Criminology Research Grants

Australia's Identity Theft Response System: Addressing the Needs of Victims

Megan Wyre
David Lacey
Kathy Allan

Report to the Criminology Research Advisory Council
Grant: CRG 10/15–16

March 2020

ISBN: 978 1 925304 37 4 (Online)

This is a project supported by a grant from the Criminology Research Grants.

Acknowledgements

The research would not have been possible without the willingness of the individuals who shared their stories in responding to the compromise and misuse of their identity information. Their resilience and commitment to share their stories enabled the authors to capture a unique lens on how Australia is currently responding to these crimes.

The authors gratefully acknowledge the support and patience of the Australian Institute of Criminology and IDCARE. The counselling staff of IDCARE performed above and beyond in dedicating an enormous amount of in-kind support over many months in working with these individuals. We acknowledge that this was at great cost to the charity, but we hope that the findings have directly contributed to advancing its own understanding of the needs of individuals and how its community services can continue to make a difference.

Finally, we also express our thanks and gratitude to the many experts across Government and industry who spared their time to test our assumptions, thinking and ideas on how to optimise the response system. We would like to particularly acknowledge the leadership shown by the Department of Home Affairs, the Australian Cyber Security Centre, and the member organisations of the Commonwealth Trusted Identity Committee. Earlier iterations and findings of this report have directly informed broader work of Government in reviewing Australia's identity system and its protection initiated by these stakeholders. We thank you for the opportunity to contribute.

Table of Contents

Table of Figures

List of Tables

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition & Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACSC	Australian Cyber Security Centre
ACORN	Australian Cybercrime Online Reporting Network
AGD	Commonwealth Attorney-General's Department
AIC	Australian Institute of Criminology
ASIC	Australian Securities and Investments Commission
CDM	Critical Decision Method
EAST	Event Analysis of the Systemic Teamwork
HTA	Hierarchical Task Analysis
SMEs	Subject Matter Experts

Executive Summary

Background

Identity credentials, such as driver licences, passports, and birth certificates, have become essential for individuals across the community to access various goods and services. This can include lines of credit, such as personal loans and mobile phone contracts, as well as access to government services.

Identity theft carried out by criminals through the compromise and misuse of this credential information has wide reaching effects on individuals, businesses, and government organisations alike. The Commonwealth Attorney-General's Department (AGD, 2016) estimates that the compromise and misuse of a person's identity credentials impact between 4 per cent and 5 per cent of Australians aged fifteen years and older each year. This is estimated to cost the economy around AUD $2.2 billion in response measures and losses per annum, on top of the estimates for preventing such crimes being a further AUD $390 million per annum (AGD, 2016). In fact, identity theft is said to now impact a higher portion of the Australian population per annum than any other household-theft related crime, such as burglary and related personal property thefts (AGD, 2016: 5-6; Smith & Jorna, 2016: xii).

Research Aim

Despite the growth and impact of these crimes, little is actually known about the response system, its functions, dependencies and performance. The research aims to address this gap through applying sociotechnical systems methodologies to systematically construct the task, social and information networks to explore the characteristics of Australia's identity theft response system from an individual victim's perspective.

Method and Approach

The research is novel in its application of the sociotechnical systems method known as the Event Analysis of the Systemic Teamwork (EAST). This approach enabled the research to systematically examine the social, task and information networks created in response to the compromise and/or misuse of a person's identity information. The integration of case study and interview data from victims with the response processes and dependencies of broader government and industry actors provided a very rich and detailed account of Australia's current identity response system as well as opportunities for its enhancement. In total 211 identity theft victims were engaged and further engaged over a 12-month period in order to capture their journey across the identity response system. These engagements allowed the researchers to map the social, task and information networks that compromise Australia's identity theft response system, and test assumptions against a library of specific identity theft response plans and actions undertaken across 120 government and industry organisations. The resultant sociotechnical system construction enabled the research to measure the centrality of key agents, and in doing so, the interdependencies and performance of the response system.

