Reflections on the reporting of fraud in Australia

Cassandra Cross
School of Justice, Faculty of Law, Queensland University of Technology – QUT, Brisbane, Australia

Abstract

Purpose – The purpose of this paper is to reflect on the reporting of cybercrime in Australia, specifically the reporting of fraud.

Design/methodology/approach – Using an evaluation of the (former) Australian Cybercrime Online Reporting Network (ACORN), this paper provides a commentary on the report findings, including both positive and negative aspects of the reporting mechanism.

Findings – The paper focuses on three key challenges that were identified in the evaluation: victim satisfaction; quality of data; and unintended consequences. Each of these topics is outlined and located within a broader context to better understand the evaluation findings.

Research limitations/implications – This viewpoint paper is a commentary based upon an evaluation of ACORN which itself has several limitations of its methodology. Despite this, the evaluation provides important insights into the challenges that currently exist with the online reporting of fraud offences both in Australia, and worldwide.

Practical implications – This paper emphasises the structural and systemic issues that exist for the reporting of fraud in Australia. It therefore warns against placing blame exclusively on police agencies as responsible for these results. Instead, it advocates the need for society to take a more coordinated and collaborative approach to the policing of fraud, which includes law enforcement, government and industry partners.

Social implications – The paper documents some of the underlying reasons for additional trauma and harm experienced by victims of fraud in their efforts to report their incident and receive what they perceive to be an appropriate criminal justice response. These must be acknowledged in order to make the required change.

Originality/value – This paper is a commentary and reflection on the current way in which fraud is reported in Australia. It points to a need to rethink this approach in some key areas. It highlights the critical need for an education campaign to dispel some of the myths that exist in relation to realistic police responses to fraud, and also calls for the need to consider alternatives to the exclusively online system currently in operation, as well as larger questions about notions of justice and appropriate responses to fraud victims.

Keywords Police, Reporting, Fraud, Cybercrime, Victim

Paper type Viewpoint

Introduction

Cybercrime is somewhat of an umbrella term which encompasses a large array of offence types. In particular, cybercrime is usually broken down into two categories: cyber enabled (or computer assisted) crime and cyber dependent (or computer focused) crime (Wall, 2007; Yar, 2013). Cyber enabled refers to traditional crimes facilitated through the use of the internet (Wall, 2007). These offences can exist across both offline and online environments. In contrast, cyber dependent crimes are those that cannot exist without technology, and are therefore restricted to the virtual environment (Wall, 2007). In this way, fraud can be understood as a cyber enabled crime in that it has existed for centuries. The advent of technology (namely the internet) has seen a change in the ways that fraud is perpetrated and has also witnessed an exponential increase in the ability of offenders to target potential victims worldwide (Yar, 2013).

Fraud is based around notions of deception, and involves both lying and cheating (Fletcher, 2007). The internet is a popular communication channel for offenders to target victims, through the use of e-mail and social media platforms. However, it is important to note that offenders will use a variety of mechanisms to target offenders, including the telephone and face-to-face contact in addition to the internet (ACCC, 2019). The number of approaches used by offenders to target victims is endless (Cross and Kelly, 2016),
nonetheless there are some common approaches used. Within Australia, investment fraud and romance fraud are the top two categories of fraud with regard to financial loss (ACCC, 2019) and this has been the case for the past decade (Cross, 2019). Investment fraud targets victims through offering an attractive opportunity for victims to capitalise and grow wealth on their required contribution (Cross et al., 2016). Sadly, many victims lose large amounts of money when they realise that in many cases, there was no investment opportunity in the first place. Romance fraud uses the guise of a perceived relationship in order to defraud a victim (Rege, 2009). The victim believes in the genuine nature of their relationship and when asked to send money for a medical emergency, criminal justice matter or other issue, they comply. Victims of romance fraud experience a “double hit” of victimisation whereby they not only grieve the loss of money but also of the relationship itself (Whitty and Buchanan, 2012).

