Sentencing Council

Research on Sentencing Online Fraud Offences

Jane Kerr, Rachael Owen, Carol McNaughton Nicholls
NatCen Social Research

Mark Button
Centre for Counter Fraud Studies, University of Portsmouth

June 2013

Research on Sentencing Online Fraud Offences

Jane Kerr, Rachael Owen, Carol McNaughton Nicholls
NatCen Social Research

Mark Button
Centre for Counter Fraud Studies, University of Portsmouth

This information is available on the Sentencing Council website at: www.sentencingcouncil.org.uk

Disclaimer

The views expressed are those of the authors and are not necessarily shared by the Sentencing Council (nor do they represent Sentencing Council or government policy).

Any enquiries regarding this publication and to request alternative format versions of this report, should be sent to us at info@sentencingcouncil.gsi.gov.uk

Acknowledgements

We are grateful to Emma Marshall and Trevor Steeples from the Office of the Sentencing Council for their advice, support and assistance for the duration of this research. Thank you also to Mehul Kotecha, Steven Coutinho, Jasmin Keeble and Sarah Dickens for their input to the project.

We would like to thank the key stakeholders and the participants in this research for sharing their views, and we would like to thank the staff of organisations that provided their time to assist with the recruitment of participants, especially Rebecca Lambot at Action Fraud. We would also like to convey special thanks to those who shared their personal experiences of fraud offences and provided valuable information on factors which should be taken into account when sentencing fraud offences.

The authors

Jane Kerr
Rachael Owen
Carol McNaughton Nicholls
NatCen Social Research

Mark Button
Centre for Counter Fraud Studies, University of Portsmouth

Contents

List of tables

Research summary

By 2011, almost 35 per cent of the world population were using the internet (Internet World Stats). Research in the UK in 2009 found that 66 per cent of 16 to 74 year olds had ordered goods online in the last year (Randall, 2010) and 22 million people in the UK were banking online (UK Payments Administration, 2009). The internet poses new opportunities for online communication and financial exchanges – but with it, also new risks.

This report outlines the findings from research conducted by NatCen Social Research focussing on fraud committed wholly or partly online, for the Sentencing Council for England and Wales. The purpose of the research was to explore three key issues: the ways that online fraud is being committed; the impact of online fraud offences on victims; and attitudes to concepts relating to sentencing online fraud offences, such as the culpability of the offender and the seriousness or harm of different types of offences.

The research was conducted to support the Sentencing Council's current review of guidelines on sentencing fraud offences, and as part of its functions to produce analysis and research on sentencing, promote a clear, fair and consistent approach to sentencing and work to improve public confidence in sentencing.[1]

Fraud offences involve offenders intending to make a gain by dishonestly exposing someone else to a risk of loss: the gain may be financial and/or involve other property (Sentencing Guidelines Council, 2009). The Sentencing Council commissioned this study to look at two specific fraud offences (of the five offence types covered by existing sentencing guidelines) when completely or partially carried out online. The term 'online fraud' is therefore used throughout the report to refer to frauds falling within the two categories below:

- **confidence fraud:** this type of offending usually involves a victim transferring money or property as a result of being deceived or misled by the perpetrator. An example of a simple confidence fraud is mass marketing fraud whereby fake goods such as tickets for events are sold online, and after payment either did not arrive or are found to be counterfeit.

- **possessing, making or supplying articles for use in fraud:** this offence can be committed in many ways. The internet may have become an effective tool for creating and disseminating *articles* for use in fraud. 'Articles' include any electronic programmes or data stored electronically. Examples of articles for use in fraud include false fronts for cash machines, computer programs for generating credit card numbers, lists of credit card or bank account details, or 'sucker lists'.[2]

The exact scale of fraud being committed in the UK is currently unknown. However, this research is situated in the context of a growing evidence base for a prevalence and diversity of fraud offences and fraud victimisation. For example, The Office of Fair Trading (OFT) found that 48 per cent of the UK population have been targeted with a mass marketing scam and eight per cent have fallen victim to one (OFT, 2006). In addition to this, identity fraud is reported to be *'Britain's fastest growing crime'* (Metropolitan Police, n.d; Piquero, Choen and Piquero, 2011), and was found to have increased by ten percent in 2012 (CIFAS, 2012). Recent Home Office figures for England and Wales found that over a year (2011/12) there were 2,667 recorded cases of fraud falling within the category of making or supplying articles or possession of articles for use in fraud (Taylor and Bond, 2012).

---

[1] Further details of the statutory duties and functions of the Sentencing Council for England and Wales can be found at: http://sentencingcouncil.judiciary.gov.uk/about-us.htm

[2] Once a victim responds to a confidence fraud their name and address may be included in what is known as a 'Sucker List' and they may be inundated with scam email or junk mail on a daily basis.

However, as many incidences of fraud go unreported the actual prevalence of fraud is likely to be much higher. Coupled with this is the growing opportunity to commit offences online, as internet access increases. Cyber-crime (a term used for any illegal activities enabled online) more generally is recognised as a growing area including identity theft (Fowles and Wilson, 2011; Goucher, 2010; Jaishankar, 2010).

Research methodology

An evidence review was completed as **phase one** of the research and a comprehensive literature search was conducted. The focus of the search was on evidence published from 2009 onwards, using a range of key words such as 'scam' and 'victim'. Copies of pre-2009 evidence cited within the articles were also obtained and included where relevant. The review included evidence from peer reviewed academic articles, research reports, websites and discursive articles in relevant mediums such as financial industry magazines.

Phase two comprised of face-to-face in depth interviews with professional stakeholders (nine stakeholders involved in addressing fraud and its impacts). **Phase three** involved research with victims of online fraud and included both face-to-face interviews (in depth interviews with 15 participants[3]) and focus groups (six focus groups with a total of 48 participants) with individuals who had experienced a type of online fraud in scope for this study. Interviews were conducted with participants that could be considered vulnerable or who had experienced very complex frauds with a high level of emotional or financial impact. They permitted an approach that was responsive and tailored to individual experiences.

Focus groups were used to bring together people who had experienced a diverse range of common types of online fraud such as buying goods that did not arrive, or receiving spam emails. The group dynamic of the focus groups allowed the research team to expose these participants to different online fraud scenarios in the form of offence vignettes and enabled them to generate rich discussion in relation to the focussed examples. The vignettes described a case of online romance fraud; identity fraud; consumer fraud; and advance fee fraud. A full version of each vignette is included in Appendix B.4 of the main report.

A qualitative approach was favoured for the research as this gave participants the opportunity to discuss in depth their experiences and knowledge of the ways online fraud is being committed and provide explanations for their views about seriousness, harm caused, culpability of offenders, aggravating and mitigating factors and sentencing (see Appendix A for more detail about the research methodology).

Research generalisability and limitations

With any research there are limitations and this study is no exception. Given the hidden nature of some types of online fraud it is difficult to know that every eventuality of online fraud has been covered in this study. While we are confident that the recruitment approaches used meant that all of the participants taking part in this study had experienced at least one of the types of fraud in scope for this study, participants could only describe the frauds they were aware of and individuals may have experienced other types of frauds without their knowledge.

The qualitative findings give a good understanding of the range of views that exist around how fraud is conducted over the internet and the factors relating to seriousness, harm and

[3] The term participant is used throughout the report to refer to the members of the public who took part in the research, all of whom had experienced some type of online fraud. This differentiates their views from findings about victims of fraud cited from the evidence review.

culpability of the perpetrator among both stakeholders and victims of online fraud. However, as is normal with qualitative research, the sample was selected purposively to obtain range and diversity of experiences and characteristics and was not designed to be statistically representative of the wider population of stakeholders and victims.

A further potential limitation in the sample was that very few victims had experienced the apprehension or conviction of the perpetrator for the fraud and therefore could not reflect upon engagement with the criminal justice process or actual sentencing of the fraud they had experienced. Lastly, opt in approaches can lead to self-selection bias as participants' decisions to participate may be correlated with certain traits. Although the sample was monitored across key sampling criteria to ensure diversity in terms of age, gender and type of fraud experienced some characteristics may have been better represented than others (of note certain groups may be under-represented in the sample, such as young people under the age of 25). A detailed breakdown of the achieved sample for participants is provided in Appendix A (see Tables A.1 and A.6).

Findings from the evidence review

Types of online fraud

- The key examples of **confidence fraud** in the literature are mass marketing frauds (where money is exchanged for goods or services which never arrive or are sub-standard), romance scams (where emotional ties are created by the fraudster and individuals encouraged to transfer money to them due to crisis or difficulties they encounter) and investment frauds (where individuals are promised some sort of gain, but need to exchange money in order to receive it).

- **Possessing, making or supplying articles for use in fraud** includes using electronic programmes or data stored electronically to facilitate fraud. Examples include computer programs for skimming credit card numbers, lists of credit card or bank account details, and copies of emails for use in advance fee frauds.

- Processes such as **phishing** and **pharming** (where consumers are tricked into transmitting personal details or financial information to a fraudulent website), and the use of **malware** (whereby computers are transformed into 'robots' or **bots** that can be controlled externally), to facilitate fraud being carried out online.

- **Emerging types of fraud** or techniques that enable fraud include: **SMishing** (personal information obtained via SMS); **vishing** (personal information obtained by telephone); new forms of **malware** (used to collect personal information via Smartphones); **spear-phishing** (highly targeted spam emails); **Koobface** on social media (where victims are sent messages via their social media site that contain a virus); **social phishing** (where the online offender gains access to an individual's social media account and then accesses their 'friend' list or as a phisher gains unauthorised access into a user's account and sends spam to all their direct contacts); **keylogging viruses** (software designed to record computer use and secretly send it to a host computer); **fraud in virtual platforms** such as 'Second Life'; and **online rental scams** (whereby fake rental flats are advertised online and victims send personal information or financial deposits to prove they can pay the rent).

The evidence review also highlighted the following key issues:

- although it is widely acknowledged that fraud can be committed in diverse ways, and the new technology available via the internet has created new forms of fraud (i.e. phishing), some types of online fraud represent the **development of**

'traditional' offline fraud methods such as selling fake goods, that have been adapted to take advantage of computer mediated communication (CMC), and the wide reach it enables.

- the evidence suggests that offenders adopt complex perpetration strategies to maximise the chance of the fraud being successful, such as: appeals to trust via legitimate appearances; assuming a professional or legitimate façade; visceral appeals, which prey on emotions; luring victims with the promise of positive reward or negative scenarios; a disproportionate relation between the size of the alleged reward and the cost of obtaining it ('too good to be true'); grooming victims by fostering emotional links to them, and giving small gifts or compliments; and withdrawing small amounts from victims' accounts before escalating to larger sums (smurfing).

- while there **does not appear to be a typical fraud victim**, the OFT (2009) report concluded that *'almost all authors'* agree that differences exist at the demographic level in terms of vulnerability to fraud, with the elderly, less well educated, and socially isolated being particularly vulnerable. Those falling for different kinds of frauds do share some similar characteristics, however, victim profiles may be influenced by the amount certain groups are targeted and this may play as much a role in a victim profile than certain groups actually being more susceptible to fraud.

  The evidence review indicated that women are most likely to fall for: internet matrix scams (free gifts are offered via adverts on the web; after buying a gift the victim goes on a waiting list to receive another gift once a set number of others have signed up, but there are more members than gifts and they do not receive the value of their contribution); miracle health and slimming scams (such as buying fake diet pills); clairvoyant and psychic scams; and career opportunity scams.

  Men are more likely to fall for African advance fee fraud, internet dialler scams (where internet routers are re-routed via an expensive telephone line), high risk scam investments, and fake property investments. The evidence also indicated that older people are most likely to fall for: high risk investments and doorstep service providers; while young people are most likely to fall for work at home scams, clairvoyant and psychic scams, and internet dialler scams. Collectively these scams cover a wide range of confidence fraud indicating that anyone can fall victim to fraud more generally.

- while **financial impacts** of fraud can be the most significant, a range of other important impacts were also identified in the literature including **emotional and psychological**, **physical health** problems, **damage to personal relationships,** and feelings of **shame** and **embarrassment.**

Findings from interviews and focus groups with stakeholders and victims

Experiences of online fraud

- Participants (both professional stakeholders and victims of online fraud) had experienced or were aware of a variety of different types of online frauds. Their knowledge and experience highlighted the sophisticated ways in which confidence fraud and possessing, making or supplying articles for use in fraud are carried out, and the role of the internet in their implementation.

- The types of **confidence fraud** that participants had experienced fell into three broad categories: mass marketing fraud, investment fraud and dating/romance fraud. The common element of the mass marketing frauds experienced was that participants had exchanged money with the fraudster for goods or services which never arrived, or were faulty/counterfeit. Common to both investment frauds and dating/romance scams were that participants had been promised some sort of gain, but needed to exchange considerable amounts of money in order to receive it. These frauds were also usually enabled by repeated contact between participants and perpetrator(s), with the perpetrator(s) taking on the role of someone else (such as a bank manager or potential partner). In the case of romance scams the 'promise' may have been that of an intimate relationship as opposed to financial gain.

- In relation to **possessing, making or supplying articles for use in fraud**, the main types of frauds experienced included personal information being collected and used covertly, computer viruses, spam and phishing emails, and fake websites used to sell fake goods or services, or to legitimise a marketing scam.

- Successful frauds usually involved an **overlap between the two offence types** described above. For example, the fraud began with a phishing email or people accessing false websites, and turned into confidence fraud if these emails were responded to, or money was transferred because the website was believed to be legitimate.

- Those who had personally experienced fraud were often **not aware of how the fraud against them had been perpetrated**, or were only able to understand it with hindsight. It was evident from their accounts of the fraud that they had experienced a **range of perpetration strategies** described in the evidence review and by stakeholders (summarised in the section above). However, they may themselves have perceived the fraud to have been 'opportunistic', although when they described it, it bore the hallmarks of highly organised frauds, well known to authorities as discussed by stakeholders interviewed.

- Participants' **vulnerability to online fraud was found to be relative** to their specific circumstances – the techniques used by fraudsters played on a wide range of 'vulnerabilities' or 'weaknesses' such as being new to the country, having a disability, not being familiar with the internet, coveting a rare consumer good. Perpetration strategies therefore appear to exploit whatever vulnerability may be evident among a range of different populations and circumstances.

- The **centrality of the internet** to the fraud experienced varied. In some cases it was the central medium for the fraud occurring; in others the internet was used alongside other methods of communication, to create the impression that the fraud was genuine (**legitimacy**) or as an **enabling tool** to lure the victim in (such as a website being seen as evidence that fraudulent goods are real).

- The internet was described by participants as being a **'normal' form of communication** that 'has' to be used in everyday life. They therefore found it difficult to ascertain how they could avoid being a potential victim of online fraud given the sophisticated perpetration strategies used (such as fraudulent websites appearing to be exactly the same as legitimate websites), and their need to use the internet.

The impact of online fraud

Participants who were victims of fraud reported experiencing a range of impacts from online fraud:

- **financial impacts** which ranged from short-term costs associated with resolving fraud such as removing a computer virus, to the long-term impacts of losing life savings, including being unable to retire or buy a house, go on holiday or visit family, and in the extreme, becoming bankrupt.

- a wide range of **emotional and psychological** impacts were reported including panic, anger, fear, stress, anxiety, self-blame and shame. Self-blame was one of the most pervasive effects of fraud which could damage participants' opinion of themselves as capable people, who could protect themselves from harm. There were participants who reported feeling vulnerable, lonely, violated and depressed and in the most extreme cases suicidal as a result of fraud. These emotional and psychological impacts could relate to both the stress of financial loss and also the loss of self-confidence that they described following the fraud.

- aside from the emotional and psychological impacts on participants' mental health, physical health impacts tended not to be reported. However, there were some exceptions to this, where the psychological distress caused by fraud had led to physical symptoms such as sleeplessness and nausea.

- the fraud could have **damaged participants' relationships with others** and made it difficult for some to trust people. Some participants had become withdrawn and socially isolated as they tried to keep the fraud secret from close friends or relatives due to the shame or embarrassment they felt, or attempted to protect themselves from people abusing their trust in the future, or obtaining their personal information.

- fraud caused considerable **time to be lost and inconvenience**. Participants described how they attempted to protect themselves and others against future fraud. In cases of consumer fraud, participants could have spent a considerable amount of time waiting for the item they paid for and re-contacting the offender to try to obtain it before they realised they had been defrauded.

- to protect themselves against fraud happening to them again, participants could make **long-term changes to their behaviour,** such as no longer buying items online, which was felt to incur time and inconvenience.

- the **wider impact on society of online fraud** was highlighted by participants and professional stakeholders, who thought that the damage to public confidence in legitimate online business could have a far-reaching impact on the UK economy.

- the **level of reparation** or resolution from the fraud that participants had experienced unsurprisingly had an impact on the level of harm reported. Those who had been reimbursed by their bank reported that this **did reduce the harm** caused, and those who had not been reimbursed cited restitution of funds as the single factor that would most help them to overcome the impact of the fraud.

- in addition, there was evidence to suggest that the support provided by others, including the police, formal agencies such as bank fraud departments, or family and friends, could influence the impact of online fraud on participants. Where participants reported that they had felt **supported or listened to** the negative **impact of the fraud could be reduced.** For example, when the police had shown an interest in pursuing the case, participants reported feeling that the

offence committed against them was legitimised and this could reduce feelings of 'self-blame'. Conversely where a fraud was reported and police indicated that they were unable to follow it up, the impact could be compounded, as participants felt unheard. General disapproval from friends, family or wider sources (such as media coverage of victims of fraud being 'duped' or naive) could also compound the emotional and psychological harm reported.

Attitudes to concepts relating to sentencing

The factors which participants felt made an online fraud offence more serious, and offenders more culpable, were also those which were regarded as aggravating the offence. Participants who were victims of fraud were able to suggest aggravating factors they agreed with, more easily than mitigating factors, demonstrating their strong feeling that whilst there was little that could make the online fraud they experienced *less* serious or harmful, there were many factors which could increase the seriousness of the fraud.

- **Aggravating factors** broadly agreed on included circumstances where the fraud:
  - had a considerable financial impact on the victim (regardless of net value – financial impact could be relative to the victim's financial circumstances);
  - was premeditated and showed careful planning (level of intent) on the perpetrator's part;
  - had involved an apparent abuse of trust/authority;
  - involved repeated contact between the perpetrator and victim, and included complex or insidious perpetration strategies (nature of the fraud);
  - involved considerable harm to the victims (both intended and actually caused);
  - affected a high number of victims;
  - targeted vulnerable victims (though vulnerability was felt to be relative, see below); and
  - involved a perpetrator who was a repeat offender and showed a high level of intent to commit the fraud.

- There was no consensus across the sample on what should be the overriding aggravating factor.

- Some participants held the strong opinion that **targeting vulnerable people** should act as an aggravating factor, in particular those who are very young or old, or those with mental health issues. Others, however, felt that that the offence should be viewed in the same way regardless of the characteristics of the victim and that **'vulnerability' is a subjective and relative issue** which can vary depending on the personality and resilience of the victim, and exact nature of the fraud (for example, participants felt that it should not be assumed older people are more vulnerable than younger people, and indeed they may be more financially solvent and aware of potential scams than young people). Vulnerability was therefore felt to be subjective and relative to the specific circumstances of a victim, and nature of the fraud they experienced, rather than wedded to any particular characteristic.

- Although involving a higher number of victims was generally felt to be an aggravating factor, there was also some debate about this. One view from participants was that a greater number of people had been affected by the fraud, but another was that to focus on the overall scale of a fraud might lead to other important aggravating factors being overlooked.

- One strand of opinion was that the **emotional, psychological and financial harm** were the most important factors to take into account when sentencing. This led both participants and stakeholders to advocate the use of Victim Personal Statements when sentencing. Another opinion was that it was problematic for harm to victims to be the overriding aggravating factor, on the grounds that the degree of harm caused may be relative depending on the circumstances of the victim and that irrespective of impact, the intent to commit the fraud remains. The argument here is that the perpetrator should be sentenced on the **intent/actions involved in the fraud** rather than just the harm caused by it.

- Participants who were victims of fraud and stakeholders, were generally reluctant to identify clear mitigating factors from the cases they had experienced. They broadly agreed mitigating factors were where the **perpetrator's role had been peripheral** and where the offender showed **remorse, made reparations and cooperated with the police during the investigation.**

Responses to online fraud

- A strongly held view was that regardless of the method, (online/offline), the crime (fraud) should be viewed as the same. However, there were also arguments made that online fraud may involve a particular invasion of an individual's privacy, and potential to affect a greater number of victims than offline fraud.

- The types of sanctions that were felt appropriate for online fraud were: custodial sentences; community orders; fines; restitution orders; seizure of assets; confiscation orders; restorative justice; and name and shame sanctions. Restitution orders and restorative justice in particular were a recurring suggestion amongst both participants and stakeholders. In relation to the former, it was felt that making reparations to the victim would ease the financial impact on the victim and be a just outcome. In relation to the latter (restorative justice) it was felt that meeting the victim could make perpetrators, of what is perceived to be a faceless or victimless crime, realise the impact of the offence. It would also help victims understand the process whereby they were defrauded and feel less responsible themselves.

1. Introduction

This chapter introduces the background to the research, outlines the aims and objectives of the research and summarises the methodology and limitations of the study.

1.1 Background to the research

The Sentencing Council for England and Wales commissioned this study to look at two specific fraud offences (of the five offence types covered by existing sentencing guidelines) when completely or partially carried out online: confidence fraud and possessing, making or supplying articles for use in fraud:

- **confidence fraud**: this type of offending usually involves a victim transferring money or property as a result of being deceived or misled by the perpetrator. An example of a simple confidence fraud is the selling of fake goods online, which after payment by the buyer either do not arrive or are found to be counterfeit.

- **possessing, making or supplying articles for use in fraud**: this offence can be committed in numerous ways. The internet has become an effective tool for creating and disseminating *articles* for use in fraud. 'Articles' include any electronic programs or data stored electronically. Examples of articles for use in fraud include false fronts for cash machines, computer programs for generating credit card numbers, lists of credit card or bank account details, 'sucker lists'[4] and draft letters or emails for use in advance fee fraud.

Within these two fraud offence categories, the types of fraud which affect individuals are diverse. This is reflected in the extensive lists of fraud described in the literature review, *Fraud Typologies and Victims of Fraud* by Button et al., (2009a), and the recently published *Little Book of Big Scams* (Metropolitan Police, n.d). Despite this variation, all fraud offences involve offenders dishonestly intending to make a gain by exposing someone else to a risk of loss. The offender may gain money and/or property or 'goods' from the victim (Sentencing Guidelines Council, 2009).

The exact scale of fraud (online or offline) being committed in the UK is currently unknown. However, this research is situated in the context of a growing evidence base on the prevalence and diversity of fraud offences and fraud victimisation (also reflected in the work of Action Fraud, the centralised UK body for reporting fraud[5]).

For example, findings from the recent Crime Survey for England and Wales (CSEW) for the year ending June 2012, found that 4.7 per cent of plastic card owners had been a victim of card fraud in the previous 12 months (ONS, 2012). The Office of Fair Trading (OFT) has commissioned research which found that 48 per cent of the UK population have been targeted with a mass marketing scam and eight per cent have fallen victim to one (OFT, 2006). CIFAS also report that facility takeover fraud has increased by 18.1 percent from last year. This is when the fraudster takes control of an existing account or policy and uses it for their own benefit. This type of fraud is facilitated online by obtaining usernames and passwords of online accounts. As a result the internet accounted for 62.4 percent of this type of offence in 2011 compared to 37.9 percent in 2010 (CIFAS, 2012).

---

[4] Once a victim responds to a scam their name and address may be included in what is known as a 'Sucker List' and they may be inundated with scam email or junk mail on a daily basis. These lists are sold at a higher value among fraudsters than other lists of personal information.

[5] http://www.actionfraud.police.uk/home; Action Fraud is the UK's national fraud and internet crime reporting centre. They provide a central point of contact for information about fraud and financially motivated internet crime. The service is run by the National Fraud Authority.

In addition to this, identity fraud is reported to be 'Britain's fastest growing crime' (Metropolitan Police, n.d; Piquero, Choen and Piquero, 2011). While it has been around in the USA for approximately 30 years it is a newer phenomena in the UK (Antokol, 2009), and was found to have increased by ten percent in 2012 (CIFAS, 2012). Alongside this, recent Home Office figures for England and Wales found that over a year (2011/12) there were 2,667 recorded cases of fraud falling within the category of making, supplying articles or possession of articles for use in fraud (Taylor and Bond, 2012) . However, as many incidences of fraud go unreported the actual prevalence of fraud is likely to be much higher.

There is also a growing opportunity to commit offences online, as internet access increases. By 2011, almost 35 per cent of the world population were using the internet (Internet World Stats). Research in the UK in 2009 found that 66 per cent of 16 to 74 year olds had ordered goods online in the last year (Randall, 2010) and 22 million people in the UK were banking online (UK Payments Administration, 2009). Cyber-crime (a term used for any illegal activities enabled online) more generally is recognised as a growing area including identity theft and scams (Fowles and Wilson, 2011; Goucher, 2010; Jaishankar, 2010).

In response to the growing evidence base of fraud offences and fraud victimisation the National Fraud Authority established Action Fraud, the UK's national fraud reporting service for information about fraud and financially motivated internet crime. However, in spite of the scale of fraud, only a relatively small amount of research has been conducted with fraud victims to explore the nature and impact of the offence experienced, and very little that has focussed on online fraud specifically (Levi and Pithouse, 1992; Levi, 1999; Levi, 2001; Fraud Advisory Panel, 2006; Pascoe et al., 2006; Croall, 2001; Button et al., 2009 a,b,c; Button et al., 2010; and Whitty and Buchanan, 2012). This, coupled with the fact that the practice of online fraud (fraud committed either completely or partially over the internet compared to fraud committed offline without any use of the internet), may be growing rapidly, alongside online interactions suggests a need for research to explore the nature and impact of online fraud, and how types of behaviour or forms of communication online may have a bearing on how fraud is facilitated. This research was commissioned in this context, and specifically to explore the impact of these types of fraud offences and inform future sentencing guidelines.

Current sentencing practice

Alongside recognition that the extent and diversity of online fraud is increasing, there has recently been considerable debate over the degree to which sentencing guidelines take into account the specific circumstances and facts of each case and match public expectations about the types of sentences that should be given. This is reflected in the Legal Aid, Sentencing and Punishment of Offenders (LASPO) Act 2012.[6] As such, the Ministry of Justice Structural Reform Plan 2011, now superseded by the Ministry of Justice Business Plan 2011–2015, set out clear objectives to review sentencing practices.[7] In addition, there is very limited literature focussing specifically on sentencing fraud offences (Levi, 2010; Copes and Vieraitis, 2009a/b; Tupman, 2010; and Goucher, 2010). This research aims to help address this gap but was intended only to begin to explore stakeholders' and victims'

[6] The relevant provisions from the LASPO Act were previously contained in the Government Green paper, *Breaking the Cycle: Effective Punishment Rehabilitation and Sentencing of Offenders* launched by the Ministry of Justice in December 2010, which noted that victims' views should be taken into greater account in the sentencing process.

[7] http://www.justice.gov.uk/publications/corporate-reports/moj/2010/structural-reform-plan/index.htm

experiences and views on the impact of online fraud and implications this may have for sentencing.[8]

Sentencing process

Sentencing occurs when a person has pleaded guilty to an offence or has been found guilty of an offence following a trial. The key purposes of sentencing are: the punishment of perpetrators; the reduction of crime; the reform and rehabilitation of perpetrators; the protection of the public; and the making of reparation by perpetrators to persons affected by their offences.

In addition to these key purposes, a judge or magistrate will use sentencing guidelines, for offences where they exist, which set out the steps they should follow and the factors they should consider when determining an appropriate sentence in terms of the length and the various different types of sanctions available. The factors considered will vary on a case by case basis.

The key determinant for sentencing offences is the seriousness of the offending behaviour. Assessing seriousness involves the consideration of culpability and harm – that is the degree of planning and intentionality to cause harm – which the perpetrator put in place to gain from the offence. Other factors that may determine the sentence include:

- relevant law including maximum, and in some cases minimum, sentences;
- specific sentencing guidelines relevant to the offence committed;
- whether the perpetrator has a previous conviction and of what kind;
- statutory aggravating and mitigating factors of sexual and racial motivation;
- personal mitigation relating to the perpetrator and their family;
- whether the perpetrator pleaded guilty (which normally results in a reduced sentence or occasionally a change from one type of sentence to another), and the stage at which the plea was entered; and
- totality, viz. whether a perpetrator is being sentenced for more than one offence (although offences can be served concurrently).

The principal offences likely to be used to prosecute **confidence frauds** are fraud under section 1 of the Fraud Act 2006 and false accounting under section 17 of the Theft Act 1968. In relation to **possessing, making or supplying articles for use in fraud**, the principal offences are possession of articles for use in fraud under section 6 of the Fraud Act 2006, making or supplying articles for use in fraud under section 7 of the Fraud Act 2006 and the general offence of fraud in section 1 of the Fraud Act 2006. The key document in relation to sentencing these fraud offences is the guideline *Sentencing for Fraud – Statutory Offences,* issued in 2009 (Sentencing Guidelines Council, 2009). The guidelines provide a framework for the sentencing of these offences and make a number of points in relation to this process.

