Is online fraud just fraud? Examining the efficacy of the digital divide

Article *in* Journal of Criminological Research Policy and Practice · June 2019

DOI: 10.1108/JCRPP-01-2019-0008

1 author:

Cassandra Cross
Queensland University of Technology
68 PUBLICATIONS **1,782** CITATIONS

SEE PROFILE

Is online fraud just fraud? Examining the efficacy of the digital divide

Cassandra Cross

Cassandra Cross is based at the School of Justice, Queensland University of Technology, Brisbane, Australia.

Abstract

Purpose – *Fraud is not a new offence. However, the recent evolution and proliferation of technologies (predominantly the internet) has seen offenders increasingly use virtual environments to target and defraud victims worldwide. Several studies have examined the ways that fraud is perpetrated with a clear demarcation between terrestrial and cyber offences. However, with moves towards the notion of a "digital society" and recognition that technology is increasingly embedded across all aspects of our lives, it is important to consider if there is any advantage in categorising fraud against the type of environment it is perpetrated in. This paper aims to discuss these issues.*

Design/methodology/approach – *This paper examines the perceived utility of differentiating online and offline fraud offences. It is based upon the insights of thirty-one professionals who work within the "fraud justice network" across London, UK and Toronto, Canada.*

Findings – *It highlights both the realities faced by professionals in seeking to ether maintain or collapse such a differentiation in their everyday jobs and the potential benefits and challenges that result.*

Practical implications – *Overall, the paper argues that the majority of professionals did not feel a distinction was necessary and instead felt that an arbitrary divide was instead a hindrance to their activities. However, while not useful on a practical front, there was perceived benefit regarding government, funding and the media. The implications of this moving forward are considered.*

Originality/value – *This paper provides new insights into how fraud justice network professionals understand the distinction between fraud offences perpetrated across both online and offline environments.*

Keywords *Police, Victims, Fraud, Cybercrime, Digital society, Fraud justice network*

Paper type *Research paper*

Introduction

Each year, millions of individuals are victims of fraud. For example, in the UK for the year ending at June 2018, there were over 3.3m fraud offences reported, relating to over 2.8m victims (Office of National Statistics, 2018). In the USA, the Internet Crime Complaint Centre (2018) reported losses of over US$1.4bn to victims in 2017; the Australian Competition and Consumer Commission (2018) reported over AUD$340m lost to fraud in 2017; and Canadians lost over CAD$105m to fraud in 2017 (Competition Bureau Canada, 2017, 2018). Fraud losses are not simply restricted to Western countries, with Hong Kong reporting HK$108m lost to romance fraud alone in 2017 (Lo and Leung, 2018).

Fraud offences involve an element of dishonesty (Smith, 2008). Fraud is based upon lying, deception and false pretences, to gain a financial advantage (Fletcher, 2007). Fraud is not a new offence; however the evolution of the internet and other technologies has changed the nature of fraud offending and victimisation and enabled offenders to perpetrate fraud on a much larger scale than previously known (Yar, 2013).

In the context of the internet and evolving technologies, fraud can be understood as a "cyber enabled" offence, meaning that while these offences use technologies such as the internet to facilitate their perpetration, they are not exclusively dependent upon it. This is noted in the following:

> We thus understand cyber-enabled crimes as crimes which can take place in two realms, both online and offline, often simultaneously, or at different phases in the commission of the crime. (Levi *et al.*, 2015, p. 11)

Received 31 January 2019
Revised 29 April 2019
Accepted 5 May 2019

This definition is important as it recognises that fraud offences can occur across both terrestrial and virtual environments. The internet has exponentially increased the reach of offenders and increased the pool of potential fraud victims. Additionally, new and emergent money transfer technologies have further increased opportunities for fraud offending. Nevertheless, traditional communication methods, such as telephone, text messages and simple face-to-face communication, remain as a vehicle for important elements of many fraud offences. In this way, it is difficult to attribute fraud solely to online or offline categorisations (though there has been a strong focus of scholars towards online or cyber fraud (see Button and Cross, 2017 for an example)).

There are many approaches offenders employ to defraud potential victims (Cross and Kelly, 2016). However some of the most common plotlines include:

- romance fraud (whereby an offender uses the guise of a personal relationship to defraud a victim) (Whitty and Buchanan, 2012);
- investment fraud (where the offender persuades the individual to invest their money in an attractive but non-existent situation) (Australian Competition and Consumer Commission, 2016);
- inheritance fraud (where an offender asserts the victim to be the beneficiary to an inheritance from an overseas relative) (Australian Competition and Consumer Commission, 2016); and
- lottery fraud (where offenders notify the victim that they have won a large amount of money) (Australian Competition and Consumer Commission, 2016).

In each case, offenders will use whatever means possible to establish trust and rapport with the victim to secure their finances. Further, it has been established that in the case of romance fraud, offenders will use psychological abuse and coercive control against the victim in order to obtain ongoing compliance with their requests (Cross *et al.*, 2018). While the use of the internet features prominently, offenders will use a variety of communication platforms and other mechanisms to maintain the ruse and perpetrate victimisation (Cross *et al.*, 2016).