There is a small but consistent body of research which explores the overwhelmingly negative experiences that fraud victims experience in seeking to report their crime and gain an appropriate response (Button et al., 2009; Cross et al., 2016). Issues relate to an inability to lodge a complaint with organisations across the fraud justice network; to high levels of shame, stigma and victim blaming; to not believing that anything can done about it (Button, 2012; Button et al., 2013; Cross, 2015, 2018a). The dynamics of reporting fraud are complex, as are the current responses to this category of crime victims.

This viewpoint paper examines the reporting of cybercrime in Australia, specifically as it relates to fraud. In particular, it provides a commentary based on an evaluation of the (former) Australian Cybercrime Online Reporting Network (ACORN), which was commissioned by the Australian Institute of Criminology (AIC). Of the offences that were reported to ACORN during the evaluation period, almost half (48 per cent) related to online scams or fraud (Morgan et al., 2016, p. 30). This was more than double the second highest category (issues buying and selling online at 21 per cent) (Morgan et al., 2016, p. 31). It is for this reason that the current paper focuses on the evaluation findings in the context of how they relate specifically to fraud victims in Australia.

Although the evaluation was completed in October 2016, it was not publicly released at the time. It was only through a successful application by the author under Freedom of Information legislation, that the report was made available to the public in September 2018. The decision not to release the report once completed, likely stems from the many negative findings contained within the analysis. However, it is important not to dismiss or ignore the findings of this evaluation, as uncomfortable as they may be, as it highlights the need for a larger conversation about the difficulties associated with the reporting of fraud and cybercrime as well as the many challenges faced by police and victims alike. It is these difficult conversations that form the basis of the current viewpoint paper.

To achieve this, the paper is set out as follows. First, there is a brief overview of the various reporting mechanisms for the reporting of cybercrime and fraud globally. Second, the paper provides an outline of the ACORN evaluation and the main findings. Third, the paper uses these ACORN findings as a catalyst for arguing for change in this area. Overall, this paper argues that the current means of reporting of cybercrime is problematic for both police and victims alike, and argues the need for systemic and structural change into the future.

**Reporting fraud and cybercrime globally**

There are a number of mechanisms available in various countries for the reporting of cybercrime and associated offences, such as fraud. There appears to be a current trend for the use of centralised reporting mechanisms for cybercrime and fraud. In this way, the reporting of these offences is taken away from a local level police agency. Rather, it is collated at a higher level before being disseminated to local agencies as required. Examples of these are as follows.
Internet Crime Complain Centre (IC3) (USA)
The IC3 is an exclusive online platform that enables the reporting of internet crime globally, where there is a connection to the USA (across both victim and offender categories). The scope of internet crime:

[...] includes any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or email. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes. (IC3, n.d.)

Under this definition, fraud is one of many offence types that can be reported to the IC3. The IC3 is hosted by the Federal Bureau of Investigation and all reports received by the IC3 are triaged and sent to the relevant agency (law enforcement or otherwise) for action as required (IC3, n.d.).

ActionFraud (UK)
ActionFraud (n.d.) is run by the City of London Police in conjunction with the National Fraud Intelligence Bureau. The City of London Police is the lead agency for economic crime and the NFIB are tasked with the responsibility of assessing all ActionFraud (n.d.) reports and forwarding those to relevant local agencies as relevant. ActionFraud combines an online reporting mechanism for a variety of fraud offences, and can also be accessed through a call centre.

Canadian Anti-Fraud Centre (Canada)
The CAFC (2019) is the central reporting agency for fraud and identity theft. The CAFC is a collaboration of the Ontario Provincial Police, the Royal Canadian Mounted Police and Competition Bureau Canada. Similar to ActionFraud, there is both an online reporting mechanism as well as a call centre through which victims can report their incident.

