Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 1836-2206 (Online) | ISBN 978 1 925304 29 9 (Online)

No. 592 March 2020

Abstract | Identity theft continues to grow in prevalence and complexity. Despite this growth, little is known about the identity theft response system and how it assists victims to recover. This study examines the response system by analysing 211 identity theft cases reported to IDCARE, a national identity and cybercrime victim support service.

The study applies a sociotechnical systems methodology to establish the social, task and information processes of the Australian identity theft response system. The study also examines identity theft victims' response activities and needs over a 12-month period.

The identity theft response system is almost entirely dependent on the victim to respond to and limit the harm caused by identity theft. Overall, the response system is disjointed and lacking in coordination.

The identity theft response system

Megan Wyre, David Lacey and Kathy Allan

Introduction

Identity credentials such as driver licences, passports and birth certificates have become essential for accessing various goods and services. These can include lines of credit, such as personal loans and mobile phone contracts, as well as government services.

Identity theft or the compromise and criminal misuse of these credentials has far-reaching effects on individuals, businesses and government organisations alike. The direct and indirect costs of identity crime in Australia in 2015–16 were estimated to be $2.65b (Jorna & Smith 2018). This estimate includes not only the direct losses incurred as a result of victimisation (eg the monetary amount obtained from misusing a victim's identity) but also indirect losses incurred in responding to such crimes, such as expenses accrued while acquiring new documentation and putting in place prevention measures (Smith & Jorna 2018a).

CRIMINOLOGY RESEARCH GRANT

Identity theft is among the most prevalent crime types affecting individuals today (Smith & Jorna 2018b). In fact, identity theft now impacts a higher proportion of the Australian population each year than any other household-theft related crime (Attorney-General's Department 2016; Smith & Jorna 2018b). Surveys conducted by the Australian Institute of Criminology indicated that more than 20 percent of respondents had experienced misuse of their identity or personal information in their lifetime (Smith & Jorna 2018b).

There is a general consensus that identity theft is a serious problem, though its nature and extent has been difficult to establish. It is difficult to estimate the number of identity theft offences and their impact on the community. Smith and Jorna (2018b) provide one of the most comprehensive studies on the extent, nature and impact of identity theft and related crimes. In their survey of 9,956 Australian respondents, 22 percent reported misuse of their credentials during their lifetime (Smith & Jorna 2018b). Occasions of misuse ranged from a single offence to 255 separate events (Smith & Jorna 2018b). Over half of the respondents who had experienced misuse incurred financial losses that ranged from $1 to $500,000, with an average loss of $3,696, excluding recovered funds, or costs associated with repairing the damage (Smith & Jorna 2018b). Notwithstanding the methodological limitations of sampling from online surveys, such as sampling control issues, self-selection bias and accessibility issues (Wright 2005), Smith and Jorna's (2018b) research highlights that identity theft and related crimes permeate the Australian community, are highly under-reported, and can have enduring impacts including psychological harm.

Defining identity theft

Golladay and Holtfreter (2017: 741–42) broadly define identity theft as the use of another person's identity information without their consent in an unlawful manner. However, this definition does not capture the intricacies of this crime type. Identity theft comes in a variety of forms. There remains a lack of a consistent definition of identity crime—an issue highlighted throughout the literature (Koops & Leenes 2006). Wall (2013: 437) uses identity crime as an umbrella term to define a diverse range of crimes that use the theft of identity documents to pursue identity fraud, thus encapsulating both theft and fraud (Jamieson et al. 2008; Kraemer-Mbula, Tang & Rush 2013; Saunders & Zucker 1999). Describing identity theft as having two distinct stages—the compromise of identity information, including identity credentials, and the misuse of that information for criminal gain—allows a broad variety of identity theft-related crimes to be captured within the scope of this study. The findings of this study would therefore be applicable to a wide range of instances where an individual's personal information is misused for criminal gain beyond traditional understandings of identity theft.

Prior research on responses to identity theft victims

Little research to date has focused on the nature, performance and impacts of the identity theft response system when identity crimes occur. The use of identity credentials is typically seen as an interaction between the individual and the organisation that allows for access to specific products or services. These interactions are often heavily influenced by the potential risk of identity theft (Lacey & Cuganesan 2004). The development of controls and processes across the identity theft response system have not had much regard for the needs, wants or experiences of victims (Marsh, Cochrane & Melville 2004). Even less is known about the needs and experiences of individuals after they have detected that their identity information has been compromised or misused (Button, Lewis & Tapley 2014). As a consequence, it has been argued that research has further overlooked how social structures and organisational networks involved in responding to identity theft victimisation can affect responses and even cause further harm to the victim (Song, Lynch & Cochran 2016).

The precise structure of the response system, its key actors and their interactions have not been adequately explored. Research has uncovered the emotional repercussions of identity crime, and that these are largely misunderstood by the criminal justice system and the community at large. These victims are more often met with dismissal than treated as genuine victims worthy of support (Marsh, Cochrane & Melville 2004). Identity theft victims have been branded as 'greedy' and 'gullible' and are met with a lack of empathy and understanding, including negative and derogatory responses when reporting their victimisation to law enforcement (Button, Tapley & Lewis 2013; Cross, Smith & Richards 2014). Evidently there is a dissonance between identity theft victims and the criminal justice system that sets these individuals apart from victims of other types of crime.

A unique aspect of identity theft victims is that they may no longer be able to access the goods and services for which the credentials were originally designed, due to damage to the credibility or reliability of those credentials. Criminals may tarnish a victim's credit history, or cause the victim to have a criminal record, which has ongoing effects for that individual and their ability to gain employment, obtain various benefits, travel, and otherwise participate in society (Lacey & Cuganesan 2004; Smith, Brown & Harris-Hogan 2015).

Though more violent or 'conventional' crimes are often seen as more harmful to the victim, victims of financial crimes such as identity theft often share many of the same psychological outcomes (Marsh, Cochrane & Melville 2004). Significant health problems, both mental and physical, may result from this victimisation. Studies have highlighted that stress, anxiety and depression are often consequences of identity theft victimisation, while many experience levels of guilt, shame and anger on par with victims of violent crime (Button, Lewis & Tapley 2014; Cross, Smith & Richards 2014; Ganzini, McFarland & Bloom 1990; Golladay & Holtfreter 2017; Spalek 1999). Individuals who have had their identity credentials compromised or misused may also suffer relationship problems, damage to their reputations and, in extreme cases, suicidal tendencies (Button, Lewis & Tapley 2014; Cross, Smith & Richards 2014).