First, the suggested starting points and sentencing ranges contained in the offence guidelines should not be treated as rigid, rather movement within and between ranges will be dependent on the circumstances of individual cases and, in particular, the aggravating and mitigating factors that are present. Secondly as for any offence, the primary consideration for sentencing fraud offences is the seriousness of the offending behaviour. As described above

[8] Future academic research, outside of the remit of the Sentencing Council might explore experiences of online fraud among specific groups (differences by age, ethnicity or gender etc), segmenting experiences or characteristics of victims. Comparative cross-national research examining differences in reported experience by victim type, and potentially taking into account issues such as cultural differences in how individuals are affected by different perpetration strategies, could also help to address existing gaps in this research area. Existing gaps could also be addressed by a robust random probability survey examining the prevalence of different types of fraud (including online fraud) within the general population.

assessing seriousness involves the consideration of culpability and harm.[9] The first step is to assess the degree of planning and intentionality to cause harm that the perpetrator put in place to gain from the fraud using an exhaustive list of factors (described below); in general terms, the greater the financial loss to the victim the greater the seriousness of the offence. The second step is then to assess the harm caused by the offending using a non-exhaustive list of additional factors.

Aggravating and mitigating factors (those factors that may lead to a more or less severe sentence) are of particular interest for this research. Within the current guidelines, factors indicating higher culpability (and aggravate an offence) include planning an offence, perpetrators operating in groups or gangs, high level profit, intention to commit more serious harm than occurred, deliberate targeting of vulnerable victims, abusing a position of trust and concealing or disposing of evidence. Factors indicating a more than usual serious degree of harm include: having multiple victims, where the victim is particularly vulnerable and the fraud involved a high value (including sentimental value) of property to the victim or substantial consequential loss. Using another person's identity to commit the fraud, the offence having a lasting impact on the victim and the offence being carried out over a long period are also of particular relevance when assessing fraud offences. Courts also currently take into account factors such as harm to persons other than the victim, erosion of public confidence, actual physical harm created by the fraud, and the difference between intended and resulting loss.

Mitigating factors (the factors that lower culpability) identified in the current guidelines include: mental illness or disability of perpetrator; youth or age of perpetrator; peripheral involvement in the offence; and the behaviour not being fraudulent from the outset (for example someone continuing to accept money they are no longer entitled to having initially legitimately been paid[10]). In addition personal mitigation may be evident in fraud cases. In the current guidelines this includes voluntary cessation of offending; complete and unprompted disclosure of the fraud; voluntary restitution; and the perpetrator being under financial pressure.

A full step-by-step approach to the decision making process involved in sentencing can be found in the current guidelines (Sentencing Guidelines Council, 2009) on page 17.

Existing sentences for fraud offences

Judges and magistrates have a broad range of sentencing options available to them: custodial sentences (including suspended sentences); non-custodial (community) sentences and fines.

Ancillary orders may also be imposed. These aim to minimise the harm caused by the perpetrator, achieve reparation for the offence or punish the perpetrator. Orders that may be considered when sentencing fraud offences include:

- **compensation orders:** compensation **must** be considered in a case where an offence has resulted in loss or damage;[11]
- **confiscation orders:** if the perpetrator has benefitted financially from their offence courts should consider if a confiscation order would draw back this gain;
- **deprivation orders:** which deprive the perpetrator of property used to facilitate an offence; and
- **restitution orders:** whereby stolen goods or a sum to the value of these goods, taken by the perpetrator, is restored to the victim.

---

9 Criminal Justice Act 2003, s.143(1).

10 Some factors are relevant to specific fraud offences, for example this latter point is mainly found in cases of benefit fraud.

11 Compensation can either be a sentence and standalone penalty in its own right or an ancillary order.

Orders may also refer to future conduct and aim to prevent reoffending, such as:

- **financial reporting order**: whereby the perpetrator's financial affairs must be reported (for up to five years via the magistrates' court and 15 years via the Crown Court);
- **serious crime prevention order:** which contains the restrictions, requirements or terms the court considers necessary to prevent reoffending; and
- **anti-social behaviour order:** which restricts behaviour in some way and has been used in a handful of cases by Trading Standards officers against those engaged in persistent fraudulent trading.

The current guidelines on sentencing fraud offences also note that in exceptional cases a fine may be imposed alongside a custodial sentence. This is where a confiscation order is not part of the sentence, there is no victim to compensate, *and* the perpetrator has resources to pay a fine.

The various orders may be imposed alone or along with a custodial sentence. Courts should consider the totality of the sentence (custody, fines or various orders) and ensure it is proportionate to the offending behaviour when making sentencing decisions.

Research on sentencing fraud

Whilst the amount of literature on fraud victims that exists is limited (see above), available evidence highlights a range of consequences that frauds can have on the victim. The most obvious impact is financial loss, whilst others are the time taken to deal with the fraud (Fraud Advisory Panel, 2006; Pascoe et al., 2006), emotional and psychological impacts and health impacts (Whitty and Buchanan 2012; Button, 2009 a,b,c). Existing sentencing decisions, whilst acknowledging additional impacts could be taken into account, appear to focus on specific aspects of the offence such as the value of the fraud. However, for the victim, the financial harm may be relative – an individual with a very low income and little savings may find their lives affected to a greater extent than someone with a very high income, when the same amount is defrauded from them (Button et al., 2009a). Ways in which frauds are committed and the degree of planning or skill involved also varies and may be difficult to identify or measure.

In this context the Sentencing Council for England and Wales commissioned Crime and Justice researchers from NatCen Social Research, in collaboration with Mark Button at the Centre for Counter Fraud Studies, University of Portsmouth, to undertake research specifically into the ways confidence fraud and possessing, making or supplying articles for use in fraud are being committed online, and the impact on victims of these types of frauds. This research was conducted to inform the Sentencing Council's current review of guidelines on sentencing fraud offences, and as part of it's functions to produce analysis and research on sentencing, promote a clear, fair and consistent approach to sentencing, and work to improve public confidence in sentencing.[12] It is intended that the findings will feed into the development of revised, definitive guidelines on sentencing fraud offences. These will replace existing guidelines on sentencing fraud offences issued in 2009.

The aims and objectives of the research were to:

- review ways that online fraud (specifically as it relates to confidence fraud and possessing, making or supplying articles for use in fraud) is currently being committed;
- outline the impact of these different types of online fraud offences on victims; and

[12] Further details of the statutory duties and functions of the Sentencing Council for England and Wales can be found at: http://sentencingcouncil.judiciary.gov.uk/about-us.htm

- explore issues relating to sentencing these online fraud offences, such as seriousness, harm, culpability of fraud offenders and aggravating and mitigating factors.

1.2 Terminology and language used in the report

This report has been written to be accessible to a wide range of audiences and with this in mind, legal terminology has been kept to a minimum. All of the victims of fraud who participated in this study had experienced a form of fraud either enabled completely or partially by the internet. However, not all would identify themselves as a 'victim' with all the attendant meaning this can bring. Some did not perceive the fraud or attempted fraud they had experienced as a 'serious crime' *per se*, and they were not comfortable using the term 'victim' to describe themselves. For this reason the term 'participant' tends to be used throughout to refer to the members of the public who took part in the research who had all experienced (and were therefore victims of) some type of online fraud.

The term stakeholder is used to differentiate the professionals who were interviewed from the other participants who took part, who were all members of the public who had experience of an online fraud committed against them. The term perpetrator or fraudster is used to indicate the person or persons who played a role in committing the fraud offence being discussed. Lastly, online fraud is used to refer to fraud either completely or partially committed over the internet, including fraud enabled or supported by some form of online communication. Offline fraud is used to refer to fraud committed without any use of the internet.

1.3 Research methodology

The research comprised three phases. **Phase one**, the evidence review, involved detailed scoping of the existing literature. This focused on the ways in which the fraud offences (particularly online fraud) in the scope of the research are committed, factors relating to their seriousness and the culpability of the offender and the impact on the victims involved. Key documents such as the existing sentencing guidelines were also included.

A comprehensive literature search was conducted, focussing on evidence published post-2009 and including evidence published pre-2009 where relevant. This included peer reviewed academic articles, reports, websites and discursive articles in relevant medium such as financial industry magazines. Relevant articles were then systematically synthesised in a matrix. A list of the search terms and databases used is included in Appendix A.1.

The literature used in the evidence assessment was summarised thematically using Microsoft Excel. On completion of the review, the entire dataset of evidence was summarised and a report provided to the Office of the Sentencing Council. The findings from the rapid evidence assessment was then used to hone the development of phases two and three of the study – qualitative research with professional stakeholders and with people who had been directly affected by online fraud. The key relevant findings from the review have also been referenced in the main body of this report.

The purpose of the next two phases of the research was to provide up to date evidence on these areas through primary qualitative research. **Phase two** therefore explored the same issues, using face-to-face interviews with nine key stakeholders who were working at the forefront of fraud prevention.[13] Interviews lasted about an hour, were audio recorded and fully transcribed verbatim. They were conducted using a topic guide and a copy of this is included in Appendix B.1. The interviews included the following key areas:

[13] To protect the anonymity of participants they have not been named.

- background information about the stakeholder's role, and their knowledge and experience of working with fraud offences;
- the ways in which fraudulent activities are currently being committed;
- the impact of online fraud on the victims involved;
- the factors that impact on sentencing; and
- the ways in which fraudulent activities will develop in the future.

Phase three involved qualitative research with members of the public who had all been victims of online fraud**.** This stage of the research adopted two distinct strands, described below:

- **focus groups** (six in total) with 48 members of the public who had directly experienced one or both of the two types of fraud in scope for this study, conducted completely or partially over the internet. The focus groups were used to explore experiences of how online fraud is committed and perceptions relating to the seriousness of online fraud offences, the culpability of the offender and what should be the key aggravating and mitigating factors. Impacts of online fraud were also explored. Discussion was prompted by the use of four vignettes, at least two of which were discussed in each focus group. This meant that different types of online fraud scenarios could be compared and contrasted. Spontaneous reactions to the vignettes were explored at first, followed by discussion of specific aspects in order to generate discussion about perceptions of seriousness of the offence, harm to the victim, culpability of the offender and aggravating and mitigating factors.

The fraud offences described in the vignettes and discussed across the six groups were:

- **online romance fraud:** a woman met a man on an online dating site, and transferred money to him following various requests e.g. when the man claimed he was having difficulty paying his rent after becoming redundant. On investigation by the police it became apparent that the man was in fact another person than his dating profile, living in another city.
- **identity fraud**: a young male received an email asking for his personal details that looked as if it was from his bank. He sent his details and these were used by the perpetrator to access his online bank account and withdraw over £2,000 from his account.
- **consumer fraud:** a woman signed up to a trial of slimming pills via a website. After three months with no effect, she tried to follow the cancellation process but her calls and emails went unanswered and payments kept being taken until she cancelled them.
- **advance fee fraud**: an older woman recently started to use the internet and received an official looking email saying she had won a large amount on the lottery. The email also asked for a fee so her prize money could be released. She subsequently sent more money to cover various fees and taxes but the prize money never arrived.

A full version of each vignette is included in Appendix B.4. Focus group participants tended to be people who had been defrauded via the offence of possessing, making or supplying articles for use in fraud or had experienced confidence frauds such as not receiving tickets purchased online. Focus groups lasted around two hours, and were audio recorded and transcribed verbatim (see Appendix A for details). Participants were given £30 in cash for taking part in the group as a thank you for their time and as a contribution towards their travel when attending a group discussion.

- **in depth interviews** (15 participants in total) were completed with people who were victims of online fraud which fell under the two types of fraud in the scope of

this study. In depth interviews were specifically used with participants who had experienced particularly sensitive or extensive frauds, such as romance scams or long-term investment scams facilitated via email contact; or participants who could be considered vulnerable due to age or disability, for example. Interviews facilitated an approach that was responsive and tailored to individual experiences. The interviews focused particularly on the way that the fraud had been committed and the type of harm and impacts they had experienced. Issues relating to the seriousness of the offence and the culpability of the offender were also discussed. Interviews lasted between one hour and one hour and thirty minutes, and were audio recorded and transcribed verbatim. Participants were given £25 in cash for taking part in an in depth interview as a thank you for their time.

Recruitment

Participants who were victims of online fraud were recruited through a number of channels using an 'opt in' approach. Agencies that assisted with recruitment included Action Fraud and professional stakeholders who had participated in interviews in the earlier phase.

Participants who were victims of fraud were recruited through the following three routes:

- **Action Fraud**[14]: individuals making contact with Action Fraud are asked if they would be willing to be re-contacted again by Action Fraud for the purpose of research or other activities. Action Fraud enter details of individuals making contact with them into a database and were able to draw from this lists of individuals who had experienced an online enabled fraud, had agreed to be re-contacted, and for the purpose of the research, were clustered within certain locations (such as around Manchester or Swansea). Action Fraud then sent an information letter and leaflet about the study on behalf of NatCen. Participants could then express an interest in opting into the study by contacting the NatCen research team directly via a free phone number or by email. On making contact with a member of the NatCen research team, participants were asked a number of screening questions designed to collect some basic demographic information and to gain a brief overview of the type of fraud they had experienced and their level of internet usage. This information was used to monitor the sample to ensure there was range and diversity across the key characteristics of age, gender and online fraud.

- **professional stakeholders participating in phase two (gatekeepers)**: each stakeholder who participated in phase two was asked whether they would be able and willing to help with the recruitment of victims of fraud to take part in phase three. Stakeholders approached victims they were in contact with and asked their permission to pass their contact details onto the NatCen research team or they provided the research team's contact details so they could make contact directly. On first contact the research team would then explain the research again fully and discuss it with the participant before asking if they would be willing to take part. A range of stakeholders who were in direct contact with people who had experienced fraud assisted with recruitment of participants. This included the police and a support group for people who had experienced fraud. As detailed in Appendix A stakeholders assisting with this part of the study were provided with a verbal briefing from members of the research team.

[14] Action Fraud is the UK's national fraud and internet crime reporting centre. They provide a central point of contact for information about fraud and financially motivated internet crime. The service is run by the National Fraud Authority.

- **a recruitment agency:** the intention at the start of the study was to recruit all focus group participants through Action Fraud. While a small number of focus group participants were recruited in this way, the numbers opting in were insufficient to organise six focus group discussions. Therefore a recruitment agency, Propellerfield, was also used to recruit participants. NatCen had previous experience of working with this agency and they were chosen for being both trusted and effective. The research team held a face-to-face meeting with Propellerfield so they could be fully briefed on the study and the recruitment process. Flow populations[15] were used, with potential participants screened via a short questionnaire to ensure all of the participants used the internet, and had experienced online fraud. All participants had therefore experienced some form of fraud over the internet. This included advance fee fraud, malware, account takeover, identity theft, fake websites (phishing and spam), and buying goods and services that did not arrive/were counterfeit (such as fake tickets).

To ensure participants were fully informed before they agreed to take part, the researchers discussed the research with them in detail before asking for their consent to arrange an interview or invite them to a group discussion. Information leaflets were also provided to participants by the research team.

Full details on the recruitment approaches and sample can be found in Appendix A.

Sample

Groups were conducted in England and Wales in areas selected to reflect geographical variation (Brighton, Bristol, Birmingham, Cardiff, Manchester and London). Characteristics of the participants were monitored to ensure diversity across and within the groups in relation to key characteristics such as gender, age, whether they lived with other people or alone, employment and health. A breakdown of participants' age and gender is presented in the tables below. A full breakdown of all sample characteristics is provided in tables A.1 and A.6 in Appendix A. In Table 1.1, the basic demographics of the focus group participants is provided.

Table 1.1 Achieved key sample characteristics for focus groups

Gender	
Female	25
Male	23
Total	**48**

Age	
16 – 24	6
25 – 40	21
41 – 59	15
60 +	6
Total	**48**

In Table 1.2, the basic demographical information about interview participants is provided:

[15] This term is used when samples are generated by approaching people in a particular location or setting (Ritchie et al., In press).

Table 1.2 Achieved key sample characteristics for in depth interviews

Gender	
Female	8
Male	7
Total	**15**

Age	
16 – 24	0
25 – 40	3
41 – 59	5
60 +	7
Total	**15**

In addition, diversity was also achieved in terms of individuals' self reported internet usage and confidence with financial matters, as shown in tables A.2, A.3, A.7 and A.8 in Appendix A. However, as is discussed in further detail in the section below, there are limitations inherent within the sample, which were necessary given the scale and scope of the research.

Fieldwork for phases two and three took place between July and October 2012.

1.4 Recording of focus groups and interviews and analysis

All focus groups and interviews were digitally sound recorded and transcribed verbatim. The transcripts were managed using Framework in Nvivo 9. Framework (Ritchie et al., in press) is a data management technique developed at NatCen. Two analytical frameworks were drawn up (one for stakeholders and one for participants), and a series of thematic charts or matrices were set up. Each related to a different thematic issue and data from each transcript was then summarised into the appropriate cells. The analytical stage involved working through the charted data, drawing out the range of experiences and views, identifying similarities and differences and interrogating the data to seek to explain emergent patterns and findings (Spencer et al., in press) – see Appendix A for further details. The research team who conducted the interviews, also conducted the data management (in Nvivo), analysis and reporting. This meant the research team was fully aware of participants' tone of voice and conduct, and could implicitly include this understanding during analysis.

1.5 Ethics

This study underwent a full review by NatCen's Research Ethics Committee (REC), which includes members from senior NatCen staff and external professional experts. This ethics governance procedure is in line with the requirements of the Economic and Social Research Council (ESRC, 2005) and Government Social Research Unit Research Ethics Frameworks (GSRU, 2005).

A number of ethical considerations were taken into account for this study. For example the research team ensured that before the interview or focus group discussion all participants were aware of the subject matter of the research, the issues likely to be raised, what participation would require of them and any other material facts which might have affected their willingness to participate. These issues were communicated to potential participants both in writing and verbally.

1.6 Methodological limitations

With any research there are limitations. This study is no exception and we have noted the potential methodological limitations below.

By using a qualitative methodology the study was able to explore individual differences among participants and stakeholders in a flexible and responsive way. In addition, the focus group discussions illuminated participants' ways of thinking to other people, thus eliciting more enriched and nuanced responses, especially in reference to each of the vignettes. Not withstanding the potential limitations in the sample flagged below, the qualitative findings give a good understanding of the range of views around how fraud is being conducted over the internet and the factors relating to seriousness, harm and culpability of the perpetrator among both stakeholders and victims of online fraud. However, findings are not reported numerically and should not be given numerical weight. As is normal within qualitative research the sample was selected purposively to obtain range and diversity of experiences and characteristics, and not to say how statistically representative those views are of the wider population of stakeholders and victims or how prevalent these experiences are within the general population. Particular limitations to the sample are discussed below.

Given the hidden nature of some types of online fraud it is difficult to know whether every eventuality of online fraud has been covered in this study. However, the frauds experienced and discussed in this report do cover the broad categories of possessing, making or supplying articles for fraud and confidence fraud.

Very few victims had experienced the apprehension or conviction of the perpetrator for the fraud (although this had occurred in some cases). This meant that few participants could reflect upon the actual sentencing of the fraud they had experienced or engagement with the judicial process and how this may have affected their experiences (which has been found to have an impact for some victims, such as those who have experienced a sexual offence; McNaughton Nicholls et al., 2012).

The research was broad in scope and aim, and with the resources and timetable available the aim was to achieve as much diversity within the sample as possible. It was not possible to segment the sample and meaningfully explore differences between types of fraud experience or the characteristic of victims, however.

In addition, opt in approaches can lead to self-selection bias as participants' decision to participate may be correlated with certain traits. Although the sample was monitored across key sampling criteria to ensure diversity in terms of, for example, age, gender and type of fraud experienced, some characteristics may have been better represented than others. Of note certain groups may be under-represented in the sample, such as young people under the age of 25. We also do not discuss differences along the lines of characteristics such as gender, ethnicity, or disability as there was not scope to include sufficient numbers in the sample to meaningfully explore experiences across these dimensions of participant's identity. Although participants who felt their financial literacy, and use of the internet was fairly low are included in the sample, they are also less represented than those with higher levels of reported financial literacy or internet usage.

1.7 Report structure

In chapter two, key findings from the evidence review and some of the findings from the stakeholder interviews are presented to set the context of the research. This includes outlining what is already known about the types of online fraud that exist, how it is committed, and a description of the concepts and processes of relevance when sentencing fraud offences (seriousness, harm, culpability, and aggravating and mitigating factors, and the range of sanctions available).

In the remaining chapters the findings from the interviews and focus groups with victims of online fraud are presented. Where relevant, data from the stakeholder interviews and evidence review is also drawn upon. In **chapter three** we explore the experience of online fraud by people directly affected by it. **Chapter four** focuses on the impact of online fraud on the victims involved. In **chapter five** we explore participants' attitudes to sentencing issues that relate to the online fraud offences in focus – namely culpability, seriousness and harm, and aggravating and mitigating factors. This chapter also explores participants' views on the different sanction options for different fraud offences, and looks at the perceived difference between online versus offline fraud.

Case studies and quotes are used throughout the report to illustrate key findings from the perspective of the participants. Names and identifying features of participants have been altered to protect their anonymity.

2. Context

To inform the research objectives a review of existing literature and evidence was conducted as phase one of the study. Interviews were then conducted with key stakeholders involved professionally in addressing or responding to fraud offences. Key findings to emerge from these two phases are presented in this chapter. This includes a description of what is already known about how online fraud is committed, who is affected by it, and the impact of fraud generally. Sentencing practice is then discussed to set the context for the remaining chapters of the report and the findings from interviews and focus groups with people who had experienced fraud.

2.1 Types of online fraud and how it is committed

The types of fraud which affect individuals are diverse, and the evidence base indicates an increasing range of fraud offences and fraud victimisation (OFT, 2006; CIFAS, 2012). As described in the previous chapter, recent research has shown how certain types of fraud are increasing, especially over the internet. However, it was clear from the evidence review that some types of online fraud can be considered developments of 'traditional' offline fraud methods that have been adapted to take advantage of computer mediated communication (CMC). This was reiterated by stakeholders who spoke, for example, about how fraudsters were now making use of online dating sites to commit romance scams, where previously they may have met via newspaper dating advertisements and communicated by letter with their victim. At the same time, there are also some new emerging ways in which fraud can be enabled specific to online fraud – and these are highlighted and discussed below.

Different examples of the two types of fraud which are the focus of this research are listed below. Most of these types of fraud are commonly discussed in the literature, and can be committed using both offline and online means.

Confidence fraud:

- **mass marketing fraud**: this is *"a misleading or deceptive business practice where you receive an unsolicited or uninvited contact and false promises are made to con you out of money"* (OFT, 2006:12, cited in Button et al., 2009a). It can occur both online and via other types of contact such as telephone or letter. The evidence review and stakeholder interviews highlighted the diverse ways in which it can be committed including bogus products and services, online auction sites where the goods do not arrive or are sub-standard, clairvoyant and psychic scams (paying premium rates for a bogus 'fortune telling'), inheritance scams, bogus holiday club scams, career opportunity and 'dream job' scams (where victims pay a registration fee for a job opportunity which does not exist) and loan scams. Advance fee fraud involves potential victims being approached by letter, faxes, or email without prior contact with the fraudster. The correspondence typically describes the need to move funds out of a country, weaves a lengthy story as to why they require the help of the individual they have contacted and contains promises that any help received will be paid for.

- **online romance scams:** to commit online romance fraud scammers create fictional online dating accounts and on making contact groom their victims into believing they have strong feelings for them, with the intent of securing financial gain from the victim by asking them to send money (an 'advance fee') to cover some activity or crisis (Consumer Direct, n.d., in Button et al., 2009a; Rege, 2009). Stakeholders described how perpetrators used various strategies to avoid detection, such as asking to move their contact onto MSN which is unmonitored. Stakeholders also described cases where romance scam fraudsters were using

technology such as webcams, asking victims to send them recordings of intimate acts which they then use for extortion purposes.

- **investment fraud**: this type of fraud is also known as 'boiler room' fraud. The term boiler room was coined to refer to a rented space from which scammers called hundreds of potential victims each day, using high pressure sales techniques (Metropolitan Police, n.d: 10). Types of fraud falling under this category include high risk investments, property investment schemes, Ponzi,[16] and Market Abuse[17] (Button et al., 2009a). Stakeholders described how perpetrators of this type of fraud sometimes cloned legitimate companies so that when the 'victim' searches for the company on the internet they believe that it actually exists. Though the telephone is often still used to contact victims for these types of scams, the internet is increasingly used as an enabling tool to provide a veneer of legitimacy for the fraud.

Possessing, making or supplying articles for use in fraud:

- **'articles'** include any electronic programs or data stored electronically. Examples of articles for use in fraud identified in the evidence review included false fronts for cash machines, computer programs for generating credit card numbers, lists of credit card or bank account details, 'Sucker Lists'[18] and draft letters or emails for use in advance fee fraud. As lists of credit card and bank account details constitute 'articles', the making of such lists are part of this offence. As people increasingly hold a main bank account online, this includes details of online bank accounts. Stakeholders described how organised criminals could place their 'own people' in legitimate businesses such as call centres to access such information, and corrupt existing professionals already in employment. Stakeholders also described how lists of contact details or personal information are also sold by both legitimate and illegitimate organisations to facilitate fraud.

- the evidence review found that processes such as phishing,[19] pharming,[20] skimming[21] and the use of malware[22] may facilitate fraud being carried out online. For example, such processes are used to gather personal information automatically online which can then be sold (see above) and used to facilitate mass marketing scams or used by the perpetrator to commit identity fraud. Identity fraud is *"the unlawful use of another person's personal identifying information"* (Piquero et al., 2011: 438). It may relate to a gain being made from stealing someone else's identity to access their bank account, or creating a fictitious identity to engage in criminal acts (Pontell, 2009) such as forging a medical diploma (Koops et al., 2009). Identity fraud may be used for account takeover, credit card fraud, utilities fraud, banking fraud, retail fraud (buying items under another person's name or credit) all of which are now possible online.

---

16 Ponzi schemes are investment operations that pay returns and redemptions to early investors, not from profits but from money from subsequent investors (Lewis, 2010).

17 Market Abuse involves manipulating the price of legitimate stocks which are traded through the main stock markets, so that stocks which victims will have paid a premium for lose their value.

18 Lists of people who have already fallen for a scam can be sold on the black market for a greater value and are known as 'Sucker Lists'. This term is felt to be offensive by victims and victim support organisations.

19 Phishing is when consumers are tricked into transmitting financial information to a fraudulent website where the information is later housed for use in fraudulent activities (Rogers 2007; Wall 2007).

20 By accessing victims' computer systems via hacking or malware, pharming can also take place whereby software redirects victims to fake websites where they enter their details.

21 Skimming is a common way to steal identities and credit card information. Machines can be bought online and people use these to 'skim' all the personal information when someone pays using their card.

22 Malware is the term used to describe the event when malicious software such as viruses are used/installed on computers and alter functions within programs and files (Bossler and Holt, 2009; Johnson, 2010; Webb, 2010).

Stakeholders also reported that facility take over fraud is also rising. This is when the perpetrator takes control over an existing account or policy and uses it for their own benefit.

The evidence review also highlighted a number of emerging types of fraud or techniques that enable fraud. These included:

- SMiShing (personal information obtained via SMS);
- Vishing (personal information obtained via phone);
- Malware used to collect personal information via Smartphones;
- Spear-phishing (highly targeted spam);
- Koobface on social media (where victims are sent messages via their social media site with a virus);
- Social phishing (whereby the perpetrator gains the trust of an individual and accesses their friend list or as a phisher gains unauthorised access to a user's account and starts sending spam to the user's direct contacts);
- keylogging viruses: these viruses capture login details or passwords for bank accounts, for example, which can then be used or sold for profit (Fraud Advisory Panel, 2009 cited in Hache and Ryder, 2011);
- fraud in virtual platforms such as 'Second Life[23]'; and
- online rental scams (whereby fake rental flats are advertised online and victims send personal information and/or deposit payments to prove they can pay the rent).

Stakeholders spoke of how fraudsters continue to compete to develop new ways in which online fraud can be committed, and the authorities are continually trying to identify all of these new methods. For example, there was a view among stakeholders that as Nigerian 419 frauds[24] had become more commonplace and potential victims became more aware of this type of fraud, perpetrators were now pitching inheritance scams instead.

The evidence review indicated that some perpetrators, especially those situated abroad would be unlikely to face prosecution within the jurisdiction of the country of the victim. While this is the case, stakeholders also described how they are now aware of perpetrators basing themselves in the UK, after possibly learning how to conduct online fraud abroad.

In addition, the literature indicated low levels of fraud being reported to the police. One study in the UK illustrated that only 44 per cent of 655 victims surveyed had reported the fraud to the police (Goucher, 2010). Low levels of reporting were partly explained by feelings of self-blame and Schichor et al. (2000), suggested that victims of fraud may experience more self-blame than those who had been victims of street crimes. These feelings are underpinned by a number of factors, including the perceived 'shame' and embarrassment of feeling 'sucked in' or taken in by offenders, and victims blaming themselves for not being informed enough before falling for the scam. These feelings were seen to play a pivotal part in the underreporting of online fraud, as victims fear criticism from family members and authorities (Croall, 2008; Webb, 2010; Hache and Ryder, 2011).

Lastly, while the literature indicated that there does not appear to be a typical fraud victim, the OFT (2009) report concluded that 'almost all authors' agree that differences exist at the demographic level in terms of vulnerability to fraud with the elderly, less well educated, and

[23] An online gaming platform whereby players take the role of avatars 'living' in the platform. Second Life currency can be bought using real currency and used to purchase 'virtual' goods or services in Second Life.

