this paper to give his side of the story but turned them down. The **articles and the fact most victims lived in the area, meant they had to relocate** but the **papers found out this new address and printed it.** As a result **his wife was physically attacked and posters of him were displayed around the new area warning people about him.** Longer term he felt it will always be a problem for him to return his home town as people don't forget. Debrief 16.

The issue of the modern internet and Google searches and the implications this has for the offender in their rebuilding their life and career was also raised.

> **Some friends shunned me who read things in the paper. Now on the internet so can't get rid of it.** My wife always searchable on the internet. Since, people have spoken to the media but regretted it. Debrief 8.

Some organisations have actively sought to publicise convicted fraudsters as part of their strategy to develop an anti-fraud culture and deter future offenders.[28] There has been limited assessment of the impact of such strategies, although the success of the media in promoting police activity has been noted in some areas to have success.[29] There would therefore seem to be some potential in

[28] The NHS Counter Fraud Service has sought to develop an 'anti-fraud culture' which has involved publishing the conviction of fraudsters, see NHS CFSMS (2001) *Countering Fraud in the NHS.* London: NHS.

[29] See Laycock, G. (1991) Operation Identification or the Power of Publicity. *Security Journal*, 2: 67-71 and Bowers, K. and Johnson, S. (2005) Using Publicity for Preventative Purposes. In, Tilley, N. (ed) *Handbook of Crime Prevention and Community Safety*. Cullompton: Willan.

publicising as part of broader deterrence strategies that convicted fraudsters are likely to face negative media coverage which may have a lasting impact upon them and their families. Secondly there may also be the potential to develop case studies of willing convicted offenders to discuss and illustrate the media coverage they received and the impact it has had upon them.

## 4.9 Attitude to victims

The survey and debrief did also raise some interesting findings regarding the victims. The survey and the debriefs suggested little regard for the victims of their crime, with just over 90% noting this in the survey who responded. There were only 2 responses where the offender was seen to have genuine remorse. This might be viewed as too cynical, but it is confirmed by other research undertaken by the authors.

Table 4.18. Offenders' attitude towards the victims

| Attitude to victim | Responses | Percentage |
|---|---|---|
| **Various no regard for the victim** | 77 | 90.6 |
| **They deserved it** | 5 | 5.9 |
| **Remorse** | 2 | 2.4 |
| **Didn't believe done anything wrong** | 1 | 1.2 |
| | | |
| **Total** | 85 | 100.0 |

The debriefs presented a slightly different picture, although would be likely to be the case, as it would be unlikely for a prisoner in prison talking to a police officer to portray a clear disregard for the victims. There were some, however, who were clearly neutralising[30] the harm they had inflicted.

> *Denial of Injury*
> Not really. **They were all corporate or people with millions in the bank.** I only took a little. I would never target little old ladies. That's wrong. Debrief 4.

> The interviewee said they **didn't think about victims because they didn't know there were any.** The interviewee **doesn't believe it would help them or the victims to meet**. They stated that they wouldn't have wanted any of them to lose their life savings. Debrief 11.

[30] See Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.for the classic description of such techniques.

The interviewee said this has always been emotive & they feel for these people. They said **that the victims took independent advice and although the victims had 100% financial security,** the interviewee realises this doesn't cover their emotional distress. They had offered to face the public & give presentations on what had happened. Debrief 6.

*Denial of victim*

In his own words when asked this question the reply was "I put plenty of people off. **One lady I knew kept asking when I would take her money. I Kept saying no because in the back of my mind I knew I was in the shit." Nothing would have put them off doing this and they kept going until there was no money left.** They knew at this point they would be going to prison and even told his wife to leave him to distance herself from him and the problems. Debrief 16.

Some of the debriefs did illustrate remorse and for some meeting the victims was something they would like to do or would consider, although some clearly noted they would not want to do this.