Online Reporting Button (ORB) New Zealand
The ORB was an online reporting mechanism for the reporting of fraud in New Zealand. It is currently redirecting victims to a different reporting platform hosted by Netsafe (n.d.), who are an independent, non-profit online safety organisation. Netsafe (n.d.) have a wider ambit than just fraud, rather they seek to educate and support victims in the broader area of online safety (including but not limited to, bullying, harassment and image based abuse). Netsafe have both an online and telephone platform for reporting and seeking advice and support for individuals who have experienced these types of incidents.

Scamwatch (Australia)
Scamwatch (n.d.) is an online reporting mechanism for fraud hosted by the Australian Competition and Consumer Commission. Importantly, Scamwatch has no ability to conduct individual investigations in response to complaints of fraud. Rather, the information submitted to Scamwatch is used as a basis for awareness and education campaigns of the ACCC.

Australian Cybercrime Online Reporting Network (ACORN) (Australia)
ACORN was established in November 2014. It was a centralised online mechanism for the reporting of cybercrime in Australia. ACORN was intended to capture reports across four categories of cybercrime, as follows:

1. online scams or fraud;
2. issues buying and selling online;
attacks on computer system or viruses; and

(4) cyber bullying, sexting, online harassment or stalking.

In the context of ACORN, online scams or fraud were defined as “an attempt by a ‘scammer’ to lure and trick a victim into giving money or personal information (excludes issues buying and selling online)” (Morgan et al., 2016, p. 29). The ACORN was hosted by the Australian Criminal Intelligence Commission (ACIC) a federal enforcement agency. However, the ACIC did not have investigative jurisdiction over these complaints, and instead forwarded them to state and territory police depending on the location of the victim and/or offender in the complaint.

Summary
The above demonstrates that there are several jurisdictions that have implemented a centralised reporting system for fraud or cybercrime more broadly. These all exist in an online environment, with some also having a call centre as an additional option to report. However, to date there is no known academic research which has explored whether this is the most appropriate option for reporting these particular offences. There is research which explores the use of online reporting mechanisms as an option for reporting, with mixed results, particularly with respect to demographics of individuals (Morgan et al., 2016, p. 18). There has been some examination of ActionFraud (Correia, 2019; HMIC, 2015; Skidmore et al., 2018) as well as many media reports focused on high levels of dissatisfaction (Boyce, 2018; Morely, 2015). In a similar vein, there have been media reports of anger and frustration levelled towards ACORN (McGrath, 2016; Wordsworth, 2017).

Nonetheless, there is no known research which specifically explores the suitability of centralised, online reporting platforms for fraud and cybercrime offences, despite their existence across several jurisdictions as detailed above. While this is beyond the scope of the current paper, it is a topic worthy of future exploration.

The evaluation of ACORN
The AIC was commissioned to undertake an evaluation of ACORN by the former federal government agency CrimTrac (which was subsequently merged into another federal government department). A working group was established to oversee the evaluation, and comprised a number of police and government representatives (Morgan et al., 2016, p. 7). The evaluation sought to determine if the establishment and implantation of ACORN had met with its four stated objectives. These were:

(1) provide a centralised, national online facility that would receive reports from members of the public;

(2) refer reports to the police and regulatory agencies for further consideration;

(3) collect and aggregate data from reports to assist police, regulatory and other government agencies to develop improved strategic and tactical responses to cybercrime; and

(4) provide ACORN users with general and targeted educational advice (Morgan et al., 2016, p. 18).

In order to achieve this, the research team employed a mixed method research strategy. This comprised the following data sources:

(1) an analysis of ACORN data from November 2014 through until June 2016;
(2) a survey of the general public’s level of cyber victimisation, reporting activity and satisfaction with this process at 12 months prior to ACORN’s launch, and again at 12 months post-implementation ($n = 1,793$ and $n = 1,853$);

(3) interviews with relevant stakeholders (including senior officials, intelligence analysts and investigators) at both pre-implementation and post-implementation periods ($n = 19$ and $n = 31$);

(4) a survey of three police agencies (Queensland, New South Wales and West Australia) across both pre-implementation and post-implementation periods; and

(5) a survey of those who had submitted an ACORN report ($n = 1,654$) (Morgan et al., 2016, pp. 21-28).