[24] Nigerian 419 scams are a type of advance fee fraud that originated in Nigeria. There are many variations of this type of fraud and they usually involve the perpetrator offering the potential victim a large sum of money which they want to transfer out of their country.

socially isolated being particularly vulnerable. Those falling for different kinds of frauds do share some similar characteristics, however, victim profiles may be influenced by the amount certain groups are targeted and this may play as much a role in a victim profile than certain groups actually being more susceptible to fraud. Button et al (2009c) for example, drawing on data from the OFT (2006) indicated that women are most likely to fall for: internet matrix scams (free gifts are offered via adverts on the web, and after buying a gift the victim goes on a waiting list to receive another gift once a set number of others have signed up, but there are always more members than gifts and they will not receive the value of their contribution back); miracle health and slimming scams; clairvoyant and psychic scams; and career opportunity scams.

Men are more likely to fall for advance fee fraud, internet dialler scams,[25] high risk investments, and fake property investments. Button et al. (2009c) also indicated that older people are most likely to fall for high risk investments and doorstep service providers; while young people are most likely to fall for work at home scams, clairvoyant and psychic scams, and internet dialler scams. Collectively these scams cover a wide range of confidence fraud, indicating a range of people can fall victim to fraud more generally.

2.2 Emerging internet fraud

Whilst it was clear from both the evidence review and the interviews with stakeholders that cyber-crime is recognised as a growing area, as mentioned above, the frauds described are not always new in themselves, but can represent 'old' techniques that have been developed and enabled in new ways by computer mediated communication. As noted in the evidence review, and observed by stakeholders, this changes their complexion and the potential reach to victims that perpetrators have, but does not necessarily fundamentally change the motivations and outcomes.

> *"With new technology you can reach millions of people at almost no cost, and therefore you set your net widely to find those who are susceptible to fraud" (Stakeholder)*

Many internet scams take place without the victim even knowing (Metropolitan Police, n.d) and they may remain unaware of the fraud being committed for a long period of time. For example, Farley and Wang (2009) describe surveillance spyware as a common derivative of malware. They explain how it is designed to export data and statistics from a victim to an attacker. Variants of such spyware are able to provide the fraudster with audio and video surveillance through peripherals such as microphones and web-cams, all of which the victim may not be aware of. Small amounts may also be taken out of bank accounts without victims noticing for long periods (known as smurfing; Tupman, 2010).

Social networking sites and virtual worlds were particularly highlighted in the evidence review as providing a broad arena for new variations of existing fraud and new emerging types of both confidence fraud and possessing, making or supplying articles for use in fraud. Examples included:

- money laundering in the virtual world;
- impersonating victims through fake accounts on social networking sites; and
- sites and companies impersonating social networking sites such as Facebook (for example Koobface) and LinkedIn and sending phishing emails under these banners.

[25] Internet dialler scams are when the computer settings are changed on a person's computer so their internet connection is re-routed via an expensive telephone line.

In addition, stakeholders spoke about how mobile phones were also providing a new arena for fraud, especially as they were now being used to access bank accounts and they will increasingly replace credit/debit cards and cash. In addition it was also noted how people do not generally have malware protection on their mobile phone (which are now often connected to the internet) which would make them even more susceptible to fraud.

Lastly, there were three main viewpoints among stakeholders around how prevalent online fraud would be in the future. First, stakeholders felt that online fraud may decrease as strategies were put in place to curtail it. However, it was suggested that this could lead to a resurgence of more traditional offline forms of fraud. Secondly, it was suggested that online fraud may increase as people generally placed more of their personal details on social networking sites and more people started using the internet (so opportunities for perpetrators increase).

> *"If you went on some people's Facebook sites or MySpace sites, it will tell you what their interests are, where they live, who their friends are, and if you want to do a confidence trick you need that type of information" (Stakeholder)*

There was also the view among stakeholders that the amount of online fraud generally taking place would remain static, as while people's awareness of how to use the internet safely, and the risk involved, may increase, perpetrators will find new and evolving ways of committing fraud, in response to the public's increased knowledge about their activities.

2.3 Sentencing fraud

Existing evidence on sentencing issues

In the evidence review some issues that may underpin the seriousness and harm of fraud offences and the factors which can mitigate or aggravate an offence were identified from the existing research and discussion on fraud. However, there was very limited literature focusing specifically on sentencing fraud offences.

Aggravating factors identified in the literature focussed on a clear element of planning being evident, including obtaining equipment or software to facilitate the offence. Evidence of a high level of planning was indicated when perpetrators adopted careful perpetration strategies to maximise the likelihood of the fraud being successful, such as appealing to trust and authority via professional or legitimate appearance and the use of legitimate sales techniques. For example Madoff, in the US, (Lewis, 2010a/b), who was sentenced to prison for 150 years in 2008 for securities fraud, had committed fraud over many years and the extensive collusive and planned quality of the fraud was viewed as an aggravating factor.

Stakeholders spoke about how the harm associated with fraud can be difficult to ascertain during the sentencing process. This is because of the wider impacts of harm on the organisations involved. For example the impact of identity theft and credit card fraud on people's confidence in using the internet for online transactions, and on the wider economy more generally, in terms of the amount of tax loss through fraudulent activities and the impacts on organisations such as banks when they paid victims for money lost, especially during times of recession.

> *"We're in a recession but then banks have to pay out money, they're losing money to fraudsters, telecoms companies are losing money to fraudsters, that's not helping recovery. How much money goes out of organisations in fraud losses which would then be subject to taxation? I think one of the guys here a few years ago tried to do a calculation about the number of hospitals that could have been funded by the amount of tax that would have been paid on the money lost to fraudsters. Yeah, there's those knock on effects" (Stakeholder)*

There was also evidence in the literature of some degree of perceived victim responsibility for the fraud experienced. For example, victims being careless with their personal information, thinking that they are entering into illegitimate activities such as money laundering for personal gain (Button et al., 2009a), or being aware that the advance fee fraud is a 'gamble' (OFT, 2009). As already discussed in the section above, victims blaming themselves for the fraud can explain low levels of reporting and additional harmful impacts. Goucher (2010) for example, notes that victims feel, and are often perceived by others to be, 'culpable' or 'stupid' for being taken in by the fraud. They are reluctant to report the fraud due to: the low value of the fraud; self-blame; belief the perpetrator cannot get caught; and not wanting to be labelled by themselves or others as a victim.

Research focusing on perpetrators' perceptions of the seriousness and harm associated with online fraud indicate that they are better able to find ways to justify the offence to themselves than if the offence had been committed face-to-face (Copes and Vieraitis; 2009a/b). Copes and Vieraitis (2009a/b) noted in their research, which involved interviewing people convicted of fraud offences in the US, that they minimised their actions by blaming the victim or highlighting that they would not have 'physically' harmed their victim.

Lastly, the literature identified that such a wide range of perpetrator types and locations makes identification and prosecution difficult. Perpetrators can range from organised criminal gangs (Gannon and Doig, 2010; Pontell, 2009; Hutchings and Hayes, 2009; Gordon et al., 2007), to middle class perpetrators attempting to maintain their lifestyle in the face of financial difficulty (Copes and Vieraitis, 2009b), and drug users conducting fraud to fund their addiction (Copes and Vieraitis, 2009b; Pontell, 2009). As discussed above, as the internet has global reach, the location of perpetrators of online fraud can be difficult to ascertain.

There is also evidence of people without criminal records being recruited to assist fraud perpetrators, sometimes without knowledge of the illegality of their acts. Students were highlighted by stakeholders as being one such population group that might be targeted to assist with fraudulent activities because they may be in need of an income and may also be financially naïve. This was confirmed in the evidence review which found that students are targeted to become 'money mules' for fraud operations whereby they set up a legitimate bank account that can be used to transfer money gained via fraud out of the country (CIFAS, 2012).

2.4 Summary

A range of different types of frauds which can be committed or enabled via online communication have been described in this chapter. Although the internet has provided a new way to reach potential victims and access information with which to commit fraud, the frauds committed can also be similar to those that have traditionally been committed offline. Research on sentencing fraud offences is very limited, but available research highlights perpetrators' various motivations for committing fraud, and the ways in which they justify their actions in an attempt to mitigate them.

Having used the findings from the evidence review and stakeholder interviews to set the research with people who had experienced fraud in context, we now move on to describe the range of frauds experienced by participants and the methods perpetrators used in order to carry them out.

3. Experiences of online fraud

A specific aim of the research was to review the ways in which online fraud is currently committed, and describe and present participants' experiences of online fraud. This chapter presents the findings from the interviews and focus groups where participants were asked to give an overview of the fraud they had experienced. First, the chapter outlines the types of fraud experienced by participants in relation to possessing, making or supplying articles for use in fraud and confidence fraud. It then turns to look at the profiles of the victims and the extent of victims' understanding of how the fraud they had experienced had occurred. Findings from the evidence review and stakeholder interviews are drawn upon in this section to help infer how the fraud experienced by participants took place, as participants were often unaware of the 'inner workings' of an online fraud. Finally, the chapter concludes by specifically describing the role the internet played in the fraud experienced.

3.1 Fraud experienced by participants

Reflecting the diverse and evolving nature of online fraud, a wide variety of fraud had been experienced among participants who took part in an interview or a focus group for the study. The fraud reported highlighted the sophisticated ways in which confidence fraud and possessing, making or supplying articles for use in fraud is being carried out and the role the internet is playing in their implementation. Participants' narratives and the group discussions suggested that where a successful fraud had occurred, this usually involved an overlap between the two categories of possessing, making or supplying articles for use in fraud and confidence fraud.

For example, whilst receiving phishing emails indicated that email addresses had been sold or used (articles for use in fraud), and this was commonplace, a fraud only occurred if these emails were then responded to. The fraud could then fall into the confidence fraud category as the victim believes the opportunity they are responding to is genuine. Similarly, articles for use in fraud were required to set up false websites but only if people were convinced by them and transferred money did a fraud occur. In addition, participant experiences also suggested that a number of different fraudulent activities were in some cases used to render the fraud successful.

Possessing, making or supplying articles for use in fraud

The types of frauds participants described that fell within this category of offence type included:

- personal identity or information being used by others to purchase goods or services online;
- computer viruses, spam and phishing emails being sent to them; and
- accessing fake websites.

Examples of personal information being used fraudulently included people's credit or debit card details being obtained and used by perpetrators to attempt to purchase goods online or for online gambling or where mobile phone contracts had been taken out in participants' names.

In relation to computer viruses, there were instances where viruses had completely corrupted participants' computers and in some cases the computer hardware as well, such as DVD drives. Viruses are used to 'infect' computers with software that can then be used by fraudsters to collect personal information stored or when accessed by individuals online. Viruses can also be used to generate spam emails aimed at participants or send spam to everyone on their contact lists; keylogging viruses capture login details which are then sold on for profit. Case study 3.1 below outlines one experience of receiving what turned out to be a fraudulent spam email which also infected the participant's PC with a virus:

Case study 3.1: Interview participant
Spam email and virus

Tom, a middle-aged married man with children, regularly used the internet. He had recently experienced a virus on his laptop at home. One morning when he switched on his laptop, he was faced with a message which read '[name of local police], you are in violation of a Great Britain law for looking at illegal child abuse images ('child porn')'. The message went on to explain how if he paid a £100 fine then no further action would be taken. Tom had not been accessing illegal pornography but was going to pay the fine due to the concern he had that further action would be taken regardless. He became suspicious however and reported it to the fraud department at the local police. He found his laptop had also been infected with a virus when he had opened the fraudulent email, which took a great deal of time and effort to remove. Tom felt this was annoying, but the email accusing him of accessing illegal pornography had a particularly negative impact:

> *"The other viruses, they were annoying as well but they hadn't got that shock element 'cause they didn't involve the police. They didn't involve being accused of child porn."*

Spam emails constitute material used to commit fraud, and fraudsters must also have access to email addresses or use software that automatically sends them via viruses to be able to successfully send spam. The spam emails may themselves contain viruses or be offering fraudulent goods or services. Interview and focus group participants who had received spam/fraudulent emails emphasised their legitimate and professional looking façade. The spam emails usually appeared to them to have been sent by a range of individuals and organisations they were familiar with, for example friends, lottery companies (for attempted gambling scams), the police, government departments, financial institutions and e-commerce businesses.

Finally, interview and focus group participants spoke about having accessed fake websites, which again appeared legitimate but were actually being run for fraudulent means. Examples included financial websites which pretended to be well known banks, an auction website where people could buy goods, a website offering job opportunities and a website claiming to be a well-known computer provider. Whilst these websites could constitute articles used to commit fraud, those participants who proceeded to then exchange money as a result of using the websites had consequently become victims of a confidence fraud, illustrating how a number of different fraudulent activities were used in the overall fraud experienced. Confidence fraud is discussed in the next section.

Confidence fraud

The types of confidence fraud that interview and focus group participants had experienced fell into three broad categories: mass marketing fraud; investment fraud; and dating and romance scams.

Many variations of mass marketing online fraud were reported, the common element of most being that participants had exchanged money with a perpetrator for goods or services which never arrived or which were faulty or counterfeit. In relation to goods, participants had paid for telephones, unlocking mobile telephone software, electrical items, tickets for concerts and sporting events, a mobility scooter and gold, which they had never received. There were also instances where goods had been received, but fell far short of participants' expectations. Examples of services which were never received included instances of people paying advance fees for career opportunities (which turned out to be fake) or signing up to 'free' trials of websites which they had subsequently been unable to cancel and thereby had money withdrawn from their accounts.

There were also instances of mass marketing fraud where participants had become victims not by attempting to buy goods, but by attempting to sell them using marketplace websites. In these cases, the goods were quickly collected by someone, face-to-face, but the participants had never received payment for the goods, which was apparently being transferred online.

As well as variations in the type of mass marketing fraud experienced, there were also variations in the ways that these frauds had been committed. In some instances, the internet was integral, with participants purchasing goods either from the types of fraudulent websites described previously, and in case study 3.2 below, or through legitimate websites which sell goods. There were also cases where participants had been specifically targeted by fraudsters who had attempted to commit mass marketing fraud against them by initially approaching them using the telephone before moving the fraud online. An example of this was where participants had received a telephone call from a person who claimed to be from a large computer manufacturer who said that they could fix 'errors' on their computers in return for either a payment or giving the perpetrator access to their computer by clicking on a website link. Some participants had completed this action. Fraud falling into the category of mass marketing fraud is discussed more fully in case study 3.2 below.

Case study 3.2: Interview participant
Mass marketing fraud

Mary, a middle-aged married woman with children, regularly used the internet for online shopping and researching topics of interest. She wanted to buy a satellite navigation system and did a Google search on 'tom tom'. She clicked on the link for a bidding site which was selling a 'tom tom' and bought £15 worth of points so she could try and bid for one. The website looked legitimate, especially as it had the PayPal logo on display and she was used to buying items using other well-known bidding sites. When she had almost won the item her computer froze. When she refreshed her screen she had to start bidding for the item again. In the end she lost £26 before realising that the website was fraudulent.

> *"It looked like… I won… then my computer froze and I had to refresh the page and when I refreshed it again there was five minutes left to the end of the auction. So yeah I was like a winner and then I wasn't a winner at the same time."*

The other two broad types of confidence fraud interview participants described were investment fraud and dating/romance scams. Common to both of these types of fraud was that, in some instances, the participants had been promised some sort of financial gain but needed to exchange considerable amounts of money in order to receive this gain. Both types of fraud also involved repeated communication between the perpetrator and victim, however, romance/dating scams were very personal, as opposed to professional in the nature of their communication.

An example of investment fraud included an African share investment fraud where the perpetrator emailed the participant to let them know that a previous investment they had made had resulted in a large profit. However, in order to release the funds the participant was told to send a series of financial payments.

Participants who had experienced romance scams met the perpetrator through online dating sites. They had then been asked to send money to the perpetrator for various fabricated reasons. For example, they had been told that they needed to send a sum of money to release the perpetrator's luggage which had been impounded and in turn contained a large sum of money that could be used to pay them back.

3.2 Who experiences online fraud?

The varied profile of people taking part in the study in terms of gender, age, employment status, and health status (Tables 1.1 and 1.2 in Chapter 1), suggests that online fraud affects a diverse range of people. The profile of participants also indicates that online fraud not only affected those who were infrequent or inexperienced users of the internet but also frequent, experienced users (Tables A.2 and A.7 in Appendix A), and can affect a diverse range of people in terms of financial literacy (Tables A.3 and A.8 in Appendix A).

Evidence from participants suggested a degree of subjectivity as to whether they regarded themselves as a 'victim' of online fraud however. They may consider the term 'victim' to denote that a serious crime has been committed, when some participants felt that low value online fraud (such as buying a ticket that does not arrive) was a 'day-to-day' risk they faced, an inevitability at some point, but not something that had greatly affected them. There were conversely participants across the focus groups and interviews who had not actually exchanged money as part of their experience of the fraud, but who nevertheless felt that they were a victim – for example their personal information had been obtained and used by someone else even if the actual fraudulent transaction was prevented.

There was also variation in the personal characteristics that could be instrumental in creating a victim's vulnerability. It was evident in some cases the characteristic which made a participant vulnerable to the fraud was also part of the explanation for why they had become victim of this specific offence. A focus group participant, for example, described how she had fallen for a career opportunity scam because she had just arrived in the UK from overseas and was looking for a job and a regular income. She responded to an online advert for work and paid a registration fee upfront because she was not familiar with the way in which people seek jobs in this country. She did not think she would have been vulnerable to such a fraud in her own country, or other types of fraud in the UK, but had been very keen to find work.

Therefore the range of types of fraud being committed played on various potential vulnerabilities people may have, and target different 'weak spots' depending on an individual's own circumstances. There was not one particular characteristic or circumstance that made a participant vulnerable to fraud or likely to be targeted *per se*. Rather a fraud was rendered 'successful' when the type of fraud matched a potential victim's specific vulnerability. The range and diversity of different types of online fraud that can occur means that everyone who uses the internet, technically, has some risk of experiencing online fraud. Issues of vulnerability are discussed in more detail in chapter 5.

3.3 The reasons for the fraud occurring

The extent to which interview and focus group participants were aware of how a fraud against them had been perpetrated varied. However, whilst a fraud may have appeared *ad hoc* or opportunistic to the participant, in fact what they experienced were often classic cases of highly organised, common frauds. In other words, although the participants may have felt the fraud was opportunistic in nature, their description of it bore the hallmarks of common types of fraud identified in the literature and by stakeholders. This section therefore first presents the reasons given by participants for the fraud occurring before moving on to consider the extent to which this fitted a recognised type of fraud, drawing on data from the evidence review and interviews with stakeholders.

Participants' views on how fraud occurs

Generally speaking, participants who had experienced confidence fraud were usually able to explain how the fraud had occurred. The realisation that they had been defrauded occurred at the point where the goods or services they had purchased did not arrive or were faulty, and the seller was unresponsive to their communications. Participants who were victims of

offences where articles had been used tended to have less awareness of how the fraud had occurred, even after it had happened:

> *"I was like, 'How did this [attempted bank account fraud] happen?'; like how do they get my details because I don't get how this happens" (Interview participant)*

There were also participants who were able to explain the workings of more complex frauds, as illustrated by case study 3.3 below, and this could help them to avoid falling for the fraud and exchanging money. In these cases, however, they usually had expert knowledge of the area that led to them being confident in rejecting the fraudsters' claims:

Case study 3.3: Interview participant
Malware

Bob, a middle aged man, had experience of working with computers. He recently received a telephone call from an individual claiming to be calling from a well-known computer company. Bob was told that his computer was running slowly, that he had been placed on a temporary server and that he would be disconnected if he did not follow the instructions given to him. The caller directed Bob to a file on his computer with lots of warning messages and told him that he had a computer virus. The caller then told him that he needed to log onto a website so that the computer company could gain remote access to his computer. Bob suspected that this was fraudulent activity and put the telephone down. Other participants had experienced similar contact but had allowed access to their computers and/or paid for fake 'software protection' cover to 'prevent' the same bogus problem occurring. Again the fraud was enabled by fraudsters trying to present a legitimate veneer, presenting normal files as 'problem malware' to unsuspecting individuals, as Bob explained:

> *"All they do is direct you to this one file, Windows Event… and [say] 'Look at all those warning messages, that's malware or viruses on your computer… these normal windows procedure failures, they claim are malware based".*

The participants were not familiar with existing literature on online fraud, but their descriptions of the fraud they experienced often matched those types of fraud outlined in literature from both the UK and US. Table 3.1 below is used to illustrate some examples of this. This is not a comprehensive list of all the fraud experienced by participants, or found in the literature, but gives examples of how some frauds that are commonly discussed in the literature were experienced by participants and enabled online.

Table 3.1 Examples of ways of perpetrating fraud online experienced by participants

Type of fraud participants experienced	Literature that refers to this fraud	How the internet enables this fraud
Phishing – participant had been sent an email asking them to pay their tax return. The link to the website took them to what appeared to be a legitimate HMRC website through which to make payment	Rogers 2007; Wall 2007	Phishing is conducted via websites and email contact. Can be used to infect computers with malware and automatically 'harvest' personal information
Spoof/fake websites – participants had bought a mobility scooter, or mobile phones via what appeared to be genuine websites, but goods never arrived	Webb, 2010	Stakeholders described how such websites could be used to provide a fake 'veneer' for a fraudulent company

Type of fraud participants experienced	Literature that refers to this fraud	How the internet enables this fraud
Malware – participants found their computers had been infected with malware after opening emails, which themselves may have been frauds (i.e. asking them to pay a fine)	Bossler and Holt 2009; Johnson, 2010; Webb, 2010	Malware can be covertly downloaded onto PCs/laptops and collect personal information or access accounts without victims knowing
Romance scams – participants had met the perpetrator on an online dating site. After repeated communication over a few months they had been asked to send money for a specific purpose such as to release baggage which the perpetrator claimed had been impounded	Button et al., 2009a; Rege, 2009; Whitty and Buchanan, 2012	Romance scams play on a number of perpetration strategies, gaining the trust of victims in the belief they are entering into a real relationship over many months or years. A number of means of communication may be used though they may have met online (on dating sites, with fake profiles) and the perpetrator may begin by asking for small monetary amounts and then increase it over time

3.4 Perpetration techniques

Participants' descriptions across the interviews and focus groups of how the fraud occurred illustrated a range of techniques which perpetrators had used in order to maximise the effectiveness of the fraud, which also mirrored those identified in the existing literature. We have categorised these as six cross cutting techniques that enabled online fraud, which are described below:

- **visceral appeals:** such appeals had been experienced by participants, emotionally. They include, for example, richly descriptive accounts of a potential romantic relationship, or how their lifestyle could change with financial security, via a lottery win:

  "They completely inundate you with it [the emails making promises of future wealth] and you're very tempted, in moments of weakness, to fall for it, and you think that it's going to happen" (Interview participant)

  Stakeholders also noted how perpetrators exploit emotions such as embarrassment, in creating scams which are unlikely to be reported to the authorities. The examples they described included a parent paying for a photo shoot for their child to become a model and then not hearing from the 'agency' again, or people paying a fee to register on a fake escort website.

- **pressure and coercion:** such techniques were intended to pressurise the participants so that they complied with the fraud. Examples reported by participants included receiving threats from the perpetrator, or being made to feel responsible for solving a specific problem the perpetrator had. The quote below is from a participant who was pressurised into paying for a bogus travel ticket, without which the perpetrator made them believe they would be stranded:

  "…and then the person that I was giving the money to… I think in the end he made you feel responsible for it all, because… He still kept telling me he wanted to go home to his family. He hadn't been home to [name of country] for months and months, and you felt that you were

holding him up from getting home as well… you felt responsible for him as well… It was sort of put onto you that if you didn't do this, and he couldn't get home… you felt as though it was your fault in the end, you know" (Interview participant)

- **carrot and stick**: perpetrators used a carrot and stick approach and had lured participants with the promise of a positive reward or a negative scenario which they would wish to avoid. An example of a positive reward was financial gain, as described above, through a lottery win or job:

  "You've had that big carrot dangled in front of you and you thought you were going to make some money to live an easy life. But there's no such thing as a free lunch" (Interview participant)

  An example of a negative scenario (stick) would be a participant being sent an email ostensibly claiming to be from the police and accusing them of accessing illegal images online. They were asked to pay a fine or face legal action, but the email was fake. Such strategies are also coercive, as detailed above.

- **authority and legitimacy**: perpetrators tapped into participants' need to find the fraud legitimate by assuming a professional or legitimate façade. This was achieved by having a professional looking website and making reference to well known legitimate companies and/or by having a 'real person' available to speak to the participant in order to reassure them every time they made contact via a telephone number on the website. Appearing legitimate was also facilitated by the perpetrator using legitimate third party agencies to enable the fraud, such as well-known auction or social networking sites.

- **disproportionate relation between size of alleged reward and cost of obtaining it ('too good to be true')**: on entering into the fraud, participants had felt that they were getting a 'good deal' and would come out of the experience better off. In one example, the participant had initially agreed to pay £125 for a deposit for a phone but then the 'seller' had told him to pay just £50:

  "Initially, he (the perpetrator) said, oh, send me half, I think it was £125, and I thought, I would have done that, but then he said, I'll tell you what, look, just send me £50, I don't want to mess you around, just send me £50, and once the phone arrives, then as long as you're happy with it, send me the rest. You've got my address, I've got your address and details, and everything like that, and let's just do it sensibly. So, you know, it was only £50; I took a bit of a punt on it. Low and behold, obviously the phone never turned up" (Interview participant)

- **grooming:** lastly participants described how a process of grooming had taken place during the fraudulent activity that led to the victim investing 'trust' in the perpetrator. For example, in the stakeholder interviews it was described how in some romance scams, perpetrators initially sent small gifts to the victim to gain their trust before asking for small and then larger amounts of money to test whether the grooming process had been successful:

  "…there's a testing to start with, small amounts just to test, test to see if the grooming is sufficient or more work needs to be done on behalf of the fraudster" (Stakeholder).

Multiple perpetration techniques were often used in the completion of a successful fraud. For example, a perpetrator may have both groomed a participant (praising their investment skills in the case of investment fraud or sending them romantic messages and e-cards in romance scams) and used legitimacy (presenting themselves as a bank manager or other professional person) to try to gain their trust. They may then have also used a 'carrot' of offering financial gain to the victim, while also playing on visceral cues, outlining the way in which the financial gain they were offering would change the participant's life, before the participant made the decision to transfer a large sum of money to them.

3.5 The internet as a fraud enabling tool

The frauds experienced across interview and focus group participants involved a range of types of contact between the participants and the perpetrators. The internet played one of three roles to facilitate the fraud, described below:

- **the central medium for the fraud occurring**: for some participants the fraud had taken place solely over the internet. Examples are consumer fraud when, for example, participants transferred money for goods which they never received, and credit and debit card fraud:

  "The availability of products over the internet and the availability of that data via various forums over the internet does seem to have changed the model for fraudsters to commit ID fraud" (Stakeholder)

- **as a form of communication alongside other methods:** in some cases the perpetrator had used the internet as a way to communicate with participants alongside other means of communication. This may have included telephone calls and physical contact to help create a façade that the fraud was legitimate. Perpetrators had made use of other methods to reassure participants that they were legitimate and to avoid detection. A participant who had experienced online fraud whereby money was being taken out of their bank account also had their telephone diverted by the perpetrator. The intention was that when the bank tried to make contact with her regarding unusual outgoings on her account, they would speak directly to the perpetrator and she would remain unaware of the fraud.

- **as an enabling tool:** lastly, for some participants the internet had been used as an enabling tool. The internet was used to lure the participant in rather than to actually commit the fraud. For example, stakeholders explained that perpetrators would set up legitimate looking websites that they could direct people to as part of their veneer of legitimacy before asking for their investment.

Participants described the internet as a 'normal' form of communication that they had to use in everyday life. Therefore they felt it was difficult to avoid being a potential victim of online fraud, especially given the sophisticated perpetration strategies used, as described above.

3.6 Degrees of legitimacy

As well as variations in the mediums used to perpetrate fraud, in which the internet now plays a pivotal role, there were also variations in the degree to which the perpetrators worked through legitimate organisations as third parties or cloned legitimate professional identities to perpetrate the fraud.

Stakeholders noted how perpetrators set up fake organisations that appeared exactly the same as 'genuine' online companies and even operated within a 'grey area' whereby some aspects of the fraud were legitimate. Some of the fraud participants experienced online, for example, had included a legitimate financial third party that had processed participants'

payments for the perpetrator. At other times, the perpetrator had made use of legitimate sites in order to commit the fraud, for example selling and buying goods via sites such as eBay.

3.7 Summary

Reflecting the diverse and evolving nature of online fraud, a wide variety of frauds had been experienced by participants taking part in focus groups and individual interviews. These highlighted the sophisticated ways in which confidence fraud and possessing, making or supplying articles for use in fraud are being carried out, and the role of the internet in their evolution. Where successful fraud had occurred, this usually involved an overlap between the two offence types which are the focus of this study. Although not all participants were able to describe the inner workings of the fraud, their accounts indicated highly organised, processes and a range of well-known perpetration strategies at play.

The centrality of the internet to the frauds experienced varied. In some cases it was the central medium for the fraud occurring, in others it was used alongside other methods of communication, to create the impression that the fraud was genuine (legitimacy) or as an enabling tool to lure the victim in (such as a website being seen as evidence the fraudulent goods were real).

4. Impact of online fraud

An aim of the research was to explore the impact of online enabled fraud on those directly affected by it. This chapter first summarises the main types of impacts identified in the literature and stakeholder interviews and then maps and describes the range of impacts that were reported by participants in this study.