Despite the limited research, we can glimpse some consequences of the response system. Research findings reveal a response system where organisational needs have primacy (Lacey & Cuganesan 2004), where individuals confront enduring risks of further identity crime (Smith, Brown & Harris-Hogan 2015), where access to established victim-support mechanisms is constrained (Marsh, Cochrane & Melville 2004), and where individual victims shoulder very high costs of recovery (Button, Lewis & Tapley 2014; Smith, Brown & Harris-Hogan 2015). This is set within a broader social context in which the individual is to blame (Cross, Richards & Smith 2016).

Aim

Despite the growth and impact of identity crime, little is known about the response journey of victims, or the organisations that perform response functions and their overall performance. This research aims to explore the characteristics of Australia's identity theft response system from the perspective of an individual victim. Previous research has struggled to describe the precise nature of the identity theft response system. How actors across the identity credential system respond to identity theft and how effective they are in minimising the impacts on victims remains a key gap in understanding (Lacey & Salmon 2015). The crime is known to have enduring effects, and victims can expect to experience further misuse of their identity information. It is also known that misuse of identity credentials can take many forms, thus making it difficult to prevent. However, little is known about how victims of identity theft actually respond to the crime and, by extension, how organisations such as financial institutions, law enforcement agencies as well as other response actors interact and rely upon each other to address the needs of victims. The primary aim of this study is to address this lack of knowledge by capturing empirical details regarding the identity theft response system, its social, task, and information requirements, and how these address the needs of victims.

Method

Data sources

The study used data from a sample of 211 individuals who had been victims of identity theft and had been previously helped by IDCARE. IDCARE is Australia's national identity and cybercrime community support service. It offers victims of identity theft specialised counselling services through a call centre, including detailed information on how to respond to identity crime and emotional support should victims desire it. Under an approved ethics research program (USC E/16/052), IDCARE provided anonymised case records and notes from these previous engagements, as well as content from interviews performed for the purposes of this study over the phone by trained counsellors with individual victims over a 12-month period following the initial detection of the identity theft. These interviews were designed to uncover the needs of victims, the organisations they engaged with, the tasks they had to perform with those organisations, and how effective these engagements had been in addressing their needs. Approximately 600 of IDCARE's clients were approached to participate in this study, of which two-thirds declined, leaving a final sample of 211.

Complementing these data were 120 organisational response plans obtained from IDCARE. These plans were a rich source of data on the needs of organisations across the identity theft response system and the experiences of victims traversing the same system.

Analysis

The study used Event Analysis of Systemic Teamwork (EAST; Stanton, Baber & Harris 2008) to construct and analyse the identity theft response system. EAST was originally developed to analyse command, control, communication, computers and intelligence activities (Stanton, Baber & Harris 2008). Though novel to the context of an identity theft response system, the EAST methodology has been applied to such diverse areas as air traffic control (Walker et al. 2010), military accidents (Stanton, Rafferty & Blane 2012), road safety (Salmon et al. 2014), submarine control systems (Stanton, Roberts & Fay 2017), darknet carding markets (Lacey & Salmon 2015), rescue systems (Plant & Stanton 2016), and sport ergonomics (Hulme et al. 2019).

An EAST analysis typically describes three networks: social, task and information. These networks are summarised in Table 1.

Table 1: EAST networks and their functions

Network	Function
Social	Represents the actors (human, technical, organisational), and the communications between them.
Task	Represents the activities performed by the actors in the system, and the relationships between them.
Information	Represents the information communicated within a system, and the relationships between differing information types.

Source: Adapted from Stanton and Harvey 2017: 222

Using content analysis methods, the interview responses and organisational response plans were coded into keyword groups pertaining to social, task and information nodes (eg financial institution, closing a bank account, and identity credential, respectively). Once the nodes were identified, relationships were established between them in order to construct the network and establish relationships between the identified nodes.

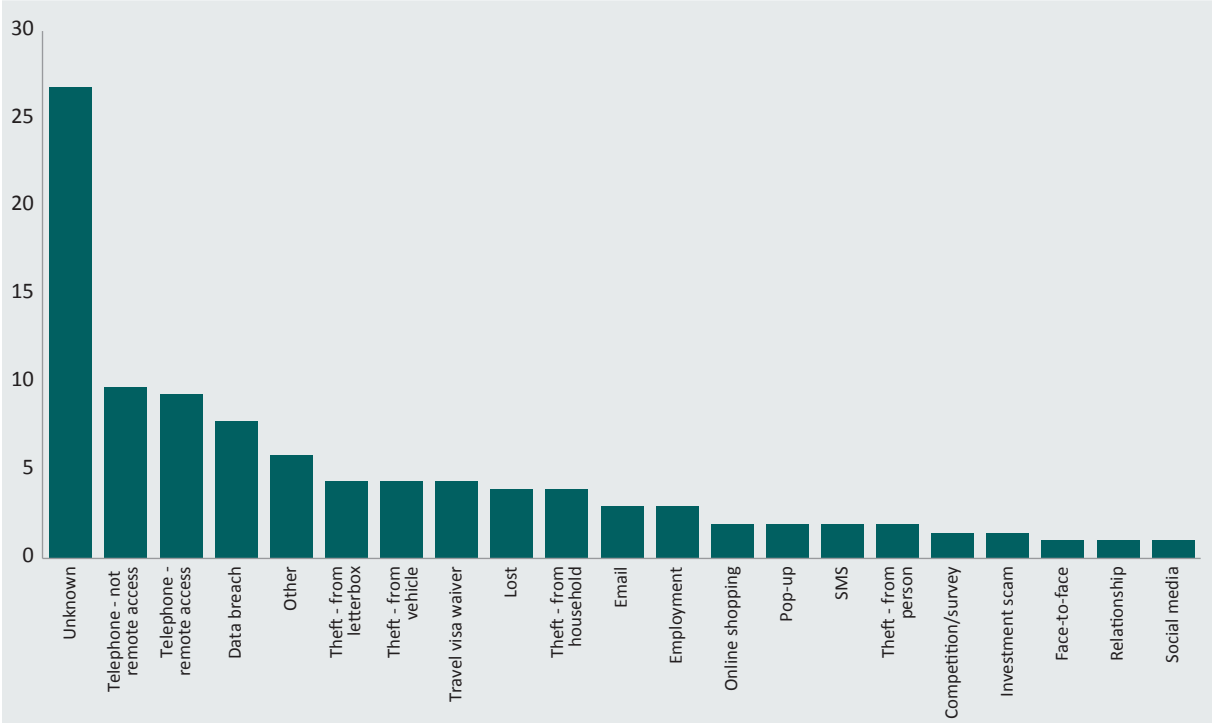
Social network analysis metrics were used to examine the structures and relationships between nodes in the EAST networks (Stanton & Harvey 2017). These metrics were used to describe individual nodes, including their reception, emission and sociometric status, in order to identify which nodes were central to the performance of the identity theft response system. Sociometric status in particular was selected to define key nodes because it indicates whether an individual node's communications are more prominent than those of others within the network. Doing so revealed the key node influencers in the identity theft response system—that is, those nodes that influence the performance of the whole system in addressing the needs of victims (Stanton & Harvey 2017).