Overall, the methodology employed by the evaluation was robust in capturing a data set that represents the views of a diverse range of relevant stakeholders to the reporting of cybercrime in Australia, and also covered both pre- and post-ACORN implementation periods. Each of these approaches to research has its own set of limitations (e.g. the police survey focused on specialist police rather than also canvassing general duties police; and the ACORN survey is a self-selecting sample of users who likely were very positive or very negative about their reporting experience (Morgan et al., 2016, p. 27)). However, the data provide important insights into the operation of ACORN across the evaluation period, and highlight both the positive aspects of ACORN and the areas for improvement. The findings articulated in the evaluation report draw on a combination of these data sources for support where appropriate. For a detailed understanding of the methodology used for the ACORN evaluation, please see the original report (Morgan et al., 2016, pp. 20-28).

**ACORN evaluation findings**

The evaluation found that overall ACORN had met its original objectives. It created a centralised, national online facility; it enabled the automatic referral of 75 per cent of complaints to police or regulatory agencies for consideration; it increased the number of intelligence products generated by law enforcement as well as investigation numbers; and it provided education and awareness material that the public has positively engaged with (Morgan et al., 2016, p. 77). These four points essentially meet the stated objectives of ACORN from its inception.

In addition to this, the evaluation articulated 14 separate findings, which cover a range of topics and issues in relation to the reporting, investigation and prevention of cybercrime. Some of these are positive in nature, while there are several others which bring to the fore areas of concern. The positive impacts of ACORN as found within the evaluation are summarised below:

- more than 65,000 reports to ACORN with an upward trend (11/14-6/16);
- relatively high levels of satisfaction with the process of reporting to ACORN;
- increased number of intelligence products and more efficient intelligence activity;
- number of investigations into cybercrime has increased, as well as associated resources;
- examples of positive investigation outcomes; and
- high level of engagement with prevention advice (Morgan et al., 2016, pp. 9-14).

In contrast to this, the areas for attention and further consideration are summarised below:

- little evidence that ACORN led to an increased prevalence in victims reporting cybercrime;
• little change in public awareness on where to report cybercrime;
• low levels of satisfaction with the outcome of ACORN reports;
• ACORN has largely shifted responsibility for referring reports between business areas and agencies rather than reduce the time spent by enforcement; and
• little evidence that prevention advice has had any impact on repeat victimisation (Morgan et al., 2016, pp. 9-14).

The remainder of this commentary focuses on these negative findings, and seeks to understand what can be learnt moving forward. The issues evident in these findings need to be examined in a broader context, to better understand why they occurred and how they can be avoided for the future. It is to this that the paper now turns.

Putting the results in context: the challenges of reporting cybercrime
While the evaluation found that ACORN had essentially met its initial stated objectives, as illustrated above, it also found a range of areas that require further attention to improve areas of concern. This section explores some of these issues in detail, particularly as they related to fraud victimisation, and also how they relate to some of the macroissues facing fraud victims globally.

Victim satisfaction
It is clear from the evaluation that victims are largely unhappy with the outcome of their report to ACORN. This is reflected primarily in the fact that over three quarters (77 per cent) of individuals who submitted a report to ACORN were dissatisfied with the outcome of their report (Morgan et al., 2016, p. 42). Lack of victim satisfaction is an issue that plagues agencies regarding the reporting of fraud (Button et al., 2009; Cross et al., 2016; Skidmore et al., 2018).