Results

The findings highlighted that Australia's response system is leveraged almost exclusively on individual victims to perform critical tasks relating to detection, disputation, protection, and correction. The tasks performed, and information shared amongst agents documented a conflicting overall purpose, where individuals were pursuing response and resilience measures at their own expense that ultimately protect industry and government agents from the consequences of identity misuse. Despite this, individuals were often pursuing these tasks with a firmly held belief that they were protecting themselves, and not the organisations where the compromise or misuse had occurred. The performance of the system also highlighted that traditional first response agents to crime, namely law enforcement and related reporting mechanisms, were not viewed as being particularly effective, inhabiting a section of the response network that was largely separate from the main interaction points. In most cases, these agencies was actually counter-productive for victims in addressing their needs, as the individual victim would most often be required to pursue extensive evidence gathering on their own behalf, regardless of whether law enforcement would concede to assist further down the response journey.

The system also displayed evidence of disjointed and at times conflicting response communications, where industry and government agents would create response circularities in requiring individuals to perform functions that were contrary or opposite to those required of other agents. Perhaps the most significant finding was the observation that the risk from the compromise and/or misuse of an individual's identity in large part endures. Put simply, there appears no present means for most individuals who confront identity theft to completely mitigate future risks of identity misuse across the system. Response measures, albeit largely leveraged on the actions of individual victims, appear temporary in addressing risks. Though only a small percentage of the total cohort reported further misuse since their first engagement with IDCARE, it was apparent that there were no distinct patterns of response choices that would have dictated the permanency of protection from identity theft risks. This was accompanied with a general view from identity theft victims engaged in the study that they simply put the event behind them if they had not noticed further misuse, and disengaged from the response system all together, regardless of the potential risk of re-victimisation. This amounts to a general sense of futility in preventing harm.

Recommendations and Conclusions

There is growing public interest in identity information, its protection and treatment on the back of a number of high-profile data breaches and cyber security-related events to impact the community. Government policies surrounding identity information is largely absent, a by-product of which is a system that appears to have come to existence without any real cohesion and planned thinking on addressing the actual needs of victims. The research has identified four key opportunities for Government, industry and special interest groups to advance the performance of Australia's identity theft response system: (1) a role for Government in developing a national identity policy that is inclusive of minimum response standards for industry and government when detecting, managing and responding to the needs of the community and other agents in the response system; (2) a consumer-consent driven model for the capture and rapid transfer of information relating to the compromise of identity credential information across the system to prevent identity misuse and reduce the centrality of individual victims to perform notification tasks on behalf of these agents; (3) the review of credit reporting and credit ban arrangements in order to identify proper consumer-driven efficiencies that further reduce the harm associated with preventing credit-related identity misuse; and (4) the

decommissioning of the Australian Cyber Online Reporting Network (ACORN) and the establishment of an enhanced identity-cyber-scam integrated crime reporting and supporting network to directly address the needs of multiple agents across the system.

Understanding the complexity of the identity theft response system provides an opportunity to gauge the extent to which individual victim needs are currently addressed against broader performance attributes of the system. The research has revealed that the Australian identity theft response system is failing multiple agents, least of which are the victims of identity theft. There is an obvious opportunity to fill this policy gap, address the underpinning deficiencies on how the system currently operates, and enhance the overall integrity of Australia's identity system.

Introduction

Identity credentials, such as driver licences, passports, and birth certificates, have become essential for individuals across the community to access various goods and services. This can include lines of credit, such as personal loans and mobile phone contracts, as well as access to government services.

Identity theft carried out by criminals through the compromise and misuse of this credential information has wide reaching effects on individuals, businesses, and government organisations alike. The Commonwealth Attorney-General's Department (AGD, 2016) estimate that the compromise and misuse of a person's identity credentials impact between 4 per cent and 5 per cent of Australians aged fifteen years and older each year. This is estimated to cost the economy around AUD $2.2 billion in response measures and losses per annum, on top of the estimates for preventing such crimes being a further AUD $390 million per annum (AGD, 2016). In fact, identity theft is said to now impact a higher portion of the Australian population per annum than any other household-theft related crime (AGD, 2016: 5-6; Smith & Jorna, 2016: xii).

