Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice?

Mark Button, Carol McNaughton Nicholls, Jane Kerr, Rachael Owen

Abstract: The advent of the internet has expanded opportunities to commit fraud and millions regularly fall victim. Fraud victims in general have been largely neglected by researchers in comparison to other crimes. There has also been very little research on issues related to the sentencing of fraudsters. This paper offers some of the first insights on what individual online fraud victims actually want regarding the sentencing of the scammers who target them. It explores their views on aggravating and mitigating factors as well as the different types of sanction which can be used. The paper particularly highlights the opportunities and attraction of restorative justice based approaches to victims. It uses data from in-depth interviews with 15 online fraud victims, 6 focus groups with a further 48 online fraud victims and interviews with 9 professional stakeholders involved in combating this problem.

Keywords: Online fraud, victims, impact, sentencing, restorative justice

Introduction

Fraud is often considered a less harmful crime than other property crimes by some (Fraud Advisory Panel, 2006). Fraud victims have also been and continue to be neglected from a number of key areas in dealing with crimes, such as support mechanisms, victimisation surveys and so on(Croall, 2007; Button et al. 2013). Frauds against individuals – which will be the focus of this paper – can have a devastating impact including: financial loss, impacts on physical and mental health, psychological problems such as stress, anger, loss of esteem; impacts on relationships; to even suicide (Button, et al. 2014; Cross, 2013). Research concerning the appropriate punishments for fraudsters, and more broadly white collar criminals, has not been common. There has been research upon the sentences fraudsters receive (Levi, 1991; Levi, 2006; 2010), the impact of imprisonment on recidivism (Weisburd, et al, 1995), alternatives to custody and particularly the utility of restorative based approaches (Levi 2002; Wenzel, 2006; Murphy and Harris, 2007), but there has been very little research on what fraud victims actually want, particularly in relation to the growing online context of fraud (Button et al 2009a and b).

This lack of research on what fraud victims want can also be juxtaposed against an internet revolution which has had a similar upheaval in the way frauds against individuals (and businesses) occur. Millions of people across the globe are targeted on a regular basis with a growing variety of scams. These range from phishing scams in spam e-mail that seek to trick victims into revealing personal information to fake lovers grooming unsuspecting victims through romance sites into giving money, 'gifts' and personal information (Whitty, 2013 and forthcoming). The limited research on victimisation illustrates substantial victimisation. In Australia 6.7 percent of the population over 15 had been the victim of a personal fraud in the previous 12 months (Australian Bureau of Statistics, 2012). In the UK in 2006, 48 percent admitted having been targeted with a scam and 8 percent had been victims (Office of Fair Trading, 2006). Research commissioned for the National Fraud Authority's Annual Fraud Indicator in 2012 found 8.8 percent of those surveyed had been victims of identity fraud in previous 12 months (National Fraud Authority, 2013). The most recent Crime Survey for England and Wales (CSEW) has explored prevalence of fraud for the first time and found 56 percent had been targeted with unsolicited communication, with less than 1 percent sending money (Office for National Statistics, 2013). In the USA in 2005 13.5 percent of adults were victims of a consumer fraud, in 2010 24 percent of US households had one person who was the victim of a fraud related crime and at least 7 percent of households having at least one householder the victim of identity fraud (Federal Trade Commission, 2007a and b; Huff *et al*. 2010; US Department of Justice, 2011). These percentages add up to millions of people.

Given the changing nature of frauds occurring and the lack of research on fraud victims there was a clear gap in research which needed to be filled. In the Summer of 2012 the Sentencing Council for England and Wales commissioned the authors to examine the nature of online fraud, the impact upon the victims and their views on sentencing, with particular reference to fraud offences relating to confidence fraud; and making, possessing or supplying articles for use in fraud (offences created under the Fraud Act 2006). The paper will focus upon the findings relating to victims' views on potential sentences, particularly restorative justice. Before we embark upon this, however, some of

the key literature relating to online fraud will be examined, with particular reference to the differences between online fraud from off-line and other volume property crimes.