The interviewee said **they do think about the victims because of what they have gone through and no they didn't deserve it.** The financial loss most of them could cope with but they felt the breach of trust would probably be harder for them. The fact that they were lied to will probably make them question everything now.
They were under no illusions that as they intend returning home after their sentence they may come across some of the victims and they are not looking forward to this. They understand that some of the **victims may need to express anger or views and this may need to happen. They would be happy to do it in a controlled environment**. Debrief 2.

Victims-I knew them all personally. Always thought about them when trading. I was always honest when trading. Fully aware of risks involved. Victims believed in me. They could only talk to the Police which put a slant on it. **Hard time because wanted to explain to my victims.** Was a period of divide but later it became ok. Most I have written to and they have written to me. Most have their money back. No animosity either way. Debrief 12.

The **interviewee said they thought about the victims and would like to apologise for their actions.** What they found hard to understand was why anyone would believe the scam to be real. They didn't really answer about meeting them but did say if they had the money they would give it back. Debrief 13.

Victims-at the time didn't think they were losing a lot. They wouldn't give me the money from their own bank, I couldn't believe it. Not deserved it at all. **Meeting the victims? My victims hate my guts. I would want forgiveness. I have written to one of my victims already as she lost her husband recently. I would sit with her and let her get something off her chest.** All she hears is the stuff in the media. I could tell her the real story. Clear things up. Massive opportunity for me. Others are more selfish. Tell her I've made a mistake I wouldn't have done it had I known. Clear my conscience. Hard to let go of the past and this would help. Debrief 15.

There has been growing interest in and use of restorative justice in recent years with evidence of the positive impact such approaches can have (Shapland et al 2008a and b).[31] There has been very little use of restorative justice for fraud related cases[32], although it has been suggested as a tool which could be very useful for fraud cases where offenders often have little direct contact with their victims and are much more able to neutralise the harms done (Button et al 2015).[33] The findings from this study would seem to suggest that further experimentation with restorative justice for certain fraud offences would be worth pursuing, along with proper evaluation of its impact. Where negative attitudes to victims are socially embedded and offenders appear to have little commitment to prosocial values, this might be challenging to put into effect.

## 4.10 Lessons to protect against future frauds?

The survey and the debriefs secured a variety of ideas on how organisations could better protect themselves to reduce the risk of frauds occurring. The discussion so far in this report has also alluded to a variety of measures which could be used or at least show some promise. The survey noted a variety of responses from the police officers which essentially could be grouped under better controls or organisational resilience. These were frauds where organisations systems had failed in some way or the counter fraud capability within the organisation was not robust enough. Figure 4.3 presents some of the responses from police which could be identified as better control or resilience to fraud that organisations involved in the fraud could have undertaken to prevent it.

| |
|---|
| Business could have had better security checks in place. |
| Better Audit Procedures within the Organisation. |
| More rigorous action by banks to ensure multiple accounts aren't set up (further vetting, KYC). |
| Further work by eBay and other online auction sites to protect users. Further education of users in relation to transferring money to accounts from their own bank accounts. |
| Fraud based around providing false information to secure vehicle hire agreements. The due diligence checks by the car dealerships and finance companies is very poor. |
| Better internal processes to prevent one person being able to sign off invoices. |
| Previously a director of a land investment company that was closed down by the High Court with debts of £6m. I feel this should have been dealt with as a criminal investigation. |

[31] See, Shapland J, Atkinson A, Atkinson, H, Dignan J, Edwards L, Hibbert, J, Howes, M, Johnstone, J, Robinson G and Sorsby, A (2008a) *Does Restorative Justice Affect Reconviction? The Fourth Report From The Evaluation Of Three Schemes*. London: Ministry of Justice; Shapland J, Atkinson, A Atkinson, H, Chapman, B Dignan J Howes M Johnstone J Robinson G and Sorsby, A (2008b) *Restorative Justice: The Views Of Victims And Offenders The Third Report From The Evaluation Of Three Schemes*. London: Ministry of Justice.

[32] The City of London Police have experimented with it for cash-for-crash insurance fraud cases with some promise. See Gill, M. and Howell, M. (2017) *An evaluation of a restorative justice trial: where the victims are businesses and the offenders are insurance fraudsters.* Tunbridge Wells: Perpetuity Research and Consultancy International.