Despite the growth and impact of this crime type, little is known about the response journey of victims, 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 an individual victim perspective.

Context

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 effectively demonstrate the intricacies that exist within this crime type. Wall (2013: 437) expands upon this and uses identity theft as an "umbrella term" to define a diverse range of crimes that use the theft of identity documents to pursue identity fraud (Saunders & Zucker 1999: 184; Jamieson et al 2008: 448; Kraemer-Mbula et al 2013: 543; Wall 2013: 437). Therefore, identity theft can be described as having two distinct stages: the compromise of identity information, including identity credentials, and the misuse of that information for criminal gain or the avoidance of loss. The lack of consistency in definition has plagued prior research and its efforts in gaining a consistent and unified view of its size and impact (Koops & Leenes, 2006).

The Australian Centre for Policing Research (ACPR) (2006) defined identity theft, identity fraud, and identity crime in the Australian law enforcement context (ACPR, 2006). ACPR defined 'identity crime' as a generic term to describe offences that involve the use of any form of false identity (stolen or fabricated) to enable the commission of a crime (ACPR, 2006: 9). This is understood to incorporate both identity theft and identity fraud under the same umbrella, similar to Wall's (2013) definition.

'Identity fraud' refers to gaining money, goods, services or other advantages using a stolen or fabricated identity. In this context, identity fraud refers not only to the misrepresentation of an identity, but also the use of said identity to inappropriately gain benefits, financial or otherwise (ACPR, 2006: 9, 10). While this may include the use of fabricated identities, the focus of this study is on the compromise of identity information, in particular, pre-established identity credentials, and their subsequent criminal misuse.

Nature of Identity theft

Identity theft is amongst the most prevalent crime types affecting individuals, business, and government organisations today (Smith & Jorna, 2018: ix). There is a general consensus that identity

theft is a serious problem, though a longitudinal study of its size, nature, and extent has been difficult to establish. It has become problematic to obtain a consistent methodological picture regarding the actual size of the number of identity theft offences and their impact on the wider community.

Past estimates indicate that approximately 40% of identity theft victims do not report their theft, or depending on the crime that has occurred, report their crime inconsistently to a variety of private sector and/or government agencies (White & Fisher, 2008: 9). Due to the anonymous nature of the crime itself, many victims may be unaware that they are victims, or may not know how their information was initially obtained or "compromised". Therefore, self-reported data may greatly underestimate the loss suffered by the community (White & Fisher, 2008: 8; Harrell & Langton, 2015: 5-6; Cross et al., 2014: 3).

Smith and Jorna (2018) provide one of the most comprehensive studies on the size, nature and impact of identity theft and related crimes. Their research in part focused on the experiences of 9,956 Australian respondents, where 21.5 per cent reported misuse of their credentials during their lifetime; occasions of misuse ranged from a single offence, to 255 separate misuse events (Smith & Jorna, 2018: xii). Over half of the respondents who had experienced misuse experienced financial losses that ranged from $1 to $500,000 AUD, with an average loss of $3,696 AUD (Smith & Jorna, 2018: xiv). Notwithstanding the methodological limitations of sampling from online surveys, Smith and Jorna's (2018) research highlights that identity theft and related crimes permeate across the Australian community, are highly under-reported, and can have enduring impacts.

The Australian Bureau of Statistics (ABS) regularly surveys the prevalence of certain crimes, focusing largely on fraud victimisation. In 2016, it was found that in 2014-2015, an estimated 1.6 million Australians experienced personal fraud, a 6.7 per cent increase from 2010-2011 (ABS, 2016). Of this group, 1.2 million individuals experienced direct financial loss due to their victimisation. The costs of these frauds were significant for victims, with the total financial loss estimated at $3 billion AUD (ABS, 2016).