The underlying reasons behind such high levels of dissatisfaction with the outcome of a fraud report, stem from a number of factors. First, one must consider the motivation for a victim in reporting to police in the first place. Research indicates that victims usually report fraud for one of two main reasons (Cross, 2018b). The first revolves around a desire for individual justice and the second centres on an altruistic notion of protecting others (Cross, 2018b). These motivations were also supported in the evaluation, whereby they were given as the top two responses as to why people reported to ACORN (Morgan et al., 2016, p. 38). Caught up in both of these reasons for reporting is an expectation by victims that their report will result in some form of action being taken, usually in the form of an investigation (Cross, 2018b). Again, this confirmed in the evaluation with 26 per cent of fraud victims expecting to be notified that a report was received and investigate, 36 per cent expecting that a report was received, investigated and action taken, and lastly 17 per cent of fraud victims expecting that a report was received, investigated, action taken and an offender arrested (Morgan et al., 2016, p. 40).

From the perspective of organisations (law enforcement and other agencies alike), these expectations are not realistic and cannot be delivered upon. There are a number of genuine reasons why police and other agencies are unable to initiate an investigation with regards to online fraud, compared to many other terrestrial crimes. This includes the transnational nature of the offence, a lack of jurisdiction, a lack of skills and resources, inadequate legislation and a lack of political priority (see Button, 2012; Cross, 2018b; Cross and Blackshaw, 2015). Each of these factors by themselves provides an obstacle to the effective policing of fraud, while in combination presents somewhat of an insurmountable barrier.

The evaluation was able to provide data on the number of arrests that were recorded as a result of the ACORN reports. Of the available data, less than 1 per cent of reports led to an offender being identified but not arrested, and a further less than 1 per cent resulted in an
offender being identified and arrested (Morgan et al., 2016, p. 66). Overall, there were only three victims who reported that their offender had been arrested (Morgan et al., 2016, p. 41).

If victims of fraud are reporting to ACORN on the premise that they are seeking an individual response to their complaint, through an investigation and the eventual arrest of an offender, then the inability of police and other agencies to deliver on this expectation undoubtedly drives a large degree of the anger and frustration experienced by victims. These figures also serve to highlight a large disparity that currently exist between the public expectation of what police can do in response to both cybercrime and fraud, compared to the reality of what police can actually do (Cross, 2018b). It is clearly an area that requires improvement in the communication between police and the public on what is realistic and what is not.

In a bid to overcome this, ACORN did insert a tick box when reporting which required the victim to acknowledge that their report may not be investigated. However, based on research with victims, it is clear that there is a lack of awareness of the frequency in which individuals are defrauded across the country and globally. For example, Cross et al. (2016) interviewed 80 fraud victims across Australia. During interviews with the researchers, victims were surprised to learn that there were 79 other victims who had volunteered to be part of the study. However, from a police perspective, and from the statistics provided by Scamwatch on an annual basis (ACCC, 2019), it is evident that there are thousands of fraud victims. It does not appear that the public as a whole have an accurate understanding of the frequency with which fraud victimisation occurs and the inability of police and other agencies to respond to such a high volume crime. Instead, victims feel that their case is unique and should elicit a response commensurate with this uniqueness from police or other relevant agency. This is arguably not a realistic outcome.

Another factor driving a lack of satisfaction with ACORN may be the online reporting mechanism itself. Research indicates that an overwhelming need of fraud victims is to simply be heard and acknowledged for what has happened (Button et al., 2009; Cross et al., 2016). The completion of an online form, which provides an automatic e-mail response to a complaint, may not be satisfactory for a number of victims. While the evaluation indicated that 60 per cent were satisfied with the process of reporting through ACORN in terms of ease and accessibility (Morgan et al., 2016, p. 38), there are still a number of victims who were not satisfied with the platform. Cross et al. (2016) found that victims overwhelmingly have a need to be heard and acknowledged when they have experienced fraud. The requirement to lodge an online complain, devoid of human interaction, may not provide a suitable method of reporting for those who wish to report through police or other agencies in an offline environment.