4.1 The impact of fraud – findings from the evidence review and stakeholder interviews

In this section the impacts of fraud identified via the evidence review and stakeholder interviews are summarised. This sets the context for exploring how participants in this research described the impact of online fraud. The main types of impacts associated with being a victim of fraud identified in the literature and stakeholder interviews were: financial impacts, emotional and psychological impacts; impacts on reputation and social standing; impacts on personal relationships; impacts on physical safety and health; and, wider impacts more generally.

It was clear from the evidence review that financial impacts were viewed as being the most significant for victims of fraud; however, estimates of this vary between authors and countries. For example, the National Consumers League estimates that the average victim of romance scams lost $3000 in 2007 and in research for the National Fraud Authority and ACPO just under 40 percent had lost between £1k and £10k and a further 14 percent between £10k and £50k (Button et al., 2009). Stakeholders noted how at the extreme end of the spectrum of financial impact victims of online fraud sometimes had lost their life savings and/or become bankrupt as a result.

The effect of losing money was often felt to be compounded by the fact that there was little chance of the victim recovering the loss. Cole and Pontell (2006), in their exploration of identity fraud, also make the salient point that the value of the object stolen is generally far less than the value of the goods whose security is endangered by the theft, such as bank accounts and credit ratings. In addition the financial impact may differ depending on the relative financial situation of the victim (Button et al., In press). Secondary impacts of losing money were also noted. Significant here were the time and cost of rectifying financial records following fraud (Pascoe et al., (cited in Button, et al., 2009a), Slosarik, 2002; Smith, 2005; Antokol, 2009), losing businesses and having to enter employment again following retirement (Button et al., 2009a). In addition to these, the literature indicated that victims of internet fraud often do not discover that fraud has been committed until credit is refused or bailiffs call to repossess property (Levi, 2009).

Emotional and psychological impacts were the next most significant impacts reported in the literature. Victims reported feeling angry, stupid, frustrated and distressed. They also lost trust in others, lost their self-esteem, and felt violated. In addition to these feelings, victims also spoke of harbouring deep feelings of shame and embarrassment, which could act as a factor in preventing them from reporting the offence.

For example, Spalek (1999) in a study on the victims of the Maxwell pension fraud found that ‘anger’ was a common emotional impact of the fraud. She also found they suffered stress, anxiety and fear as a result of their loss. A study of victims of a Ponzi scheme found many were afflicted with depression as a consequence (Ganzini et al., 1990). Another common theme amongst victims is self-blame and Schichor et al (2000) suggest that victims of fraud may even experience more self-blame than those who had been victims of street crimes. These feelings rest on a number of factors, including the perceived ‘shame’ and embarrassment of feeling ‘sucked in’ or taken in by offenders and victims blaming

themselves. It is also worth noting that a small number of participants in studies on the impact of fraud reported very little adverse effect.

There have been various cases of identity fraud where an individual's reputation and social standing have been compromised, sometimes as a part of an attempt to acquire money illicitly. This includes instances where false Facebook or Twitter accounts have been created for malicious ends. Notable examples of this include a Dutch prime minister whose account was faked on Twitter and politically inappropriate messages were 'tweeted' under this account, which defamed his reputation (Tsoutsanis, 2012). The stolen identity may also be used to commit additional criminal acts, which are then linked to the victim of the identity theft.

There was limited coverage in the literature of physical safety and health; however, these are areas of important impact to note. Physical harm to victims tended to be in relation to romance scams. For example, Whitty and Buchanan (2012) argued that an element of sexual abuse may also occur during romance scams – for example, if the victim is asked to make an explicit video and send it to the fraudster who then blackmails them with it. In addition, while much of the literature focuses on the impact of fraud on mental and emotional health, as described above, there is an acknowledgement that mental health issues can have a knock-on effect on physical health (Button et al., 2009a). The limited discussion in the literature focused on physical health conditions precipitated by stress such as skin conditions (Button et al., In press), or, at the most extreme end, victims being closer to death, either as a result of stress and/or suicide attempts. As an example of the latter, Spalek (1999) found in a study on the victims of the Maxwell pension fraud that some victims felt that their husband's deaths were accelerated because of the scam.

That the impact of fraud is not just confined to the victim was evident both from the evidence review and the interviews with stakeholders. In the literature, it was described that being a victim of fraud can jeopardise personal relationships as close relatives come to terms with how their income has was lost (Button et al., 2009a). This was confirmed by stakeholders, who described how victims of fraud often become isolated from their families either because families become suspicious of their behaviour, or because it is family income that has been defrauded.

In relation to wider impacts, there was evidence from the literature that online fraud can undermine the trust people have in institutions and the form of communication that has enabled the fraud i.e. online mediums (Button et al., In Press). In addition to this, stakeholders recognised the wider impacts of fraud across the following three areas: on public confidence in using the internet for online banking and shopping; on the economy in terms of the amount of tax lost and the subsequent wider social harm; and on funding the criminal economy.

4.2 The impact of fraud – findings from victims of fraud

Participants who were victims of fraud described a range of impacts (mirroring those found in the literature) which related to the following aspects of the fraud:

- financial impact and loss (which occurred both with confidence fraud and when articles had been used to commit fraud without participants' knowledge);
- the emotional and psychological implications and the perception and judgement of others;
- impact on personal relationships;
- the time and resources involved in resolving the problems caused by the fraud and their subsequent change in behaviour, specifically regarding how they used the internet;
- wider impact on society and loss of confidence (in institutions, or in the case of confidence fraud, in themselves); and

- the type of support they had received and the outcome of the case.

The impacts described in this chapter could also interact with and compound each other.

4.3 Financial impact and loss

The financial loss experienced by participants ranged from negligible, where the amount of money lost was under £10, to high, where the amount lost totalled hundreds of thousands of pounds. It was clear that financial loss that occurred via online fraud could have both short and long-term financial impacts. The more immediate impacts included those associated with resolving the fraud, such as paying to fix a computer that had been contaminated with a virus, or the costs associated with attending a trial in cases where the perpetrator lived abroad. The more far-reaching impacts tended to occur in cases where the financial loss was greatest, especially in relation to an individual's overall financial solvency. In these cases participants had to cut back on household expenditure by forgoing, for example, trips to visit family, a holiday or home improvements (as is explored in the remainder of this chapter, this could then have secondary impacts such as a feeling of isolation).

The fraud could also make participants more financially risk-averse, which in some instances had a detrimental effect on their ability to generate income in the future. Participants described, for example, that they had abandoned plans to set up a business and invest money, as they had become fearful and distrustful of others following the fraud. Participants who were in debt due to fraud reported being contacted by creditors who charged interest on the money owed, compounding the financial implications. At the most extreme end of the spectrum, a participant was made bankrupt as a result of the money they had lost through an advance fee fraud:

> *"This involvement in fraud, to a certain extent, by these various fraudsters, who are very slick and very professional, forced me into bankruptcy" (Interview participant)*

Losing large sums of money through fraud could have very significant long-term impacts on participants' lives. For example, participants who were past retirement age were forced to return to work indefinitely to be able to pay their bills, or had to remortgage their house. As will be discussed in chapter five, it is also important to note that the impact of actual loss versus relative loss is determined by the individual's own financial solvency.

4.4 Emotional and psychological implications

Participants also described a range of emotional and psychological impacts of fraud, which could both occur as a 'knee jerk' reaction to the fraud and outlast the immediacy of financial impacts of the crime. In some cases the psychological impact was profound. Importantly, the emotional and psychological impacts were not necessarily linked to the amount of financial loss on the part of the participant. Participants could also experience emotional impacts even when no money had been exchanged. These tended to relate to feeling that their privacy had been invaded, or the breaking down of trust in institutions that participants described. In other cases, the financial and emotional impacts were closely intertwined, with financial loss directly resulting in anxiety, stress and depression.

Emotional and psychological impacts included the following:

- **stress and anxiety:** online fraud caused anxiety on account of the uncertainty the participants felt around the potential risks they could face either from fraudsters or from losing income/credit ratings in the future. As noted above, stress and anxiety could also be caused by the loss of money – for example, participants' concern about whether they could pay their bills. Some frauds also

deliberately created stressful or anxious situations for participants as part of the perpetration strategy (i.e. they had a limited amount of time to make a payment and the fraudster was 'relying on them'), which caused considerable stress even before they found out the situation was a scam.

- **anger**: feelings of anger and annoyance were linked to the perception of having been 'cheated', and the injustice of someone making money out of causing others harm. Significantly, the perpetrator not having being caught (and this tended to be the case) compounded this anger. Participants associated their anger with feelings of frustration and impotence at not being able to do anything to punish the perpetrator and prevent them from doing the same to others. Anger was also directed at the self, as participants felt angry with themselves for having fallen for the scam.

- **feeling violated**: the knowledge that someone had obtained the participant's personal details felt intrusive. Participants who had experienced various types and levels of online fraud reported feeling as if the perpetrator had physically violated them in some way:

  "It borders on almost dirty doesn't it, it's horrible… it leaves you feeling contaminated… touched by that person" (Interview participant)

- **embarrassment, shame and self-blame**: participants who had experienced different types of online fraud reported feeling 'stupid' or 'like an idiot' for having fallen for the scam (this was particularly pronounced when they had been the victim of confidence fraud). The sense that it was somehow their own fault led participants to question their own identity in terms of their intelligence, judgement and ability. Participants felt confused as they struggled to work out how they could be capable people who were responsible for their own safety, and yet incongruently have fallen for the scam. They identified this self-doubt as one of the most pervasive and damaging types of harm caused to participants, as it altered their self-perception and could remain with them indefinitely.

- **depression:** at the most extreme end, stress and anxiety could lead to participants reporting they suffered from depression, in some instances almost to the point of feeling suicidal. Stakeholders reported cases where victims of advance fee and boiler room investment scams had committed suicide after being so devastated at having lost their life savings, and the case study 4.1 below illustrates how a participant described coming close to experiencing suicidal feelings.

Case study 4.1: Interview participant
Virus and advance fee fraud

Harriet was a victim of a confidence fraud in which perpetrators managed to 'freeze' her computer and would not unfreeze it until she paid them money. Harriet paid nearly £1000 to them in total. Once she realised it was a fraud she started to doubt herself, and feel vulnerable, embarrassed, foolish and annoyed. She has since changed her telephone number and email address. Whereas she was happy to use her computer before the fraud, now she does not trust herself to do so and has asked a friend for help. Not being able to trust herself to keep herself safe was the worst impact of the fraud for Harriet, and she described how even though she would not have committed suicide the experience made her feel like 'jumping off a cliff'. This suggests that the intense self-doubt, caused by the fraud, can be very damaging:

> *"[Before] I could manage to do an audit of a big company… and here I am, at my age, sitting here worrying and it makes me feel ill… I completely doubted myself… if I had to think about how to get anywhere or what to do… I don't like the feeling that I now don't trust myself"*

Secondary impacts of stress and anxiety

Emotional and psychological impacts of the fraud could also relate to secondary impacts described by some participants:

- **fear of physical threat:** as discussed, not knowing exactly how the perpetrator had obtained the information about them, or what information the perpetrator had, fuelled participants' fears, which in some cases included fears for their own or their family's physical safety. A participant, for example, described how they were now afraid the perpetrator might go to their children's school, use the password they had set for other adults to collect their children, and abduct them. A participant of a romance scam was afraid that the perpetrator, who knew their address, might come to their house.

- **physical health:** The impact of online fraud on participants' emotional and psychological health has been described above. On the whole, participants did not report that experiencing online fraud had affected their physical health, although in certain cases psychological distress had led to physical symptoms such as insomnia. They described how they had experienced sleeplessness and nightmares about the fraud. Others reported physical symptoms of the anxiety caused by fraud, such as the nausea that accompanied panic when they first found a virus on their computer that displayed a (fake) message saying child sex abuse images had been found on it. Stakeholders argued that the long-term impact on participants' physical health was often not sufficiently recognised, as they had seen elderly victims become withdrawn, cease eating, become ill and sometimes even die within a year or two of experiencing fraud: *"Frauds take apart people's lives and send people into a downward spiral"* (Stakeholder interview).

4.5 Impact on personal relationships

The emotional and psychological impacts of online fraud described above, coupled with the perceptions and judgements of others, meant that fraud could have a significant impact on participants' personal relationships. This could also lead to a feeling of loneliness or social isolation.

The self-blame and shame felt by participants meant that they tended not to tell anyone but one or two of their closest friends or family what had to happened to them. Participants were

sometimes too embarrassed to tell their grown-up children, siblings, friends and even their spouses, for fear that they would be criticised or blamed. Stakeholders noted how some types of online fraud deliberately created a situation whereby a degree of secrecy was enforced by the perpetrator, which served to isolate the participant from any outside support sources and further increase their vulnerability. They said, for example, that perpetrators devised stories to reinforce to participants that they must not tell anyone what they were doing. This was a form of grooming, adopted as a perpetration strategy to facilitate the fraud.

The case study below shows an example of a participant who felt that the fraud had impacted on their personal relationships and quality of life.

Case study 4.2: Interview participant
Advance fee fraud

Matt, who was disabled and housebound, sent money to an online company to pay for a mobility scooter. On the day of delivery, no scooter arrived, and after emailing and telephoning the company for weeks, Matt realised the scooter was never going to come. He felt very angry and went to the police but was told the police could do nothing about it. Not getting his money back was what hurt Matt the most, but it made it worse that he felt the law was not on his side and neither the police nor any other authority seemed to want to know about what had happened to him. Matt now has great distrust when buying items online and even though he has been told that using PayPal to shop online is very safe and the nearest shops are a considerable journey from his house, he will not shop online. Matt has not told anyone except his wife what happened; he is too ashamed to tell his daughters. He blames himself for not having carried out more checks before he sent the money and thinks he was stupid for having fallen victim to the fraud. He and his wife have also had to cut back on the few trips they used to make to visit family. Matt feels very isolated, but also guilty that his wife has also been affected:

> *"How stupid I've been to have been sucked in by those adverts… it's caused a bit of upset in the house between my wife and I, understandably because I've lost £1500 which we can't afford to lose… we used to go down and see my [relatives], it's a lovely day out, but with the cost of petrol down there and back we had to stop… I felt really miserable after, I was very touchy..."*

Participants cited a lack of awareness or understanding about the true nature and impact of online fraud as a further reason for being reluctant to tell anyone about their victimisation, as they felt people did not understand the level of manipulation perpetrators used. For example they may not have told anyone at their work that they had experienced online fraud for fear that they would be perceived by their employer as being untrustworthy with money, if they handled it in their day-to-day role.

Victims of romance scams in particular spoke of being unable to form new romantic relationships. This, in turn, exacerbated feelings of isolation and loneliness:

> *"You might have two dates, then you find a reason to stop it. You just tell yourself it's not worth it, but it leaves you still very lonely and vulnerable, you don't know how to go forward… I would love to have a partner, but it's whether I could ever trust anybody enough to be able to do it [again, following the fraud] (Interview participant)"*

4.6 Time and resources

The experience of online fraud also caused participants considerable inconvenience as they spent time resolving the problems it caused and trying to protect themselves and others from

becoming a participant of online fraud again. This could compound the level of financial loss they had experienced, as they had to pay to resolve the fraud. Participants who had experienced computer viruses, for example, spent a number of hours learning how to rid their computer of the virus and had to pay for legitimate anti-virus software.

Cases of online consumer fraud in which the participant was kept waiting by the perpetrator, or had to chase the perpetrator before realising it was a fraud, also took up participants' time and caused inconvenience. Participants talked of having made repeated phone calls and written many emails and letters in attempt either to obtain the item they had paid for, or get their money back:

> *"It's the time that it takes, because when I ordered the Wii they said, 'Right you're going to have it within ten to twelve days', so you wait for that ten to twelve days, you don't receive it, so then you're emailing them and you're really nice… they take their time to be nice back saying, 'Oh we're really sorry'… and then you email back. It's then a couple of months before I even then reported it" (Group participant)*

It was pointed out that the drawn-out nature of some online frauds was a particular inconvenience when the item was needed by a deadline, for example tickets for a festival or a Christmas present. Delayed reporting of fraud to banks or credit card companies could also lead to victims being no longer eligible for recompense by the time they realised they had been defrauded.

4.7 Change of behaviour

There were also cases where online fraud led participants to make long-term changes to their behaviour. In particular, participants were more wary of the how they used the internet, how they shopped, and how they treated salespeople since experiencing fraud. For example, they may no longer use online dating sites and or shop online.

On the one hand, participants felt that these changes in behaviour had made them less vulnerable to fraud. On the other hand, they also resented the extra precautions for the inconvenience they caused. For example, a participant reported feeling so concerned about fraud that they checked their online bank account every ten minutes to ensure that no fraudulent activity had occurred. These changes of behaviour were also recognised as leading to fraud having broader societal impacts, explored below.

4.8 Wider impact on society

Participants recognised that online fraud had impacts beyond those affecting them directly. It can have adverse effects on legitimate business carried out online. As discussed in the section above, online fraud caused some participants to stop using the internet to shop online or for other purposes, and stakeholders pointed out that this damage to public confidence in using businesses online could have an overall effect of undermining online business:

> *"There is a greater social harm that happens, along with the possible undermining of the way that people do business with the organisations they are in contact with" (Stakeholder)*

A stakeholder claimed that fraud was second to drug trafficking as the biggest black market enterprise in the UK, and as online fraud could happen to anyone who uses the internet, it potentially has a much wider reach than drug trafficking.

4.9 Support received and resolution of the fraud

The type of support or response participants had received from others when they reported the fraud could also have a significant influence on their experiences. This is explored below.

Support received

There was evidence to suggest that support provided by others, including the police, family, friends and the press could reduce the negative impact felt by participants of online fraud. However, few received such support, even if they did report the fraud, and participants often reported being unsure where to go for help, advice or support when online fraud occurred.

Impact of gaining support for fraud

In cases where the police had shown an interest in pursuing the case, participants felt that the offence had been legitimated and taken seriously. Participants could, for example, describe the process of making a formal statement to the police as helpful because it allowed them to vent some of the frustration they had felt during the experience of fraud. Others, had not spoken to anyone about what had happened, until the Serious Organised Crime Agency contacted them, having detected that they had been a victim of fraud. They described it as a '*great relief*' to be able to finally talk to someone about what had happened. In these instances feeling that they were being taken seriously also helped to reduce the feeling of 'self blame' that participants had regarding the fraud.

Impact of a lack of support

Conversely, there were instances where a lack of support compounded the negative impact of the fraud. This occurred in cases where participants had reported the fraud to the police, but no further action could be taken. Aside from feeling a perceived lack of justice, participants reported a sense of not being listened to.

The negative reaction of others to participants' experiences could also compound the emotional and psychological harm caused. Negative or unsupportive reactions from family and friends could exacerbate participants' sense of isolation and shame. Wider disapproval had also sometimes occurred, with negative consequences for the participant such as media coverage of a similar type of fraud inferring victims were to blame.

Therefore, it appears that wider recognition about the nature and impact of online fraud, and also acknowledgement by authorities when it is reported, would help reduce some of the negative impacts described above, particularly those relating to self-blame among victims.

Resolution of the fraud

The outcome of the fraud experienced unsurprisingly affected the way in which participants described the impact. Those who had been reimbursed by their bank reported that this did reduce the harm caused, and those who had not been reimbursed cited restitution of funds as the single factor that would most help them to overcome the impact of the fraud. In cases where there was no financial impact, such as the case of a computer affected by a virus, fixing the computer was the key factor described as alleviating the harm caused.

However, regardless of the extent of loss and restitution, participants had a strong desire to see justice carried out. Whether or not the perpetrator was caught, prosecuted and admitted the offence also had a significant affect on the impact the fraud was felt to have, though it was rare for any of the cases to have involved the identification of the perpetrator. In one example, a participant reported that the crime no longer had any significant impact on them because the perpetrator had admitted the fraud to the participant themselves, and then to the police, been found guilty of the offence and been ordered to repay the participant in full. After having played '*cat and mouse games'* with the perpetrator to try to recover the item they had paid for, the participant explained that the perpetrator's admission of guilt made them feel instantly better:

"As soon as he said, 'There's no [item], I tricked you, I'm sorry', that was what made it better for me" (Interview participant)

Conversely, in cases where the perpetrator had never been traced, this was a significant source of frustration for the participant. Therefore, the very process of a perpetrator being identified, charged and a case being brought against them for the fraud they committed could help minimise the negative impacts.

Moving onto the sentencing stage of the process in the next chapter, participants' and stakeholders' views on issues and concepts that relate to sentencing fraud offences are discussed. As already noted, most of the participants had not been involved in a case where a perpetrator had been identified or sentenced, but their views on the factors to take into account when sentencing online fraud offences, similar to those they had experienced, were explored in the focus groups and interviews.

4.10 Summary

Participants reported a range of impacts as a result of the fraud they had experienced. These impacts fell into the following four broad categories: financial impacts (both short-term and long-term); emotional; psychological and health impacts; relationships with others; and lastly, time and convenience. Stakeholders and participants also noted the wider negative impact fraud has on society more generally, including the UK economy. The level of reparation or resolution from the fraud that participants had experienced unsurprisingly had an impact on the level of harm reported. Where participants had felt supported or listened to by the police, other formal agencies or family or friends when they reported the fraud, the negative impact of the fraud had sometimes been reduced. Conversely, where police indicated that they were unable to follow up on a case of online fraud, the impact could be compounded, as participants felt unheard and that a lack of justice had occurred.

5. Attitudes to sentencing issues

A key aim of this research is to explore the way in which online fraud is being committed and the impact this has. This is considered in this chapter alongside issues relevant to sentencing online fraud offences.

This chapter begins by outlining the factors that participants felt underpinned the seriousness and harm of online fraud offences, and the culpability of the perpetrator. These findings are set out in relation to aggravating and mitigating factors. The findings are presented in this way as it was clear from the interviews and group discussions that the factors which participants felt made an online fraud offence more serious and harmful, were also those which they regarded as aggravating factors to the offence. Conversely, the factors which they felt led to an online fraud offence being less serious and less harmful, and the perpetrator less culpable, corresponded to what they felt could act as mitigating factors.

The chapter then goes on to explore the sanctions participants felt were relevant for the two types of fraud offences in the scope of this study. Lastly, the chapter concludes by discussing any differences reported between the nature of online versus offline fraud.

It should be noted that participants' views may not have been informed by expert knowledge of the criminal justice system, sentencing, or the efficacy of the different sanctions available when someone is convicted of a fraudulent offence. Some basic information about the sentencing process was discussed at the start of the groups in order to ensure a common level of understanding. This included explaining to participants that the sentencing process involves an individual being found or pleading guilty to an offence, information about the case being assessed, including aggravating and mitigating factors and then an appropriate sentence being decided upon. Participants were asked to suggest the different type of sanctions available (such as fines, custodial sentences) and the researcher would prompt them to ensure a range was suggested overall. Handouts about the actual current sentencing ranges given within the guidelines for fraud offences were withheld until the end of the discussion so that this information did not influence participants' views.

5.1 Summary of main aggravating and mitigating factors

The table below summarises the features which participants and stakeholders felt were aggravating and mitigating factors in relation to online fraud. These are discussed in detail in the ensuing sections of the chapter. The findings were developed following a thematic analysis of the complete dataset. It included participant views that drew on the vignettes provided, and also those based on their own experiences of fraud, or in the case of stakeholders, fraud cases they were familiar with. Generally speaking, the same aggravating and mitigating factors were felt to apply to the two types of fraud offence under consideration in this research: confidence fraud; and making, possessing or supplying articles for use in fraud. Any issues relating in particular to one or the other have been drawn out in the table and in the main text of the chapter. Participants generally found it difficult to agree on the most significant aggravating factor which should be taken into account. For example, whilst some participants may have felt the impact of the offence on the victim was most important, others may have felt strongly that the level of planning and premeditation should be the primary factor taken into account.

As the nature of qualitative research is to map and explore diverse views and experiences – rather than give 'weight' to these differences – in the table below, and throughout this chapter, the whole range of possible aggravating and mitigating factors discussed during interviews and focus groups are presented. Where it has been possible to draw out the relative significance these factors had with participants, this is presented, but the high level of variation evident from participants should be recognised.

Table 5.1 Aggravating and mitigating factors

	Confidence fraud and making, possessing or supplying articles for use in fraud
Aggravating factors	• Degree of (non-financial) harm (both intended and actually caused); • Financial impact on victim or level of perpetrator's financial gain • Premeditation and careful planning (intent); • Abuse of trust/authority; • Nature of fraud (duration, frequency, and techniques used); • Vulnerability of victims*; • Number of victims**; • Motivation or history of the perpetrator; • Extent of wider impact of the fraud; and • Invasion of privacy, use of identity.
Mitigating factors	• Peripheral involvement of perpetrator**; • The perpetrator's response to the crime once uncovered (personal mitigation) such as early plea, cooperation or remorse; • Financial circumstances of the perpetrator**; • Mental illness or impairment of perpetrator**; and • Coercion**.

* Vulnerability was felt to be difficult to define in absolute terms and there were mixed views about taking this into account.

** Views about whether these were factors to take into account were mixed.

5.2 Aggravating factors

Aggravating and mitigating factors were discussed as part of the stakeholder and participant interviews and were explicitly discussed with the participants during the focus groups in relation to the vignettes. To do this, the vignettes were kept brief, and participants' spontaneous views of issues pertaining to the seriousness and harm caused by the offence, culpability of the offender and aggravating and mitigating factors were explored. Then, additional details of the offence were introduced, for example about the perpetrator and the nature of the offence, in order to further aid debate around aggravating and mitigating factors.[26] A full copy of each vignette and the factors used are included in Appendix B.4.

It was striking that participants were generally able to suggest aggravating factors much more easily than mitigating factors. This demonstrates how participants tended to feel that there was very little that could make online fraud less serious or harmful, or a perpetrator less culpable, but many factors could increase the seriousness of online fraud, the harm it caused and consequently, the culpability of the offender. However, opinion in relation to the aggravating factors set out below was not always unanimous and where a range of views existed or disagreement occurred, this has been described.

[26] In reality all the information about a perpetrator would be available at the time of sentencing, but this convention was used in the focus group discussions to ensure individual factors relating to offenders' past and present circumstances could be discussed.

5.3 Degree of harm intended and caused by the perpetrator

Where there had been a significant level of harm to victims, this was felt to be an aggravating factor (this tended to relate to psychological or emotional harm where, for example, victims reported that they had lost trust in business or personal relationships following fraud). The nature of the harm experienced has been explored in chapter 4. The degree of harm experienced was felt likely to relate to other aspects of the offence that may be considered aggravating factors, such as level of planning and value of the fraud, so these factors may be viewed as interrelated. That is to say, victims could report a greater level of emotional harm to them had occurred when they had been 'taken in' by an elaborate scam over a long period of time, compared to an single, relatively low value offence.

In relation to harm, participants also sometimes distinguished in their discussion between the degree of harm *intended* by a perpetrator, and the degree of harm that an offence *actually* caused.

There was a strand of opinion that the seriousness of online fraud was closely linked to the harm *actually* caused to participants, and that this was more important in sentencing than the nature of the fraud (such as level of planning) if no such harm had occurred. When discussing the vignettes, for example, some participants felt it was very important that the potentially serious emotional and psychological impacts on the participant were taken into account as they could be serious, and this was reiterated in the stakeholder interviews. However, as has been discussed in chapter 4, participants then also tended to concede the relative and subjective nature of vulnerability and harm to victims. What may be very harmful to one individual, may not be so for another. The prevailing view therefore was that online fraud offences should be considered on the basis of the perpetrator's intentions – the level of planning, gain, and harm the perpetrator *could* have caused. The actual impact on victims was felt to be something that should also be taken into account when it was clear a negative impact had occurred and there was evidence from the victim to illustrate what this was. But a lack of this evidence was not felt to necessarily reduce the seriousness of the fraud, because the offender implemented a fraud that could have led to negative consequences.

Financial impact on victim or level of perpetrator's financial gain

Given the nature of online fraud – with a key motivation for perpetrators being financial gain – the financial aspect of the fraud was felt to be a potentially significant but complex aspect of sentencing. Rather than judging the seriousness of the offence based on the absolute amount of money lost by victims or gained by perpetrators, participants and stakeholders felt that it may be more appropriate to consider the relative impact of the financial loss on the victim, which should be determined by their own financial circumstances. Participants explained that whilst the amount of money they had lost might be small for someone wealthier, to them it was often a significant loss in terms of the ensuing impact it would have on their life (e.g. concerns about how to pay bills, unable to have a planned holiday, unable to leave the house for social events when already socially isolated):

> *"I know that £1500 is not a lot of money in some respects, but it's an awful lot of money to us, especially when I've not worked for five or six years… my £1500 was an awful lot of money to me, as £5million would be to Richard Branson" (Interview participant)*

Having said this, participants were also clear that it did not make fraud 'alright' if it was committed against someone who was wealthy and in cases where participants reported being defrauded for large sums of money (such as their 'life savings' or hundreds of thousands of pounds) they did report particularly negative impacts (the fraud had *'ruined their life'*). The point was that fraud of different values would have different impacts on victims depending on their financial circumstances. It was also noted that perpetrators may commit a high number of low value frauds to try to avoid detection and although this may not impact on

victims to the same extent, the perpetrator benefitting from such deception still involved intent and carefully planning an offence.

The alternative view was therefore that 'fraud is fraud' and the offence should be assessed on seriousness regardless of the financial gain to perpetrators or loss to victims. In this approach the nature of the fraud offence (i.e. degree of planning) was felt to be the key aggravating factor. A caveat to this, however, was that clear evidence of a very high value/highly harmful fraud being committed was seen as particularly serious. Where this was not evident, however, the nature of the fraud (such as premeditation) was instead felt to be a significant aggravating factor.