This paper seeks to position fraud against the backdrop of victimisation. Fraud victims commonly experience deep dissatisfaction with current police and prosecutorial responses (Button *et al.*, 2009; Cross *et al.*, 2016) and experience additional trauma at the hands of the system (Cross, 2018). In this way, it is imperative to identify ways to improve the current response to fraud.

An emergent question is whether fraud investigation should be positioned as a specialist area of policing, as opposed to being integrated into police general duties. There is a currently disagreement as to what is the most appropriate response. The inability of scholars and practitioners to agree on this has consequences for how police respond to cybercrime (and in this case fraud). The current paper focuses solely on the category of fraud, and examines whether or not having a distinction between online fraud offences and offline fraud is useful.

To achieve this, the paper is as follows. First, it provides a summary to current debates and research that has explored specialist vs generalist policing in response to cybercrime (of which encompasses fraud). Second, the paper outlines the methodology. Third, the paper presents insights from fraud justice network professionals on arguments both for and against the differentiation of fraud offences dependent upon the means in which they are perpetrated. Overall, the analysis in this paper demonstrates that the majority of professionals do not see a benefit in differentiating fraud offences committed across online and offline means, and instead assert this distinction to be a barrier to effective action. The paper concludes with a consideration of the implications for this finding.

A context to the policing of fraud (and cybercrime)

It is well-established that there has not been a priority afforded to the policing of fraud (Button, 2012; Gannon and Doig, 2010; King and Doig, 2016; Levi *et al.*, 2015; Doig *et al.*, 2001; Frimpong and Baker, 2007). While much of this research has focused on a UK context, it is arguably consistent with other countries (Button and Cross, 2017). Several studies have noted the reduction in levels of resourcing allocated to investigating fraud offences (Doig *et al.*, 2001;

Fraud Review Team, 2006; Button *et al.*, 2014). This lack of resourcing has been attributed to several factors, including the lack of fraud in published police priority areas (Button *et al.*, 2007, p. 193; Doig *et al.*, 2001, p. 108) the lack of reporting by victims to law enforcement agencies (Button *et al.*, 2014) and a focus on street offences and front line policing initiatives (King and Doig, 2016, p. 903).

It is important to note that discussions on the policing of (cyber)fraud need to be located within a context of police responses to cybercrime more broadly (of which fraud is one category). It is generally accepted that police are ill-equipped to effectively respond to cybercrime (Willits and Nowacki, 2016), and this is reflected in the overwhelming negativity experienced by victims who experience these types of offences (Cross, 2018). For example, an evaluation of the Australian Cybercrime Online Reporting Network (ACORN) portal found that over three quarters of those who reported (76 per cent) were dissatisfied with the outcome of their report (Morgan *et al.*, 2016). This is also reflected in popular opinion as evidenced in media reports (Willits and Nowacki, 2016, p. 107). While in some cases this can be attributed to a disparity in victim expectations compared to what agencies can realistically deliver (Cross, 2018), these levels of dissatisfaction appear to be consistent, particularly when examining fraud (Button *et al.*, 2009; Cross *et al.*, 2016). Given the large amount of fraud that is now perpetrated through online means, a discussion of the challenges posed by cybercrime are somewhat interchangeable with those barriers noted against the investigation of fraud.

There are many genuine challenges that are argued to exist with the policing of cybercrime. Primarily they revolve around the transnational nature of these offences, which occur across multiple (usually international) jurisdictions (Brenner, 2006; Svantesson, 2016). Policing has historically been premised upon geographical physical borders, and police derive their power and authority from local legislation. Issues of state sovereignty are called into question with the internet (Brenner, 2006). In this way, while the internet has globalised both offending and victimisation, the police response to this is still founded upon local concepts of criminality (Finklea, 2013).

Further to this, it is argued that the successful investigation of cybercrimes requires a level of skill and knowledge that is currently not present. There is a distinct lack of training and development identified across many police agencies (Hinduja and Schafer, 2009, p. 280). For many police, this inability to respond to cybercrime in the same way as more routine offences, leaves many with feelings of powerlessness (Hadlington *et al.*, 2018).

With specific reference to fraud, there are additional barriers identified with regards to policing. First, there is the inability of victims to recognise their own victimisation, which contributes to an established low level of reporting for these offences (Cross and Blackshaw, 2015). Second, given the diverse range of agencies potentially able to respond to a fraudulent complaint, many victims are unsure where to lodge a complaint or alternatively, cannot find an agency who will take their complaint. This has been referred to as the "merry-go-round effect" (Button *et al.*, 2013).

In an attempt to overcome some of these policing challenges, many law enforcement agencies have established specialist units to address cybercrime (Hinduja, 2004; Hinduja and Schafer, 2009) and this has been argued to be an important element of responding to cybercrime (Pisaric, 2017). The formation of specialist units has been growing in prevalence in recent years. For example, Willits and Nowacki (2016, p. 118) found that "from 2000 to 2013, the use of cybercrime units has tripled (from 9 to 27.5 per cent)". This demonstrates an increased acceptance of the need for specialist units and their perceived role in being able to more effectively respond to cybercrimes, or the creation cybercrime units as a new "norm" (Harkin *et al.*, 2018, p. 520).