Results and discussion

The 211 respondents were compared to the total pool of IDCARE clients for 2017 to determine whether the sample was representative of IDCARE's general clientele. A standard chi-square test found the sample was representative of the general population of IDCARE clients. Of the 211 respondents, 53 percent identified as female, and 40 percent were between 25 and 45 years old. The majority of the respondents resided in New South Wales, Victoria or Queensland. These key statistics are indicative of IDCARE's general client population, as well as being reflective of the general population of Australia. Thus, the results from this study can be considered generalisable to the broader client population of IDCARE, as the only specialist support service for victims of identity theft operating in Australia.

On average, the misuse of credentials occurred 36 days after their initial compromise. Respondents first discovered the misuse of their credentials an average of 62 days after their initial compromise. This demonstrates that there is a lag between the initial identity theft and the point at which a victim begins to respond. Approximately 68 percent of survey respondents were the first to detect their identity theft, as opposed to being notified by an outside entity. This suggests that, for the majority of identity theft victims, self-detection is central to initial engagement or response. The gap between identity compromise and initial detection (by the individual or others) is likely to be the optimal period in which further identity misuse occurs.

Figure 1: Methods used to compromise respondents' identity information (%)



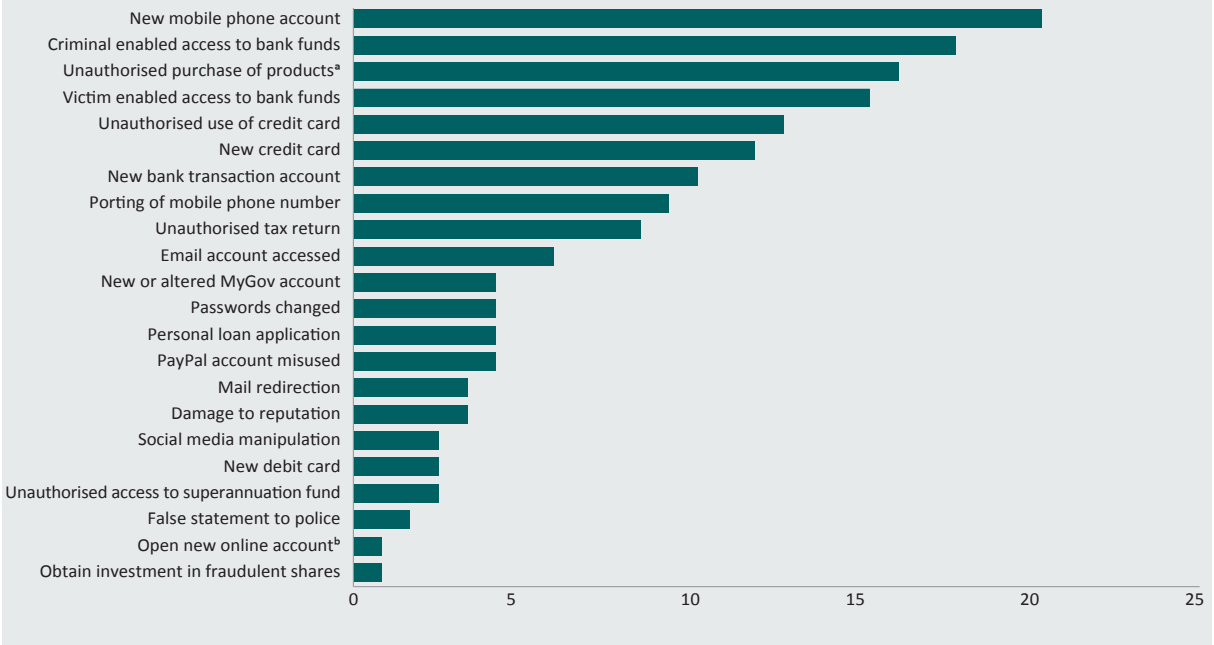
A diverse range of methods were used to compromise identity information. Telephone scams in general represent the most common identifiable compromise experience, but a significant portion of individuals (27%) did not know how their identity information was compromised (Figure 1).

Of those who knew the types of information compromised (63% of respondents), an average of nearly four credentials were compromised during the identity theft event. Of the government-issued credentials, those most commonly compromised were driver licences (32% of cases), passports (18% of cases), tax file numbers (17% of cases), Medicare cards (13% of cases) and birth certificates (6% of cases).

Of the 211 cases studied, 29 percent experienced misuse in the three months following the known initial compromise of identity information. On average these individuals experienced 1.6 misuse events in addition to their initial compromise event (ie 2.6 alleged identity crime events). This equated to 147 known individual criminal acts of compromising and misusing the identity information of individuals. The most common form of misuse detected during this period was a new mobile phone account being established in the victim's name (approximately 20% of misuse). The second most commonly reported form of misuse was unauthorised access to bank funds (see Figure 2).