The Nature of Online Fraud

Online fraud is different from off-line frauds and volume property crimes in a number of areas. This section will illustrate some of these differences as it will then be interesting to see if this has any impact on the views on sentencing. The advent of the internet has spawned a wide range of new opportunities to commit crimes, particularly frauds (Smith, 2010; Jewkes and Yar, 2010; Wall, 2007). Old frauds perpetrated by mail have been repackaged and massively expanded due to the ease and economy the internet provides, such as Nigerian 419 scams and bogus lotteries (see figure 1). Opportunities for new frauds have also occurred through the advent of social networking and online dating sites. There are a wide range of frauds committed which are perpetrated online and some of the most common are listed below in figure 1 and can be divided between those which seek some form of payment from the victim against those which seek the personal information, so other frauds (such as identity) can be perpetrated. Some of these frauds may seek both. There is also evidence beginning to emerge that some criminals are turning from traditional methods of committing crime to the internet and the lack of accurate measurement of cyber-crime may explain why general crime trends have been falling (Treadwell, 2011; Fitzgerald, 2014).

Figure 1. Common online frauds

Money seeking frauds

419 scams: the victim is contacted by someone claiming to be a corrupt official with a large sum of money they have misappropriated. They are looking for someone to help launder the money which in return for they offer to pay a substantial fee. To start the venture, however, they require a payment from the victim. Those who fall for this end up been sucked into paying more and more as they seek to secure their 'investment'.

Bogus inheritance scams: victims are contacted and told they have inherited a large sum of money from a long lost relative, but need to pay fees to release the money.

Bogus lottery: victims are contacted and told they have won a lottery but need to pay a fee to

release the funds.

Bogus products: a wide range of products and services are often marketed on the internet for sale which are either defective or non-existent. Some of the most common include: holidays, tickets, designer goods, DVDs, slimming drugs, drugs such as Viagra etc.

Career opportunity scams: jobs and training are offered online, usually for lucrative jobs, but the reality is there is no chance of work.

Clairvoyant and psychic scams: victims are sent communications saying that something bad will happen to them unless they pay money.

Loan scams: victims are sent demands for debt repayment with threats if they do not pay for non-existent loans or scammers offer to renegotiate debts or amend adverse credit ratings.

Person in distress fraud: in some cases people are targeted with a tragic story of a stranger and asked to send money or in a variation a person's E-mail account is hacked and all their contacts are mailed to say they are in distress in a foreign country and could monies by wired urgently.

Romance frauds: there are a wide variety of different romance frauds, with the most common including the victim falling in love with usually a fake person and been tricked into sending gifts or money for emergencies or their costs of travel to meet them.

Share sale scams: victims are convinced to buy worthless or overvalued shares using high pressure sales.

Virus scam: victims computers are hit with virus and told to phone number where they are charged fee to rescue the computer. A variation on this is where there is a suggestion of some illegal files held on the computer.

Personal information seeking frauds

Fake websites and E-Mails: one of the most common scams used by fraudsters to harvest personal data is the sending of fake E-Mails or the creation of fake websites. A common version of this is an E-Mail which arrives from a 'bank' stating the victim's account has been compromised and they need to enter personal information to 'restore' the account.

Social networking: another common tactic is for fraudsters using fake identities to befriend individuals online and then harvest any online personal data displayed or trick them into parting with the information.

Malware: more sophisticated fraudsters use programmes, viruses and hacking to secure the personal information of a victim.

These frauds can be perpetrated by a variety of techniques:

- Phising (personal information obtained through E-mail);
- SMiShing (personal information obtained via SMS);

- vishing (personal information obtained via phone);
- Malware used to collect personal information;
- 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 unauthorized access to a users 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'; 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).

One of the first differences is the potential for mass targeting across borders relatively cheaply. For offline frauds committed by post and telephone this is possible, but costs involved mean schemes are often limited to smaller numbers for perpetrators who have the resources to do so. For volume crimes such as burglary multiple victims are also common, but sheer time and resources required mean victims at worst are in hundreds and dozens, rather than thousands and above.

Online fraud also differs from offline fraud and other volume crimes in the degree of interaction with the perpetrator. Online frauds are usually at a distance with the victim and perpetrator in some cases having no interaction whatsoever, such as when information is stolen to perpetrate identity fraud. They can, however, also involve substantial personal contact at a distance via Skype (and related technology) which can even involve intimate sexual acts (such as watching one another

masturbate). There can also be sometimes limited interaction via e-mail, but this is often at a distance with no actual face-to-face or telephone contact. Off-line fraud can also be like this when perpetrated via the mail. However, in most off-line frauds there is inter-action on the phone or even face-to-face. Volume property crimes like burglary involve the perpetrator invading the private space of the victim, so although the victim may not actually come into contact with the burglar (some do), they have actually invaded their private physical space. Therefore online frauds offer a mix of both distant anonymous crimes, as well as distant very intimate contact, but distinguished in general by no physical contact.