It is also worth acknowledging at this point, that ACORN is exclusively an online reporting mechanism. For many fraud victims across Australia, if they attempted to report their victimisation to a local police station, they were unable to lodge a complaint in person and were instead referred to the online ACORN portal. Almost 20 per cent of fraud victims stated that they reported through ACORN because they were directed to by police, financial institutions or other body (Morgan et al., 2016, p. 38). The lack of alternative means of reporting offences (such as in person, over the telephone etc.) may be problematic for some groups of victims. For example, both ActionFraud and the Canadian Anti-Fraud Centre offer victims the ability to lodge a complaint over the phone in addition to their online website. The inability to choose an appropriate reporting platform for the individual victim may also contribute to lower levels of satisfaction with ACORN as a whole.

Having looked at the challenges associated with victim levels of satisfaction, the following section unpacks issues relating to the quality of data available in ACORN.

Quality of data

Any system is reliant upon the quality of the information entered in the first instance. If the quality of the information provided is lacking in detail, clarity or relevance, this imposes
challenges to those who are trying to interpret and respond to complaints. Overall, the ACORN evaluation found that the quality of data being entered into the system was not sufficient enough in a large number of cases to initiate an investigation (Morgan et al., 2016, p. 45). Several issues were identified as compromising the integrity and accuracy of the ACORN data:

- many individuals were reporting attempts rather than actual incidents where there had been a loss (of either money or personal information);
- victims were articulating the financial losses as those they were promised, rather than those that they may have actually incurred;
- victims were inflating their actual losses, in an attempt to get the attention of law enforcement; and
- victims were reporting the same incident multiple times in order to try and get a response from police (Morgan et al., 2016, pp. 45, 63).

Each of these demonstrates some of the inherent problems with an online reporting mechanism and the lack of human interaction or screening associated with the tool. Further, it also demonstrates the frustration that many victims felt, in trying to get the attention of police for an investigation. This is consistent with Cross (2018) and her documentation of the many (often unrealistic) expectations that victims have about the likelihood of a police response. While the online reporting tool overcomes a previous issue of victims being unable to lodge a complaint and being subject to a “merry-go-round” of agencies (Button et al., 2009; Cross et al., 2016), it does carry an expectation that victims will understand what is required and relevant from their case for police agencies.

As stated earlier, Scamwatch is also an online reporting mechanism for fraud. However, unlike ACORN, there is no ability for the ACCC to investigate individual incidents. Instead, the information submitted to Scamwatch is used primarily for awareness and education of the public. In this way, the Scamwatch website is more appropriate to report any fraudulent attempts received by individuals. The existence of this platform and the crossover between it and ACORN may help explain to an extent, why so many individuals reported attempted fraud through ACORN even though it is meant to be a police reporting mechanism (and therefore only taking actual complaints). It is also worth noting the definition of scams employed by ACORN, as “an attempt by a ‘scammer’ to lure and trick a victim into giving money or personal information” (Morgan et al., 2016, p. 29). This definition does not restrict actual incidents where an offender has successfully gained either money or personal information, but explicitly defines it as an “attempt”. This may have further contributed to the large number of reports which did not detail actual losses incurred on the part of the person reporting.

The above factors impede the timeliness in which police can respond to incidents reported through ACORN. This operates in two ways. The first is simply that the above factors mean that limited time and resources are used to canvass reports that are incomplete or inaccurate. Second, the above also signal delays in police being able to action any intelligence or useful leads that are evident in reports. The evaluation found that it was no uncommon for there to be three to five month delays in the processing of reports (Morgan et al., 2016, p. 45). This means that if a report did contain a piece of relevant information that police could follow up on, the usefulness of this information several weeks or months later rendered it of little use. Cyber offenders move quickly, and the identification of an active phone number, bank account or e-mail address may be squandered after the fact. In many cases, offenders have simply moved on.

Overall this section speaks to the importance of timely, accurate and relevant data that enable the police to have the highest chance possible to investigate an incident. The evaluation report is clear evidence that the current online reporting system itself, and the ways in which it operates across state and territory police, are exposed to a number of
challenges and problematic practices. While there are many legitimate reasons why police are unable to investigate the majority of fraud offences (Button, 2012; Cross and Blackshaw, 2015), there may also be some tangible leads that could initiate an investigation, but are lost through the consequences of the above data quality issues.