Knowledge of Identity Theft Victim Response

Current research has had little focus on the nature, performance and impacts of the identity theft response system when identity crimes occur. The identity system itself is one that is typically reserved as an interaction between an individual and an organisation, based on access to specific products or services. It is a system characterised by transactions between an individual and a relying party, heavily influenced by the latter's need to respond to the identity theft risk to their own products and services (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 the victims themselves (Marsh, 2004: 95). Even less is known regarding the needs and experiences of individuals after they have detected that their identity information has been compromised or misused (Button et al., 2014: 38). In the context of cyberspace and related cybercrimes, victims have often been saddled with the responsibility for their own safety in a form of self-regulation (Williams, 2015: 22). The consequence of this has been argued to include the research overlooking how the actual social structures and networks that confront victims in their response actually affect further victimisation (Song et al., 2016).

Traditionally, victims of crimes only feature in the criminal justice system as witnesses or complainants. A recent shift in the Western criminal justice system has seen victims' rights and needs become more recognised (Cross et al., 2014: 4). This has resulted in a body of research that seeks to identify these needs. Insights have been provided into the experiences of the victim, both in the

reporting of their crime as well as their recovery, but importantly, have addressed the needs of the victim from the support system available to them. These crimes have included stalking and harassment crimes (Taylor-Dunn et al., 2017), sexual assault (Jordan, 2013), domestic violence (Brosi & Rolling, 2010) and homicide (Englebrecht et al., 2014). Research has been conducted in aide of characterising the experiences of victims of crime more generally, aiming to identify the experiences of victims as they interact with the criminal justice system and associated support networks (Wemmers, 2013; Tapley et al. 2014; Fuller, 2015; Wedlock & Tapley, 2016).

Due to this movement, under the National Framework of Rights and Services for Victims of Crime 2013–2016 (SCLJ 2013), victims are now guaranteed certain rights when receiving assistance from law enforcement (QPS, 2018; NSWPOL). Assistance and services provided for under this framework are a generalised standard for all victim types, and do not consider the potential of the unique needs of specific crime victims, including those experiencing identity theft. Prior research has highlighted that the ability of identity theft victims to receive compensation or counselling support may be influenced by an absence of understanding or recognition of their specific needs (Cross et al., 2014). An unhelpful gap has been the limited research that captures the needs and experiences of identity theft victims.

The precise structure of the response system, its key actors and their interactions, have not been adequately explored. The research has uncovered the emotional repercussions of these forms of crimes, and that these are largely misunderstood by the current criminal justice system, and the community at large. These victims are more often met with ridicule for what has happened to them, rather than be treated as authentic victims' worthy of support (Marsh, 2004: 127). 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 attempting to report their victimisation to law enforcement (Cross et al., 2014: 4; Button et al., 2013: 48). Evidently there is a dissonance between identity theft victims and the criminal justice system that way set these individuals apart from other types of crime response experiences.

A unique aspect to victims of identity theft is that they may find themselves no longer able to access the goods and services for which the credentials were originally designed, due to damage to the credibility or reliability on that credential. 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, or otherwise participate in societal infrastructure (Lacey & Cuganesan, 2004: 244; Smith et al., 2015: xi). To gain assistance, the victim must go through extensive processes that require the repeated use of their now compromised and likely misused identity, as well as reveal copious other details about themselves and their incident or suffer further issues should they accidentally omit or make a mistake resulting in their case not being accepted (Whitson & Haggerty, 2008: 580-581).

These processes, as well as the prevention strategies that preceded them, are largely based on assumptions about how the public generally copes with technological, bureaucratic, or informational demands. Not all social groups, as evidenced by Cross' study of the elderly (2017), have the same capabilities for being responsible for their identity, especially in the context of growing technological dependence (Whitson & Haggerty, 2008: 588).