Data were also collected on the costs victims accrued as a result of their identity theft event. A total of $256,186 was lost from identity misuse, with an average loss of $6,568.87. Four percent of the survey respondents indicated that they were able to recover lost funds, and the total amount recovered was approximately $95,500. The exact methods of recovery were unclear, though some respondents indicated that their banks reimbursed them for initial costs. These numbers do not account for further costs that may be accrued during the recovery process, including the costs of preventing further compromise or misuse.

Figure 2: Forms of identity misuse experienced (%)



a: Includes rentals/mobile phones

b: For example, social media/email/etc

Approximately 18 percent of individuals indicated that they had taken steps to change their behaviour during the three months following the identity theft event in an attempt to prevent further identity theft events. Around 71 percent of these individuals ended their relationship with the organisation they attributed the compromise or misuse event to by closing their account or cancelling their identity credential (eg a passport). Around 16 percent indicated that they had stopped using the computers or devices involved in the compromise or misuse event. Interestingly, these cases did not differ greatly in their compromise or misuse experiences from those of others who had not stopped using their computers or devices.

Of the 29 percent who experienced misuse in the three months following the compromise of their identity information, six percent experienced further misuse of their credentials over the ensuing nine-month period. Interestingly, among those who did not experience any known misuse during the three months following the compromise event (71% of the sample), 11 percent experienced misuse over the following nine-month period. In total this meant that, across the entire sample, nine percent of identity misuse events occurred between month three and month 12 following the initial compromise event, where this was known (ie where the individual knew when their identity information was initially compromised).

Around one in five respondents (19%) reported psychological impacts. These most commonly related to feelings of anxiousness about what could happen and a sense of frustration and dismay at the lack of information sharing among response organisations. Both of these impact types reflect the knowledge asymmetry between the individual who experiences identity theft and the organisations they engage with to understand more about the criminal event and how they should respond.

In fact, 13 percent of individuals indicated that, 12 months after the initial compromise, they had not been able to put the incident behind them and move on. This cohort felt that the response system was not adequate and that the initial compromise had not been 'resolved'. Exploration of the reasons behind these feelings revealed that 35 percent of these respondents felt that they were a vulnerable person and that it could happen again. Further, 32 percent acknowledged that, despite their participation in the response system, there was no guarantee that misuse would not happen again. Twenty-seven percent revealed that they still felt a sense of helplessness that their details were 'out there' and that they had not received the support they needed.

The majority of individuals (87% of the sample) expressed that they had no residual needs or concerns, primarily because there had been 'no evidence of any ongoing misuse' (around 96% of these respondents) and because they knew they had 'done everything they could to protect themselves' (19% of these respondents). Interestingly, these views were not associated with any specific act or response.

Social network

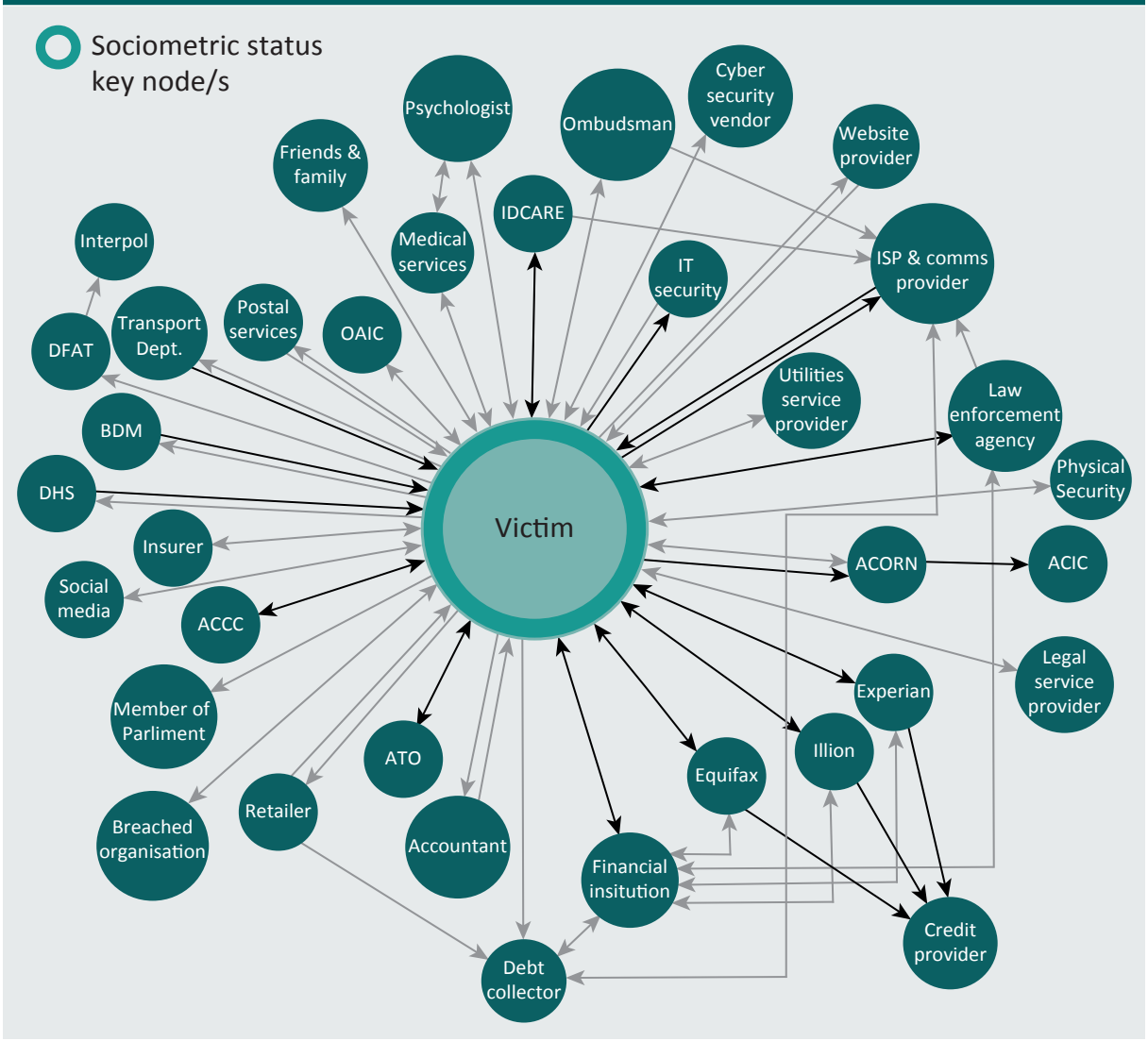
The social network depicts the victims' aggregate interactions with the identity theft response system. An interaction in this case is defined as any instance where participants indicated during their responses to the survey that information was exchanged between social actors. The analysis identified 37 social actors within the identity theft response system, including the victim. These are represented in Figure 3. These nodes were further tested by subject matter experts the researchers recruited from IDCARE and its partners as a reasonable representation of the main actors within this system.