Research also suggests low levels of cases of online fraud being reported to the police. One study in the UK illustrated that only 44 percent of 655 victims surveyed had reported this to the police (Goucher, 2010). Low reporting is also common for fraud in general for a variety of reasons such as not knowing who to go to, the embarrassment, expectations that nothing will be done, to name some (Button et al, 2009b). However, for crimes such as burglary, reporting tends to be higher because usually reporting is a condition of an insurance claim. Some other property related volume crimes like theft, however, generally have lower reporting rates too, unless the artefact stolen is linked to some form of insurance.

Previous research on fraud victims has identified a wide range of impacts on individual victims as a result of fraud. Button et al (2009b; 2014; Cross, 2013) found: no impact at all, financial loss, psychological impacts, damaged relationships, physical and mental health problems, suicide, fear of violence, worries over persons impersonating them to changes in behaviour. Research on online fraud victims confirmed a similar range of impacts to fraud victims in general victims (Kerr et al 2013). Such impacts are also typical for burglary victims (Maguire, 1980; Beaton et al 2000).

Literature focusing on perpetrators' perceptions of the seriousness and harm associated with online and telephone initiated fraud indicate that they are better able to find ways of justifying their behaviour to themselves than if the offence had been committed face to face (Shover et al, 2003;

Copes and Vieraitis (2009a/b). They adopt a range of strategies to minimise their actions such as blaming the victim or highlighting that they would not have 'physically' harmed their victim. In addition, offenders may ascribe to a perception that their offence was not likely to or intended to cause harm, and therefore will not warrant severe sanctions. Shover et al's (2003) work nevertheless does highlight the importance of the perpetrators considering their victims to be greedy and deserving of victimisation as one of the most important factors, which with the limited research on perpetrators in this area may suggest this is more important than other distancing factors. Copes and Vieraitis (2009a/b) noted in their research, which involved interviewing people convicted of fraud offences in the US, that some offenders did not expect to get as long a sentence as they were given. Other types of offenders, such as burglars, also develop such coping mechanisms, but there is a much greater chance there will be some contact with the victim and invasion of their privacy (Maguire and Bennett, 1982).

Attrition is a common problem for most volume property crimes. There is a lack of research on rates of attrition for online and offline fraud. One study, however, for all fraud did suggest a rate of 98.5 percent not resulting in a formal report or criminal sanction with only 1.5 percent reported and only 0.4 percent resulting in a sanction/detection (Button et al 2012). This is much higher than rates for general volume crimes, where 45.2 percent were reported, 24.3 percent were recorded, 5.5 percent were cleared up, 3 percent resulted in a caution or conviction (Barclay and Tavares, 1999). Given the greater cross-border dimension to online frauds, combined with evidence on attrition, it is reasonable to conclude less offenders are detected and punished for online fraud, compared to offenders such as burglars.

There are therefore some major differences between online fraud vis-à-vis off-line and volume property offences in the extent, interaction, reporting, but also some similarities in impact and offender perceptions. Some of these differences the paper will later show make restorative justice

an attractive option in sentencing online fraudsters. Before these issues are considered, the methods for this research will be outlined.

Methods

The research comprised three phases. Phase one, the evidence review, involved detailed scoping of the existing literature, focusing on the ways in which the fraud offences in the scope of the research are being committed, factors relating to their seriousness and the culpability of the offender and the impact on the victims involved. The purpose of the next two phases was to provide up to date evidence on these areas through primary research. Some of the findings from this stage have already been discussed. 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.

Phase three involved primary research with victims of online fraud and adopted two distinct strands. Six focus groups with 48 members of the public who had been directly affected by fraud in scope for this study, which had been 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, which helped to meet the overarching objectives of the research. 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. Focus group participants tended to be people who had been defrauded via the offence of possessing, making or supplying articles for use in fraud (such as their online banking details being used to remove money from their account) or had experienced

confidence frauds such as not receiving tickets purchased online. Focus groups lasted around 2 hours, and were audio recorded, and transcribed verbatim.

In addition a further 15 individuals took part in in-depth interviews . 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 that could be considered vulnerable due to ill health 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 to one hour and thirty minutes, and were audio recorded and transcribed verbatim. In total, therefore, 63 victims took part in this study and these were recruited through Action Fraud, stakeholders who had been interviewed in phase two and a recruitment agency which specialises in recruiting different types of individuals for marketing surveys. The latter was used largely for the focus groups. All victims were screened by the research team before they were able to participate to ensure they were appropriate victims for the study.