[33] Button, M., McNaughton-Nicholls, C., Kerr, J. and Owen, R. (2015) Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *Howard Journal of Criminal Justice,* 54: 193-211.

More rigorous KYC by lenders, better processes within Land Registry.

The banks could have conducted proper checks. This suspect opened an account at an address he did not live at, using fake address documents. He had only been in the UK a few weeks, and had no credit presence here. Clearly a mule account.

Better examination by mortgage providers of applications e.g. verification of genuine companies, examination of bank account statements, liaison with other banks etc.

Better AML checks with banks.

Check email headers, call suppliers to query invoice.

Proper accounting practice at the victim organisation.

Greater scrutiny and management of the offender by the victim's audit function and relationship managers.

Complete lack of LEA coordination in investigating investment fraud. This defendant was initially involved in the miss-selling of wine as investments which were not investigated or taken seriously by LEA's and then allowed to progress on to more overt misrepresentations. Insufficient resources are placed on fraud investigation.

Better examination by mortgage providers of applications e.g. verification of genuine companies, examination of bank account statements, liaison with other banks etc.

The companies affected carried out no due diligence, they only realised they'd been defrauded once the police contacted. They did all dealing by phone/email and had no idea who they were dealing with.

The banking sector could be more robust and make better use of the whistleblowing and debriefing process. Crime could of been uncovered long before it was.

Banking protocols should be vastly improved in respect of staff training, probing questions as this would identify potential criminals intending to open bank accounts. The criminals when an account is opened and are given notice to close by the bank still have a period of time before closure and therefore launder more money. The money launderers expect an account to only be open for a month and therefore are well versed in abusing the account moving millions. In addition debriefing offenders to ascertain tactics that can be shared so others can target harden their processes or attitudes as the money launderers are very eloquent when they talk to bank employees and sucker them in or entice/bribe them.

More internal checks and controls within the practice.

Better monitoring of spending patterns, with automatic suspensions of the transactions prior to confirmation from the account holder by other means.

Bank / Gambling company could have recognised high value gambling pattern from his expenditure

and reported to NCA.

Better checks of monies being transferred on internal computer systems.

Figure 4.3. Police responses identifying how controls and resilience in organisations could be enhanced

All the suggestions made by police officers point to measures which could be used to enhance the resilience of organisations in fraud. They amount to some of the traditional situational crime prevention measures discussed at the start of this report. The protect part of the strategy to deal with economic crime could be enhanced with more advice and guidance to organisations on how to develop measures and controls which enhance organisational resilience to fraud.

There were also a number of responses which highlighted the need to raise awareness of potential frauds amongst victims. Some of these are identified in figure 4.4 below.

More public awareness adverts on TV.

Complete their own due diligence checks prior to investing their funds into a fictitious investment scheme.

More prevent / awareness info to public but even so some would have continued to give money. Basic computer searching or research on clearly unrealistic investment opportunities. Wider reaching FCA warnings rather than just on their website.

Figure 4.4. Police responses identifying means for raising victim awareness of frauds

There were a variety of responses linked to banking and probate which called for better regulation and better control of payment transfers as a means to reduce the risk of fraud.

*Probate*

The business of probate research and inheritance is completely unregulated and lends itself to abuse by those of a mind to take advantage. Regulatory body needed to be instigated by Gov't.

Regulation of non-solicitor organisations carrying out probate work.

*Banking*

More robust legislation in respect of the management of companies and companies handling customers money in particular. Although the company had to be registered with the FCA (FSA as was) they conducted no enquiries into how this company was run. Within the foreign exchange industry questions were asked about how this company could operate with the rates offered. The company had turnover of over £200 million p.a. and yet their accounts did not require auditing. The accounts to

Companies House were false.

Tighter bank regulation would have assisted in preventing the frauds from being perpetrated initially, thereby removing the need for a launderer.