With regards to fraud, the creation of specialist police units and reporting mechanisms is evident across the globe, with examples in the UK (ActionFraud), Canada (The Canadian Anti-Fraud Centre), and Australia (Scamwatch). However, the above arguments continue to exist in terms of the numbers of police dedicated to the investigation of fraud, and the challenges faced by these units in maintaining their staff and ability to focus on fraud. For example, the ACORN evaluation previously referred to also found that a number of reports were related to child exploitation concerns, and required immediate action on the part of police (Morgan *et al.*, 2016). In this way,

those within fraud and cyber units are tasked with responding to non-fraud-related matters, restricting their ability to focus on fraud offences.

In contrast, there is also a growing body of scholarship which posits that cybercrime is so prevalent, that is does not always require a specialist police response. In this way, the literature asserts all police should be able to perform the role of first responder, and in some cases, undertake any subsequent investigation. Notable in this field is the work of Holt and Bossler, who have undertaken surveys with general duties police in the US and UK (Bossler and Holt, 2012; Holt *et al.*, 2010, 2018; Holt and Bossler, 2012a, b).

These studies underscore an acknowledgement that cyber offences are now a routine part of both offending and victimisation, and that while many may have a cyber component to them, they do not necessarily require high-tech specialist skills to respond. Rather the use of the internet is simply a means to perpetrate the offence, in the same way that other existing technologies operate. This is evident in the notion of a "digital society" whereby the distinct boundaries between the offline and online worlds are increasingly blurred and difficult to distinguish in any meaningful way (Powell *et al.*, 2018). Criminal offending is not committed online or offline, but a hybrid model that uses all means relevant in order to successfully perpetrate the offence.

It is this tension that the following paper seeks to explore. At the moment, there is a combination of both specialist and generalist approaches to the policing of fraud (and cybercrime). In some ways, the existence and advocacy of both is likely a source of some confusion for police and victims. Therefore, it is the purpose of this paper to explore whether there is any benefit to differentiating fraud offences based on the medium through which they are committed (either online or offline). However, prior to gaining the insights from professionals across the fraud justice network, the following section outlines the research methodology.

Methodology

This paper uses data obtained for a study examining potential ways to improve the response to fraud victims by the fraud justice network. In total, 30 in depth, semi-structured interviews were conducted with 31 fraud justice professionals across England and Canada in October and November 2017. The research was approved by Queensland University of Technology's Ethics Committee on 14 September 2017 (Approval No. 1700000730).

Sampling and recruitment

Professionals across the fraud justice network were recruited through a targeted and purposive sampling strategy. Direct e-mail invitations were sent to known contacts of the author. Second, participants were recruited through the referrals of existing contacts. Finally, invitations were sent directly to other organisations in each country that were deemed relevant to the current study. Overall, this resulted in a diverse sample of professionals across the fraud justice network in both countries.

Eligibility for the study was premised on the following factors: participants had to be aged 18 years or older; be capable of providing informed consent to participate in the project; and be currently employed within an organisation across the fraud justice network. Given the nature of employment of many of the participants and the organisations they are part of, both confidentiality and anonymity were assured. In this way, it was the personal perspectives of the participants that were sought, rather than the official position of any agency they worked for.

Data collection

The author conducted the interviews in London and Toronto during October–November 2017. Most were conducted in person ($n = 25$). For participants who agreed to be interviewed in person, the interview took place at either their place of work or a local coffee shop. This choice was completely at the discretion of the participant. The remaining interviews ($n = 5$) were conducted over the telephone. This allowed for the participation of those outside of either London or Toronto as well as for convenience in other circumstances. Participants were each asked a range of questions regarding their perspectives on the ways that their organisation interacts with

fraud victims. This included questions about their ideal outcomes for victims; what they thought victims wanted; and also questions about the various challenges and tensions that exist in seeking to respond to fraud incidents. A small number of demographic questions were also completed by the majority of participants. With permission, all interviews were digitally recorded.

Data analysis

All interviews were transcribed clean verbatim and imported into NVivo (version 11), which is a computer assisted qualitative data analysis tool. The use of NVivo as a tool allows the data to be managed in a central place, and the coding process is both rigorous and replicable. The transcription of the interviews in full allowed for the author to be familiar with the data during the entire research process, and ensured that the analysis undertaken reflected accurately the comments and insights provided by the participants. Thematic coding was undertaken by the author, around the questions contained in the interview schedule. This utilised a general inductive coding approach, where no pre-determined themes were applied to the data. Rather, in reading the transcripts, categories were created based on what was read.

The current paper focuses on responses to the following question:

Do you think it is useful to differentiate between online and offline fraud offences, or do you think it is problematic?