Evidence that the online fraud was premeditated and carefully planned (intent)

The level of organisation and advance planning involved in an online fraud was felt to be a key factor in determining the level of culpability of the offender, because it showed that the offence was premeditated. This also indicated that the perpetrator clearly had the intention to commit online fraud, and would go to some lengths to do so. It was therefore felt, by both participants and stakeholders, that strong evidence of organisation and planning would be an aggravating factor:

> *"If it's a person who's come across something, or altered a particular article, and committed what could be defined as a spontaneous offence, that cannot be the same as somebody who's routinely committed criminality in that fashion" (Stakeholder)*

The typical view amongst participants and stakeholders was that most online fraud by its very nature involves a high level of organisation and planning. Drawing on both their personal experiences of fraud and the vignettes discussed in the focus groups, they listed the various ways that they felt premeditation and planning could be in evidence. These were when fraud:

- **was large scale and professional:** for example, where fake companies had been set up with the sole intention to commit consumer fraud;
- **appeared legitimate and credible:** for example, where articles had come into play in order to facilitate confidence fraud. This included simple strategies such as using logos of legitimate and well-known companies on 'fake websites' as described in Chapter 3, and more complex strategies such as where a participant of a romance scam had been spoken to over the phone by a person pretending to be in a position of authority. This demonstrates the complex nature of some forms of online fraud, as in this case the perpetrator directed the participant to call a person claiming to be in a position of authority to make their story (that they needed money from the victim to help them) appear more believable. Therefore planning could also be indicated by fraud that:
  - **involved individuals ostensibly in 'positions of authority or trust':** for example, corrupting and impersonating officials, which stakeholders noted required a great amount of organisation and pre-planning; and
  - **systems having been put in place to support the fraud:** for example, bank accounts specifically to deal with the financial transactions involved in the fraud, letters and emails being composed for fraud and also perpetrators using a range of techniques to maximise the success of the fraud.

These factors being evident were felt to indicate that the fraud was being 'professionally' run and committed by an organised group of perpetrators or individuals. Therefore participants and stakeholders felt that any evidence that the perpetrator had been running the fraud in a professional and organised way was felt to be an aggravating factor.

However, an alternative view was that non-premeditated harmful frauds could also be committed. When discussing the hypothetical romance scam (vignette one), some participants felt that it could not be assumed that the perpetrator would have been more culpable if they had set out to cause the offence than if they had committed fraud after developing a genuine relationship with someone and had been 'chancing it' trying to obtain financial gain from them (see Appendix B.4 for vignettes). Likewise a legitimate business being in financial difficulty could potentially lead to it committing fraud (for example, not sending goods that have been paid for). A lack of planning was not therefore felt to mitigate the offence, but evidence of planning and premeditation was felt to aggravate the fraud offence.

The following case study, 5.1, from a focus group discussion illustrates some of the points made above.

Case study 5.1: Focus group
Vignette 2 identity theft and fraud

Participants were given a vignette (see vignette 2 in Appendix B.4) about a victim who had experienced identity theft whereby the perpetrator had withdrawn a sum of money from his personal bank account. Participants felt that this fraud was clearly premeditated rather than opportunistic, which indicated a higher level of culpability. One view was that the perpetrator must have a list of people's personal details in order to commit the fraud.

There were two distinct views over whether seriousness and the severity of punishment should depend on how they obtained these details. One view was that the method used could indicate a higher degree of planning. For example, participants in one group felt that if the perpetrator was in possession of special software to help access people's details, then this indicated a high degree of premeditation and planning and subsequently made the offence more serious. The alternative view was that the method by which the perpetrator obtained the details had no bearing on the seriousness of the offence as the perpetrator had gathered the details to do something which they should not have done (commit fraud) regardless of how they obtained them. One participant also highlighted how the perpetrator had intended to make money by setting out to hurt people:

> *"He's decided to go out and steal £2000 out of someone's account. He hasn't happened to come across a wallet on the floor with £2000 in. He's decided with his conscience to intentionally go out and defraud somebody"*

Additional factors that related to the nature of how the fraud was committed (outlined below) were also felt to aggravate the offence, regardless of there being a high degree of planning or organisation.

Abuse of a position of trust/authority

Where a position of trust or authority was used to perpetrate the fraud, this was felt to be a further aggravating factor, which increased the seriousness of the offence and the culpability of the perpetrator. Perpetrators could gain the trust of victims by using manipulative strategies, for example developing a (false) intimate relationship with them in the instance of romance scams, or pretending to be the police, a bank manager or a member of the medical profession. Adopting these positions was felt to make it more likely that the fraud would be successful but also indicated a degree of planning on the part of the perpetrator. They could also undermine confidence in these types of relationships, professions or related institutions in the future.

Nature of the fraud (duration, frequency, and techniques)

The nature of the online fraud (i.e. the type of perpetration strategies used or repeated contact by fraudsters with victims) were also felt to aggravate the offences.

In cases where fraud had been carried out over a long period of time (in an extreme case experienced by an interview participant, an advance fee fraud that continued for over a decade) the amount of money lost and the time the participant had invested also tended to be greater, and consequently the various types of harm caused were more severe. It was also the case that frauds of longer duration were regarded as particularly serious because they enabled the participant to be groomed by the perpetrator during repeated contact. For example, participants felt that this would have applied to the hypothetical participant in vignette three, the consumer fraud (see Appendix B.4 for vignettes).

The frequency with which participants were targeted also caused additional 'hassle' and inconvenience, for example, they may have been sent several emails relating to advance fee frauds on a daily basis over many years. This also put psychological pressure on the participant to capitulate and believe the scam:

> *"They completely inundate you with it and you're very tempted, in moments of weakness, to fall for it, and you think it's going to happen. In your heart of hearts, you know it's a scam but you seem to think maybe this time it'll be different, and that's what they play on" (Interview participant)*

One strand of opinion was that where frauds involved emotional and psychological duping (the type of perpetration strategies outlined in chapter 3), they were more serious. This was because they indicate the perpetrator had intended to defraud the victim, and also used techniques which may harm them, via embarrassment, anxiety or the disappointment this then caused. Examples were felt to include cases which had involved being accused of accessing child abuse images (illegal pornography) as discussed in Chapter 3. Participants of romance frauds argued that the harm caused to them was greater because of the extent to which they were 'brainwashed' by the perpetrator, believed the elaborate stories the perpetrator fabricated and made an emotional investment in the perpetrator which was subsequently dashed. Such a case is described in case study 5.1, above.

Motivation or history of the perpetrator

The final set of aggravating factors related specifically to the perpetrator of online fraud. Two areas were discussed here as factors that increased culpability and the seriousness of the offence.

Repeat offending

Participants felt that previous convictions, evidence of previous offending, or the fraud being linked to other criminal activities should all be taken into account as aggravating factors. In addition, stakeholders felt that alongside previous convictions, evidence which indicated that the fraud had been used to finance other crimes should also be treated as an aggravating factor.

However, there was a view among stakeholders that if these were aggravating factors, it did not mean the same should happen in reverse. That is to say, the fact that a fraud offence was a first offence should not act as a mitigating factor. They felt that currently, given the level of priority fraud offences have in the criminal justice system compared to other types of crime, only the more prolific perpetrators of fraud tended to be caught.

Motivation for fraud – a financial 'business'

In relation to the level of planning and premeditation evident, participants felt that where an offender seemed to be committing fraud as purely a means to make money this could be an

aggravating factor. This was the converse of circumstances such as extreme financial hardship being a potential mitigating factor.

Vulnerability of victims

There were mixed views around whether certain factors would increase the vulnerability of the victim, and in turn the seriousness and harm of an online fraud. One view was that the characteristics of the victim should not be taken into consideration. As already discussed in Chapter 3, vulnerability was also felt to be subjective and relative to assess in online fraud offences, as the perpetration strategies play on different vulnerabilities that people may have. Therefore, by their very nature, online frauds will play on differing vulnerabilities, being successful when they match the 'weak spot' of a potential victim. As such everyone may potentially be 'vulnerable' to fraud playing on their weakness. There was also a view that the offence should be judged the same, regardless of the specific characteristics of the victims:

> *"It's the same as if somebody's mugged on the street: it doesn't matter whether they're an old person, a young person, middle-aged, middle class, upper class. It's still a mugging" (Interview participant)*

There was a view amongst some participants that caution needed to be exercised in the use of the word 'vulnerable' given that the concept of vulnerability could be subjective, and vary depending on the nature of the fraud and the personality and resilience of the participant. A middle-aged participant of a romance scam, for example, spoke about how she had time to rebuild her life after her experience of fraud, which would not have been the case if she had been older. In contrast, some focus group participants argued in relation to the romance scam vignette that its long-term impact on younger people could be particularly harmful given their long life expectancy. This complexity is also illustrated by the discussion in the case study below about an elderly victim.

Case study 5.2: Focus group
Vignette 4 Lottery scam

A group of victims of online fraud discussed the seriousness of a lottery scam vignette in which the victim was eighty years old (see vignette 4 in Appendix B.4). They felt that because the victim was elderly, the harm caused to her could be greater, as she might have worked all her life to save the money she lost through fraud. An elderly victim was thought to be less likely to be able to cope with the stress caused from their victimisation. However, this view was contested by some group members, who argued that an elderly victim was not necessarily more vulnerable than a younger victim.

> *"…because she was elderly she wouldn't maybe think [the item offered for sale] was not real… perhaps [s]he wasn't very good on the internet like me and not used to different things, I get flummoxed at it and she's 80 isn't she?...probably new to the internet…"*

> *"…I actually can't see any difference because I mean I know 80 year old people who are really up to the mark and everything else, and they're quite bright buttoned"*

However, an alternative view among both participants and stakeholders was that targeting vulnerable people made the perpetrator more culpable and the fraud more serious. It was felt the perpetrator had deliberately set out to abuse certain weaknesses, and make a profit in doing so. A stakeholder likened premeditated frauds that target those vulnerable to fraud, to crimes being committed against children:

"If they're buying sucker lists of emails, you know, older people's email addresses then… they know exactly who they're going for...these people haven't got a chance. It's a bit like crimes against children. I mean if somebody attacks a child, that child's vulnerable and the sentence is a lot higher than if a bloke attacks another bloke that's the same age and build. D'ya know what I mean? You know they're going for weaker prey, let's put it that way. Aren't they?" (Stakeholder)

In relation to *actual* harm caused, there was discussion about certain characteristics increasing the likelihood of negative impacts being experienced by victims. This was felt to apply to:

- **age:** on the whole participants, including those who were elderly themselves, thought that elderly participants were more vulnerable to the impact of online fraud as they were less likely to be aware of and know how to identify an online fraud attempt due to less familiarity with the internet. Those in much older age groups who may have dementia or other organic mental illness were felt to be vulnerable to 'falling for a scam' due to a lower level of comprehension. Age was also considered to have an impact on a participant's financial circumstances. Participants who were interviewed that were past retirement age and had lost their life savings felt that their age made them less able to recover financially from the impact of fraud. Conversely, however, being young was also felt to increase people's level of vulnerability with young people perceived as being perhaps more 'naïve' and vulnerable to a scam.

  However, as was illustrated in case study 5.2, it was debated whether age (younger or older) should be an automatic predictor of vulnerability, as both participants and stakeholders highlighted that an elderly person or young person could be particularly internet-savvy or financially secure. On further distillation of these views, it was agreed that it was potential frailty due to physical or mental ill health, or their financial circumstances, that could make someone more vulnerable, not their age *per se.* This relates to the category below;

- **mental health issues:** participants that had mental health issues felt that the impact of fraud had been particularly harmful because it had exacerbated their mental health problems. Stakeholders also noted that older people with dementia or people with learning disabilities may be viewed as particularly vulnerable to confidence fraud *per se* (though not necessarily online confidence fraud).

Despite the subjective nature of assessing harm, participants felt that the degree of harm intended or caused was also likely to increase with the agreed aggravating factors identified in the opening section of this chapter. In addition, the complexity of the perpetration strategies (and with them the degree to which the participant felt duped) was also identified as a factor which could increase harm.

Number of victims

There was also debate about whether the number of victims should act as an aggravating factor to online frauds. Some stakeholders argued that this should be taken into account in terms of the greater harm caused across the population. Some participants noted that potentially victimising a high number of people (i.e. sending spam to thousands) made the offence more serious than if a spam email was sent to just one person.

Another argument, however, was that focus on the overall scale of the fraud might overlook the nature of the offence. In a romance scam, for example, there may have only been very few victims but the fraud might have involved a high degree of planning and premeditation and led to significant financial and emotional harm to the victim.

Some participants also argued that even committing a fraud against just one person is still against the law. A number of stakeholders emphasised how important they felt it was to stop fraud at its initial stages in order to prevent escalation and the creation of more victims, and therefore felt even one episode of fraud should be taken seriously at the sentencing stage:

> *"Taking a court case where someone says, 'Oh, there was one victim, it was £1000.' And [the view would be] probably, 'Why on earth are you bringing it here? Couldn't you sort this out in a civil way?' Rather than [what we would say, which is], 'Please look at the, the wider aspects of this. If this had continued for a year, then we'd have been [defrauded by], you know, £1 million'..." (Stakeholder interview)*

This view was especially felt where there was evidence of preplanning and organisation – where the perpetrator had intended to commit a large-scale fraud.

5.4 Additional aggravating factors

In addition to those discussed above, there were two factors which were felt to be potentially important to take into account when sentencing fraud offences. These were:

- **the extent of the wider impact of the fraud:** this was a further aggravating factor raised during a group discussion about vignette three (slimming pills website, see Appendix B.4 for vignettes), where a consequence was felt to be that people would lose trust in buying medical pills online. General harm to the economy was also suggested by one stakeholder as an aggravating factor of fraud which should be taken into account; and

- **invasion of privacy, use of identity:** when the fraudulent activity had involved an invasion of the participant's privacy, this was felt to be an aggravating factor. Group participants felt that vignette one (romance scam, see Appendix B.4 for vignettes), should include invasion of privacy as an aggravating factor because the participant's personal details had been obtained through a dating site. In addition, using another person's identity to facilitate the fraud was also felt to be an aggravating factor.

5.5 The relative weight of aggravating factors

Participants were asked to identify the most significant aggravating factor to take into account. However, they were unable to identify one overriding aggravating factor. This was due to two issues. First, the aggravating factors discussed were felt to interact with each other to determine the level of seriousness of the fraud offence. For example, it was felt that a high degree of planning and long-term contact with the victim could lead to greater harm to the victim. It could also lead to a greater amount, financially, being defrauded from them, which in turn could also compound the impact the fraud had on a victim. Secondly, participants could simply differ in opinion with, for example, one feeling strongly the financial value of the fraud was the most significant, and another that the impact on the victim was most important to consider.

Generally, however, it appeared that three factors: harm to victim, level of premeditation and organisation, and value of the fraud, were the most significant aggravating factors. Where there was a high value/high level of negative impact on the victim this was felt to be important to take into account as aggravating factors. However, the potential relativism of these issues was also highlighted by participants. That is to say, what may be considered a high value and high impact offence to an individual on a lower salary for example, may not be considered the same to another who is much more financially solvent. Further, a lack of negative impact or financial loss to an individual being evident in the fraud was not felt to mitigate the offence, rather in these instances the degree of planning and organisation (and

with it the *potential* and *intended* harm and financial gain) was felt to be the most significant aggravating factor.

Lastly, there was also a strand of opinion that 'fraud is fraud, and a 'crime is a crime', meaning that specific details were of less consequence than the fact an online fraud offence of some sort, had been committed at all.

5.6 Mitigating factors

Both participants and stakeholders were generally reluctant to identify clear mitigating factors from the cases they had experienced. This reluctance was based on their feeling that fraud always came about as a result of a perpetrator's conscious decision to do something wrong (illegitimate financial gain), and therefore that their intention was always to defraud:

> *"I just think there shouldn't be any mitigating circumstances for that person who's done the crime… they've hurt somebody, they've caused monetary loss, emotional, physical stress… I don't think there should be any mitigating circumstances just because his mother's died or whatever… if they don't do the time, don't do the crime" (Group participant)*

However, alongside this general viewpoint, there was some debate over whether or not certain circumstances could be considered mitigating factors. These are discussed below.

Peripheral involvement

There were two distinct views around whether the role the perpetrator had played in the offence should be taken into account when determining their level of culpability. The first was that a more 'peripheral' role did not have a bearing on a perpetrator's culpability and was therefore not a mitigating factor. Reasons for this included the perpetrator still having some role to play in the fraud, and they had still made a conscious decision to commit a crime:

> *"In the end they're all still in it, they should all be the same...whatever one does, they're all going to benefit from it...I would imagine they know what they're doing out there" (Interview participant)*

Stakeholders emphasised how a peripheral role could in some cases be integral to the crime, for example, in the case of a telecommunications worker who had supplied perpetrators with a list of customers who had Alzheimer's disease. This was likened by stakeholders to a driver in a bank robbery still having an integral role in the offence, even if they do not actually enter the bank.

By contrast it was felt by stakeholders and participants that in certain circumstances a peripheral role could be a mitigating factor. This was because it illustrated less planning on their part compared to the primary organiser of the fraud. In addition, it was felt that those who acted on the periphery might even in some cases have been deceived by the perpetrator themselves, and in this respect they could even be perceived as a 'victim'. Examples given included mass marketing scam staff who had been recruited on legitimate terms, only to realise later they were working on a fraudulent activity.

Personal mitigation – the perpetrator's response to the crime once uncovered

The perpetrator's reaction to the crime was also felt by both participants and stakeholders to have a bearing on their level of culpability. Where they did cooperate and/or make amends this was felt to potentially mitigate. Conversely, where they had not cooperated with the police, or where the perpetrator concealed evidence, this was felt to indicate higher culpability and therefore to be an aggravating factor. An example of this was the romance scams described in Chapter 3 where the perpetrators had made sure any evidence relating

to the fraud was disposed of as they went along. These issues are discussed in more detail below.

Early plea and cooperation

Stakeholders pointed out that if the perpetrator cooperated with the police at an early stage in the investigation then considerable savings could be made for the public purse. Notably however, this was presented as a factor that could mitigate the level of harm caused rather than change the overarching culpability of the perpetrator or seriousness of the offence they committed.

Remorse on the part of the perpetrator

Where a perpetrator admitted the harm they had caused, that the crime they committed was wrong, and made an attempt at restitution, this was felt to act as a mitigating factor. However, stakeholders took the view that this did not happen very frequently.

Financial circumstances of perpetrator

One view among both participants and stakeholders was that if the perpetrator was under financial pressure to carry out the fraud then this could mitigate the offence. However, those who held this view also tended to feel that fraud was committed for reasons of greed rather than financial hardship, or to maintain a particular lifestyle, rather than avoid destitution. For this reason, they thought it was unlikely that perpetrators were ever justified in committing fraud due to financial hardship and therefore it was not a mitigating factor likely to be relevant in most cases. They argued that most people who experience financial hardship do not resort to criminal acts to resolve this and it is therefore not an 'excuse'.

> *"We sometimes struggle for money and I don't go and steal off people so…" (Group participant)*

Mental illness or impairment of perpetrator

Participants (victims and stakeholders) felt that in instances where the perpetrator had a mental illness, this could potentially mitigate the offence. However, this was not felt to be a likely factor in online fraud offences. Participants felt that the degree of pre-planning and skill required to commit a successful online fraud would indicate the perpetrator was functioning well and capable of knowing 'right from wrong'. This was raised by participants unprompted.

Coercion or forced to commit fraud

Coercion to commit fraud by others was not seen as an excuse and therefore not a mitigating factor, as it was argued that the perpetrator would still know what is right and wrong. However, participants conceded in the case of highly organised criminal gangs, there could be individuals who become involved as a perpetrator under duress, with fears for their own safety. This would be a mitigating factor.

The final theme to emerge in terms of assessing the relative seriousness of an online fraud offence and the aggravating and mitigating factors to take into account was the role of the victim in the offence, which is explored below.

Actions and motivations of the victim

There were mixed views on whether a victim's naivety or the risks they took should be taken into consideration. There was acknowledgement from stakeholders that there could be a degree of responsibility amongst some victims, who for example replied to lottery scams that claimed they had won the lottery in Spain, even though they had never entered the Spanish lottery, or who thought they would be engaging in illegal acts such as money laundering for their own personal gain in the implementation of the fraud.

This was echoed in the views of group participants, some of whom felt that the victims presented in the vignettes should have been more aware of the risks involved. For example,

it was argued that a woman who bought diet pills that fraudulently claimed to help lose weight should have been aware that they might not work, and that a victim of a romance scam was foolish for sending large sums of money to someone they had never met.

However, these views could also be seen as inadvertently reinforcing the negative 'stereotypes' or perceptions of victims of fraud that were seen in the previous chapter to compound the negative impact of online fraud.

In the next two sections additional findings are discussed that relate to sentencing: the types of sanctions that are felt to be appropriate for online fraud and whether there is a fundamental difference between online versus offline fraud.

5.7 Support for different types of sanctions

Participants did not necessarily feel that the severity of the sentence should be solely influenced by the financial amounts involved in the fraud, though it should play a role. A reason given for this was that it is impossible to *'put a price on crime'* and a person should be sentenced on principles involved rather than the monetary value.

Three key factors were therefore felt to be significant for sentencing: the impact on victims, the value of the fraud and the degree of pre-planning and organisation. Any one of these being evident could aggravate the offence, but a lack of any of these factors was not necessarily felt to mitigate.

Taking into account the harm to victims, a Victim Personal Statement was highlighted by both participants and stakeholders as a useful feature to include when sentencing fraud offences, so the court could take into account the true extent of the impact experienced.

Once all of the information about the case had been gathered, participants felt that there were three main aims to the sentencing process for online fraud: punishment; rehabilitation; and to act as a deterrent, both to the convicted perpetrator and to other potential perpetrators, from committing fraud in the future more generally. When prompted by the interviewers, they spoke about a range of sanctions which they regarded as appropriate for online fraud, both in relation to their own experiences of fraud and in relation to the focus group vignettes. Seven main types of sanctions were discussed, set out below.

- **Custodial sentences:** participants' views (both stakeholders and victims of fraud) about the appropriateness of custodial sentences for online fraud were mixed. On the one hand, they argued that a custodial sentence was appropriate if sufficient aggravating factors were present and that perpetrators should serve the full custodial sentence given and not be released from prison early. On the other hand, some participants doubted that custodial sentences reduced reoffending and instead suggested combining custodial sentences with other sanctions described below. Finally, some participants felt that custodial sentences were not appropriate for this type of offence. They felt that a prison environment could help to encourage reoffending and did not always act as a sufficient deterrent:

  > *"I think there is something big that needs to be done [to prevent online fraud] other than just a jail sentence" (Group participant)*

  Stakeholders felt that the potential of custodial sentences to act as adequate deterrents varied hugely depending on the individual perpetrator as the following quote illustrates:

  > *"It depends on the fraudster, some of them I'm led to understand are quite happy to go to prison for six months a year, provided they can*

come out, and they've still got the money that they've accrued through committing fraud...but some would be scared by the prospect of going to prison" (Stakeholder)

- **Community orders:** there were two views around whether a community sentence was appropriate for this type of offending. The first was that these, and particularly community orders towards the lower end of the guidelines, did not provide enough of a punishment or a deterrent:

  "Community Order… it's not an awful lot, is it, that's not going to stop them doing that [fraud], because if they know they can go out and do it again, and what are they going to get, sort of six weeks of going out and sweeping up the roads, or tidying up. It's not going to deter them, is it?" (Interview participant)

  The second was that using community orders for fraud offences was appropriate but the degree to which they were used should be dependent on each individual case and the aggravating and mitigating factors present and they should be accompanied with restitution for the victim.

- **Fines:** fines were suggested as an appropriate sanction to use when it was felt that they were able to 'hurt' the perpetrator financially and make them aware of the financial implications of their offending on victims. However, participants of romance scams and investment frauds felt that fines were too lenient, and would not act as a sufficient deterrent or punishment. This was in the context of these being highly planned, organised frauds involving long-term contact between victim and perpetrator with significant harm to the victim ensuing. Concerns were also raised among stakeholders and participants that a perpetrator may not pay the fine, or commit more fraud as a result in order to pay it.

- **Restitution orders:** this type of sanction was a recurring suggestion among participants and stakeholders. Some participants felt that it should be an obligatory order when sentencing fraud offences and treated as a separate element from the actual sentence given. Participants that had received financial recompense following an online fraud offence reported being pleased with this outcome even when it was a relatively small amount (£50). This money being restored to the victim would help ease the financial impact of the offence on them. However, it was also noted that for some types of fraud this would not be enough to address the wider range of impacts of the fraud, for example severe emotional or psychological impacts:

  "The financial side of life could be eased, it goes a long way. But the emotional side will never be mended" (Interview participant)

  It was also suggested that the amount of money the perpetrator was made to pay back should not just be equal to the amount of money that had been exchanged as a result of the fraud, but should also take into consideration the further financial impacts entailed by the fraud, for example the cost of making telephone calls to resolve a fraud.

- **Confiscation order (involving the seizure of assets gained via the fraud):** participants felt that it should take priority in the sentencing process. Stakeholders also viewed this as a good sanction to use in the sentencing process and felt that it may serve as more of a deterrent for 'career' criminals. The fact that these orders cannot be issued in magistrates' courts was felt in

need of review, however, especially as many fraudulent offences would be seen in a magistrates', rather than a Crown Court.

- **Restorative justice:** participants and stakeholders particularly felt that restorative justice for online fraud offences was appropriate. Online fraud was generally perceived to be a 'faceless crime' as it was unlikely that the perpetrator would have met their victim. Participants generally felt that they would have been willing to take part in such an exercise and meet with the perpetrator who had committed the fraud against them, especially as it could potentially help the perpetrator to realise the impact of the crimes they had committed:

  "Maybe [the perpetrator] would turn around and go, 'I never thought of it that way. We just thought money, money, money this is easy, you don't hurt anybody, there's no physical violence, you don't have to see anybody…' or face up to what you're doing to somebody, it's completely and utterly faceless" (Group participant)

- **'Name and shame' and other sanctions:** other sanction options were also suggested apart from those listed above. Some participants felt that the sentencing of fraud offences should involve an element of 'naming and shaming'. An alternative view was that this should be avoided as a perpetrator may be proud of the fraud they had committed and therefore look upon such a sanction as a 'badge of pride'. In addition participants also suggested charity work, (which would have a level of 'social benefit' beyond that of 'unpaid labour'), 'hard labour', and conscription to the army as appropriate sanctions to use with perpetrators who have been convicted of a fraudulent offence. A further alternative view was that going to court formed part of the punishment in itself, especially where the fraud had involved smaller monetary amounts, which had been repaid. Alongside the sanctions discussed above, participants also spoke about stopping a fraudulent company from operating or banning the individual involved in the fraud from being in charge of a company, as currently included as part of the ancillary orders in the sentencing guidelines.

5.8 Online fraud versus offline fraud

In the final section, the views of participants and stakeholders on whether online fraud should be perceived differently to offline are presented. These were found to be mixed, although generally the method of the fraud was felt to be of less consequence than the fact it had occurred at all.

A prevailing view was that the offline or online nature of the method of fraud made no difference to the seriousness of the offence and how it should be viewed for sentencing purposes. It was felt that both represented methods through which fraud could be committed and regardless of the method, the offence should be viewed as the same. The impact of online and offline fraud were considered to be the same in that both methods could cause victims to lose money, confidence and faith in themselves or institutions. The culpability of the online perpetrator was thought to be equal to that of the offline perpetrator because the offence was considered to be the same: "*Whether it's done online, offline, it doesn't really matter, stealing is stealing"* (Group participant).

However, there was a suggestion from some participants that online fraud could be more serious than offline. They argued that the faceless nature of the fraud meant it was particularly harmful and may be one reason why victims did not feel they could report it to the police, the Trading Standards Office or a relative, as someone who experienced an offline crime might do.

There was also perceived to be greater potential to commit fraud online – and with it to impact on a greater number of victims globally, simultaneously, which was thought to make it potentially more serious than offline fraud. There was also a sense that due to the ubiquity of the internet, people now have to use it to conduct their day-to-day interactions, therefore they cannot escape the risk of online fraud the internet poses.

Finally, a view existed that online fraud had less of an impact than offline fraud precisely because the victim did not have to meet with the perpetrator face-to-face, and it was therefore not as personal. Participants who held this view tended to have lost relatively small amounts of money through fraud (less than £50) and did not report any emotional impacts of fraud.

So it appears that online communication provides new means by which fraud can be committed, in ways that may reach a high number of people across the world. However, the fundamentals of the offences – how it is carried out, the offender's motivation, and impacts on the victims, tend to reflect the same 'old' fraud as before.

5.9 Summary

Generally speaking, the same aggravating and mitigating factors were felt to apply to the two types of fraud offence under consideration in this research. However, participants were generally able to suggest aggravating factors much more easily than mitigating factors. This demonstrates how participants tended to feel that there was very little that could make online fraud less serious or harmful, or a perpetrator less culpable, but many factors could increase the seriousness of online fraud, the harm it caused and consequently, the culpability of the offender.

Agreed aggravating factors related to a range of aspects of online fraud offences included in the research and participants were unable to identify one overriding aggravating factor. It was not necessarily felt that the severity of the sentence should be influenced by the financial amounts involved in the fraud. This was in part because of a feeling that it was impossible to *'put a price on crime'* (group participant) and a person should be sentenced on principles involved rather than the monetary value. In addition, it was felt that the sentencing process should take into account the impact on the victim.