Regulation of unregulated 'investment' companies. Increased liability for FCA regulated money transfer companies (and solicitor client accounts)which provide escrow client accounts for boiler room companies. Increased investment in law enforcement with a new policy of sending law enforcement 'crime prevention' teams into boiler rooms as soon as one is identified - to ascertain who stands behind it, and to close down the company as quickly as possible where appropriate and remove its website.

*Payment transfer reforms*

Banking institutions question overseas payment over £10,000.

Better banking processes to prevent large transfers being made immediately.

Prevent faster payments to bank accounts outside of the UK and have a system of non clearance of funds (like cheques)..... Not that anyone will want to do that.

Figure 4.5. Police responses identifying areas which need better regulation to reduce fraud

Finally there were a mix of responses which pointed to better co-ordination between agencies, publicising the harm fraud does to victims, earlier reporting of frauds, better controls of offenders and more help for those with addictions.

*Better co-ordination*

HMRC had investigated the matter back in 2013 whilst the majority of the monies were still in UK bank accounts. Their failure to take any positive action or report the matter to more appropriate authorities has seen those funds lost outside the jurisdiction of the UK and further victims made.

This is a large scale fraud and, following the disruption of this small group, it is evident that this boiler room is still ongoing. Other similar bank accounts, which were outside of our scope of investigation, are still being used to receive victims money. This is a multi million pound fraud across many police forces, but each force is only looking at one small aspect and not the centre - and this is a major fault of the police services and NCA.

Closer ties between the Police and VOSA.

*Publicising harm done to victims by fraud*

Education around the harm caused to victim's by this type of crime.

*Earlier reporting by victims*

The banks could have reported it early. He has clearly been involved in this for a long time.

*Better controls of offenders*

My fraud committed whilst on bail for previous land banking fraud. Should have been locked up

A serious crime prevention order or financial reporting order should have been placed on him the last time he was sentenced.

*Help for addictions*

As it was due to an addiction no. He would only have got help if he asked for it.

*Better assessment by Companies House of prospective directors*

Had companies house carried out some checks in relation to his previous business and the reasons they were struck off. The address is used for more than one business but appears to be a dwelling.

Figure 4.6. Other ideas from the survey to better protect against fraud

The economic and social cost-effectiveness of these recommendations is outside our brief and means, but we report these views of reflective practitioners, to go alongside broader studies of fraud and cybercrime prevention, which have become more extensive in recent years.

## 4.11 Changes in methodologies

The data collected in this study have not yielded as much insight as we hoped into changing criminal methodologies, as direct access to offenders' judgments and police intelligence about the evolution of their exploitation of crime opportunities was unavailable. However, we can make some comments about trends.

Complete time series of trends in all economic crime offences cannot be reconstructed. However, on-line frauds have risen over time, except for those affected by the introduction of Chip and PIN onto payment card transactions, which have fallen significantly in the UK and elsewhere, despite being displaced somewhat to the US where Chip and PIN have only recently and gradually been implemented (ECB, 2015; FFA UK, 2016a). These technological changes have reduced ICT-enabled frauds, namely 'skimming' - the widespread copying of magnetic stripe data onto blank or other payment cards. Thus now, remote purchase frauds constitute 70% of all bank payment card fraud – almost doubling since 2011 to £398.2 million in 2015, with a further 7% of payment card fraud being identity frauds; remote banking fraud has more than doubled since 2011, now totalling £168.6 million (FFAUK, 2016b). Online and offline crimes should not be treated as two totally separate categories: combined email and telephone-based social engineering methods have become very common in inducing people to transfer funds to fraudsters, sometimes inducing victims to deliver large sums in cash to couriers who call at their homes.[34] We do know that there are some offenders

[34] This has been the subject of several radio consumer programmes and City of London police warnings. To include the telephone in an aggregated count of ICT may be unhelpful: the fraudsters may have used VOIP (Voice Over Internet Protocol) to reduce criminal running costs and traceability. But it is harder to disguise sex, age and ethnicity if there is human communication compared with email and text.