Responses to this question were coded thematically, based on different aspects that were identified in the data, both for and against the differentiation. In NVivo, a node was created specifically for this question and then further child nodes were created underneath the parent node, based on the themes which were evident. The results of this coding are presented further in the paper.

The participants

In total, 30 interviews were conducted with 31 participants (one interview comprised of two participants). In total, 20 interviews were conducted in England, and 10 interviews were conducted in Canada. Of the participants, 25 were male and the remaining 6 were female. Of those who provided their age ($n = 24$) the average age was 47 years (min = 26 and max 62).

A diverse array of agencies across the fraud justice network was represented, as illustrated in Table I.

When asked about the number of years each had been in their current job, the average response was 11.6 years (min = less than one year, max = 39). When asked about the number of years each had been involved across the fraud justice network, the average was 15.3 years (min = 3, max = 43).

Overall, the current sample provided a diverse range of insights from across the fraud justice network. In addition, it is clear that there was also a variety in the experience of participants. While some were relatively new to the area, others brought with them many decades of experience and knowledge on the topic at hand.

Table I Agency representation of the current sample

Participant sector	*Number of participants*
Police (both sworn and unsworn staff)	12
Consumer protection	5
Financial sector	4
Non-government agency	3
Advocacy organisation	2
Government	1
Not-for-profit	1
Private sector	1
Victim support agency	1
Other	1
Total	31

Note: $n = 31$

To ensure the anonymity and confidentiality of responses provided by respondents, only an interview number and a country will be provided with all the direct quotes used throughout the remainder of this paper.

The "fraud justice network"

An important concept regarding the participants interviewed for this paper is that of the "fraud justice network". Originally developed by Button *et al*. (2014), it acknowledges the unique position that fraud holds in relation to the potential reporting of offences across a multitude of agencies. For example, a victim can pursue a fraud complaint through the criminal justice system, the civil system, other statutory systems and also private systems (Button *et al.*, 2013, pp. 42-3). In their study, Button *et al*. (2013, p. 49) list over 20 different organisations across the UK that may be relevant in the event of fraud, and this is not exhaustive. The same situation exists in Australia. In their research of online fraud victims Cross *et al.* (2016) also list over 20 different organisations that victims may report to, in addition to several online reporting mechanisms. While no research specifically documents the fraud justice network across Canada or other countries, it is arguable that the same level of complexity exists and includes a combination of police, consumer protection, banks and other financial institutions, government, non-government and private sector organisations.

Having outlined the methodology for the paper, the following section starts to present the insights of the fraud justice network professionals as they relate to the topic at hand.

Perspectives of the fraud justice network on differentiating between online and offline fraud offences

The following section presents a range of insights provided by professionals on the perceived utility of maintaining a distinction between online and offline fraud offences. While arguments were both in favour and against the need for a distinction, they largely advocate against differentiating fraud offences depending on which environment they were perpetrated in. It is to these arguments that the paper now turns.

The futility of maintaining an online/offline divide

Professionals who put forward arguments against differentiating online and offline fraud offences ($n = 19$) did so under several reasons: Fraud is fraud; Cyber is routine, everyday activity; the cyber distinction makes it difficult for organisations; and victim outcomes are the same regardless. Overall, many argued that the distinction was unhelpful. Each of these will be examined in turn.

Fraud is fraud. There were a small number of explicit comments from professionals who simply stated that fraud was fraud, no matter how it was perpetrated. This is evident in the following:

> I think we've created a problem for ourselves because we label everything. Whereas actually, we should just be saying stop trying to define what cybercrime is. Stop trying to define what cyber enabled fraud is. It's a fraud and however it has happened has happened and let's just get on with dealing with how we intervene with it. Because we spend more time arguing the toss about definitions than we do about what we could do. (Interview 7, UK)

> Then you get into this thing, is it enabled by, is it dependent upon? Is it used as a research tool? Well like, who cares. It's like fraudsters are fraudsters really. (Interview 20, UK)

> The medium isn't the thing that allows it, it's the mechanism. The medium is just an exploitation of an old problem. It's a new manifestation of it […] So no, I don't think it's particularly helpful to create these divisions in it. It's a singular problem, a singular criminality. (Interview 22, Canada)

These comments each indicate the belief that fraud should be understood as such regardless of how it is committed. There was also an acknowledgement on the part of some professionals that fraud was still being perpetrated across physical environments and this could not be ignored:

> I think that in the main when you look at it there is still a lot of offences being committed in the physical world. If you're talking out of 3.3 million, 57 per cent are committed online. That's 40 odd per cent which is committed in the physical world. (Interview 13, UK)

These comments point to the fact that the offence of fraud is central regardless of the online/offline distinction. Further arguments that elaborate this are detailed below.