Views on whether online fraud should be perceived differently to offline fraud were mixed. However, a prevailing view was that the offline or online nature of the method of fraud made no difference to the seriousness of the offence and how it should be viewed for sentencing purposes. It was felt that regardless of the method used, the crime is the same.

6 Conclusion

There are myriad ways in which fraud can be committed. Fraud offences, in England and Wales, are defined as acts involving the dishonest intention to make gain, by exposing someone else to risk of loss. Two specific types of fraud offences have been the focus of this research – confidence fraud, and possessing, making or supplying articles for use in fraud. In addition, the research specifically aimed to provide greater understanding of how these two fraud offences are enabled or committed via online communication or technology; the impact of these types of fraud on victims; and, the relative weight given to aspects of these offences in terms of level of seriousness and harm, by those affected by them.

It was clear that victims of these offences may not even be aware that fraud has occurred, or of the different definitions of fraud offences that exist. They would rarely, for example, define their own experience as confidence fraud. In addition, it was clear that one offence type often predicates or is enabled by the other – for example, articles such as potential victims' email addresses, 'fake' websites, and payment facilities must first be set up. These may then be used to gather personal information or access victims' accounts, and in this way defraud them without them knowing. These articles could also be used to facilitate confidence fraud, with perpetrators using them to have email contact with victims, or victims believing they are purchasing genuine goods from a website set up using 'articles' for use in fraud.

Participants in this research described a range of specific online fraud offences. These indicated the complexity, and high level of planning and premeditation that goes into successfully facilitating online fraud. The most complex (and highly planned) offences appeared to be those that involved long-term contact between the victim and perpetrator characterised by investment and romance scams. However, regardless of the exact nature of the fraud, complex perpetration strategies tended to be adopted by perpetrators and in some cases meant a number of different fraudulent activities were used successfully to make a gain. Examples of these include diverting victims' phones so that their bank could not alert them to unusual online transactions after they had withdrawn money from their account, setting up professional quality websites that 'copy' those of government agencies or organisations and then accepting payment for goods which they never intended on sending, or telephoning victims and using 'normal' files on their PC as a cover for 'corrupted' files that need to be fixed by purchasing (fake) software.

Given the ubiquity of the internet in day-to-day life (for communication, banking, shopping, etc.) and the complexity of the perpetration strategies adopted, participants could report feeling powerless against the risk of online fraud. At the same time, however, they also reported a deep sense of shame or embarrassment that they had 'fallen for a scam' or when talking about others' experience of online fraud could themselves hold a view that the victim was somehow 'culpable'. This feeling of shame or confusion could, for some participants, be a reason why they did not report the offence; for others, it was more a sense that online fraud was almost inevitable, and a day-to-day nuisance.

Regardless of the attitude to the offence, participants reported a range of impacts flowing from it. Financial or other monetary types of loss (i.e. exchanging goods and not being paid for them), was one of the key impacts cited. This was not just in relation to the actual immediate loss but also the cost of then resolving the fraud (for example paying interest because they are overdrawn). Participants noted that the harm experienced due to financial loss is also relative to the financial situation of an individual, and so the seriousness of a fraud should not relate entirely to the absolute financial loss experienced. Financial loss could also lead to increased stress or anxiety for participants as they wondered how they would 'pay their bills' in the future. At the extreme end (and perhaps countering the view that the financial value of the fraud was not the most significant aspect when financial loss is

great) some participants had lost their life savings and with it had to significantly change their life.

The impact of online fraud participants had experienced was also felt emotionally and psychologically. For example, participants described how losing money had led to them feeling stressed. The actual process of the fraud occurring had also affected participants. Participants reported feeling 'duped', losing confidence in their own judgement, or being deeply shocked when they realised what they believed to be a genuine opportunity or relationship was in fact not. They were concerned that their personal information was being used and felt impotent to stop this. These reactions, for some, underpinned more severe manifestations of depression, family and relationship tension or breakdown (as participants did not want to tell people they knew about the fraud or felt they would 'blame' them when they did) and changes in behaviour, such as no longer using social media or buying goods online. Therefore, online fraud offences could have wide-reaching impacts, beyond that, and not always directly related to the financial value.

Having said this, financial reparation was a key outcome that participants felt would help assist to minimise these negative impacts; but this was also alongside feeling that the fraud had been taken seriously by the authorities, and the perpetrator realised the impact of their actions.

In terms of defining fraud offences as more or less serious, three key factors were felt to be significant: the impact on victims, the value of the fraud and the degree of pre-planning, complexity and organisation. Any one of these being evident could aggravate the offence, and a lack of any of these factors was not necessarily felt to mitigate. Perpetration strategies such as pretending to be in a position of authority, prolonged contact and 'grooming', of the victim, or targeting vulnerable people were also felt to increase the seriousness of the offence, and indicate a high level of planning.

On further detailed discussion with participants, however, another finding to emerge was the relative and subjective nature of defining harm and vulnerability in relation to online fraud. What may be harmful to one victim may not be felt to be so for another, particularly in relation to the value of the financial loss they experienced. Online communication can enable thousands of potential victims to be contacted regardless of their situation, with different fraud strategies playing to different vulnerabilities people may have.

Successful confidence frauds tend to play on a variety of different vulnerabilities, making it difficult to define exactly which type of vulnerability would make the offence more serious. Suggestions were made that people who are younger, older, or have a disability due to mental ill health such as learning disabilities or dementia could be considered particularly vulnerable, but participants caveated this with the recognition of the relative nature of this, depending on individual circumstances.

Online communication and technology seem to provide numerous opportunities for perpetrators to exploit or make contact with victims with which to commit fraud. However, on close examination, the key perpetration strategies used, types of fraud, and impact of the frauds, do not always differ greatly from those already familiar regarding fraud *per se.* The difference may be the potential reach and number of victims, and the facelessness of the crime, which can compound the impact it has.

References

Antokol, J. (2009). Identity theft: learning from the US experience. *Data Protection Law & Policy,* November 2009.

Bossler, A.M. and Holt, T.J. (2009) 'On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory (RAT)', *International Journal of Cyber Criminology,* Jan–Jun 2009, Vol. 3 Issue 1, pp 400–420.

Button, M., Lewis, C. and Tapley, J. (2009a) *Fraud Typologies and the Victims of Fraud Literature Review,* London: National Fraud Authority.

Button, M., Lewis, C. and Tapley, J. (2009b) *Support for the Victims of Fraud: An Assessment of the current Infra-Structure in England and Wales,* London: National Fraud Authority.

Button, M., Lewis, C. and Tapley, J. (2009c) *A Better Deal for Victims,* London: National Fraud Authority.

Button, M., Gee, J., Lewis, C. and Tapley, J. (2010). *The Human Cost of Fraud: A Vox Populi,* London: MacIntyre Hudson/CCFS.

Button, M., Lewis, C., and Tapley, J. (In press) 'Not a victimless crime; the impact of fraud on individual victims and their families', *Security Journal,* 1 (19).

CIFAS (UK Fraud Prevention Service) (2012) *Fraudscape: Depicting the UK's fraud landscape,* www.cifas.org.uk; March 2012.

Cole, S.A. and Pontell, H.N. 2006. ''Don't be low hanging fruit' Identity theft as moral panic' In: T. Monahan (Ed.), *Surveillance and security,* London, UK: Routledge.

Copes, H. and Vieraitis, L. (2009a) 'Bounded rationality of identity thieves: using offender-based research to inform policy', *Criminology and Public Policy,* 8 (2) pp 237-262.

Copes, H. and Vieraitis, L.M. (2009b) 'Understanding Identify Theft: Offenders' accounts of their lives and crimes', *Criminal Justice Review,* 34(3), pp 329-349.

Croall, H. (2007) 'Victims of White Collar and Corporate Crime', In: P. Davies, P. Francis and C. Greer (Eds), *Victims, Crime and Society*, pp. 78–108, London: Sage.

Croall, H. (2008) 'White Collar Crime, Consumers and Victimisation', *Crime Law and Social Change* (2009), 51, pp 127–146.

The Economic & Social Research Council (2005) *Research Ethics Framework*, Swindon: ESRC.

Farley, R. and Wang, X. (2009) 'Roving bugnet: Distributed surveillance threat and mitigation', *Computers and security,* 29 pp 592–602.

Fowles, T. and Wilson, D. 2011. 'Penal Policy File No. 130 January–March 2011', *The Howard Journal of Criminal Justice,* pp 331–332.

Fraud Advisory Panel (2006) *Victims of Fraud,* London: Fraud Advisory Panel.

Gannon, R. and Doig, A. (2010) 'Ducking the answer? Fraud strategies and police resources', *Policing and Society: An International Journal of Research and Policy.* 20 (1), pp 39–60.

Ganzini, L., McFarland, B., and Bloom, J. (1990) 'Victims of Fraud: Comparing Victims of White Collar and Violent Crime', *Bulletin of the American Academy of Psychiatry and Law,* 18 pp 55–63.

Gordon, G., Rebovich, D., Choo, K., and Gordon, J. (Eds.) (2007) *Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement*, Utica, NY: Center for Identity Management and Information Protection.

Goucher, W. (2010) 'Becoming a cybercrime victim', *Computer Fraud and Security,* Oct 2010, Feature, pp 16–18.

Government Social Research Unit (2005) *GSR Professional Guidance: Ethical Assurance for Social Research in Government,* Cabinet Office.

Hache, A. C. and Ryder, N. (2011) 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminal on the Web lurking to scam shoppers this Christmas: a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud', *Information and Communications Technology Law,* (20) 1, pp 35–56.

Hutchings, A. and Hayes, H. (2009) 'Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'?', *Current Issues in Criminal Justice,* 20 (3) pp 434–451.

Internet World Stats. (2012) *Internet Usage Statistics*, Retrieved December 2012, from https://www.internetworldstats.com/stats.htm.

Jaishankar, K. (2010) 'The Future of Cyber Criminology: Challenges and Opportunities.' International *Journal of Cyber Criminology,* Jan–Dec 2010, 4 (1/2), pp 26–31.

Johnson, M. (2010) 'The difficulty in managing e-gaming cybercrime risks', *World Online Gambling,* August 2010.

Koops, B-J., Leenes, R., Meints, M., van der Meulen, N. and Jaquet-Chiffelle, D-O. (2009) 'A typology of identity-related crime' *Information, Communication and Society,* 12 (1) pp 1–24.

Kvale, S. and Brinkman, S. (2009) *Interviews – Learning the Craft of Qualitative Research Interviewing*, London: Sage.

Levi, M. (1999) 'The Impact of Fraud', *Criminal Justice Matters,* 36: 5–7.

Levi, M. (2001) 'White Collar Crime Victimisation', In: N. Shover, and J.P. Wright (Eds), *Crimes of Privilege,* Oxford: Oxford University Press.

Levi, M. (2009) 'Suite Revenge? The Shaping of Folk Devils and Moral panics about White-Collar Crimes', *British Journal of Criminology*, 49, pp 48–67.

Levi, M. (2010) 'Hitting the suite spot: sentencing frauds', *Journal of Financial Crime,* 17 (1) pp 116–132.

Levi, M. and Pithouse, A. (1992) 'The Victims of Fraud', *Unravelling Criminal Justice,* In: D. Downes (Ed.), London: MacMillan.

Lewis, L. (2010) 'Madoff's Victims and Their Day in Court', *Society,* Vol. 47 Issue 5, pp 439–450.

Lewis, L. (2010b) 'Madoff's Victims Go on the Offensive', *Society,* Vol. 47 Issue 6, pp 534–542.

Mason., J. (2002) *Qualitative Researching*, 2nd edition, London: Sage.

McNaughton Nicholls, C., Mitchell, M., Simpson, I., Webster, S. and Hester, M. (2012) *Attitudes to Sentencing Sexual Offences*, London: The Office of the Sentencing Council.

Metropolitan Police. (n.d) *The Little Book of Big Scams*.

Ministry of Justice (2010) *Breaking the Cycle: Effective punishment, rehabilitation and sentencing of offender,* Green Paper presented to parliament December 2010.

Office of Fair Trading (2006) *Research on Impact of Mass Marketed Scams,* London: Office of Fair Trading.

Office of Fair Trading (2009) *The Psychology of scams: Provoking and committing errors of judgement,* Prepared for the Office of Fair Trading by the University of Exeter School of Psychology.

Office for National Statistics (2012) *Crime in England and Wales, year ending June 2012 Statistical Bulletin.*

Pascoe, T., Owen, K., Keats, G. and Gill, M. (2006) *Identity Fraud: What About the Victim.* Leicester: Perpetuity Research and Consultancy International.

Piquero, N.L, Choen, M.A. and Piquero, A.R. (2011) 'How much is the public willing to pay to be protected from identity theft', *Justice Quarterly,* 28 (3).

Pontell, H, N. (2009) 'Identity theft: Bounded rationality, research, and policy', *Criminology and Public Policy,* 8 (2) pp 263–270.

Randall, C. (2010) *E-Society*, London: Office for National Statistics.

Rege, A. (2009) 'What's love got to do with it? Exploring online dating scams and identity fraud', *International Journal of Cyber Criminology,* 3 (2) pp 494–512.

Ritchie, J. and Lewis, J. 2003. *Qualitative Research Practice,* London: Sage.

Ritchie, J., Lewis, J., McNaughton Nicholls, C. and Ormston, R. (In press) *Qualitative Research Practice,* 2nd Edition, London: Sage.

Rogers, J. (2007) *Gartner: Victims of Online Phishing up nearly 40% in 2007,* SC Magazine.

Shichor, D., Sechrest, D. and Doocy, J. (2000) 'Victims of investment fraud', In: H. Pontell and D. Shichor (Eds.), *Contemporary issues in crime and criminal justice: Essays in honor of Gilbert Geis:* pp 87−96.

Spencer, L., Ritchie, R., O'Conner, W., Morrell, G., and Ormston, R. (In press) 'Analysis in practice', In: J. Ritchie, J. Lewis, C. McNaughton Nicholls and R. Ormston (Eds) *Qualitative Research Practice,* 2nd Edition, London: Sage.

Sentencing Guidelines Council (2009) *Sentencing for Fraud – Statutory Offences.* London: Sentencing Guidelines Council.

Slosarik, K. (2002) 'Identity theft: An overview of the problem', *Justice Professional,* 15, pp 329–343.

Smith, A.D. (2005) 'Identity theft and e-fraud as critical CRM concerns', *International Journal of Enterprise Information Systems,* 1, pp 17–36.

Spalek, B. (1999) 'Exploring the Impact of Financial Crime: A Study Looking into the Effects of the Maxwell Scandal upon the Maxwell Pensioners', *International Review of Victimology,* 6, pp 213–230.

Taylor, P. and Bond, S. (2012) 'Crimes detected in England and Wales 2011/12', *Home Office Statistical Bulletin,* 8/12.

Tsoutsanis, A. (2012) 'Tackling Twitter and Facebook Fakes – ID theft in Social Media', *World Communications Regulation Report,* April 2012, 7(4).

Tupman, W. (2010) 'Keeping under the radar: watch out for 'Smurfs', *Journal of Financial Crime,* 17 (1) pp 152–162.

UK Payments Administration (2009) *Number of internet users now banking online exceeds 50% for first time ever,* Retrieved February 2013, from https://www.ukpayment.org.uk

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

Webb, R. (2010) 'A new approach to online consumer protection in the UK', *E-commerce Law & policy,* April 2010.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A. and Craparo, G. (2012) *European Online Grooming Project: Final Report*, European Commission Safer Internet Plus Programme: http://www.europeanonlinegroomingproject.com/

Whitty, M. and Buchanan, T. (2012) *The psychology of the online dating romance scam,* University of Leicester: UK.

Yeo, A., Legard, R., Keegan, J., Ward, K., McNaughton Nicholls, C. and Lewis, J. (In press) 'In-depth interviews', *Qualitative Research Practice,* 2nd Edition, London: Sage.

Appendix A Methodology

This appendix provides further detail about the way in which the research was conducted. The research comprised three phases: a Rapid Evidence assessment; qualitative research with key professional stakeholders who were working at the forefront of fraud prevention across a range of relevant organisations; and, people who had directly experienced some form of online or online enabled fraud which fell within the two categories of fraud offences in scope for this study.

Phase 1: Rapid Evidence Assessment

The evidence assessment involved a detailed scoping of existing evidence sources. It focussed on different types of fraud within the two categories of focus for this study, including emerging fraud, how fraud occurs and issues of culpability, mitigating and aggravating factors inherent, and, the impact of fraud including the seriousness and harm of the offence. In addition, online fraud was explored as a key emerging issue. Additional key documents such as the existing sentencing guidelines were also included. A comprehensive literature search was conducted, focussing on evidence published post-2009 and including evidence published pre-2009 where relevant. This included peer reviewed academic articles, reports, websites and discursive articles in relevant medium such as financial industry magazines. The databases searched were: Web of Science, International Bibliography of the Social Sciences (IBSS), SocINDEX, Criminal Justice Abstracts, and Legal Journals Index.

To ensure that literature was fully explored and collected, comprehensive database searches were conducted using the following search terms:

- ‘confidence fraud’, ‘confidence scam’;
- ‘possessing, making or supplying articles for use in fraud’;
- ‘online fraud’, ‘online scam’, ‘cyber scam’, ‘cyber fraud’;
- ‘fraud’ and ‘victim’;
- ‘scam’ and ‘victim’;
- ‘fraud’ and ‘criminal justice’;
- ‘fraud’ and ‘sentencing’;
- ‘vishing’, ‘phishing’, ‘botnet’, ‘trojan’, ‘pharming’;
- ‘social engineering’;
- ‘identity theft’ and ‘victim’; and
- ‘financial crime’ and victim’.

This generated a high volume of literature. The abstracts of these were then individually reviewed and assessed for relevance by a member of the research team. At this point it was decided that 65 articles and 9 reports were relevant. This literature was assessed and summarised thematically in a matrix in Excel using the following dimensions:

- author and reference details;
- year and country of focus;
- source – peer reviewed, policy report, grey literature etc;
- online, offline or mixture; and
- methods, sample size and validity.

Findings related to:

- type of fraud and how it was carried out (specifically focussing on nuances among confidence fraud, possessing making and supplying articles for use in fraud and new emerging fraud);
- impact of fraud;
- evidence of seriousness;
- evidence of culpability of offender;

- general – any findings relevant to sentencing;
- other; and
- additional references or sources identified.

The review criteria were agreed among the team and subsequently with the Office of the Sentencing Council. Relevant articles were then systematically synthesised in the thematic matrix, and pre-2009 references were also included where relevant.

On completion of the review, the entire dataset of evidence was summarised in a report which was provided to the Office of the Sentencing Council. The findings from the review were then used to hone the development of phases two and three of the study – qualitative research with stakeholders and people who had been directly affected by online fraud. Relevant literature and evidence has been referenced in the main body of this report. To ensure comprehensive coverage a greater number of articles were reviewed during the evidence assessment stage than are cited in the main report with only particularly relevant evidence drawn on in the report.

Phase 2: Research with professional stakeholders

The aim of this phase was to draw on stakeholders' knowledge, expertise and experience to address the aims of the research. Stakeholders' experience at the forefront of fraud prevention and victim support work, alongside their knowledge of specific cases, equipped them with the most up-to-date information that could be used to cover all three research strands.

Nine stakeholders took part in the study by being interviewed face-to-face, or where it was more convenient for them, over the telephone. Stakeholders were selected from a range of organisations which included the National Fraud Authority, the police and a support group for people who had experienced fraud.[27]

Interviews lasted between 50 and 85 minutes, and were audio recorded and fully transcribed verbatim. The interviews were conducted using a topic guide (full version available in Appendix B.1). The main areas covered are listed below:

- background information about the participant's role and their knowledge and experience of working with fraud offences;
- the ways in which fraudulent activities are currently being committed;
- the impact of online fraud on the victims involved;
- the factors that impact on sentencing; and
- the ways in which fraudulent activities will develop in the future.

Phase 3: In depth interviews and focus groups with people who have been directly affected by online fraud

Phase three involved primary research with victims of online fraud and adopted two distinct strands, described below:

- **focus groups** (six in total) with 48 members of the public who had been victims of fraud conducted completely or partially over the internet. The focus groups were used to explore experiences of how online fraud is committed and perceptions relating to the seriousness of online fraud offences, the culpability of the offender and what should be the key aggravating and mitigating factors. Impacts of online fraud were also explored. Discussion was prompted by the use of four vignettes, at least two of which were discussed in each focus group.

[27] Stakeholders were offered anonymity and are therefore not listed in the report.

- **in depth interviews** with 15 people who were victims of the online fraud which was in scope for this study. This format permitted a detailed exploration of individuals' experiences of online fraud, in particular the way that the fraud had been committed and the type of harm and impacts they had experienced. Issues relating to the seriousness of the offence and the culpability of the offender were also discussed.

Focus group participants tended to be people who had been defrauded generally via possessing, making or supplying articles for use in fraud or had experienced low level confidence frauds. Focus groups were used to bring together people who had experienced a diverse range of common types of online fraud such as buying goods that did not arrive. They were conducted with the use of a topic guide (a full version is available in Appendix B.3). The group dynamic allowed the research team to expose participants to different online fraud scenarios in the form of vignettes and generate rich discussion in relation to these focussed examples. The fraud offences discussed across the six groups were:

- **online romance fraud**: a woman met a man on an online dating site, and had given him money following various requests e.g. when the man lost his job he claimed he was having difficulty paying his rent. On investigation by the police it became apparent that the man was in fact another person than his dating profile, living in another city;
- **identity fraud**: a young male received an email asking for his personal details that looked as if it was from his bank. He sent his details and they were used by the perpetrator to access his online bank account and withdraw over £2,000 from his account;
- **consumer fraud**: a woman signed up to a trial of slimming pills on a website which was promoting them. After three months with no effect, she tried to follow the cancellation process but her calls and emails went unanswered and she kept receiving the pills;
- **advance fee fraud**: an elderly lady recently started to use the internet and received an official looking email saying she had won a large amount on the lottery. The email also asked for a fee so her prize money could be released. She subsequently sent more money to cover various fees and taxes but the prize money never arrived.

A full version of each vignette is included in Appendix B.4.

Given the breadth of issues to cover in the discussion, two vignettes on online fraud were covered in each group, with a third also briefly discussed if time permitted. This meant that different frauds could be compared and contrasted, which helped to meet the overarching objectives of the Sentencing Council. Spontaneous reactions to the vignettes were explored at first, followed by discussion of specific aspects of the offences (for example financial amount involved, level of planning, duration of offence, personal circumstances of offender). This generated discussion around the factors affecting perceptions of seriousness of the offence, harm to the victim, culpability of the offender and aggravating and mitigating factors. Each specific offence vignette was discussed three to four times within the focus groups overall, with a sample of 25 to 34 participants. This approach enabled a range of different offences to be explored, in depth, within the parameters of the research.

In depth interviews were conducted with participants who had experienced more sensitive and extensive frauds and therefore permitted an approach that was responsive and tailored to individual experiences. They were conducted with the use of the topic guide (a full version is available in Appendix B.2), and the main areas covered included:

- background and context information about the participant's general circumstances;
- an overview of the online fraud they had experienced;

- their experience of harm associated with the online fraud;
- views on factors which influence culpability of the offender and seriousness of the offence; and
- views on reporting the fraud and the sentencing process.

Fieldwork for phases two and three took place between July and October 2012.

Recruitment

Participants who had experienced fraud were recruited through the following three methods:

- **Action Fraud**[28]:individuals making contact with Action Fraud were for a set period of time asked whether they would be willing to be re-contacted again by Action Fraud to see if they would like to take part in some research. Following this exercise, the research team selected six recruitment areas. Those individuals within the six research areas who had agreed to be re-contacted and who had been victims of the type of fraud that fell within the scope of this study (potential participants) were sent an information letter and leaflet about the study by Action Fraud. Participants could then express an interest in opting into the study by contacting the NatCen research team directly via a freephone number or by email. On making contact with a member of the NatCen research team, participants were asked a number of screening questions designed to collect some basic demographic information and to gain a brief overview of the type of fraud they had experienced and their level of internet usage. This information was used to monitor the sample to ensure there was range and diversity across the key characteristics age, gender and online fraud.

- **stakeholders participating in phase two (gatekeepers):** each stakeholder who participated in phase two was asked whether they would be willing to help with the recruitment of victims of fraud to take part in phase three. Stakeholders approached victims they were in contact with and asked their permission to pass their contact details onto the NatCen research team. Alternatively, they gave the individual the research team's contact details so they could make contact directly and find out more about the study and what taking part would involve. A range of stakeholders who were in direct contact with people who had experienced fraud assisted with recruitment of participants. This included the police and a support group for people who had experienced fraud. As noted in the main report all stakeholders assisting with this part of the study were provided with a verbal briefing from members of the research team. Stakeholders were also provided with copies of the information leaflet they could pass on to potential participants regarding the research. Potential participants could then contact the research team directly or give their consent for their contact details to be passed on to the research team. On making contact the research team ensured that information about the research process was then fully reiterated to each participant before asking if they were still willing to take part, as it was impossible to be sure of the level of detail that had been communicated by stakeholders to potential participants.

- **a recruitment agency:** the intention at the start of the study was to recruit all focus group participants through Action Fraud. While a small number of focus group participants were recruited in this way, the numbers opting in were insufficient to organise six focus group discussions. Therefore a recruitment

[28] Action Fraud is the UK's national fraud and internet crime reporting centre. They provide a central point of contact for information about fraud and financially motivated internet crime. The service is run by the National Fraud Authority.

agency, Propellerfield, was also used to recruit participants. NatCen had previous experience of working with this agency and they were chosen for being both trusted and effective. The research team held a face-to-face meeting with Propellerfield so they could be fully briefed on the study and the recruitment process. Flow populations[29] were used, with potential participants screened to ensure all of the participants firstly used the internet, and secondly had experienced online fraud. All had therefore experienced some form of fraud over the internet. This includes advance fee fraud, malware, account takeover, identity theft, fake websites (phishing and spam), and buying good and services that did not arrive/were fake (such as tickets).

Given that the research was advertised widely (via letters, on newsletters and via stakeholders) it is impossible to know how many potential participants came into contact with information about the research and decided not to take part. It was also impossible to know the level of detail regarding the research process that was communicated by stakeholders when they first informed potential participants about the research. To ensure participants were fully informed, the research team, on making contact with potential participants for the first time, provided them with additional information regarding the research: who it was being conducted for, the nature and content of the interview/ group discussion, and how data would be used and stored. An information leaflet about the research was also provided to each participant by the researcher, and the consent process repeated before the interview took place.

Focus groups were conducted in England and Wales in areas selected to reflect different parts of the country (Brighton, Bristol, Birmingham, Cardiff, Manchester and London). Participants who fitted specific selection criteria (i.e. the fraud they had experienced was in scope for the study and in terms of the key sampling criteria described below), were then either invited to a group discussion or an individual interview was arranged. It is standard practice to give participants a small payment as a thank you for the time they have given to take part in a study and enable participation by ensuring any costs they may have incurred to take part (such as travel costs or car parking when attending a group discussion), are covered. Therefore participants were given £25 for taking part in an in depth interview and £30 for taking part in a group discussion. The differing amounts were given due to the need for local travel to attend focus groups, and recognition of the cost this could incur. Interviews tended to take place in participants' homes.

Contact with prospective participants was monitored to try and achieve a range of experiences within and across the groups according to gender, age, ethnicity, whether they lived with other people or alone, their employment and health. The breakdown of characteristics is presented in the section on the sample below.

Sample

The ability to draw wider inference from qualitative research depends, in part, on the nature and quality of sampling. The rationale in selecting those to be included was to ensure diversity of coverage across certain key variables rather than to select a sample that was statistically representative of the wider population. The sample was monitored across key sampling criteria to ensure diversity in terms of age, gender and type of fraud experienced. However there were also some limitations to the sample, discussed previously in the main report.

[29] This term is used when samples are generated by approaching people in a particular location or setting (Ritchie et al., in press).

Focus group sample

The final sample achieved across the focus groups is shown below. Quotas for age and gender were set to ensure each group included a range of participants in terms of these two characteristics. Out of a total of 48 focus group participants, six were recruited through Action Fraud and 42 were recruited through the recruitment agency.

Table A.1 Achieved sample characteristics for focus groups with participants

Gender	
Female	25
Male	23
Total	**48**
Age	
16 – 24	6
25 – 40	21
41 – 59	15
60 +	6
Total	**48**
Ethnicity	
White British	43
Other White	1
Mixed	2
Asian	1
Black (Caribbean)	1
Total	**48**
Household	
Live alone	8
Live with others	40
Total	**48**
Socio-economic activity	
Full time or part time work	36
Education or training	2
Unemployed	2
Retired	7
Other	1
Total	**48**
Health	
Visual or hearing impairment	3
Limited physical activity	1
Long-standing physical/psychological condition	4
None	40
Unknown	5
Total	**53**[30]

[30] Some participants reported more than one type of disability.

All participants had experienced some form of fraud over the internet. This includes advance fee fraud, malware, account takeover, identity theft, fake websites (phishing and spam), and buying goods and services that did not arrive/were fake (such as tickets). Additionally, participants were asked to rate their financial literacy and describe their internet usage and the responses are shown in Tables A.2 and A.3 below.

Table A.2 Internet usage - focus group participants

Rarely	0
Frequently	14
Daily or uses the internet in more than 6 different ways	34
Total	**48**

Table A.3 Financial literacy – focus group participants

Very confident	13
Confident	29
Not very confident	6
Not confident at all	0
Total	**48**

As shown above, the groups were all mixed gender and mixed age; the make-up of each group is summarised in Table A.4 below.