The 'victim' node was identified as the key actor in the identity theft response system, based on its sociometric status. The victim node communicates with 33 of the 37 nodes within the identity theft response system. As such, this node also scored the highest on emission and reception, as the victim is receiving information from and providing information to nearly all of the other social actors. The victim also acts as the conduit for the majority of the identity response system, or the link between organisations. For example, the victim reports to police and then sends that report to various organisations as proof of the identity theft. Information passes through the victim to reach other areas of the network.

These results strongly indicate that the victim is vital in the social structure of the identity theft response system. It is evident that the victim provided the largest amount of information to other actors. There appears to be little to no communication between other actors in the network except via the victim. The second most influential node in the system was the 'financial institutions' node, which had a much lower sociometric status and largely only interacted with other financially orientated organisations, such as the credit reporting agencies. Government organisations were very dispersed and did not appear to interact with each other. Law enforcement had some connectivity but ultimately remained disconnected from the majority of the network.

The social network's critical dependence on the individual victim reinforces the view of many participants that organisations were not interested in their needs or the risks to other parties but focused only on the 'specific risks to the organisation'. The subject matter experts noted that, while the individual appears to be central to Australia's identity theft response system, the risk of any future misuse is likely to be a risk borne by the parties relying on the identity (eg financial institutions, mobile phone providers and government service providers). Put simply, individual victims are performing a considerable amount of work, ultimately to protect government and industry bodies that may rely upon their compromised credentials when providing products and services.

Figure 3: Social nodes in the identity theft response system



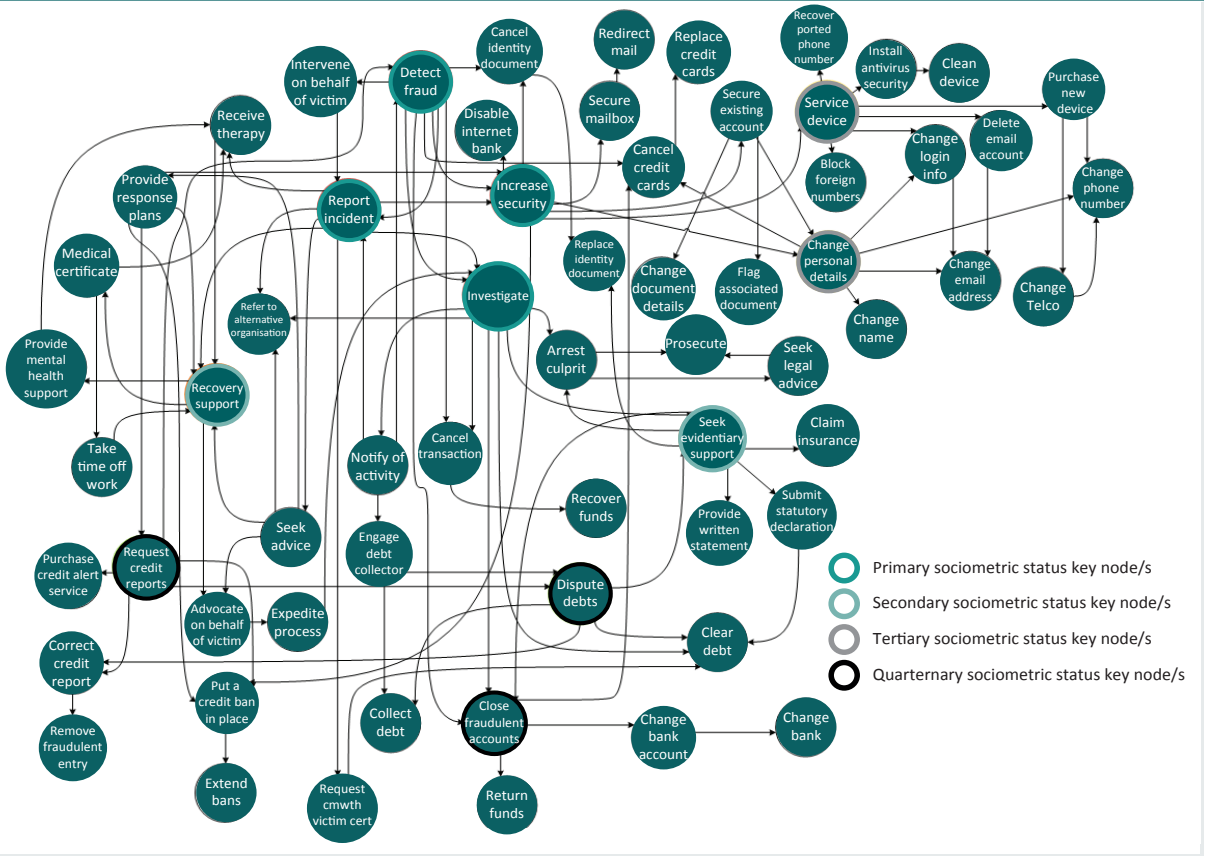
ACCC=Australian Competition and Consumer Commission. ACIC=Australian Criminal Intelligence Commission. ACORN=Australian Cybercrime Online Reporting Network. ATO=Australian Taxation Office. ISP=internet service provider. OAIC=Office of the Australian Information Commissioner. DFAT= Department of Foreign Affairs and Trade. BDM= Births, Deaths and Marriages. DHS= Department of Human Services.