Characteristics of the participants were monitored to ensure that diversity was achieved across and within the groups in terms of their gender, age, whether they lived with other people or alone, employment and health to meet the purposive sampling criteria set decided upon from the outset of the study. The breakdown of participant characteristics is presented in the table below.

Table 1. Achieved sample characteristics for focus groups and in-depth interviews – participants who had experienced online fraud

	Focus Groups	In-depth Interviews
Gender		
Female	25	8
Male	23	7
Total	*48*	*15*
Age		
16 – 24	6	0
25 – 40	21	3
41 – 59	15	5
60 +	6	7
Total	*48*	*15*
Household		
Live alone	8	4
Live with others	40	11
Total	*48*	*15*
Socio-economic activity		
Full time or part time work	36	9
Education or training	2	0
Unemployed	2	2
Retired	7	2
Other	1	1
Unknown	0	1
Total	*48*	*15*
Health		
Visual or hearing impairment	3	0
Limited physical activity	1	5
Learning difficulty	0	1
Long-standing physical/psychological condition	4	1
None	40	10
Unknown	5	0
Total	*53*	*17*

Note: Disability does not add up to totals due to some participants reporting more than one disability.

In addition diversity was also achieved in terms of individuals' self reported internet usage and confidence with financial matters. Fieldwork for phases two and three took place between July and October 2012. The participants had experienced a diverse range of frauds perpetrated online including:

- romance scams
- fake online auctions

- downloading/discovering they had malware
- malicious spam (for example fraudulent emails advising the recipient they had been recorded as accessing indecent images of children online and should pay a fine to avoid further action)
- purchasing of goods found to be counterfeit or faulty on arrival
- purchasing goods or service that did not exist/arrive
- employment scams (for example online websites advertising employment which required registration fees)
- investment scams
- identity theft (fraudsters purchasing goods or services or opening accounts online using stolen personal details)
- account takeover (money being taken by fraudsters from existing online bank account)

The complex nature of fraud made it difficult to put the fraud experienced into clear categories. Often a number of different types of fraudulent activity may be undertaken before the fraudster successfully obtained money from the victim. For example, what began as a romance scam with the victim meeting the fraudster on an online dating site, could become an investment fraud if the victim was convinced to send money for bogus shares. The following sections provide evidence from the research on the victims' views on potential sanctions, but other findings relating to why the victims actually fell victims to the scams are examined in (Button et al, forthcoming). Space constraints makes consideration of some of these important issues not possible in this paper.

Victims' Views on Potential Sanctions

Recent qualitative research on victims of crime in general has suggested more sophisticated views on the sentences offenders should receive. Victims interviewed wanted punishments to fit the crime

and work and were not just interested in tougher prison sentences (Commissioner for Victims and Witnesses in England and Wales, 2011). This research, however, did not offer any insight on the views of fraud victims specifically. Given research on the sentences fraudsters in general receive shows they receive lighter sentences than for comparable property offences, securing information on what the victims think and whether because of this, they would advocate much tougher sentences, would be very useful to discover (Levi, 2006; 2010). Previous research on fraud victims has only touched upon their views regarding the punishment of fraudsters. Button et al (2009b) undertook a telephone survey with closed questions including one asking whether the victims wanted tougher sentences for fraudsters on a scale of 1 to 7 where 1 is not very important and 7 is very important. Of the 675 victims that responded to this 78.7 percent rated this 7. This was reflected in some of their face-to-face interviews too. However, there was also a realisation many fraudsters do not reach the end-game of sentencing after a criminal trial. There were therefore many other needs of victims and views on sentencing for fraudsters was not considered in enough in-depth to offer any sophisticated analysis. This research represents one of the first considerations of the views of online fraud victims in relation to sentencing. First aggravating and mitigating factors are considered, before views on specific types of sentence.

Aggravating and Mitigating Factors

An important part of the research was to identify aggravating and mitigating factors that victims would identify in relation to online fraud. The table below summarises the features which participants and stakeholders felt were aggravating and mitigating factors in relation to online fraud. 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 was most important, others may have felt strongly that the level of planning and premeditation should be the primary factor taken into account. The aim of the qualitative research

was to map out and explore diverse views and experiences – rather than give 'weight' to these differences. Therefore the table below shows the whole range of possible aggravating and mitigating factors, which came from both the group discussions and individual interviews. 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.