Table A.4 Number of participants taking part in each focus group and type of group

Group 1	7, mixed age and mixed gender
Group 2	10, mixed age and mixed gender
Group 3	10, mixed age and mixed gender
Group 4	4, mixed age and mixed gender
Group 5	9, mixed age and mixed gender
Group 6	8, mixed age and mixed gender

Conduct of the focus groups

The focus groups lasted approximately two hours with a short break in the middle. They were facilitated using a topic guide and vignettes agreed with the Sentencing Council that related to specific scenarios involving different fraud offences.

Participants were asked to discuss their experiences of online fraud. Basic information about different types of fraud (see Appendix B.7) and sentencing guidelines (see Appendix B.5) were provided at the end of the discussion, as well as information on help and advice (see Appendix B.6). Information was withheld until the end so that this did not influence participants' thinking. This was felt to be appropriate to ensure the suggested sentences reflected perceptions that had not been unduly biased by the introduction of specific information.

The fraud offences discussed in each group, and the ordering of the discussion, are shown in Table A.5. Participants were asked to give an overview of the fraud they experienced and about their general awareness of fraud offences and the sentencing of them. The facilitators then discussed the vignettes with the group. Participants were asked about the harm, seriousness and culpability of the offence, and what they thought an appropriate sentence would be. The facilitator then varied the specific details of the vignette in order to stimulate further discussion of factors linked to perceptions of culpability, harm to victims/survivors and factors that might be considered aggravating or mitigating in various circumstances.

Table A.5 Fraud offence vignettes and order of discussion for each focus group

Group 1	Identity theft fraud, consumer fraud, advance fee fraud
Group 2	Advance fee fraud, online romance scam
Group 3	Identity theft fraud, online romance scam
Group 4	Consumer fraud, advance fee
Group 5	Identity theft fraud, consumer fraud, online romance scam
Group 6	Advance fee fraud, online romance scam

Interview sample

The final sample achieved across the interviews is shown in Table A.6 below. Interviewees had experienced online romance scams, investment frauds, and a range of advance fee frauds, malwares, fake websites and spam. The nature of online fraud (as discussed in the report) means that a number of different fraudulent activities often were used to successfully make gain (financial or otherwise) from the victim.

Table A.6 Achieved sample characteristics for in depth interviews with participants

Gender	
Female	8
Male	7
Total	**15**

Age	
16 – 24	0
25 – 40	3
41 – 59	5
60 +	7
Total	**15**

Ethnicity	
White British	12
Other White	1
Mixed	0
Asian	1
Black (Caribbean)	0
Unknown	1
Total	**15**

Household	
Live alone	4
Live with others	11
Total	**15**

Socio-economic activity	
Full or part time work	9
Education or training	0
Unemployed	2
Retired	2
Other	1
Unknown	1
Total	**15**

Health	
Visual or hearing impairment	0
Limited physical activity	5
Learning difficulty	1
Long-standing physical/psychological condition	1
None	10
Total[31]	**17**

Interview participants were also asked to complete some additional self-reporting information about their internet usage and confidence with financial matters. The results of this are presented below in Tables A.7 and A.8.

Table A.7 Internet usage – interviews

Rarely	1
Frequently	2
Daily	8
Unknown	4
Total	**15**

Table A.8 Financial literacy – interviews

Very confident	4
Confident	7
Not very confident	2
Not confident at all	1
Unknown	1
Total	**15**

Conduct of interviews

The interviews were conducted at a time and place convenient for participants. This was usually at their home. Given the potentially sensitive nature of these interviews this was felt to be an appropriate setting. Interviews lasted between 60 to 90 minutes. Interviews covered similar issues as those in the focus groups but participants were not asked to comment on vignettes, instead discussing their own experience in more detail including their views on concepts relevant to sentencing fraud offences, and appropriate sanctions. Interview participants included those who had been defrauded out of hundreds of thousands of pounds and who had had long term repeated contact with the perpetrator. The one to one nature of in depth interviews allowed participants to recount complex fraud offences at their own pace and in detail.

Analysis of data – stakeholder interviews, and focus groups and in depth interviews with victims of online fraud

All interviews and group discussions were transcribed verbatim. The data was managed and analysed using the Framework approach developed by NatCen (Ritchie et al., 2003; Ritchie et al., in press). Key topics which emerged from the interviews and groups were identified through familiarisation with the transcripts. Two analytical frameworks were then drawn up (one for stakeholders and one for participants) and a series of thematic charts or matrices were set up, each relating to a different thematic issue. The columns in each matrix represented the key sub-themes or topics and the rows represented individual participants or

[31] This was a multiple response question and therefore the total number of responses was greater than 15.

groups. Data from each transcript was then summarised into the appropriate cells. Bespoke software enabled the summarised data to be hyperlinked to the verbatim transcript text. This approach meant that each part of every transcript that was relevant to a particular theme was noted, ordered and accessible. The final analytic stage involves working through the charted data, drawing out the range of experiences and views, identifying similarities and differences and interrogating the data to seek to explain emergent patterns and findings (Spencer et al., In press).

The findings that emerged are presented in the main report. The report deliberately avoids giving numerical findings, since qualitative research cannot support numerical analysis. This is because we seek to describe the range and diversity among sample members rather than to build a statistically representative sample, and because the questioning methods used are designed to explore issues in depth rather than to generate data that can be analysed numerically. Qualitative research provides an in depth insight into the range of experiences, views and recommendations. Wider inference can be drawn on this basis rather than on the prevalence of responses. The focus of the findings presented has been on the perceptions and experiences of the participants, which have been evidenced with quotes and case studies and numerical weight not given to these.

Reporting

The findings have been organised thematically across the report, with the findings from the research with participants who took part in an in depth interview reported alongside the focus group data, rather than being reported separately. This strategy recognises the fact all the participants who took part in this study had experienced online fraud to varying degrees and that many of the key findings were similar across the sample. However where appropriate, the perceptions of the different participant groups have been made explicit within the text.

An important limitation of the research is that, while the qualitative approach adopted is able to demonstrate the range of views on how online fraud is being carried out and the issues relating to sentencing, it is not possible to say without quantitative research how statistically representative those views are of people who have been directly affected by online fraud more generally. Therefore the findings are not reported numerically but represent the range and diversity of views expressed.

Ethical considerations and data security

Research always requires careful consideration of ethical practice. However research such as this, focussing on sensitive but important issues requires particularly careful management.

Recruitment was conducted via an ‘opt-in’ basis. Potential participants were provided with information regarding the research, who it was being conducted for, the nature and content of the interview/group discussion, and how data would be used and stored. They were then asked if they would be willing to take part and if they agreed were asked to contact the NatCen research team directly or gave permission for their contact details to be passed on. On making contact the NatCen research team asked them some screening questions to confirm that the type of fraud they had experienced was in scope for this study and to collect some monitoring data from them. This was so the sample could be monitored across key characteristics to ensure range and diversity. Participants were then either invited to take part in a focus group discussion or an individual in depth interview was arranged. The choice of method was determined by both the nature of the fraud experienced and participants’ wishes about how they wanted to take part in the study.

Focus groups which bought together members of the public who had experienced fraud, took place in neutral, accessible public venues such as hotel conference rooms. The consent process was repeated before the group discussion commenced and participants were informed of the voluntary nature of their contribution and that they could leave the room, or take a break and return at any point in the discussion. Given the potential for the individual

in-depth interviews to cover potentially more sensitive areas, they were arranged at a time, date and location that suited participants and generally took place in participants' homes. The option of having the interview in a neutral setting was offered; however, no participants opted for this. A small number of interviews took place over the telephone at the participant's request.

Information about the research was circulated and included details of who was conducting the research, who it was being conducted for, the aim of the research, the nature of the interview and how the data would be used and stored. This was reiterated during recruitment and before commencing an interview. The interviews could include discussion of highly sensitive or distressing information and were conducted by experienced research staff.

Appendix B: Fieldwork materials

Mason (2002) and Kvale and Brinkman (2009) stress the range of tasks that interviewing involves. At any one time the researcher needs to: listen to what is being said and understand it; assess how it relates to the research questions; be alert to contradictions with what has been said earlier; decide what to follow up or explore in more detail now and what to return to later; decide how to phrase the next question; pick up on nuances, hesitation, emotion and non-verbal signals; pace the interview; keep an eye on recording equipment, and deal with any distractions or interruptions that arise. Concentration and stamina are essential qualities for coping with these simultaneous demands. Carefully designed topic guides are essential aides to the process as are the skills and preparation of the interviewer.

The research team involved in this study were all highly experienced. Tailored topic guides were developed and used in all interviews and groups to help ensure a consistent approach across interviews/ groups and between interviewers. However, the guides were used flexibly to allow interviewers to respond to the nature and content of the discussion, so the topics covered and the order in which they were discussed varied, especially between interviews. Interviewers used open, non-leading questions and answers were fully probed, especially in the in depth interviews. Probes were responsive; follow-up questions which elicit more information, description or explanation, such as ‘How?’, ‘In what way?’ (Yeo et al., In press) were used. Outlines of the main headings used in topic guides for in depth interviews with stakeholders and in depth interviews and groups with participants are provided below. Full copies of the vignettes used for the focus groups follow the group topic guide.

B.1 Topic guide for stakeholder interviews

The study

Aims:

- review ways fraud is being committed;
- outline issues relating to culpability/seriousness of offences; and
- outline impact of different types of online offences/activities on victims.

The overall objective of the study is to inform future sentencing guidelines regarding 'confidence fraud' and 'possessing, making or supplying articles for use in fraud'.

Generally:

- map and describe the range and diversity of ways in which the two offence categories' are currently being committed, online or otherwise, including any changes or new ways of committing the offences and the impact of the proliferation of new technologies;
- map the factors impacting on the culpability of offender/seriousness of offence, including mitigating and aggravating factors; and
- explore the impact of online fraud offences on victims, including which types of 'harm' are most significant to victims.

Guidance for interpretation and use of the topic guide

The following guide does not contain pre-set questions but rather lists the key themes and sub-themes to be explored with each participant. It does not include follow-up questions like 'why', 'when', 'how', etc. as participants' contributions will be fully explored throughout in order to understand how and why views and experiences have arisen. The order in which issues are addressed and the amount of time spent on different themes will vary between interviews.

Due to the different roles of participants this topic guide is aimed to function in such a way as to cover the range of roles that could be involved in the interviews.

1. Introduction

- Introduce researcher and NatCen
- Explain who the research is for – Sentencing Council
- Explain research:
  - the overall objective of the study is to inform the development of future sentencing guidelines around two types of fraud offences – **'confidence fraud'** and **'possessing, making or supplying articles for use in fraud'.** (Note: we understand they may not use these terms and will explore what types of fraud this includes in the interview. However, it is important to be clear that the offences discussed fall under the two categories above).
- Explain the interview will last around 1 hour. The discussion will focus on:
  - their awareness of ways in which fraudulent activities are being committed;
  - their views on the factors that impact on how these offences are sentenced such as the culpability of offender and seriousness of offence;
  - their views on the impact of fraud in victims, especially online; and
  - their awareness of how fraudulent activities are currently changing over time and the extent and nature of change they envisage in the future (including how this might change the culpability of the offender and cause different harm to the victim).

- Explain voluntary nature of interview:
  - no right or wrong answers;
  - participation is voluntary – can have a break or choose not to discuss any issue/answer any question; and
  - we are happy to obtain additional material, statistics or evidence following the interview if they identify any as we discuss it.
- Explain recording, data storage and confidentiality;
- Confirm that we wish to avoid using full names or addresses of any stakeholders/victims mentioned including locations where they work/live;
- Explain reporting process and that no individual will be identified in the report. Data will be destroyed on completion of the research and study findings will be available if interested;
- Check if any questions before starting; and
- Ask for permission to start recording and explain that you will ask for their verbal consent to take part in the interview once you have turned the recording on.

START RECORDING

- Ask the respondent for verbal consent – highlight the disclosure policy.

2. Background and context

Aim: To set participants' knowledge of fraudulent offences in context and to provide some background information about the nature of their role and organisation they work for.

- Ask to specify their professional position:
  - nature and role of organisation;
  - their specific role in the organisation; and
  - typical working day.
- Ask to provide an overview of their previous experience of working in the area of fraud:
  - nature of their involvement;
  - experience of working with victims; and
  - experience of working with offenders.

3. Awareness of ways in which fraudulent activities are currently being committed

Aim: to explore participant's knowledge of how fraudulent activities are currently being committed. To explore their views on how different methods of committing fraud have recently changed and the extent to which the CJS recognises any newer methods.

Interviewer note:
***Confidence fraud** involves a victim transferring money and/or property as a result of being deceived or misled by the offender.*
***Possessing, making or supplying articles for use in fraud** can be committed in many ways. Examples of 'articles' include any electronic programs or data stored electronically, false fronts for cash machines, and draft letters or emails for use in fraud.*

- Way in which 'confidence fraud' is being conducted in UK:
  - types of fraud they are familiar with that fit this category; and
  - types of victims.

- Ways in which 'possessing, making or supplying articles for used in fraud' conducted in UK:
  - types of fraud they are familiar with that fit this category; and
  - types of victims.
- Perceived prevalence of different types of fraud:
  - examples of offence/activity types;
  - sources of information; and
  - specific victim types that map onto different frauds;
- Changes in recent past:
  - case examples.
- Drivers of change:
  - Online; and
  - other technological advances.

4. Impact of (online) fraud on victims

Aim: to explore the impact of fraudulent activities on the victims involved, especially when the offence has been carried out online. Explain key focus is online fraud however if they feel these impacts are cross-cutting please indicate this.

- Range and diversity of ways in which victims are harmed by online fraud offences and activities:
  - financial;
  - psychological;
  - social;
  - physical;
  - emotional; and
  - short term and longer term impacts.
- Views on which types of harm are most significant for victims; reasons why:
  - sources of evidence.
- Views on wider impact
  - other people in the victim's social network e.g. family, peer group; and
  - wider social and economic harm.
- Extent to which the impacts for online are the same as offline fraud.
- Extent to which the impacts for online are different to offline fraud:
  - reasons for difference.

5. Factors that impact on sentencing

Aim: to explore the factors which affect how serious the fraudulent activity is and the factors that impact on the culpability of the offender.

With the impact on victims in mind, we would like to explore sentencing practice and the issues they think should be taken into account when sentencing.

NOTE: the researcher may want to refer to some of the actual issues taken into account in the existing guidelines and gain their view on them.

- Awareness of current sentencing practice for offences discussed.
- Views on what should be taken into account.
- Factors that impact on seriousness of the 'harm' offence/activity causes victim:

  - characteristics of victim (e.g. vulnerability);
  - online manipulation/disinhibition;
  - number of victims targeted;
  - nature and method of fraudulent offence/activity;
  - relationship between victim and offender (contact/non-contact);
  - duration of offence/activity;
  - extent of financial loss; and
  - ongoing effect on victim.
- Factors that impact on culpability of the offender:
  - motivation for fraud;
  - extent of pre-planning vs. opportunistic;
  - deliberately targeting vulnerable victim(s);
  - complexity of fraud;
  - acted along or with others/role in offence;
  - fraudulent commercial enterprise;
  - characteristics of offender (e.g. vulnerability, repeat offender); and
  - wider social and economic harm.
- Perception mitigating factors:
  - what may lead to a shorter sentence:
    - opportunistic;
    - financial duress of perpetrator;
    - mental health;
    - addiction;
    - not aware they were committing/involved in fraud; and
    - anything else.
- Views on appropriateness of aggravating and mitigating factors currently recognised by CJS – COULD REFER TO ACTUAL GUIDELINES HERE
  - comparisons to other types of crime; and
  - give examples.
- Extent to which the factors which impact on sentencing are different for online compared to offline fraud:
  - reasons for difference.

6. Fraudulent activities in the future

Aim: as a final section explore how fraudulent activities could develop in the future, and how sentencing guidelines will reflect these changes.

- Expectations of how ways of committing fraudulent activities could develop in the future:
  - drivers of change;
  - technology;
  - type of fraud;
  - enablers of fraud;
  - social media;
  - smart phone;
  - virtual worlds; and
  - gaming.
- Expectations of how future developments may impact on sentencing fraud offences if at all.

- How future developments might change the nature and extent of impact/harm to the victim:
  - financial;
  - psychological;
  - social;
  - physical;
  - emotional; and
  - short term and longer term impacts.

7. Concluding thoughts

Aim: Wrapping up discussion

Remind participant that a core aim of the research is to make recommendations for future sentencing guidelines around confidence fraud and possessing making or supplying articles for use in fraud

- Key recommendations for future sentencing guidelines:
  - areas to change; and
  - areas to retain.
- Any other areas to consider; and
- Any final comments on the research – messages for the Sentencing Council re: sentencing fraud offences or emerging fraud.

Check if the participant has any questions or comments about the discussion
Don't forget to cover the points on the next page

****

Thank participants for their time and thoughts.
Check they have the research information letter/email informing them of the research.
Reassure re confidentiality.
Distribute contact details should they wish to add anything about their comments or in case they have questions about the research later.

Discuss victim recruitment and the possibility of their support with this.

- The next stage of the study is to recruit victims of the two types of fraud that has been committed or enabled via online communication or technology to take part in focus groups and interviews.
- We would like to check whether they are able to help with this/know anyone who could help with this next stage?
- Recruitment could take place in a variety of ways e.g. the organisation sends advance letters on our behalf (if they have permission to contact victims for research), place an advert on their website, hand out leaflets about the study etc.
- We would welcome any further thoughts on how recruitment could take place.

B.2 Topic guide for interviews with people directly affected by fraud

The study

Aims:

- review ways fraud is being committed with a focus on online fraud;
- outline issues relating to sentencing these offences such as culpability/seriousness of offences and aggravating or mitigating factors; and
- explore the impact of different types of online fraud offences on victims.

The overall **objective** of the study is to inform future sentencing guidelines regarding **'confidence fraud'** and **'possessing, making or supplying articles for use in fraud'**. *NOTE: The participants are unlikely to be familiar with these offence categories. The interviewer should ask them to describe the fraud offence they have experienced in detail and use this information to ascertain the type of offence they have experienced. All of the participants will have been 'screened' to ensure they fit in at least one category prior to setting up an interview.*

Generally

- Explore their experience of online fraud;
- Understand the impact of this online fraud offence on the victim;
- Explore the different types of 'harm' victims experience because of fraudulent activities; and
- Map the factors impacting on the culpability of offender/seriousness of online and offline fraudulent offending, including mitigating and aggravating factors.

Guidance for interpretation and use of the topic guide

The following guide does not contain pre-set questions but rather lists the key themes and sub-themes to be explored with each participant. It does not include follow-up questions like 'why', 'when', 'how', etc. as participant's contributions will be fully explored throughout in order to understand how and why views and experiences have arisen. The order in which issues are addressed and the amount of time spent on different themes will vary between interviews.

It is important to note that the interviews may deal with sensitive information for the participant. Researchers should allow participants to lead the discussion and make clear they do not have to answer any question they do not wish to. Probing should be done sensitively. Researchers should also plan time for general chatting at the beginning and end of the interview to create a safe discussion space for participants.

Introduction

- Introduce researcher(s) and NatCen;
- Explain who the research is for (describe Sentencing Council and their role);
  - SC produces guidelines on sentencing for Judges and magistrates;
- Check that they have read the research leaflet and that they understand the content;
- Explain research:
  - SC review the appropriate sentence for different offences;
  - SC would like to know about how fraud is being implemented and how this impacts on victims, especially focussing on online fraud;

  - duty to incorporate views of victims; and
  - one to one interviews allow views to be explored in depth and privately.
- Explain the interview will last between 1 and 1.5 hours. The discussion will focus on:
  - their views on the impact that different types of online fraud offences have on victims, including their own experience of fraud;
  - their views on the different types of 'harm' victims experience because of fraudulent offences;
  - their views on the factors which impact on the seriousness of the offence; and
  - their attitudes towards sentencing fraud offences, both generally and with a focus on online fraud.
- Check that they understand the content of the interview.
- Explain voluntary nature of interview:
  - no right or wrong answers;
  - participation is voluntary – can have a break or choose not to discuss any issue/answer any question;
  - potentially sensitive to discuss but they are in control of the interview; and
  - check that they understand that participation is voluntary and that they can withdraw at any time without giving a reason.
- Explain recording, data storage and confidentiality.
- Explain we wish to avoid using full names or addresses of any victims/offenders mentioned.
- Explain that the interview will be digitally recorded and written out word for word afterwards and that the recording and interview transcript will be stored in accordance with the Data Protection Act 1998.
- Explain reporting process and that no individual will be identified in the report or details of their offence that may identify them. Data will be destroyed on completion of the research.
- Explain disclosure policy i.e. everything they say will be treated confidentially, in accordance with the Data Protection Act. Their answers will only be used for research purposes. The only potential breach to their confidentiality may be if they talk about a suicidal intent or a risk of harm to themselves or somebody who can be identified and is not able to speak for themselves, and/or they talk about an identifiable offence for which they or others have not been charged or convicted.
  - Check that they are happy with data and disclosure policy.
- Check if any questions before we start (remind them they can have a break or stop at any time and only answer questions they wish to).
- Check to see if they happy with the process and gain verbal consent for them to take part in the research study.

Interviewer note: Verbal consent does not need to be recorded as long as you are confident that the respondent is well informed of the process and happy to take part.

- Ask for permission to start recording.

START RECORDING

Background and context

Aim: to get respondent talking and to find out some contextual information about his/her current circumstances and allow them to feel at ease in the interview situation.

- Age, main daytime activity;
- Household, family and relationships (where living, whether live alone or with others, level of contact with family/friends);
- Spare time activities/interests;
- Relationship and employment history;
- Current state of health (mental/physical); and
- Experience of the internet and being online.

Overview of fraud experienced

Aim: to briefly explore the offence that was committed again them.

Interviewer note: Some participants may wish to recount this in some detail and the researcher should balance active listening and allowing them to 'control' the interaction with ensuring they do not become overly focused or upset by the description. If participant has experienced a variety of fraud we want to focus on those that are in scope for this study i.e. confidence fraud and possessing, making or supplying articles for use in fraud (participants may not be familiar with these terms).

- Ask the participant to describe the online fraud they have experienced chronologically:
  - what happened;
  - who was involved;
  - what was the value of the fraud?
  - how was it uncovered/prevented; and
  - was it reported to any agency/person (bank, police, Action Fraud)?

IF ONLINE FRAUD REPORTED TO POLICE – *will cover in more detail in section 5*:

- investigation/Charges brought;
- court appearance; and
- outcome (i.e. guilty or not); charges and sentencing.

IF NOT REPORTED TO POLICE:

- reason;
- overview of any other fraud(s) they have experienced:
  - type/nature of fraud;
  - when this took place; and
  - who was involved.

Experience of harm (online) and most significant harm

Aim: to explore the experiences/impacts of fraudulent offences on the victim, the different types of harm that exist and the extent of this.

- Impact of fraudulent offence;
- Description of harm caused by offence; and

- Types and dimensions of harm.

Note: Interviewer to ensure each dimension is mapped but without listing these terms verbatim. Allow participant to lead on identifying harm to them.

  - financial (e.g. during and consequent repercussions)/extent of financial loss;
  - emotional/psychological (e.g. anxiety, anger, distrust, loss of self-esteem, self-doubt);
  - social/social standing;
  - physical and physical safety (e.g. blackmail);
  - physical health;
  - personal relationships (e.g. relationship strain);
    - wider impact;
    - other people in the victim's social network e.g. family, peer group;
    - wider social and economic harm; and
    - change to their behaviour (i.e were they more/less confident dealing with financial issues before the fraud).
- Extent harm caused affected by:
  - characteristics of perpetrator;
  - characteristics of victim;
    - vulnerability;
    - financial status, including extent of financial loss; and
    - repeat victim;
  - nature and method of the offence;
  - duration of offence;
  - relationship between victim and offender (contact/non-contact);
  - embarrassment/humiliation of victim;
  - online manipulation/disinhibition;
  - ongoing effect on victim;
  - number of offences committed/victims targeted;
  - extent of support received;
  - any press reports on case;
  - satisfaction with resolution of case;
    - whether funds reimbursed;
    - whether outcome involved criminal prosecution and sentencing;
  - any other factors.
- Types of harm that were most significant/had most impact;
  - why these were most significant; and
  - how they impact on victim.
- Factors that have supported participant/reduced harm:
  - press reports;
  - experience of known others;
  - support received;
  - time taken to rectify situation;
  - friends/family; and
  - financial recompense.

Views on factors that influence culpability of offender and seriousness of offence

Aim: to explore what factors influenced the culpability of the offender and seriousness of the offence (in relation to culpability)

Interviewer note: Explain how having explored their own experience of fraud and its impact we would now like to think about the offence they have experienced in relation to other areas which are an integral part of sentencing – culpability of offender, seriousness of offence, and aggravating and mitigating factors. Briefly explain what each term means.

- Views on factors that influenced culpability of offender:
  - financial gain/high level of profit from offence;
  - motivation for fraud;
  - extent of pre-planning vs. opportunistic;
  - number of offences committed/victims targeted;
  - deliberately targeting vulnerable victim(s);
  - relationship between victim and offender (contact/non-contact);
  - abuse of position of trust;
  - complexity of fraud;
  - acted along or with others/role in offence;
  - fraudulent commercial enterprise;
  - characteristics of offender (e.g. vulnerability, repeat offender);
  - attempt to conceal or dispose of evidence; and
  - harm to others (e.g. family members).
- Other perceived aggravating and mitigating factors.

Views on reporting the fraud and the sentencing process

Aim: to explore the experience of reporting the fraud and the sentencing process (if they experienced this and more generally)

Note: Interviewer may provide information on sentencing practice here to assist participant make informed suggestions if they have limited knowledge of sentencing fraud

- Awareness of different sentence and sanction types for online fraud offences more generally:
  - types of sentence;
  - appropriateness of sentence(s); and
  - sources of evidence.
- Awareness of aggravating and mitigating factors for other online fraud offences; views on these:
  - sources of evidence.
- Which body/bodies fraud was reported to:
  - CJS; and
  - voluntary support groups.

IF FRAUD WAS REPORTED:

- Extent to which body/bodies reported to recognised impact on victim, types of harm caused and the most significant:
  - any differences in views between victim and body/bodies reported to; and
  - reasons for differences.

IF PARTICIPANT HAS SEEN THEIR CASE PROSECUTED:

- Experience of the sentencing process:
  - overview of process – steps involved; were they in court to hear the sentence;
  - how they found the process/experience;
  - outcome of sentencing process;
  - views on sentence given; what factors were taken into account by the judge
  - what was the effect of the sentence on them;
  - sentence proportionate to the effect/harm (as described previously);
  - sentence proportionate to the culpability of offender (as described previously);
  - how important was the sentence to them;
  - or was the conviction more important (the recognition that offender guilty); and
  - anything else on how sentencing has affected them.

ASK TO ALL (AND PROBE FULLY):

- Sentence they think should have been given/think most appropriate for the fraud activity they experienced.
  - Thinking about the impact of the offence on you what kind of sentencing is appropriate:
    - custodial;
    - community;
    - fine; and
    - other.
  - If this sentence had been given do they think that would have impacted on them differently, or how would the sentence have impacted on them?
  - Any other factors to take into account when sentencing (not already discussed)?

Attitudes to other fraud offences

Aim: to explore participants' knowledge of the different sentences and sanctions that exists for different types of fraud offences

- Awareness of differences between others' and own experience of online fraud offences:
  - sources of evidence/examples.
- Extent of difference between online and offline fraud offences:
  - impact on victim;
  - seriousness of offence;
  - culpability of offender; and
  - sentencing;

Concluding thoughts

Aim: to summarise key issues that have come up, give participant the opportunity to raise anything that has not been covered and to wind down

- Single message about the harm caused by fraud offences they would communicate to the Sentencing Council;

- Single message about the factors that influence culpability of offender and seriousness of offence would they communicate to the Sentencing Council; and
- Any other messages to think about/anything else to add.

Stop recording * Thank participant * Reassure about confidentiality * Explain next steps of research

Encourage participant to chat and pass on helpline numbers and £25 cash to thank them for their participation and to cover their expenses for taking part. Ask them if they will complete the sample monitoring questionnaire.

B.3 Topic guide for focus groups

The study

Aims:

- review ways fraud is being committed with a focus on online fraud;
- outline issues relating to culpability/seriousness of offences and aggravating or mitigating factors; and
- explore the impact of different types of online fraud offences on victims.

The overall **objective** of the study is to inform future sentencing guidelines regarding **'confidence fraud'** and **'possessing, making or supplying articles for use in fraud'**. *NOTE: The participants are unlikely to be familiar with these offence categories. The interviewer should ask them to describe the fraud offence they have experienced in detail and use this information to ascertain the type of offence they have experienced. All of the participants will have been 'screened' to ensure they fit in at least one category prior to setting up an interview.*

Generally

- Explore their experience of online fraud;
- Understand the impact of this online fraud offence on the victim;
- Explore the different types of 'harm' victims experience because of fraudulent activities;
- Map the factors impacting on the culpability of offender/seriousness of online and offline fraudulent offending, including mitigating and aggravating factors; and
- Map and explore the range and diversity of views on what appropriate sanctions/sentences are for the offences in scope and how these compare to each other.

Guidance for interpretation and use of the topic guide

The topic guide should be accompanied by the focus group planning document, sentencing guidelines handout and types of fraud handout. Moderators should re-familiarise themselves with this prior to each group discussion.