who make it their business to corrupt insiders in banks and in the police to reduce the effectiveness of controls, and at least some 'professional enablers' who, despite the extension of anti-money laundering controls, offer services to assist in establishing offshore and onshore companies with disguised ownership. Whether there are more such people today than in the past is too difficult to determine objectively, but our awareness of them is greater. Likewise, the availability of exploitation kits for use in malware and computer extortion has become significantly easier over time, reducing the barriers for entry. But if it was extremely easy, we would have expected an even greater incidence of cyber-dependent and cyber-enabled crime than has actually occurred, so plainly many 'street kids' as well as middle class kids with a taste for experiment do not avail themselves of what objectively are opportunities.

In what ways is online transformative for levels and organisation of crime or for the balance between disruption and detection, investigation and prosecution processes in criminal justice responses? Even when economic crimes were mostly or (in the 1970s) entirely offline, we knew very little about their cost, incidence and prevalence, or about how effective policing methods were. Measuring the impact of ICT on volume frauds should not be mistaken for measures of the influence of ICT on management frauds such as some of those committed by offenders in this study, or on more general corporate crime. Whatever data we are using, our societies and law enforcement agencies need to face up to significant challenges in how to respond to the flood of cases about which – even in the comparatively well-resourced US – very little reactive enforcement follow up normally happens. This includes responding to the crimes, promoting cyberfraud prevention and resilience, and more general 'reassurance policing'.

## 5. Law enforcement responses to cyber-enabled economic crimes: some comments

The majority of cyberfrauds are high-volume, low value with low levels of recovery, usually targeted at individuals. Does a response require after the fact investigation and/or a technical-led investigative capability? Should the emphasis be on awareness and education and how should any response balance volume, loss, harm, perpetrator or deterrence as the main drivers of any response. Such a response should also take into account the empirically tested effectiveness of individual and national level reduction mechanisms.

Any response has to take account of a landscape that changes dramatically as networked technologies transform the way that fraud could be organised, as cybercrime has become more professional, harder to identify and/or recognise and in a context where our digital forensic capability is very restricted? The police struggle to meet an expectation of protection from the public, due not just to resources and skills but to a perceived lack of actionable intelligence on emerging cyber threats. The ease and cheapness of digital harm mechanisms will continue to grow the pool of both potential victims and criminal actors. Easier access means a greater proportion of users than previously may be unfamiliar with technologies, making them 'easy targets' both as intermediaries for (e.g. botnets, money mules) and as victims of fraud. Strategic planners need to consider what it would take to produce a much higher (or lower) cyberfraud rate.

There may be a symbolic need for law enforcement to show particular criminal networks and individuals that involvement in crime has its costs, even if – as has been shown in the rapid revival of

alternative drug and identity data cryptomarkets following take downs such as DarkMarket, Silk Road and Onymous (see Décary-Hétu and Giommoni, 2017 and Dupont, 2017) – the impact on crime and precursor availability is modest. We need to carefully consider who and where our target audience for disruption, Prevent activities and Prepare are: and what does good 'reassurance policing' look like in this context? The technical knowledge from investigations and inter-country cooperation are essential inputs into organisations in both public and private sectors to ensure their in-house capacity is informed with credible awareness and alert campaigns. If part of the police reaction is to be intelligence -led and proactive, how is this to be achieved? What kinds of fresh and existing sources can be deployed to get a better and quicker picture of offending and offender networking than exist at the present?

Everyone is agreed that we cannot prosecute our way out of either online or offline fraud. So what symbolic messages are important and can we find a rational way of directing them? The evidence is not clear yet on these points. However if we review specifically targeted significant awareness and prevention campaigns ('Protect' and 'Prepare') that aim to encourage new and bolster existing individual level security behaviours, some of which have been shown to be effective in reducing cybercriminal victimisation (Williams 2016). Even once messages are disseminated, on radio, television, the press, and via friends and families, however, there are always some that do not follow the advice or who wrongly interpret the message and engage in economically damaging avoidance behaviours, and consideration may have to be given to automated security with opt-out rather than opt-in requirements (for example, for on-line banking), especially if insecurity can cause problems for others, like botnets.