Task network

The task network was constructed by identifying the different tasks that survey respondents indicated they had pursued when contacting each social node. These tasks were then linked using input from subject matter experts and background understanding of the various processes associated with each major task. As shown in Figure 4, 63 task nodes were identified, including 11 nodes with high sociometric status. The four nodes with the highest sociometric status—'detect fraud', 'increase security', 'report incident' and 'investigate'—were deemed to be the most vital to the network.

It is important to note that the scope of the network was kept as simple as possible, so it would not be overburdened by the minutiae of the smaller tasks involved in each individual task. As such, this network does not capture the full complexity of completing each of these tasks. For example, the paperwork and identification processing requirements needed to apply for a credit report were not captured in great detail. Therefore, Figure 4 is a tip-of-the-iceberg representation of the task network.

Figure 4: Task nodes in the identity theft response system



It is clear that the task network has a higher number of nodes than the social network but, unlike the social network, it does not have one centralised node. Instead, there are several key nodes that are interrelated and correspond to the victim's needs. The interconnected nature of the nodes indicates the reliance that each task node has on the rest of the network. All these tasks rely on each other in some respect in order to be accomplished, with the social network revealing that the responsibility for each remains with the individual victim.

The task network highlights the importance of the 'detect fraud', 'investigate', 'increase security' and 'report incident' tasks from the victim's perspective and shows that these four tasks are the most central and integral to the function of the identity theft response system. The network key sociometric status of the 'seek evidentiary support' node also highlights the importance placed on victim-driven evidence seeking.

It is interesting to note that more proactive protection measures such as 'change document details' and 'put a credit ban in place' have less focus in the task network. For example, implementing a credit ban with the three major credit reporting agencies effectively prevents a criminal from accessing a line of credit in the victim's name, making a purchase using a payment plan and other common types of misuse. The relatively low sociometric status of this node may be attributed to a lack of knowledge about credit reporting agencies among the general public. Most victims who were surveyed indicated that they were unclear about the procedures around credit reports. Since the main three credit reporting agencies are also for-profit businesses, many victims were under the impression that they had to pay for the services that credit reporting agencies provide and were unaware that they were entitled to a credit ban under Australian regulations (the *Privacy (Credit Reporting) Code 2014 (Version 2)*). The lesser focus given to permanently changing identity credential information probably reflects the fact that presently only three Australian states allow for this to occur, and only after various complex tasks have been completed.

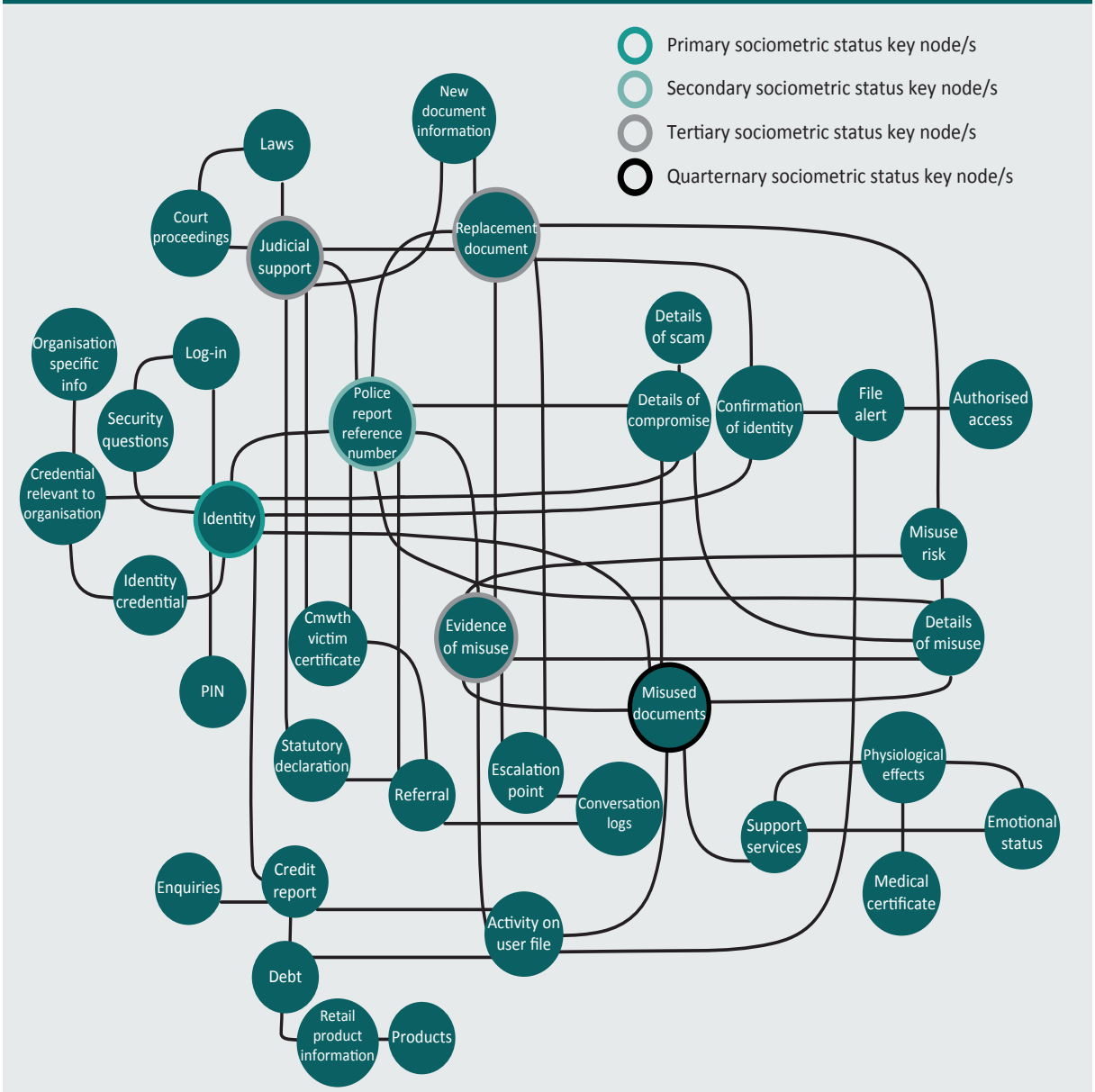
Similarly, respondents paid little attention to requesting a Commonwealth Victims' Certificate. Victims can apply for these certificates and present them to government agencies, financial institutions or credit agencies as evidence that they have been a victim of identity theft (Jorna & Smith 2018). However, they are generally underused (Jorna & Smith 2018), and the task network further demonstrates that they are not a focal task for victims of identity theft.