The following guide does not contain pre-set questions but rather lists the key themes and sub-themes to be explored in the group. It does not include follow-up questions like 'why', 'when', 'how', etc. as participants' contributions will be fully explored throughout in order to understand how and why views and experiences have arisen. The order in which issues are addressed and the amount of time spent on different themes will vary between groups – the approximate length provided for each section can be used as a guide.

Introduction (10 minutes)

- Introduce researcher(s) and NatCen;
- Explain who the research is for (describe Sentencing Council and their role):
  - SC produces guidelines on sentencing for Judges and magistrates.
- Explain research:
  - SC would like to know about how fraud is being implemented and how this impacts on victims, especially focussing on online fraud;
  - duty to incorporate views of victims; and
  - group discussion allows these views to be explored.
- Explain the discussion will last between 1.5 – 2 hours. The discussion will focus on:

  - their views on the impact that different types of online fraud offences have on victims, including their own experience of fraud;
  - their views on the different types of 'harm' victims experience because of fraudulent offences;
  - their views on the factors which impact on the seriousness of the offence;
  - 2 to 3 vignettes (explain – examples of) of different types of fraud offences to aid a discussion around different types of seriousness and harm for different types of online fraud;
  - their attitudes towards sentencing fraud offences, both generally and with a focus on online fraud. We will particularly focus on certain aspects of sentencing – seriousness, harm to victim and, culpability of offender – briefly explain what these terms mean; and
  - explain that the current sentences for these offences will be provided as a handout at the very end of the discussion as we would like to explore what is felt to be appropriate regardless of existing recommendations.
- Emotive issue for some and potentially sensitive/distressing to discuss:
  - no right or wrong answers – wish to hear from everyone;
  - participation is voluntary – can leave the room, have a break or choose not to discuss any issue;
  - short scheduled break in the middle of the discussion;
  - participants should speak one at a time, listen to what other people have to say and respect one another's answers, different opinions and confidentiality of the group discussion; and
  - would like an open discussion and debate – feel free to add your comments but respect each other's views and speak one at a time.
- Explain recording, data storage and confidentiality.
- Explain we wish to avoid using full names or addresses of any victims/offenders mentioned.
- Explain that the discussion will be digitally recorded and written out word for word afterwards and that the recording and interview transcript will be stored in accordance with the Data Protection Act 1998.

Explain reporting process and that individuals will not be identified in the report or the location of the group

- Explain disclosure policy i.e. everything they say will be treated confidentially, in accordance with the Data Protection Act. Their answers will only be used for research purposes. The only potential breach to their confidentiality may be if they talk about a suicidal intent or a risk of harm to themselves or somebody who can be identified and is not able to speak for themselves, and/or they talk about an identifiable offence/illegal acts for which they or others have not been charged or convicted/been reported previously.
  - Check that they are happy with data and disclosure policy.
- Check if any questions before we start (remind them they can have a break or stop at any time).
- Check to see if they happy with the process and gain verbal consent for them to take part in the research study.

Interviewer note: Verbal consent does not need to be recorded as long as you are confident that the respondents are well informed of the process and happy to take part.

- Ask for permission to start recording.

START RECORDING

2. Participant introduction (8 minutes)

Aim: to obtain information about the participants, introduce participants to one another and allow them to feel at ease in the group situation.

- Participant backgrounds – very brief round robin, *ask each participant to give details of:*
  - name;
  - briefly describe why you decided to take part today;
  - how they feel about taking part in the group:
    - may be useful to acknowledge concerns/anxiety regarding content and reassure group.

3. Overview of fraud and impact experienced (15 minutes)

Aim: to briefly explore the offence that was committed against them, their experience of the offence and its impacts.

Interviewer note: Can explain to group – we only want a brief overview of the type of fraud experienced among the group, aware that this can be sensitive for some. Some participants may wish to recount this in some detail and the researcher should balance active listening and allowing them to 'control' the interaction with ensuring they do not become overly focused or upset by the description or go into too much detail. If any participant has experienced a variety of fraud we want to focus on those that are in scope for this study i.e. confidence fraud and possessing, making or supplying articles for use in fraud (participants may not be familiar with these terms).

- Experience of online fraud:
  - what happened;
  - who was involved;
  - what was the value of the fraud;
  - how was it uncovered/prevented; and
  - was it reported to any agency/person (bank, police, Action Fraud)?

IF ONLINE FRAUD REPORTED TO POLICE:

- investigation/charges brought;
- court appearance; and
- outcome (i.e. guilty or not); charges and sentencing.

IF NOT REPORTED TO POLICE:

- reason.

Impact of fraudulent offence:

- description of harm caused by offence;
- types and dimensions of harm;

Note: Interviewer to ensure each dimension is mapped but without listing these terms verbatim. Allow participants to lead on identifying harm to them:

  - financial (.e.g. during and consequent repercussions);

  - emotional/psychological (e.g. anxiety, anger, distrust, loss of self-esteem, self-doubt);
  - social/ social standing;
  - physical and physical safety (e.g. blackmail);
  - physical health;
  - personal relationships (e.g. relationship strain);
  - wider impact:
    - other people in the victims social network e.g. family, peer group; and
    - wider social and economic harm.
  - change to their behaviour (i.e. were they more/less confident dealing with financial issues before the fraud).
- overview of any other fraud(s) they have experienced:
  - type/nature of fraud;
  - when this took place; and
  - who was involved.

4. General awareness of sentencing and fraud offences (10 minutes)

Aim: to set context of existing knowledge/awareness of sentencing process before moving onto the vignettes

Interviewer note: Explain the key issues which are important for sentencing and what these mean – culpability of offender, seriousness, harm to victim and aggravating and mitigating factors. Interviewer may then need to lead on this section of the discussion as participants may not be clear about the process.

- Describe process when someone is sentenced for an offence:
  - found/plead guilty;
  - reports to judge; and
  - decision on sentencing made on different occasion.
- specific types of sentences or penalties for fraud offenders (specific):
  - custodial (prison) sentence;
  - fines; and
  - ancillary and other orders (compensation, confiscation, deprivation, restitution – *explain what each of these mean*).
- custodial sentences and licence (aim here is to briefly ensure the group are aware that not all time sentenced may be spent in custody i.e. they may serve half in custody and half on licence. Where they are released may abide by certain conditions for remainder of sentenced time and if they do not, they are in breach of licence and may be recalled to prison. This is not the case for indeterminate or extended sentences however).
- what is taken into account when sentencing.
- different types of fraud offences – refer to handout to give to each, with example list of offences.
- are these the expected or anticipated offences?
- explain we will explore 2–3 of these in detail in the following discussion.
- views on what the **purpose** of sanctions for fraud offences should be:
  - punishment;
  - prevent offending again (recidivism);
  - retribution; and
  - other.

- relative weight given to each (i.e. is one more significant an outcome than others).

5. Vignette one – first offence (up to 30 minutes)

This will alternate between online romance scam/identity theft via hacking/consumer fraud/advance fee fraud. Please consult moderator guide
Aim: to explore one fraud offence in detail with the group

Hand out a copy of the vignette to each member and explain that the next 30 minutes will be used to discuss the factors affecting the harm experienced and the culpability of the offender for this fraud offence. We will also ask the group to think about what the appropriate sentence would be for this type of offence.

Interviewer note: the aim is to firstly map the range of factors associated with harm and culpability for this offence, and then briefly explore the type of sentence the group think should be given for this offence. The range of sentences can then be used as a tool to help explore how the aggravating and mitigating factors would affect the sentence in terms of level of seriousness of the offence.

Culpability and harm (10 minutes)

- Elements that affect how serious the offence is (ask group to identify a list of factors then use prompts)

  Harm:
  - characteristics of perpetrator;
  - characteristics of victim:
    - vulnerability;
    - financial status, including extent of financial loss; and
    - repeat victim.
  - nature and method of the offence;
  - duration of offence;
  - relationship between victim and offender (contact/non-contact);
  - embarrassment/humiliation of victim;
  - online manipulation/disinhibition;
  - ongoing effect on victim;
  - number of offences committed/victims targeted;
  - extent of support received;
  - any press reports on case;
  - satisfaction with resolution of case:
    - whether funds reimbursed; and
    - whether outcome involved criminal prosecution and sentencing.
  - any other factors.
- Whether types of harm/impact are different for fraud conducted online compared to offline:
  - extent of harm; and
  - type of harm.

  Culpability:
  - financial gain/high level of profit from offence;
  - motivation for fraud;
  - extent of pre-planning vs. opportunistic;

  - number of offences committed/victims targeted;
  - deliberately targeting vulnerable victim(s);
  - relationship between victim and offender (contact/non-contact);
  - abuse of position of trust;
  - complexity of fraud;
  - acted along or with others/role in offence;
  - fraudulent commercial enterprise;
  - characteristics of offender (e.g. vulnerability, repeat offender);
  - attempt to conceal or dispose of evidence; and
  - harm to others (e.g. family members).
- harm to victim increase/remain same with these factors.

**This discussion may cause some disagreement – be prepared to carefully moderate the discussion, probing fully for factors that participants may identify as increasing seriousness or harm, whilst respecting that some participants may wish to state that all types of fraud are serious and not define them as more or less harmful.*

Sentence (5 minutes)

- Check sentence expectation (i.e. if 5 year suggested is this 5 in custody or 2.5 and 2.5 on licence);
- Reasons for suggested sentences (range):
  - purpose/aim of sentences (range);
  - agreements/disagreements;
  - perceived harm/seriousness of the offence; and
  - general consensus (i.e. length of years in prison) among group (*Note: do not try and encourage the group to reach a consensus – we are not focusing on what sentences should be given, but instead want to use the suggested sentences as a tool to explore factors which should feed into the guidelines).*

Aggravating and mitigating factors (10 minutes)

Revisit the suggested sentences (Note: the sentences can be used as a tool to aid the discussion below)

- Extent factors listed as increasing seriousness should be taken into account for sentencing:
  Moderator:
  - select a couple of factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - how should this affect the sentence previously agreed (suggested increase/change/additional condition to sentence);
    - probe reasons for suggestions.
- Extent factors listed as decreasing seriousness should be taken into account for sentencing:
  Moderator:
  - select a couple of factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - how should this affect the sentence previously agreed (suggested decrease/change/drop conditions to sentence);
    - probe reasons for suggestions.
- Identify factors to be taken into account that decrease sentence/seriousness in terms of personal mitigation (ask group to identify a list of factors then use prompts).

  - Mitigating factors:
    - peripheral involvement.
  - Personal mitigation:
    - voluntary cessation of offending;
    - complete and unprompted disclosure of extent of fraud;
    - voluntary restitution; and
    - financial pressure.
- Relative weight to give to each (which issue should be taken most into account – mitigating or aggravating).
- Other factors that should be taken into account when sentencing this offence:
  - list any identified by group and probe on reasons for suggestion.
- Final comments on sentencing first offence.

Note: can suggest a break at this point

6. Vignette two – second offence (up to 30 minutes)

This will alternate between online romance scam/identity theft via hacking/consumer fraud/advance fee fraud. Please consult moderator guide
Aim: to explore contrasting fraud offence in detail with the group

Hand out a copy of the second vignette to each member and explain that the next 30 minutes will be used to discuss the factors affecting the harm experienced and the culpability of the offender for this fraud offence. We will also ask the group to think about what the appropriate sentence would be for this type of offence.

Interviewer note: as for the first vignette the aim is to firstly map the range of factors associated with harm and culpability for this offence, and then briefly explore the type of sentence the group think should be given for this offence. The range of sentences can then be used as a tool to help explore how the aggravating and mitigating factors would affect the sentence in terms of level of seriousness of the offence. If necessary in terms of time the interviewer can encourage the group to compare and contrast this offence with the one just discussed for each area below.

Culpability and harm (10 minutes)

- Elements that affect how serious the offence is (ask group to identify a list of factors and use prompts as for first offence above/in moderator guide):
  - any factors different from first offence/vignette?
- Harm to victim increase/remain same with these factors.
- Whether types of harm/impact are different for fraud conducted online compared to offline:
  - extent of harm; and
  - type of harm.

Sentence (5 minutes)

- Check sentence expectation (i.e. if 5 year suggested is this 5 in custody or 2.5 and 2.5 on licence).
- Reasons for suggested sentences (range):
  - purpose/aim of sentences (range);
  - agreements/disagreements;
  - perceived harm/seriousness of the offence; and

- try to obtain a general consensus (i.e. length of years in prison) among group.

Aggravating and mitigating factors (10 minutes)
Revisit the suggested sentences:

- extent factors listed as increasing seriousness should be taken into account for sentencing.
  Moderator:
  - select a couple of factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - how should this affect the sentence previously agreed (suggested increase/change to sentence):
    - probe reasons for suggestions.
- Extent factors listed as decreasing seriousness should be taken into account for sentencing.
  Moderator:
  - select two factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - how should this affect the sentence previously agreed (suggested decrease/change/drop conditions to sentence)?
    - probe reasons for suggestions.
- Identify factors to be taken into account that decrease sentence/seriousness in terms of personal mitigation (ask group to identify a list of factors then use prompts as above for first offence/in moderator guide).
- Relative weight to give to each (which issue should be taken most into account – aggravating or mitigating).
- Other factors that should be taken into account when sentencing this offence.
- Final comments on sentencing second offence.
- Final comments on vignettes (if not including third vignette below).

7. Vignette three – third offence (up to 5–10 minutes if time)

This will alternate between online romance scam/identity theft via hacking/consumer fraud/advance fee fraud. Please consult moderator guide
Aim: to explore contrasting fraud offence in detail with the group

Interviewer note: Only include a third vignette if you have time

Hand out a copy of the third vignette to each member and explain that the next 5–10 minutes will be used to discuss the factors affecting the harm experienced and the culpability of the offender for this fraud offence. We will also ask the group to think about what the appropriate sentence would be for this type of offence.

Interviewer note: Instead of fully mapping the range of factors associated with this offence the interviewer should encourage the group to compare and contrast this offence with the previous two.

Culpability and harm (4 minutes)

- Elements that affect how serious the offence is compared to previous two (ask group to identify similar/different factors from previous 2 offences and use prompts if aids discussion as in moderator guide):
  - any factors different from other offences/vignettes?
- Harm to victim increase/remain same with these factors.

- Whether types of harm/impact are different for fraud conducted online compared to offline:
  - extent of harm; and
  - type of harm.

Sentence (2 minutes)

- Check sentence expectation compared to previous 2 offences (i.e. if 5 year suggested is this 5 in custody or 2.5 and 2.5 on licence).
- Reasons for suggested sentences (range):
  - purpose/aim of sentences (range);
  - agreements/disagreements;
  - perceived harm/seriousness of the offence; and
  - try to obtain a general consensus (i.e. length of years in prison) among group.

Aggravating and mitigating factors (4 minutes)

Revisit the suggested sentences

- Extent factors listed as increasing seriousness should be taken into account for sentencing.
  Moderator:
  - select two factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - how should this affect the sentence previously agreed (suggested increase/change to sentence)?
    - probe reasons for suggestions.
- Extent factors listed as decreasing seriousness should be taken into account for sentencing.
  Moderator:
  - select a couple of factors from the vignette guide that alters the offence;
  - remind of suggested sentence;
  - How should this affect the sentence previously agreed (suggested decrease/change/drop conditions to sentence)?
    - probe reasons for suggestions.
- Identify factors to be taken into account that decrease sentence/seriousness compared to previous two offence in terms of personal mitigation (ask group to identify factors and can use prompts as above for first offence/in moderator guide).
- Relative weight to give to each (which issue should be taken most into account – aggravating or mitigating).
- Other factors that should be taken into account when sentencing this offence.
- Final comments on sentencing second offence.
- Final comments on vignettes.

Recent changes and how fraud will develop in the future (5–15 minutes)

Aim: to explore views on how fraud will develop in the future and the impact this will on the sentencing process

Note: If time is running out this section can be covered very briefly/not covered

- Thinking about the future how much do you think online fraud is going to be an issue?

- Other areas of emerging fraud/areas of risk/technological advances:
  - Iphone/smartphone takeover;
  - Personal information being taken from social media sites;
  - Fraud in the virtual world:
    - Differences this may bring.
  - Any other areas of emerging fraud.

Conclusion (5 minutes)

Aim: to summarise key issues that have come up, give participants the opportunity to raise anything that has not been covered and to wind down

- Single message/key issue about sentencing fraud offences which should be communicated to the Sentencing Council;
- Anything to add; and
- How does each feel about having taken part in the group now (return to round robin introduction process)?

Explain that handouts on the actual recommended sentence for the offences discussed are available at the front of the room and they are welcome to take these with them. These also have helpline/support numbers on.

Stop recording * Thank participants * Reassure about confidentiality * Explain next steps of research

Encourage participant to chat and pass on £30 cash to thank them for their participation and to cover their expenses/travel costs for taking part. Encourage participants to remain for further refreshments or to ask questions.

B.4 Vignettes used in focus groups

N.B. participants were given the vignettes in the grey boxes only. Other prompts were used to vary the circumstances of the vignette to see how this might affect the sentence/s given within the group.

Vignette one – Online romance scam

The offence

E is a 40 year old woman living in London. She recently started visiting online dating sites. On one site she met a man, F, who claimed he was based in Edinburgh. They started a long distance relationship through regularly emailing and E felt she had found her perfect partner who really understood her. This continued over five months. F then told E that he had bought a train ticket to come and see her but that it had been stolen. He had no money for a new one so she offered to send him £100 so he could buy another one. E sent the money but F was unable to make the journey due to 'illness'. F then explained he had lost his job and was very stressed, and could E send £1000 to help him pay his rent. These requests for money went on for another six months, and over this time E gave F about £5,000.

E told her friends who persuaded her to contact Action Fraud. She then reported it to the police. They investigated and found out that F was in fact another person than his dating profile, living in another city.

F has been convicted of the offence of confidence fraud.

Ask the group about their views on this offence in terms of:

- seriousness;
- harm to victim; and
- culpability of offender.

What sentence they would suggest for this offence.

Additional information/variations you could provide to explore these issues further include:

- E had also spoken to F on the phone regularly and not just via email;
- F had a false dating profile pretending to be an army veteran using someone else's photo and identity;
- E suffered from panic attacks after this experience and finds it very difficult to trust new people she meets now;
- F was also found to be doing the same type of fraud with seven other women;
- F managed to obtain £50,000 from E via the fraud; and
- F threatened E when she said she was going to report him, and said he would post the romantic emails she had sent him on a social media site if she did so.

Do these factors change their view on seriousness, harm or culpability (and with it the suggested sentence):

- F obtained about £200 from E via the fraud;
- F willingly gave the names and addresses of the other victims he had targeted when approached by the police; and
- F never intended to commit fraud when he joined the internet dating site. The idea only occurred to him once he had received the £100 from E for his train ticket. He kept the money but never made contact with E again.

Vignette two – Identity theft fraud

The offence

L is 20 years old. He was recently a victim of identity theft. He was sent an email asking for his personal details that looked as if it was from his bank. He sent his details and they were used to access his online bank account. The perpetrator, P, took out over £2,000 from L's account. L reported this to the bank, and was contacted later by the police who have apprehended P by finding him with a list of personal information he was using to take over online accounts in this way.

P has been convicted of the offence of possessing, making, or supplying articles for use in fraud.

Ask the group about their views on this offence in terms of:

- seriousness;
- harm to victim; and
- culpability of offender.

What sentence they would suggest for this offence.

Additional information/variations you could provide to explore these issues further include:

- L's computer was hacked into as opposed to him providing the personal information;
- P managed to obtain £100,000 in loans via the personal information he stole and handled;
- although L is not liable for the money, he has spent months trying to sort out his credit history and recently had a loan refused because of his poor credit history. He is also very anxious as he believes his personal details are 'out there' and he feels like he could be a victim of fraud again at any moment;
- P accessed illegal pornography using L's personal bank details to pay for it, which was traced back to L by the police; and
- P was part of an organised crime gang which has targeted over 100 victims.

Do these factors change their view on seriousness, harm or culpability (and with it the suggested sentence):

- P sold L's personal details to others to commit fraud but did not actually use the details himself;
- L did not have a firewall installed on his computer;
- P stole L's details by going through his rubbish bin rather than online; and
- P has lost his job and only committed the fraud so he could help to pay his bills.

Vignette three – Consumer fraud

The offence

S came across a website promoting a new pill that stated it would help her to slim down without exercise. The site offered a free two week trial of the pill and included lots of before and after photos from satisfied customers. S received the pills and started to take them, but they had no effect. She thought she would try for three months and a new box of pills arrived every fortnight. On her credit card statement she saw that she had been charged £50 for each fortnightly supply. After three months, and still no effect, S decided to follow the cancellation process as outlined on the website. She tried to contact the company to do this, but her calls and emails went unanswered.

S continued to receive the pills for another three months and then contacted Action Fraud. She also reported it to the police.

The fraudster who was running the scheme has been convicted of the offences of possessing, making or supplying articles for use in fraud, and confidence fraud.

Ask the group about their views on this offence in terms of:

- seriousness;
- harm to victim; and
- culpability of offender.

What sentence they would suggest for this offence.

Additional information/variations you could provide to explore these issues further include:

- the ‘miracle pill scheme’ was being run by a gang of 10 fraudsters who between them had 50 such schemes in operation. They were convicted of the offence of consumer fraud;
- the gang used ‘sucker’s lists’ to approach vulnerable people and had over 100 other such schemes in operation. They ran a sophisticated factory for producing the pills and the accompany packaging and literature;
- the gang sold S’s personal details onto another perpetrator who ran a list of vulnerable people who could be targeted for this kind of fraud. As a result, S received up to 30 letters / emails a day from other fraudsters running similar schemes;
- the site was recommended to S by a friend who had used the pills and thought she had lost weight; and
- S was buying tickets to an event (not pills that actually arrived) via a website that looked legitimate and only found out they were fake when she went to pick them up at the box office.

Do these factors change their view on seriousness, harm or culpability (and with it the suggested sentence):

- the ‘miracle pill scheme’ was run by one individual who got S to sign up to the scheme by sending her a letter in the post;
- some of the gang members had more of a peripheral involvement and did not know the extent of the fraud; and
- when convicted, the gang immediately offered to re-pay S all of the money which she had spent on the scheme.

Vignette four – Advance fee fraud

The offence

T is an 80 year old woman who lives alone. She has four grandchildren who live overseas. She recently started to use the internet so she could send emails and talk to them via 'Skype'. T received an official looking email saying she had won a large amount of money in a lottery. In order to release her winnings she would have to pay a small fee. T sent £100 so that her prize money could be released. She was very excited and sent the £100 straight away. After two weeks she contacted the 'lottery company' again who told her that she would need to send another £100 to cover taxes, which she did. This process went on for 6 months, with T contacting the 'lottery company' and sending money to cover various fees. Over a period of six months, T sent £500 to try and claim her prize.

T eventually told one of her friends, who persuaded her to contact Action fraud. T then contacted the police.

It took the police a couple of years to track down the fraudster behind the scam. He was convicted of the offences of possessing, making or supplying articles for use in fraud, and confidence fraud.

Ask the group about their views on this offence in terms of:

- seriousness;
- harm to victim; and
- culpability of offender.

What sentence they would suggest for this offence.

Additional information/variations you could provide to explore these issues further include:

- T became very anxious after the experience and felt like she was being 'watched' all the time, especially as the police did not find the fraudster for a couple of years;
- T eventually suffered a mental break down because of the experience; and
- T sent £20,000 to the fraudster involved.

Do these factors change their view on seriousness, harm or culpability (and with it the suggested sentence):

- the advance fee scam was being run by a gang but some of the members had more of a peripheral involvement and did not know the extent of the fraud;
- the scam was being run by one individual who was unemployed. He claimed he was under financial pressure to commit the fraud;
- T just sent a one off payment of £100 and then did not send any more money to the perpetrator; and
- T contacted Action Fraud straight away and never sent any money to the perpetrator.

B.5 Information on sentencing guidelines provided to participants at the end of the focus group or interview

Confidence fraud

Maximum penalty: **Fraud, 10 years' custody**
False accounting, 7 years' custody

	Value of property or consequential loss			
Nature of offence	£500,000 or more **Starting point based on:** £750,000	£100,000 or more and less than £500,000 **Starting point based on:** £300,000	£20,000 or more and less than £100,000 **Starting point based on:** £60,000	Less than £20,000 **Starting point based on:** £10,000
Large scale advance fee fraud **or** other confidence fraud involving the deliberate targeting of a large number of vulnerable victims	**Starting point:** 6 years' custody **Range:** 5–8 years' custody	**Starting point:** 5 years' custody **Range:** 4–7 years' custody	**Starting point:** 4 years' custody **Range:** 3–6 years' custody	**Starting point:** 3 years' custody **Range:** 2–5 years' custody
Lower scale advance fee fraud **or** other confidence fraud characterised by a degree of planning and/or multiple transactions	**Starting point:** 5 years' custody **Range:** 4–7 years' custody	**Starting point:** 4 years' custody **Range:** 3–6 years' custody	**Starting point:** 3 years' custody **Range:** 2–5 years' custody	**Starting point:** 18 months' custody **Range:** 26 weeks – 3 years' custody
Single fraudulent transaction confidence fraud involving targeting of a vulnerable victim			**Starting point:** 26 weeks' custody **Range:** Community order (HIGH) – 18 months' custody	**Starting point:** 6 weeks' custody **Range:** Community order (MEDIUM) – 26 weeks' custody
Single fraudulent transaction confidence fraud not targeting a vulnerable victim, and involving no or limited planning			**Starting point:** 12 weeks custody **Range:** Community order (MEDIUM) – 36 weeks' custody	**Starting point:** Community order (MEDIUM) **Range:** Fine – 6 weeks' custody

Possessing, making or supplying articles for use in fraud

This includes the following three offences:

- possession of articles for use in frauds;
- making or supplying articles for use in frauds; and
- fraud.

Maximum penalty: **Possession of articles for use in fraud, 5 years' custody**
For both other offences, 10 years' custody

	Type of offence	
Nature of offence	Making or adapting **or** supplying or offering to supply	Possessing
Article(s) intended for use in an extensive and skilfully planned fraud	**Starting point:** 4 years' custody **Range:** 2–7 years' custody	**Starting point:** 36 weeks' custody **Range:** 6 weeks – 2 years' custody
Article(s) intended for use in a less extensive and less skilfully planned fraud	**Starting point:** 26 weeks' custody **Range:** Community order (HIGH) – 2 years' custody	**Starting point:** Community order (MEDIUM) **Range:** Community order (LOW) – 26 weeks' custody

B.6 Information on help and advice provided to participants at the end of the focus group or interview

HELP AND ADVICE

If the group discussion or interview has raised any issues for you regarding fraud offences or previous experience of victimisation then you may find the following telephone numbers helpful.

ACTION FRAUD – the UK's national fraud and internet crime reporting centre:

Website: www.actionfraud.police.uk

Telephone: 0300 123 2040

Email: action.fraud@nfa.gsi.gov.uk

VICTIM SUPPORT – a national charity giving free and confidential help to victims of crimes, witnesses, their families and friends and anyone else affected across England and Wales:

Website: www.victimsupport.org.uk

Telephone: 0845 30 30 900

Email: supportline@victimsupport.org.uk

THINK JESSICA – a non profit making organisation providing information and advice about scam mail:

Website: www.thinkjessica.com

Email: advice@thinkjessica.com

……..

The following publication also provides information on what to do if you have been affected by fraud and on fraud more generally.

METROPOLITAN POLICE – the Metropolitan's police publication The Little Book of Big Scams is available to download here:
http://www.met.police.uk/fraudalert/docs/mps_little_book_big_scams.pdf

B.7 Information on types of fraud offences provided to participants during the focus group.

Some examples of different types of fraud offences

Confidence fraud – this is an attempt to defraud someone by gaining their confidence and usually involves a victim transferring money and/or property as a result of being deceived or misled by the offender. Examples of confidence frauds are provided in the table below.

Possessing, making or supplying articles for use in fraud – this is when articles – see below for examples – are made or supplied in order to commit fraud.

Confidence fraud (these types of fraud may be committed using the articles listed in the next column)	**Possessing, making or supplying articles for use in fraud**
Advance fee frauds – *this involves the perpetrator asking victims to make advance payments for some kind of financial gain.*	Computer programmes *for generating credit card numbers.*
Bogus charity collectors – *this involves people claiming to be collecting money for charity when they intend to keep the money.*	Draft letters or emails *for use in fraud for example advance fee frauds, texts for romantic emails for romance fraud.*
Career opportunity scams and money-making work from home scams – *this is where people are asked to pay money for an employment opportunity up front, where no genuine employment exists.*	Lists of credit card or bank account details.
Romance scams – *this involves people creating fictional online dating accounts and making their victims believe they have strong feelings for them in order to secure financial gain from them.*	Malware – *this is malicious software that consists of programming designed to disrupt the performance of PCs, laptops, handheld devices, etc. This can include enabling access to personal information.*
Non-delivery of goods and defective products and services – *this includes paying for tickets for events or holidays that then do not exist, or paying for goods that are never sent or are lower quality than advertised.*	Phishing – *sending what appear to be legitimate emails asking for personal information such as usernames, passwords and credit card details, which are actually from illegitimate sources.*
Premium rate, telephone prize scams and foreign lottery scams – *incurring costs to enter competitions, which actually have no real prize or a very low value prize.*	Spam emails – *these are emails which are sent out by the perpetrator to try and gain personal information such as credit card numbers and bank account details.*

Additional information on different types of fraud and to report concerns can be found on Action Fraud's website: http://www.actionfraud.police.uk

Any enquiries regarding this publication should be sent to us at info@sentencingcouncil.gsi.gov.uk

This publication is available for download at www.sentencingcouncil.judiciary.gov.uk