Figure 2. Aggravating and mitigating factors

Aggravating factors	• Degree of harm (both intended and actually caused) • Financial impact on victim or level of perpetrators' financial gain • Premeditation and careful planning (intent) • Abuse of trust/authority • Nature of fraud (duration, frequency, and techniques used) • Motivation or history of the perpetrator • Extent of wider impact of the fraud • Invasion of privacy, use of identity • Vulnerability of victims* • Number of victims**
Mitigating factors	• The perpetrators response to the crime once uncovered (personal mitigation) including early plea, cooperation and remorse • Peripheral involvement of perpetrator** • Financial circumstance of the perpetrator** • Mental illness or impairment of perpetrator** • 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.

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 could play a role. One reason for this was the

feeling that it was impossible to *'put a price on crime'* and a person should be sentenced on principles involved rather than the monetary value. At the time of writing (May 2013), the sentencing guidelines for fraud start for offences involving £20,000 or less. It was also felt that sentencing guidelines should be in place for lower values of fraud as victims could be emotionally and psychologically affected by frauds involving smaller amounts of money, and perpetrators may deliberately defraud victims for a smaller amount with a view of getting a lighter sentence if they get caught.

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, and a lack of any of these factors was not necessarily felt to mitigate. Linked to taking into account the harm to victims, a victim impact statement was highlighted by both participants and stakeholders as a possible useful feature to include when sentencing fraud offences, so the court could take into account the true extent of the impact involved.

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. When prompted by the interviewer, participants 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. The views on the different sentences are set out below. It is important to stress again the nature of qualitative research was to map out and explore diverse views on sentences, rather than give 'weight' to these differences.

1. Custodial sentences

Views about the appropriateness of custodial sentences for online fraud were mixed. One opinion that was strongly held was that a custodial sentence was appropriate if sufficient aggravating factors

were present. Another view was doubt that this type of sanction alone had a direct positive impact on reducing reoffending. Those who felt this way therefore suggested combining custodial sentences with other sanctions described below. Finally, some participants felt that custodial sentences were not appropriate for this type of offence. It was felt that a prison environment could help to encourage reoffending, be costly to the state, 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 deterrent 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)*

2. Community orders

There were two views around whether a community sentence was appropriate for this type of offending. The first was that community orders did not provide enough of a punishment or a deterrent. The second was that using community orders for fraud offences was appropriate and the degree to which they were used was dependent on each individual case and the aggravating and mitigating factors present. It was also noted by a participant who had received a virus on his laptop, that while a community sentence may be appropriate, it did not provide restitution to the victim directly affected by the fraud. Therefore they felt the perpetrator should pay the money back, and then also receive the community sentence. Lastly, some participants perceived community orders as being less expensive for the taxpayer, and therefore preferable, especially where it was felt the offence did not warrant a custodial sentence.

3. 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 could disappear and not pay the fine, pay it but not from their own money, or not be able to afford to pay it and commit more fraud as a result in order to pay it.

4. Restitution orders

This type of sanction was a recurring suggestion among participants and stakeholders. Some participants even 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 the money back were pleased with this outcome even when it was a relatively small amount (£50.00). The feeling was that giving the money back to the victim showed that justice had been done and would help ease the financial impact of the offence on them. However, it was also noted that for some frauds 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 equal 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 money spent making telephone calls to resolve a fraud.

5. Seizure of assets and various orders

When the seizure of assets was suggested as an appropriate sanction for fraud offences, participants felt that it should take priority in the sentencing process. This was so the perpetrator could not profit from fraud in the future. 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.

There are various Orders which could also be applied to offenders. A Confiscation Order could be used if the offender had financially gained from the crime to seize computers. Another is a Deprivation Order which can be used to seize property used in a crime. There are also Serious Crime Prevention Orders which can attach conditions of behaviour on an offender to prevent re-offending, which could include activities relating to the internet. These orders do offer scope to restrict access of offenders to tools to perpetrate online crime. Although suggested among participants, the effectiveness of these was questioned among stakeholders.

6. Other sanctions

In addition participants also suggested charity work, 'hard labour' and conscription to the army as appropriate sanctions to use with perpetrators who have been convicted of a fraudulent offence. An 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.

Restorative Justice

Finally restorative justice was considered as a sanction and the views and opportunities on this warrant deeper consideration. There has been growing interest in restorative justice in recent years, greater use of it and growing evidence of a positive impact on offender recidivism (Braithwaite, 1989; Sherman and Strang, 2007; Shapland, et al 2008a and b). Research has also been conducted upon victims and their views of restorative justice which has suggested high levels of satisfaction amongst those who experience restorative justice and greater acceptance of the sentence the offender received, amongst many other (Shapland, et al, 2008b). This research, however, has not investigated fraud victims who have experienced restorative justice or those that might. There has, however, been some research on fraud and related offenders to suggest restorative type punishments deserve more consideration. For example Wenzel (2006) found enforcement letters issued according to restorative justice principles were more effective than stigmatising letters and Murphy and Harris (2007) found tax offenders less likely to offend if they felt they had experienced sanctions according to the principles of restorative justice. Levi (2002) has also suggested the importance of shame may mean greater opportunities for such approaches with business orientated offenders.