Here we suggest more attention to the effectiveness of individual level security behaviours, and behavioural studies on mechanisms of security adoption. There is a need to develop 'teachable moments' to nudge people to take action to protect themselves and make better informed judgments about their own risky conduct.
There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, including the identification of and support for organisations and media sources that have an established engagement with individuals who may thus be more predisposed to listen. Similarly, there is a role for law enforcement or other approved bodies to set up educational 'mock operations' to warn users who respond to fraudulent offers of different kinds (created by the authorities) that they could have become victims of fraud, via on-screen 'pop ups' (such tactics could also be used on criminal marketplaces as warnings to those seeking illicit products or co-offenders on the web.) This may have particular resonance for repeat victims.

For public reassurance and for deterrence/incapacitation, some police action is needed and more up-skilling for existing officers – or employing specialist civilian staff - is necessary. Some 5,000 police have been given a modest amount of training via the College of Policing, and this is a beginning. Our suggested next steps for this include the need for better, early education of risk management and a focus on helping vulnerable citizens to appreciate and manage the risks of both online and offline fraud, and this may be better done via peers and the third sector than by the police and websites alone, however user-friendly.

# 6. Conclusion and recommendations

Using the small base of available literature, a survey of police officers who have dealt with serious fraudsters and the debriefs of fraudsters undertaken by police officers from the City of London Police, this report has explored the pathways, profiles and some of the methodologies used by fraudsters. The nature of the research undertaken precludes definitive conclusions on what will work in preventing, protecting and pursuing those engaged in economic crime more effectively. However, the findings do suggest a number of promising areas – some of which are by no means new – which the law enforcement and wider counter fraud community might wish to develop further.

*Contributing to the pursue strategy*

These findings suggest the importance of more efforts to encourage victims to report frauds as early as possible. This could possibly lead to fraudsters being identified, disrupted and detected earlier. This, however, must be balanced against giving victims, who do come forward, too much expectation that their case will be successfully investigated through to prosecution. This could be achieved in a number of ways but principally by better funded and targeted campaigns encouraging victims to come forward. It is nevertheless an issue which requires further detailed consideration if larger numbers of reports overload the systems and lead to very disappointed victims at the lack of progress with their case.

The extent of organised crime groups and co-offending serve to highlight the importance of the police and other relevant bodies – including those in the private sector - continuing to invest in staff and tools which enable network analysis to be conducted to detect those involved in economic crime earlier.

Further experimentation with restorative justice for certain fraud offences would be worth pursuing, though these would require rigorous evaluation.

*Contributing to the prevent strategy*

There would seem to be some potential in publicising as part of broader deterrence strategies that convicted fraudsters are likely to face negative media coverage which may have a lasting impact upon them and their families. Secondly there may also be the potential to develop case studies of willing convicted offenders to discuss and illustrate the media coverage they received and the impact it has had upon them.

*Contributing to the protect strategy*

The research revealed many frauds are the result of simple opportunities and failures in systems within organisations. The protect part of the strategy to deal with economic crime could be enhanced with more advice and guidance to organisations on how to develop measures and controls which enhance organisational resilience to fraud and reduce gaps and opportunities in systems to prevent fraud. The development of better advice and guidance which is widely disseminated could be undertaken by a wide range of potential tools within and beyond the police (standards, websites and other literature, trained persons offering advice and testing systems etc).

Two areas that deserve particular mention in protecting organisations are:

- Ensuring organisations adequately vet persons, whether employees, contractors, clients etc who are likely to be in positions where there are significant opportunities for fraud.
- Monitoring the lifestyle of persons in positions where there are significant opportunities for fraud.

# References


ACFE (2016) *Report to the Nation on Occupational Fraud and Abuse*. Austin: ACFE.

Aiken, M., Davidson, R. and Amman, P. (2016) *Youth Pathways into Cybercrime*. London: Paladin Group.