**Unintended consequences of ACORN**

The evaluation highlighted a number of unintended consequences of establishing ACORN as an online reporting tool. In particular, this was evident that the ACORN platform was used to report other offences types that were outside of ACORN’s scope. Of the 65,000 reports to ACORN across the evaluation period, 16 per cent of these were not within scope of the four offence categories. Instead, they were a combination of reports concerning offensive, illegal and prohibited content, child offences and other offences (Morgan et al., 2016, p. 30). Other offences includes the reporting of offences related to domestic violence, such as breaches of domestic violence orders perpetrated online (Morgan et al., 49), as well as sexual assaults (Morgan et al., 2016, p. 55).

The use of ACORN for the reporting of these offences creates a number of problems. First, the platform is not suitable to take complaints relating to matters that require an immediate response by law enforcement. The processes contained within ACORN do not enable the same level of response compared to complaints that are reported through other means (such as the telephone or in person). Victims who use this platform to report serious offences such as these may be at risk of further harm, given that the platform is not designed to respond to these circumstances, and the known delays in processing reports detailed in the above section.

Second, it creates problems for police and their required response to the reporting of these offence types. The evaluation notes that police agencies prioritised the identification of these offences and spent time triaging these offences as appropriate. This is arguably justified, given the nature of the offences, the potential need for immediate action and the possibly fatal consequences should the matter be ignored. However, in doing this, police within specialist units are taken away from responding to incidents of fraud. For example, the evaluation notes that for one police agency, despite having a mandate for fraud offences, officers have been focused on responding to incidents relating to domestic violence (Morgan et al., 2016, p. 55). Consequently, there has been a large backlog of up to 1,400 fraud reports left unprocessed (Morgan et al., 2016, p. 55).

The unexpected use of ACORN to report other categories of offence, including domestic violence, highlights the challenges experienced by many groups of victims in seeking an appropriate police response. It may point to a need to examine the other current reporting avenues available to victims of domestic violence and these other offence types. It also demonstrates a clear need to better communicate the boundaries of what specialist online reporting platforms can and cannot accept.

**Recent developments**

As of the 30 June 2019, ACORN was decommissioned and is no longer active. Instead, the ACORN website now directs individuals to the Cyber Issue Reporting System (www.cyber.gov.au). This is another online reporting mechanism that is operated by the Australian Cyber Security Centre under the Australian Signals Directorate. It has reporting options open to individuals, small to medium business, large organisations and government. Depending on the incident, it provides a variety of options on what to report, which appears to be broader than what was captured through ACORN. The Cyber.gov.au platform was initially launched into alpha release by the Australian Federal Government in August 2018 (Crozier, 2018). At the time, it was advocated as providing “a coordinated end-to-end advice reporting and response capability” (Crozier, 2018), which would replace existing services and government websites including ACORN (Chadwick, 2018; Crozier, 2018).
To date, there is little public information available about the new reporting platform including any similarities, differences or improvements compared to ACORN. There was no public announcement of the shift from ACORN to Cyber.gov.au. It is not known how the new portal is similar or different to ACORN, or how it processes complaints that are lodged. It is likely that without significant changes, the Cyber.gov.au platform will experience the same challenges and difficulties highlighted in the ACORN evaluation. However, at this present time, it is all speculation in the absence of any media release or publicly known facts about the operation of the new platform.

Conclusion
Overall, this paper has provided a commentary on the issue of reporting fraud in Australia, through the results of an evaluation of ACORN. While the establishment of ACORN as a centralised, online reporting mechanism for reporting cybercrime in Australia was argued to have met its stated objectives, the evaluation also highlighted a number of areas for concern. This paper has explored three of these with the intention of locating them within the wider discourses surrounding the challenges of policing fraud globally. Specifically, issues surrounding victim satisfaction, quality of data and unintended consequences were detailed.