Cyber is routine. The strongest argument against the distinction between offline and online was centred on the premise that "cyber" is not that different, and instead has become a routine part of everyday activity. This is evident in the following:

> This is just the modern crime type. It's not cybercrime. It's crime that's committed online. We don't call a cash in transit robbery a vehicle enabled robbery, do we? Or they drove a car to get there so it's vehicle. No, no, it's a robbery. (Interview 7, UK)

> Cyber crime is kind of almost all encompassing these days. This goes wider than fraud in terms of how can self-respecting police force really consider cyber a specialism now? (Interview 11, UK)

> I think it's problematic because often there's a blending of the two […] for example romance fraud is also a cyber fraud because typically the method of engaging with the victim is online; the method of payment is often through online, is facilitated online, and yet there might be - there might be face to face meetings, there might be phone conversations. So what is it? Is it a cyber fraud? I think just about every investigation […] now have some cyber component […] But just the fact that they simply use - it has a cyber component, I would be careful about calling that a cyber fraud. (Interview 24, Canada)

In this way, the above excerpts put forward an argument that the online (or cyber) world is increasingly the standard for business and communications across society. In this way, the need to distinguish it from the offline world can be seen as redundant, given the recognised "blending of the two".

Cyber is difficult for organisations. A few professionals spoke of the difficulty that they and their agency experienced regarding the practicality of differentiating online and offline fraud. For these participants, the cyber distinction did not aid their activities, and was seen as unnecessary. This is evident in the following:

> Whether there's a need to rebrand it or whether there's a need just to bring it into every day policing. I think if you're going to do that you need to be much clearer about what it is you're talking about. Because I mean a lot of the frauds that I see are online enabled. Doesn't necessarily mean the investigator needs to be a programmer to deal with it. (Interview 11, UK)

Further to this, there was a belief that the cyber distinction could also act as a barrier to any investigation, as it was deemed to be too complicated:

> I think you're right in terms of the investigative ability, about immediately thinking this is too difficult and it's probably gone overseas and it's probably someone elsewhere, when that's not always true. (Interview 12, UK)

> By being rigid and calling things cyber or calling things whatever […] it ultimately undermines police's ability to react to it. (Interview 21, Canada)

> I have no doubt that the intention was good, but the effect is not, to - so I think what practically happens is when people use the term cyber fraud they write it off as that's not solvable or that's not workable or it's in the air, we can't figure that out, so it almost becomes an excuse by, let's say, law enforcement or Government investigative bodies just to put that over in the cyber fraud pile and not deal with it. I think, in that sense, it's a negative differentiation […] It creates this waste basket. (Interview 23, Canada)

Essentially, several professionals put forward a belief that the distinction was simply "unhelpful" as illustrated in the following:

> But I don't think it's really entirely helpful, not really. (Interview 20, UK)

> It's enormously unhelpful when it comes to fraud. (Interview 21, Canada)

> For my purposes categorising something as cyber fraud or not cyber fraud doesn't in any way assist me in what I'm doing. (Interview 23, Canada)

In combination these comments highlight the futility of the distinction as perceived by several professionals.

Victim outcome is still the same. Finally, there were comments which focused on the outcome for the victim, and argued that regardless of the medium used to perpetrate fraud, it did not affect the impact on these individuals. This is illustrated below:

> It's the buzz word of the time. Yeah, fraud is fraud for me […] I've spoken with victims who've lost tens and hundreds of thousands of pounds on a telephone call. It's the same principal as being online. Or being cyber enabled. They've just used a telephone to do it. They get the same treatment from me as an investigator as if whether it was cyber enabled. (Interview 14, UK)

> We didn't think it was a helpful distinction in terms of our work. A lot of areas we're looking at - so victims, where there's an online or an offline experience - it will be very different for them but, ultimately, the law enforcement response is probably similar, I guess, at the moment. (Interview 15, UK)

> But whether it's by phone or whatever or through cyber, at the end of the day the money is lost. (Interview 26, Canada)

These comments indicate the notion that the online/offline distinction is neither a useful concept for victims in seeking a response from organisations, nor does it impact on their outcomes.

Summary of the case against a digital divide. This section has provided insights from fraud justice professionals about why they do not believe that distinguishing between fraud committed across either online or offline mediums provides any benefits, either to themselves or to the victims involved. Rather, they advocate for an integrated understanding of fraud across all communication platforms.

While arguments against the differentiating the environment that fraud is perpetrated in were dominant, a smaller number of arguments in favour of retaining the distinction also existed. This is detailed below.

The need to differentiate cyber fraud

In a small number of interviews ($n = 8$) participants advocated reasons why they perceived that a cyber distinction could work favourably. Some of these arguments revolved around a perceived need to utilise different investigative tools for online fraud cases. This is highlighted below:

> I suppose it matters in terms of if you want to deliver prevention advice, it might matter in terms of what your investigative opportunities are. (Interview 11, UK)

> But it's important to make the difference from an investigation point of view, because the tools are very different and much harder to trace people back […] I think it's very important to have the right tools. (Interview 28, Canada)

> Cyber fraud is so complex. There's so many different channels of evidence that you need to follow that required greater expertise, I think there really is; and there is an emerging need to differentiate them. They certainly require a lot more resources […] to acknowledge that complexity, they should be differentiated. (Interview 29, Canada)

One professional argued that the distinction was needed for the recording of incidents:

> I agree with the point that fraud should just be fraud. But I think there needs to be recorded of how it's been committed. I think it's important to categorise it in such a way. (Interview 14, UK)

All other arguments that supported the use of the cyber distinction revolved around political notions linked to funding as well as media attention:

> So I do think that it's double-edged, because still, if we wanted to get money, you put cyber in front of it […] But cyber fraud, I think gets sexy. (Interview 12, UK)

> I think a lot of it's quite political. So I think it suits people to tag it to the word fraud or tag it to the word cyber, depending on which organisation you're in and where your funding's coming from. (Interview 20, UK)

The attractiveness of the term "cyber" is also recognised in the following:

> The media uses cyber because it's a catchphrase and it's very catchy. (Interview 13, UK)

Overall, there were fewer arguments supporting a belief in the need to differentiate cyber fraud from its offline counterpart. Of those arguments that were in favour, they revolved around a

perception of different tools needed to investigate as well as the political environment in which organisations currently operate in.

Having put forward the arguments shared by fraud justice professionals both for and against the need to differentiate cyber fraud, the final section discusses the implications of these arguments.

Discussion

The majority of participants did not support distinguishing fraud offences across the virtual or physical environments. Instead, they saw this distinction as arbitrary and either a barrier or simply redundant to their work.

Many themes evident in the responses support the notion of a digital society, whereby activities and behaviours are so enmeshed between online and offline mediums that there is no longer an ability to make a useful distinction between the two. Powell *et al.* (2018, p. 4) advocate for an understanding of a digital society as one that "refers to the integrated whole represented by digital societies and society". In doing this, they seek to challenge dichotomies such as "online/offline, real/cyber and virtual/terrestrial" (Powell *et al.*, 2018, p. 7). Many of the above quotes from professionals support this notion of the digital society and the idea that one must move beyond the dichotomies when thinking about fraud. "Fraud is fraud" is a sentiment that was reiterated numerous times throughout the interviews.

The integration of technologies in the perpetration of fraud is evident in the literature. For example, Cross *et al.* (2016), conducted interviews with victim who were approached primarily online. However the resulting narratives reveal the diverse communication platforms that offenders used to perpetrate their offence, and how these traversed the internet, telephone and in some cases, face-to-face contact. It is evident that offenders will use whatever means considered necessary to maintain their control and exploitation of fraud victims, and this may cross both online and offline means. Many of the professionals in the current sample were able to identify with and support this point.

Finally, there was recognition by professionals that the victim outcome is the same regardless of how the offence has been perpetrated. This acknowledges the negative impact of fraud on an individual in both financial and non-financial terms (Button *et al.*, 2009; Cross *et al.*, 2016). Further, it counters the myth that exists on fraud being a "victimless" crime (Gee in Button *et al.*, 2010). However, while these comments demonstrate an understanding of the trauma and suffering of victims, this does not appear to translate into the provision of adequate support services or recognition to fraud victims in the aftermath of their incident. Instead, the literature demonstrates that there is a lack of support services and an overwhelming negativity experienced by victims in response to fraud (Button *et al.*, 2009; Cross *et al.*, 2016). In this way, while it is important that professionals appear to acknowledge the harm caused by fraud to victims, more practical, concrete support is required.

Overall, the notion that "fraud is just fraud" and there is little use in differentiating the medium through which it is perpetrated supports the current scholarship seeking to better understand how general duties police approach "cybercrime" as first responders. It reinforces the need to improve the ability of police to respond to these offences at the front line. It also supports the need to shift the view of police that "cyber fraud" should be a specialist area designated for specialist police units, and instead advocates that general duties police and detectives should have the capacity to investigate many of offences. In the same way that Cross and Kelly (2016) argue that it is redundant to categorise the many different plotlines of fraudulent approaches, the current paper asserts that there is little perceived benefit in categorising fraud with regards to the way in which it is committed.

Of those who did advocate for a distinction, the reasons revolved mainly around the political nature of "cyber" as it relates to government and funding. Governments worldwide are currently committing large amounts of money in an effort to combat these offences. It is not surprising that participants mentioned the political nature of this term and how it can be used to attract funds. In strict economic times (particularly in the UK which has been plagued by austerity for a number of years) this strategy is understandable. However, it must be understood as simply that a political

strategy to secure funding and attention in a highly competitive market. It does not appear to be one that is based upon other perceived benefits, outside of the political sphere and within a practical, day-to-day context.

Conclusion

This paper has challenged the current practice of differentiating fraud offences based on an arbitrary method of perpetration. In doing this, it locates the findings within the notion of a "digital society" (Powell *et al.*, 2018) and lends support to the utility of this approach in understanding fraud offences. As a result, the paper is clear in advocating the need for general duties police to be able to act as appropriate first responders to fraud offences, regardless of the medium in which they are committed. In connection with this, it also argues against the need for fraud to be seen as a specialist area, within the context of current cybercrime and high-tech crime units.