Benson, M. (1990). Emotions and adjudication: Status degradation among white-collar criminals. *Justice Quarterly*, 7, 515-528

Benson, M. (1984). The Fall from Grace. *Criminology*, 22, 573-593

Benson, M. and Cullen, F. (1988). The special sensitivity of white collar-offenders to prison: A critique and research agenda. *Journal of Criminal Justice*, 16, 207–215.

Bethune, RA. (2015) *Profiling White-Collar Criminals*. London: Gansen.

Bowers, K. and Johnson, S. (2005) Using Publicity for Preventative Purposes. In, Tilley, N. (ed) *Handbook of Crime Prevention and Community Safety*. Cullompton: Willan.

Bussmann, K., D. and Werle, M., M. (2006) Addressing Crime in Companies First Findings from a Global Survey of Economic Crime. *British Journal of Criminology*, 46, 1128-1144.

Button, M., Blackbourn, D., and Tunley, M. (2015). 'The Not So Thin Blue Line After All?'; Investigative Resources Dedicated to Fighting Fraud/Economic Crime in the United Kingdom'. *Policing*, 9 (2), p.129-142.

Button, M., McNaughton-Nicholls, C., Kerr, J. and Owen, R. (2015) Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *Howard Journal of Criminal Justice,* 54: 193-211.

Button, M., Pakes, F. and Blackbourn, D. (2016) 'All Walks of Life': A Profile of Household Insurance Fraudsters in the United Kingdom. *Security Journal.* 29 (3). pp. 501-519.

Canter, D. (1994) *Criminal Shadows: Inside the Mind of the Serial Killer*. London: Harper Collins

Cohen, S. (2000) *States of Denial*, Cambridge: Polity.

Condry has noted the impact of media coverage of the families of serious offenders Condry, R. (2007). *Families Shamed: The Consequences of Crime for Relatives of Serious Offenders*. Cullompton: Willan;

Copes, H. and Hochstetler, A. (2010) Interviewing the Incarcerated: Pitfalls and promises. In W. Bernasco (Ed.), *Offenders on Offending*. Cullompton: Willan

Doig, A., and Levi, M. (2013). A case of arrested development? Delivering the UK National Fraud Strategy within competing policing policy priorities. *Public Money and Management*, *33*(2), 145-152.

ECB (2015). Fourth report on card fraud. Frankfurt: European Central Bank.

Europol (2014) *Internet-enabled Organised Crime Threat Assessment 2014*. The Hague: Europol.

FFA UK. (2016a). Fraud the Facts 2015. London: Financial Fraud Action UK.

FFA UK. (2016b) Year-end 2015 fraud update: Payment cards, remote banking and cheque. London: Financial Fraud Action UK.

Felson, M. (2002) *Crime and Everyday Life*, 3rd ed., London: Sage.

Glaser, B., & Strauss, A. (1967). The discovery of grounded theory: strategies for qualitative research, Chicago: Aldin Pub.

van der Geest, V. R., Weisburd, D., and Blokland, A. A. (2016). Developmental trajectories of offenders convicted of fraud: A follow-up to age 50 in a Dutch conviction cohort. *European Journal of Criminology*, online first.

Hollingshead, A. (2011). Four factor index of social status. *Yale Journal of Sociology, 8*, 21-53.

Jackson, J. and Bekerian, D. (1997) Offender Profiling: Theory, Research and Practice. Chichester, UK: Wiley.

Kalof, L., Dan, A. and Dietz, T. (2008). *Essentials of social research*. Maidenhead: Open University Press

KPMG (2011) *Who is the Typical Fraudster*. London: KPMG.

KPMG (2013) *Global profiles of the fraudster: White-collar crime – present and future*, London: KPMG.

KPMG (2016) *Global Profiles of the Fraudster*, London: KPMG.

King, J. and Doig, A. (2016). A dedicated place for volume fraud within the current UK economic crime agenda? The Greater Manchester police case study. *Journal of Financial Crime*, 23(4), 902-915.

Laycock, G. (1991) Operation Identification or the Power of Publicity. *Security Journal*, 2: 67-71.