Information network

The information network illustrates the types of information communicated in the identity theft response system and the connections between them (Figure 5). EAST identified 37 information nodes and their corresponding connections based on organisational response procedures and response plans collected previously by IDCARE from the organisations identified as actors in the social network. These surveys were further supported by engagement with subject matter experts, who provided further details relating to the precise information requirements of each task.

A total of 37 information nodes were identified, including six key nodes. These include 'identity', 'misused documents', 'evidence of misuse', 'replacement documents', 'police report reference number' and 'judicial support'. Of these, 'identity' had the strongest sociometric status, reinforcing the need to use the compromised or misused identity information in order to complete the required tasks. This further highlights the complexity of the identity theft response system. Often victims were asked to prove their identity by using the same credentials that had been stolen—despite the obvious risk associated with using a compromised credential.

Figure 5: Information nodes in the identity theft response system



Based on this network, the majority of information being transmitted is identity credential information, shared for the purpose of demonstrating that misuse has happened. This underscores the experience of many identity theft victims: they are often expected to restore their identity by repeatedly re-exposing their identity information to various organisations across the system. Many respondents felt revictimised by the process of continually reproducing the very credential information that had been stolen. For example, it was common for law enforcement to ask individuals whose identity information was compromised or misused online to submit the very same information via online forms, such as on the Australian Cybercrime Online Reporting Network. Dissatisfaction with this process was high across this cohort of the sample (averaging an overall satisfaction level of 3.42 out of 10).

This may have had a significant influence on the reporting decisions made by victims of identity theft. A survey by Goldsmid, Gannoni and Smith (2018) found that 57 percent of respondents reported their experience only to a family member or friend, indicating that no official agencies were notified of the crime. When victims of identity theft choose to report their crime, particularly to law enforcement, their experiences are often compared to those of sexual crime victims (Reyns & Randa 2017). Victims of sexual assault often decide not to report their victimisation due to a concern regarding a lack of proof that the crime occurred or fear that they will be blamed. Similarly, identity theft victims often do not report the crime to law enforcement due to fears they will not be believed, that they will be blamed, or that it would be impossible to apprehend the offender based on the information they have (Cross, Richards & Smith 2016; Reyns & Randa 2017). Not only does this result in poor reporting rates, thus limiting responses to the crime as a whole, but it also forces identity theft victims into repeated rounds of self-identification and processes designed to help them only when there is irrefutable evidence their identity has been misused. This not only enables criminals to continue perpetrating identity crimes, but also causes continuing harm to the victim, even when they are attempting to resolve the issue.

Conclusion

This study used EAST to describe Australia's identity theft response system. This novel approach identified the key actors, tasks and information flows involved in addressing the needs of identity theft victims. Repeated engagement with individual victims over a 12-month period was critical in extracting relevant data on the nature and performance of the system, particularly from the perspective of victims. Based on participants' responses, victims appeared to reach a point while navigating the response system where they felt the issue had been resolved. This was largely because they had 'done everything possible' to prevent future misuse. But a smaller cohort (13% of the sample) held residual concerns following several months of responding and made an equally valid observation: that no-one can guarantee that future misuse will not occur.

The identity theft response system is a definable system, but one that is complex and highly dependent on the actions of individual victims. Individuals pursue response and resilience measures at their own cost in the belief that they are protecting themselves, when in fact those measures benefit businesses and government agencies more than victims. In other words, the victim is forced to perform arduous bureaucratic processes repeatedly in order to alert businesses and government agencies that their products and services have caused harm, even though the financial losses from stolen identities are usually incurred by the businesses and government agencies via their insurance. Yet the majority of the harm is still felt by the victim, particularly when they interact with the response system, due to its inefficient, disconnected and redundant structure. Therefore, system actors other than the victim must develop stronger responses and take responsibility for protection measures in the future.

This idea is further supported by the performance of business and government actors within the response system. Despite relying on identity information and identity credential providers, their responses are almost exclusively oriented towards protecting their own products and services, not other actors across the system, such as other agencies and individual victims. For example, transport departments, which are responsible for issuing driver licences—heavily misused documents—do not communicate at all with financial institutions, where those licences are frequently misused. In the absence of an overarching response mechanism, the individual victim was forced to connect these disparate actors. Based on these observations, it is evident that there is no overarching, coordinated response to identity theft in Australia. The responses available to victims largely appear to have been designed without understanding of the wider system and how processes affect one another. It is clear that the lack of defined processes has forced the victim to take responsibility for responding to identity theft, and this reliance on individual victims is neither fair nor sustainable.

The identity theft response system demonstrated disjointed and at times conflicting requirements. Industry and government actors required individuals to perform functions that were contrary to those required by other actors. Victims highlighted these experiences and the inefficient circularity of response efforts, which caused emotional distress and frustration and discouraged them from taking appropriate action. For example, in multiple cases law enforcement agencies refused to provide victims with a police report as the incident did not occur within their jurisdiction. Not having a police report number ultimately prevented the victim from completing tasks such as cancelling fraudulent mobile phone account debts.

In addition to this, the risk associated with the misuse of an individual's identity largely endures. At present, most individuals who confront identity theft have no means of ensuring that they can totally mitigate future risks of identity misuse across the system. Response measures, albeit largely dependent on the actions of individual victims, appear to reduce the risk only temporarily. While the time frame for criminal misuse of a stolen identity has not been established, victims need to be able to put more permanent changes in place to better protect their compromised identity.