It is important to recognise the broader context to the issues raised by the evaluation in the policing of fraud and appropriate responses to this category of crime. Notably, the blame cannot be solely attributed to police agencies for the results of this evaluation. Police are only one agency within the fraud justice network, and many of the issues identified are beyond the control of any police agency, either here in Australia or overseas. The issues highlighted by the evaluation and referred to in this paper point to a need for wider society to acknowledge and respond. The need for collaboration between government, police and private industry to overcome some of these challenges cannot be overstated.

There are some points which can be addressed in the immediate future. For example, the large disparity between the expectations of those reporting fraud compared to the reality of what police can deliver, needs immediate attention in terms of educating people about the limitations and constraints on what is realistic in their case (Cross, 2018b). The communication between police and those reporting can also be improved, specifically around likely outcomes to their incident. Victims overwhelmingly wish to be acknowledged on what has happened, and appreciate honesty in what can and cannot be done in their case (Cross, 2018b). This can assist with overcoming some of the unrealistic expectations of police and other agencies and could potentially alleviate the uncertainty of their case. At the moment, victims appear to have unrealistic expectations of what police and other agencies in the fraud justice network can achieve, and an inability to deliver this is driving a large amount of avoidable anger and frustration. With the risk of sounding clichéd, it may be beneficial to conduct a public awareness and education campaign about fraud and a realistic response from the fraud justice network. This must not circumvent the responsibility of agencies to respond to victims of fraud, but should be honest in terms of the challenges, timeframes, resources available and likely outcomes. This may then drive further change or advocacy in the area to improve these factors.

However, other issues are decidedly more complex in their nature and require a more sophisticated response. The evaluation brings sharply into focus the challenge of gaining satisfaction for victims of fraud and other cybercrime. It is arguably clear the current system has some inherent structural obstacles. Some of these may arise from the fact that ACORN was an exclusively online reporting mechanism. It would seem appropriate to expand this to offer a variety of options for victims to report their incident. This would include the option of online reporting (as currently exists) but should also include the ability
to report through telephone and in person (at police stations). Both of these methods could still feed into the one online portal (particularly the face-to-face reporting at a police station), but offer individuals a choice in how to best report their incident as appropriate for their situation. For many victims who have been defrauded through online means, the inability to report outside of the same virtual environment is cause for additional anxiety and concern (Cross et al., 2016). However, it is acknowledged that the addition of reporting mechanisms carries financial and human resource implications for consideration, though the inclusion of a human element may improve the quality of data input in the system and reduce the difficulties noted in the evaluation report.

The abolishment of ACORN and the introduction of the new Cyber.gov.au platform provides a potential opportunity to improve responses to fraud victims (and cyber victims more broadly). However, at this present time it is unknown as to how this new reporting portal differs in any attempt to overcome the concerns raised in the ACORN evaluation. There is still no ability to report outside of the online form, and a problematic Frequently Asked Question page which directs individuals to the Cyber.gov.au platform to report “cybercrime” but directs individuals to the Scamwatch website to report “scams”, knowing that the ACCC has no investigative power and that these incidents (including romance fraud and online shopping fraud) are captured by the Cyber.gov.au portal.

Moving forward, an important question emerges on what constitutes “justice” for victims of fraud, as well as what constitutes a “satisfactory response”? It is clear that the current system in unable to deliver an acceptable outcome for both victims and the fraud justice network alike. Even if there were a change in the logistics of how individuals can report to the platform, this alone does not overcome many of issues highlighted in the evaluation. In the absence of any likely substantial change, it is therefore important to ask these bigger questions. The Australian Federal Government is currently reviewing its Cyber Security Strategy (Commonwealth of Australia, 2019), which could feasibly canvass some of the issues highlighted in the ACORN evaluation. It is clearly an area for ongoing research and consideration.

References


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