The different nature of online fraud compared to off-line and other volume crimes made restorative justice particularly interesting to many of the victims in this research. First, because of the technological sophistication of some fraudsters using malware, victims may have no idea how they were victimised and wanted to know how and why. Second, the anonymous nature of the internet also created a desire to meet the offender and make clear the impact of the crime, particularly as the offender may have become 'cushioned' because of the anonymity as well as the implications for their victims. Third, there was a feeling that it was unlikely the offenders would have ever met the

victims and it would be good for them to see the damage they had done and that this may impact upon their future behaviour. Some of the following comments from the interviews and focus groups illustrate these arguments further.

> *"…these people need to see what harm they've done to other people really. See the effects it has on their lives as well because, all right, they'll be on the computer screen taking money, they don't see the detrimental affect it has on other people's family lives and personal lives and then there's obviously the financial effects it has on people as well, especially some of the people struggling in this day and age. People just don't realise they're taking money from someone -- -- and that affect it has later on down the line, so they need to be faced with this and actually shown the problems they are causing" (Group participant).*

> *"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).*

One participant thought they should meet victims in general, rather than their actual victims.

> *"… or actually meeting the victims, or go round to, possibly not their victims, but other victims of fraud, to face them and say, 'I done this'. And you see an old lady, an old chap who's fought through at least one world war, and he's got scammed and is broke, brought down to their knees because they're financially ruined. This, you know, that has got to be quite powerful" (Group participant).*

Another interview participant thought that the fraudsters having to help the victims could also be beneficial.

> *"…if possible, they could work with people who have been affected by such crime. People that have had hardships because of the crime. You know, they [the perpetrator] might be able to help them in some way..(Interview Participant)"*

Some of the stakeholders could also see the benefits of such an approach.

> *"…why not have the fraudster face their victims like a, a mugger or a burglar? Because actually this could be a really interesting thing to look at, because if one of their motivations, or why they choose fraud compared to other [crimes] is that they never have to actually face anybody, which they probably couldn't do in their normal lives, having to get them to face up could be a really good way of making them think, 'When I sent those emails out and I took those pic-, and I sent those emails to that woman, who I said I was her, you know, GI in America and I love her very much, and I string her along for a long time,' to maybe have that person in front of you and then for them to tell you how they felt about it all could be a very good way of making sure they don't do it again. Or at least it could have an impact" (Stakeholder).*

Participants and stakeholders therefore felt that restorative justice for online fraud offences was particularly 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.

The nature of online fraud would also pose a number of practical challenges to restorative justice approaches compared to other crimes. First and foremost many of these types of offenders are rarely brought to justice in the UK or abroad. Second, the cross-border offending and punishment of some offenders in their home countries would make restorative justice contingent upon the prosecution country and offender's consent. If that was agreed there would be additional costs of travel or the challenge of mediating restorative justice online by 'skype-like' technology. If the conferencing occurred in the fraudster's country, and even if resources were available for travel, there might be reluctance amongst many victims to travel to the country. There are, nevertheless, offenders convicted in the UK and this research suggests there is an appetite amongst victims for this approach. This research has only touched upon this issue, but there is clearly a case for experimentation in this area and more research to evaluate such measures, and assess the extent to which restorative justice is especially effective for addressing specific types of online enabled fraud.

Conclusion

This paper has illustrated the growing problem of online fraud and the diversity of ways in which it is perpetrated and how it differs in some aspects from offline fraud and other volume property crimes. This paper has provided some of the first findings from research on online victims of fraud and their views on sentencing. Research on fraud victims and particularly online victims is rare and this paper presents findings on their views on the impact of the crime upon them and their views on