However, it is important to note that this paper is not calling for the abolition of specialist units. Rather, it is imperative to recall the definition of fraud as a cyber-enabled offence, in that it can occur across both online and offline environments. In this way, the intertwining of technology is evident across many victimisation narratives and is relevant (or in this case not) to the reporting and investigation of the offence. This is not argued to be the case for those offences that are cyber-dependent, or would not exist if not for the internet (such as malware and hacking). While these can still be understood within the context of a digital society, in terms of policing, they may not fit the same framework spoken about by professionals in the current sample. It would be interesting to ascertain the view of professionals working across this field and responding to these cyber-dependent offences. The current research speaks only to fraud, as a cyber-enabled offence that has existed (and arguably will continue to exist) across all available communication platforms, now and into the future.

In looking to the future of fraud and how the fraud justice network responds to these offences, there are distinct challenges. If the efficacy of maintaining a digital divide is questioned, it becomes imperative for these professionals to advocate for a consistent and integrated approach to fraud and its victims. It is likely to require further training and skills for police to be able to adequately respond to fraud in the first instance. Most importantly, it will require a cultural shift in understanding the severity, impact and consequences of fraud victimisation and the need to invest resources into it. This will require a change in attitudes to fraud across police, government, and society as a whole. Historically, the evidence is not in favour of this, and it will undoubtedly remain a challenge into the future. Sadly, what is guaranteed is the continued number of victims and the trauma they continue to suffer through their losses. In this way, arguments about whether fraud is committed in an online or offline environment find little relevance, and instead the focus should be on taking whatever means necessary to improve current responses to fraud victims.

References

Australian Competition and Consumer Commission (2016), "The little black book of Scams", available at www.accc.gov.au/system/files/Little%20Black%20Book%20of%20Scams_0.pdf (accessed 31 January 2019).

Australian Competition and Consumer Commission (ACCC) (2018), "Targeting scams: report of the ACCC on scam activity 2017", available at www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2017 (accessed 31 January 2019).

Bossler, A. and Holt, T. (2012), "Patrol officers' perceived role in responding to cybercrime", *Policing: An International Journal of Police Strategies & Management*, Vol. 35 No. 1, pp. 165-81.

Brenner, S. (2006), "Cybercrime jurisdiction", *Crime, Law and Social Change*, Vol. 46 Nos 4-5, pp. 189-206.

Button, M. (2012), "Cross-border fraud and the case for an 'Interfraud'", *Policing: An International Journal of Police Strategies and Management*, Vol. 35 No. 2, pp. 285-303.

Button, M. and Cross, C. (2017), *Cyber fraud, Scams and Their Victims*, Routledge, London.

Button, M., Lewis, C. and Tapley, J. (2009), *A Better Deal for Fraud Victims*, Centre for Counter Fraud Studies, London.

Button, M., Lewis, C. and Tapley, J. (2013), "The 'fraud justice network' and the infrastructure of support for the individual fraud victims in England and Wales", *Criminology and Criminal Justice*, Vol. 13 No. 1, pp. 37-61.

Button, M., Frimpong, K., Smith, G. and Johnston, L. (2007), "Professionalizing counter fraud specialists in the UK: assessing progress and recommendations for reform.crime prevention and community safety", *Crime Prevention and Community Safety*, Vol. 9 No. 2, pp. 92-101.

Button, M., Gee, J., Lewis, C. and Tapley, J. (2010), *The Human Cost of Fraud: A Vox Populi*, Centre for Counter Fraud Studies & MacIntyre Hudson, London.

Button, M., McNaugton Nicolls, C., Kerr, J. and Owen, R. (2014), "Online frauds: learning from victims why they fall for these scams", *Australian and New Zealand Journal of Criminology*, Vol. 47 No. 3, pp. 391-408.

Competition Bureau Canada (2017), "Archived –fraud facts 2017 – recognize, reject, report fraud", available at: www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html (accessed 31 January 2019).

Competition Bureau Canada (2018), "Fraud facts – recognize, reject, report fraud", available at: www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04334.html (accessed 31 January 2019).

Cross, C. (2018), "Expectations vs reality: responding to online fraud across the fraud justice network", *International Journal of Law, Crime and Justice*, Vol. 55, pp. 1-12.

Cross, C. and Blackshaw, D. (2015), "Improving the police response to online fraud", *Policing: A Journal of Policy and Practice*, Vol. 9 No. 2, pp. 119-28.

Cross, C. and Kelly, M. (2016), "The problem of 'white noise': examining current prevention approaches to online fraud", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 806-28.

Cross, C., Dragiewicz, M. and Richards, K. (2018), "Understanding romance fraud: insights from domestic violence research", *British Journal of Criminology*, Vol. 58 No. 6, pp. 1303-22.

Cross, C., Richards, K. and Smith, R. G. (2016), "The reporting experiences and support needs of victims of online fraud", *Trends and Issues in Crime and Criminal Justice*, No. 518, pp. 1-14.

Doig, A., Johnson, S. and Levi, M. (2001), "New public management, old populism and the policing of fraud", *Public Policy and Administration*, Vol. 16 No. 1, pp. 91-113.