Many of the victims surveyed in this study concluded that, because they had not noticed further identity misuse, the threat had passed. This was their only indication of recovery, as there was no definitive way to determine whether or not they were still at risk. As such, this view was often found to be held in conjunction with a sense of resignation—they had done what they could, and accepted that it was possible they could suffer further harm in the future, even if they had not noticed further identity misuse at the time of interview. For some, this could lead to ongoing anxiety and stress, waiting for the 'other shoe to drop'.

This research offers significant opportunities to identify better processes for helping victims of identity theft and related crimes. It also suggests potential avenues for a similar style of research into responses to other victims of crime who face similar struggles, such as victims of sexual assault. Overall, the research demonstrates that the response measures put in place to help victims do not consider their needs, and that the measures designed to prevent identity theft in Australia are at this stage not sufficient to prevent long-term harm to the individual.

References

URLs correct as at November 2019

Attorney-General's Department (AGD) 2016. *Identity crime and misuse in Australia 2016*. Canberra: AGD

Button M, Lewis C & 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 & Lewis C 2013. The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice* 13(1): 37–61

Cross C, Richards K & Smith RG 2016. *Improving responses to online fraud victims: An examination of reporting and support.* Report to the Criminology Research Advisory Council. Canberra: Australian Institute of Criminology. https://crg.aic.gov.au/reports/201617.html

Cross C, Smith RG & Richards K 2014. Challenges of responding to online fraud victimisation in Australia. *Trends & issues in crime and criminal justice* no. 474. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi474

Ganzini L, McFarland B & Bloom J 1990. Victims of fraud: Comparing victims of white collar and violent crime. *Bulletin of the American Academy of Psychiatry and the Law* 18(1): 55–64

Goldsmid S, Gannoni A & Smith RG 2018. *Identity crime and misuse in Australia: Results of the 2017 online survey.* Statistical Report no. 11. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr11

Golladay K & Holtfreter K 2017. The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders* 12(5): 741–60

Hulme A, Thompson J, Plant KL, Read GJ, Mclean S, Clacy A & Salmon PM 2019. Applying systems ergonomics methods in sport: A systematic review. *Applied Ergonomics* 80: 214–25

Jamieson R, Land L, Sarre R, Steel A, Stephens G & Winchester D 2008. *Defining identity crimes*. Australasian Conference on Information Systems 2008 Proceedings, 107, 442–51. https://aisel.aisnet.org/acis2008/107/

Jorna P & Smith RG 2018. *Identity crime and misuse in Australia 2017*. Statistical Report no. 10. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr10

Koops BJ & Leenes R 2006. Identity theft, identity fraud and/or identity-related crime. *Datenschutz und Datensicherheit* 30(9): 553–56

Kraemer-Mbula E, Tang P & Rush H 2013. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change* 80(3): 541–55

Lacey D & Cuganesan S 2004. The role of organizations in identity theft response: The organization–individual victim dynamic. *Journal of Consumer Affairs* 38(2) 244–61

Lacey D & Salmon P 2015. It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. *Engineering Psychology and Cognitive Ergonomics* 117–28

Marsh I, Cochrane J & Melville G 2004. *Criminal justice: An introduction to philosophies, theories and practice.* London: Routledge

Plant KL & Stanton NA 2016. Distributed cognition in Search and Rescue: loosely coupled tasks and tightly coupled roles. *Ergonomics* 59(10): 1353–76

Reyns BW & Randa R 2017. Victim reporting behaviours following identity theft victimization: Results from the National Crime Victimization Survey. *Crime & Delinquency* 63(7): 814–38

Salmon P, Lenne MG, Walker GH, Stanton NA & Filtness A 2014. Using the Event Analysis of Systemic Teamwork (EAST) to explore conflicts between different road user groups when making right hand turns at urban intersections. *Ergonomics* 57(11): 1628–42

Saunders KM & Zucker B 1999. Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology* 13(2): 183–92

Smith RG, Brown R, Harris-Hogan S 2015. *Identity crime and misuse in Australia: Results of the 2014 online survey.* Research and public policy series no. 130. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp130

Smith RG & Jorna P 2018a. *Counting the costs of identity crime and misuse in Australia, 2015–16.* Statistical Bulletin no. 15. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sb/sb15

Smith RG & Jorna P 2018b. *Identity crime and misuse in Australia: Results of the 2016 online survey.* Statistical Report no. 6. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr6

Song H, Lynch MJ & Cochran JK 2016. A macro-social exploratory analysis of the rate of interstate cyber-victimization. *American Journal of Criminal Justice* 41(3): 583–601

Spalek B 1999. Exploring the impact of financial crime: A study looking into the effects of the Maxwell scandal upon the Maxwell pensioners. *International Review of Victimology* 6(3): 213–30

Stanton N, Baber C & Harris D 2008. *Modelling command and control: Event analysis of systemic teamwork.* Aldershot: CRC Press

Stanton N & Harvey C 2017. Beyond human error taxonomies in assessment of risk in sociotechnical systems: A new paradigm with the EAST 'broken-links' approach. *Ergonomics* 60(2): 221–33

Stanton N, Rafferty L & Blane A 2012. Human factors analysis of accidents in system of systems. *Journal of Battlefield Technology* 15(2): 23–30

Stanton N, Roberts A & Fay D 2017. Up periscope: understanding submarine command and control teamwork during a simulated return to periscope depth. *Cognition, Technology & Work 19*(2–3): 399–417

Stanton N, Salmon P, Rafferty L, Walker G, Baber C & Jenkins D 2013. *Human factors methods: A practical guide for engineering and design*, 2nd ed. Aldershot: Ashgate

Walker G, Stanton N, Baber C, Wells L, Gibson H, Salmon P & Jenkins D 2010. From ethnography to the EAST method: A tractable approach for representing distributed cognition in Air Traffic Control. *Ergonomics* 53(2), 184–97

Wall DS 2013. Policing identity crimes. *Policing and Society* 23(4): 437–60

Wright K 2005. Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication* 10(3): JCMC1034

Megan Wyre is a Master's student at the University of the Sunshine Coast.

David Lacey is Professor of Cybersecurity at the University of the Sunshine Coast.

Kathy Allan is a PhD student at the Australian National University.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 1836-2206 (Online)

ISBN 978 1 925304 29 9 (Online)

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

aic.gov.au