sentencing. In line with other research published on victims views on sentencing, this paper has showed there is more sophistication to victims views than to just 'hang um and flog um' (Commissioner for Victims and Witnesses in England and Wales, 2011). Victims understood there was a wide range of potential sanctions which could be applied, which went beyond prison sentences. What was most interesting, however, was the interest shown by the victims and stakeholders in the potential for restorative justice. Clearly the anonymous nature of many online frauds made it very attractive to victims to find out who did it and why they were selected. However, there was also a more sophisticated realisation that online fraudsters can escape the impact of their crimes through the anonymity of the internet. They do not see the harm they do. As such there was view amongst the victims and the stakeholders that providing an opportunity for the victims to meet the fraudsters and articulate the damage it had done would be beneficial to both the victims and the offender. The global nature of online fraud would pose more practical challenges compared to other volume property crimes. However, there are offenders based in the UK and with modern technological developments the challenges are not insurmountable. This research has only touched upon these issues and more work needs to be done. However, the findings and the nature of online fraud in the authors' view warrant experiments in the use of restorative justice for fraud victims backed by independent evaluation both UK based and cross-border. As Duffield and Grabosky (2001: 5) argue in relation to the internet: 'Overall, these media serve to distance the fraudster from the prospective victim, making the predatory conduct less difficult for those offenders with some semblance of conscience.' By making the fraudsters consider their conscience this may have a much more significant impact on their future behaviour, not to mention the satisfaction it may give the victims.

References

Australian Bureau of Statistics (2012) *Personal Fraud Costs Australians $1.4 billion*. Available at: http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbytitle/B634CE9C7619C801CA25747400263E7E?OpenDocument (accessed 5 February 2013).

Barclay, G C., and Tavares, C. (1999) Digest 4: Information on the Criminal Justice System in England and Wales. London: Home Office.

Beaton, A., Cook, M., Kavanagh, M., and Herrington, C. (2000) The Psychological Impact of Burglary. *Psychology, Crime and Law*, 6 (1): 33-43.

Braithwaite J (1989) *Crime, Shame and Integration*. Cambridge: Cambridge University Press

Button, M., McNaughton-Nicholls, C., Kerr, J. and Owen, R. (Forthcoming) Online Frauds: Learning From Victims Why They Fall For These Scams. *Australian and New Zealand Journal of Criminology.*

Button M, Lewis. and Tapley J (2014) Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families. *Security Journal* 27(1) 36-54.

Button M, Tapley J and Lewis, C (2013) The 'Fraud Justice Network' and the Infra-structure of Support for Individual Fraud Victims in England and Wales. *Criminology and Criminal Justice,* 13(1): 37-61.

Button, M., Lewis, C., Shepherd, D., Brooks, G and Wakefield, A. (2012) *Fraud and Punishment: Enhancing Deterrence Through More Effective Sanctions*. Portsmouth CCFS.

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). *A Better Deal for Victims*. London: National Fraud Authority.

Commissioner for Victims and Witnesses in England and Wales (2011*) Victims' Views of Court and Sentencing Qualitative research with WAVES victims*. Available: http://www.justice.gov.uk/downloads/news/press-releases/victims-com/victims-views-court-sentencing1011.pdf (accessed 15 February 2013).

Copes H and Vieraitis L (2009a) Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review* 34(3): 329-349.

Copes, H and Vieraitis, L (2009b) Bounded Rationality of Identity Thieves: Using Offender-Based Research to Inform Policy. *Criminology and Public Policy* 8(2):237-262.

Croall H (2009) White Collar Crime, Consumers and Victimisation. *Crime Law and Social Change* 51(1): 127-146

Croall H (2007) Victims of White Collar and Corporate Crime. In: Davies, P., Francis, P. and Greer, C. (eds.) *Victims, Crime and Society.* London: Sage.

Cross, C. (2013). ‘‘Nobody’s holding a gun to your head. . .’’ examining current discourses surrounding victims of online fraud. In Richards, Kelly & Tauri, Juan (Eds.) *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference* (pp. 25–32). Crime and Justice Research Centre, Queensland University of Technology, Queensland University of Technology, Brisbane, QLD.

Duffield G and Grabosky P (2001) *The Psychology of Fraud. Australian Institute of Criminology: Trends and Issues in Criminal Justice*. Canberra: Australian Institute of Criminology.

Federal Trade Commission (2007a) *Consumer Fraud in the United States: The Second FTC Survey*. Available: http://www.ftc.gov/opa/2007/10/fraud.pdf (accessed 7 February 2013).

Federal Trade Commission (2007b) *FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005*. Available: http://www.ftc.gov/opa/2007/11/idtheft.shtm (accessed 7 February 2013).

Fitzgerald, M. (2014) The Curious Case of the Fall in Crime. Available: http://www.crimeandjustice.org.uk/resources/curious-case-fall-crime (accessed 23 June 2014).