Finklea, K. (2013), "The interplay of borders, turf, cyberspace and jurisdiction: issues confronting US law enforcement", *Congressional Research Service Report for Congress*, Congressional Research Service, Washington, DC.

Fletcher, N. (2007), "Challenges for regulating financial fraud in cyberspace", *Journal of Financial Crime*, Vol. 14 No. 2, pp. 190-207.

Fraud Review Team (2006), "Final report", The Legal Secretariat to the Law Offices, London.

Frimpong, K. and Baker, P. (2007), "Fighting public sector fraud: the growth of professionalism in counter-fraud investigators", *Crime Prevention and Community Safety*, Vol. 9 No. 2, pp. 130-7.

Gannon, R. and Doig, A. (2010), "Ducking the answer? Fraud strategies and police resources", *Policing and Society: An International Journal of Research and Policy*, Vol. 20 No. 1, pp. 39-60.

Hadlington, L., Lumsden, K., Black, A. and Ferra, F. (2018), "A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime", *Policing*, doi: 10.1093/police/pay090.

Harkin, D., Whelan, C. and Chang, L. (2018), "The challenges facing specialist police cyber-crime units: an empirical analysis", *Police Practice and Research*, Vol. 19 No. 6, pp. 519-36.

Hinduja, S. (2004), "Perceptions of local and state law enforcement concerning the role of computer crime investigative teams", *Policing: An International Journal of Police Strategies & Management*, Vol. 27 No. 3, pp. 341-57.

Hinduja, S. and Schafer, J. (2009), "US cybercrime units on the world wide web", *Policing: An International Journal of Police Strategies & Management*, Vol. 32 No. 2, pp. 278-96.

Holt, T. and Bossler, A. (2012a), "Police perceptions of computer crimes in two Southeastern cities: an examination from the viewpoint of patrol officers", *American Journal of Criminal Justice*, Vol. 37 No. 3, pp. 396-412.

Holt, T. and Bossler, A. (2012b), "Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments", *Cyberpsychology, Behavior, and Social Networking*, Vol. 15 No. 9, pp. 464-72.

Holt, T., Bossler, A. and Fitzgerald, S. (2010), "Examining state and local law enforcement perceptions of computer crime", in Holt, T. (Ed.), *Crime On-line: Correlates, Causes, and Context*, Carolina Academic Press, Raleigh, NC, pp. 3-28.

Holt, T., Burruss, G. and Bossler, A. (2018), "An examination of English and welsh constables' perceptions of the seriousness and frequency of online incidents", *Policing and Society*, available at: https://doi.org/10.1080/10439463.2018.1450409

Internet Crime Complaint Centre (2018), "2017 Internet crime report", available at: https://pdf.ic3.gov/2017_IC3Report.pdf (accessed 31 January 2019).

King, J. and Doig, A. (2016), "A dedicated place for the volume fraud within the current UK economic agenda? The Greater Manchester police case study", *Journal of Financial Crime*, Vol. 23 No. 4, pp. 902-15.

Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, D. (2015), *The Implications of Economic Cybercrime for Policing*, City of London Corporation", London, available at: www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf (accessed 31 January 2019).

Lo, C. and Leung, C. (2018), "Number of Hongkongers falling prey to online romance scams surges almost 250 per cent", available at: www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2156831/number-hongkongers-falling-prey-online (accessed 31 January 2019).

Morgan, A., Dowling, C., Browns, R., Mann, M., Vice, I. and Smith, M. (2016), "Evaluation of the Australian cybercrime online reporting network", available at: https://aic.gov.au/sites/default/files/2018/08/acorn_evaluation_report_.pdf (accessed 31 January 2019).

Office of National Statistics (2018), "Crime in England and wales: additional tables on fraud and cybercrime", available at: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables (accessed 31 January 2019).

Pisaric, M. (2017), "Specialization of criminal justice authorities in dealing with cybercrime", *Journal of Criminal Justice and Security*, Vol. 17 No. 2, pp. 230-42.

Powell, A., Stratton, G. and Cameron, R. (2018), *Digital Criminology: Crime and Justice in Digital Society*, Routledge, New York, NY.

Smith, R.G. (2008), "Coordinating individual and organisational responses to fraud", *Crime Law and Social Change*, Vol. 49 No. 5, pp. 379-96.

Svantesson, D. (2016), "Internet jurisdiction: today and in the future", *Precedent*, Vol. 132, February, pp. 4-9.

Whitty, M. and Buchanan, T. (2012), "The psychology of the online dating romance scam", available at: www.scribd.com/document/296206044/The-Psychology-of-the-Online-Dating-Romance-Scam-copypasteads-com (accessed 31 January 2019).

Willits, D. and Nowacki, J. (2016), "The use of specialized cybercrime policing units: and organizational analysis", *Criminal Justice Studies*, Vol. 29 No. 2, pp. 105-24.

Yar, M. (2013), *Cybercrime and Society*, 2nd ed., Sage, London.

Corresponding author

Cassandra Cross can be contacted at: ca.cross@qut.edu.au