Van Koppen MV and De Poot CJ (2013) The truck driver who bought a café: Offenders on their involvement mechanisms for organized crime. *European Journal of Criminology* 10: 74–88.

Levi, M. (2002) 'Suite justice or sweet charity? Some explorations of shaming and incapacitating business fraudsters', *Punishment and Society*, 4(2): pp. 147-163.

Levi, M. (2006) 'The Media Construction of Financial White-Collar Crimes', *British Journal of Criminology*, Special Issue on Markets, Risk and Crime, 46: 1037-1057.

Levi, M. (2008a) 'White-collar, organised and cyber crimes in the media: some contrasts and similarities', *Crime, Law and Social Change*, 49: 365–377.

Levi, M. (2008) *The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud*, 2nd edition, Andover: Ashgate.

Levi, M. (2015) 'Qualitative Research on Elite Frauds, Ordinary Frauds and "Organized Crime"', in M. Miller and H. Copes (eds.) *Handbook of Qualitative Criminology*, New York: Routledge (pp.215-235)

Levi, M. (2016) 'Sentencing Respectable Offenders', in S. van Slyke, M. Benson, and F. Cullen (eds.), *Oxford Handbook of White-Collar Crime*. New York: Oxford University Press. (pp.582-602, Ch.28).

Levi, M. and Suddle, S. (1989) 'White-collar crime, shamelessness, and disintegration: the control of tax evasion in Pakistan', *Journal of Law and Society*, 16: 489-505.

Middleton, D. J. (2008). Lawyers and client accounts: sand through a colander. *Journal of Money Laundering Control*, *11*(1), 34-46.

Middleton, D. and Levi, M. (2005) The role of solicitors in facilitating 'Organized Crime': Situational crime opportunities and their regulation, *Crime, Law & Social Change* 42 (2- 3): 123–161.

Middleton, D. and Levi, M. (2015) 'Let Sleeping Lawyers Lie: Organised Crime, Lawyers and the Regulation of Legal Services', *British Journal of Criminology.* 55(4): 647-668.

NCA (2016) *Pathways into Serious and Organised Crime*, London: National Crime Agency.

NCA (2017) *Pathways into Cyber Crime*. London: National Crime Agency.

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

ONS (2017) Crime in England and Wales: Year Ending Sept 2016. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016#whats-happening-to-trends-in-fraud

Piquero, NL and Weisburd, D. (2009) Development trajectories of white-collar crime. In: Simpson S, Weisburd D (eds) *The Criminology of White-collar Crime*. New York: Springer, 153–171.

Piquero, N. L., Piquero, A. R., and Weisburd, D. (2016). Long-Term Effects of Social and Personal Capital on Offending Trajectories in a Sample of White-Collar Offenders. *Crime and Delinquency*, *62*(11), 1510-1527.

Piquero, A. R., and Piquero, N. L. (2016). White-Collar Criminal Participation and the Life Course. In *The Oxford Handbook of White-Collar Crime* (p. 238). Oxford University Press.

Robbers, M. L. (2009). Lifers on the Outside Sex Offenders and Disintegrative Shaming. *International Journal of Offender Therapy and Comparative Criminology*, *53*(1), 5-28.

Shapland J, Atkinson A, Atkinson, H, Dignan J, Edwards L, Hibbert, J, Howes, M, Johnstone, J, Robinson G and Sorsby, A (2008a) *Does Restorative Justice Affect Reconviction? The Fourth Report From The Evaluation Of Three Schemes*. London: Ministry of Justice.

Shapland J, Atkinson, A Atkinson, H, Chapman, B Dignan J Howes M Johnstone J Robinson G and Sorsby, A (2008b) *Restorative Justice: The Views Of Victims And Offenders The Third Report From The Evaluation Of Three Schemes*. London: Ministry of Justice.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

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

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56 (1): 21-48.

Willig, C. (2001). Introducing Qualitative research in psychology: Adventures in theory and method. Maidenhead: Open University Press.