Fraud Advisory Panel (2009) Cybercrime - Social Networks and Virtual Worlds. *Fraud Facts*, Issue 4, October 2009.

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

Goucher W (2010) Becoming a Cybercrime Victim. *Computer Fraud and Security,* Oct 2010, Feature, 16 - 18.

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): 35—56.

Huff R, Desilets C, Kane J (2010) *The 2010 National Public Survey on White Collar Crime*. Fairmont (WV): National White Collar Crime Center.

Jewkes Y and Yar M (2010) Introduction: The Internet, Cybercrime, and the Challenges of the 21st Century. In: Jewkes Y and Yar M (eds.) *Handbook of Internet Crime* . Cullompton: Willan.

Kerr, J., Owen, R., McNaughton Nicholls, C. and Button, M. (2013) *Research on Sentencing Online Fraud Offences*. London: Sentencing Council.

Levi M (2010) Hitting the Suite Spot: Sentencing Frauds. *Journal of Financial Crime* 17(1): 116-132.

Levi, M (2008) Organized Frauds and Organising Frauds: Unpacking the Research on Networks and Organisation. *Criminology and Criminal Justice* 8(4): 389-419.

Levi M (2006) Sentencing Frauds: A Review. Available: http://www.cf.ac.uk/socsi/resources/Levi_GFR_Sentencing_Fraud.pdf (accessed 28 March, 2009).

Levi M (2002) "Suite Justice or Sweet Charity? Some Explorations of Shaming and Incapacitating Business Fraudsters. *Punishment and Society* 4(2): 147-63.

Levi M (1991) Sentencing White Collar Crime in the Dark? Reflections on the Guinness Four. *Howard Journal*, 30 (4): 257-279.

Maguire, M. (1980) The Impact of Burglary Upon Victims. *British Journal of Criminology*, 20(3): 261-275.

Maguire, M. and Bennett, T. (1982) *Burglary in a Dwelling*. London: Heinemann.

Murphy K and Harris N (2007) Shaming, Shame and Recidivism. A Test of Reintegrative Shaming Theory in the White Collar Context. *British Journal of Criminology* 47(6): 900-917.

National Fraud Authority (2013) *Annual Fraud Indicator*. London: National Fraud Authority.

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

Office for National Statistics (2013) *Chapter 4: Mass Marketing Fraud*. Retrieved 16 December 2013 from http://www.ons.gov.uk/ons/dcp171776_309772.pdf

Payne B (2013) *White Collar Crime – The Essentials*. Thousand Oaks (CA): Sage.

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

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

Sherman, L and Strang, H (2007) *Restorative Justice: The Evidence*. London: The Smith Institute.

Shover, N., Coffey, G., S. and Hobbs, D. (2003) Crime on the Line. Telemarketing and the Changing Nature of Professional Crime. *British Journal of Criminology* 43(3): 489-505.

Smith, R G (2010) Identiy Theft and Fraud. In Jewkes Y and Yar M (eds.) *Handbook of Internet Crime*. Cullompton: Willan.

Treadwell, J. (2011) From the Car Boot to Booting it Up? Ebay, Online Counterfeit Crime and the Transformation of the Criminal Marketplace. *Criminology and Criminal Justice*, 11(1): 1-17.

US Department of Justice (2011) *Identity Theft Reported by Households 2005-2010*. Available: http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf (accessed 7 February 2013).

Wall, D S (2007) *Cybercrime*. Cambridge/Malden, MA: Polity.

Weisburd D, Waring E and Chayet E (1995) Specific Deterrence in a Sample of Offenders Convicted of White Collar Crime. *Criminology* 33(4): 587-607.

Wenzel M (2006) A Letter from the Tax Office: Compliance Effects of Informational and Interpersonal Justice. *Social Justice Research* 19(3): 364-53

Whitty, M. (2013) The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, 53: 665-884.

Whitty, M. (Forthcoming) The Anatomy of an Online Dating Romance Scam. *Security Journal*.

Acknowledgements

We are grateful to Emma Marshall and Trevor Steeples from 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.

Biographies

Mark Button is Professor of Criminology and Director of the Centre for Counter Fraud Studies at the University of Portsmouth.

Carol McNaughton Nicholls is a Senior Research Director in the Crime and Justice Team at the National Centre for Social Research (NatCen Social Research).

Jane Kerr is a Senior Researcher in the Crime and Justice Team at the National Centre for Social Research (NatCen Social Research).

Rachael Owen is a freelance Social Research Consultant, specialising in criminology.