Lacey and Cuganesan (2004) demonstrate that individuals cannot rely on assistance from organisations to re-establish their identities. Organisations have three main roles in relation to identity theft: as a site of identity use and potential misuse, as detectors of identity theft, and as a site of responsibility to act against this form of crime (Lacey & Cuganesan, 2004: 245). It was found that organisations had a high orientation of resources towards prevention strategies, but ultimately were inadequate when responding to individual victims. The data demonstrates that resource constraints

when reacting to identity theft and fraud related events resulted in a lack of reporting to law enforcement by affected organisations (Lacey & Cuganesan, 2004).

A crime response system predicated on victim responsibility results in exacerbating burdens on the victim. Survey estimates of the costs of identity theft rarely address the costs to individual victims that go beyond the initial financial harm experienced from the crime. Often, the victim must take immense time in order to deal with what has occurred to them. Victims have been estimated to spend around 48 hours addressing their identity theft and misuse, or in some cases spending up to 500 hours dealing with the consequences of their misused personal information (Button et al., 2014: 38; Smith et al., 2015: xi).

Consequences of Identity Theft for Victims

Victims of identity thefts often experience ongoing harm as a result of their victimisation. Some victims may lose their means of employment during this time and suffer further financial losses as a result of attempts to repair their compromised identity. Victims of identity theft have indicated that further costs incurred after the initial crime can reach up to $100,000 AUD (Smith et al. 2015: xi). In extreme cases, victims have declared bankruptcy as a result of their experiences (Button et al. 2014: 38).

Though more violent or 'conventional' crimes are often seen as more harmful to the victim, victims of financial crimes such as those that fall under the identity theft umbrella often share many of the same psychological outcomes as their counterparts (Marsh, 2004: 127). 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 (Spalek, 1999; Ganzini et al., 1990; Button et al., 2014: 42-43; Golladay & Holtfreter, 2017: 751,755-6; Cross et al., 2014: 3). Individuals who have had their identity credentials compromised or misused may also suffer issues with their relationships, damage to their reputations, and in extreme cases, suicidal tendencies (Cross et al., 2014: 3; Button et al., 2014: 52).

Due to the effects of identity theft on a victim being largely misunderstood by current processes, individuals may not have the same open access to welfare, legal assistance or support systems such as therapy provided to them that conventional crime victims do, causing further financial stress to secure these services themselves, or otherwise go without. This suggests that there is a pervasive victim blaming discourse that exists in society towards victims of identity crime, which only serves to exacerbate the fear and shame already felt by these individuals (Marsh, 2004: 127; Cross et al. 2016: 13). Various studies have been conducted that summarise these repeating themes of guilt experienced by the victim when they try to use the identity crime response systems currently in place.

Despite the limited research, we can point to glimpses of what the response system consequences may be. The convergence of these research findings points to a response system where organisational needs have primacy (Lacey & Cuganesan, 2014), where individuals confront enduring risks of further crimes through identity misuse (Smith et al., 2015), that there are significant constraints in access to established victim-support mechanisms (Marsh, 2004), there are very high-costs of recovery shouldered on individual victims (Button et al., 2014; Smith et al. 2015), and this is set within a broader social context that the individual is to blame (Cross et al., 2016).

Study Aim and Method

Articulating the precise elements of the identity theft response system has remained elusive to date. A view of the how actors across the identity system have responded to such events, how effective these measures have been in addressing needs, and minimising the impact of victimisation remains a key gap in our knowledge (Lacey & Salmon, 2015). It is therefore not clear what the response should be, or how effective current responses have been in addressing the needs of individual victims. We know from prior research that response is harmful. We know that the crime itself is likely to endure and individuals could experience at any moment further misuse of their identity information. We know that misuse, like the initial compromise, can take on an almost infinite diversity of form, which in itself is difficult to prevent. What we don't know is how victims of identity theft today actually respond and how response actors, organisations and others, address their needs. This represents the study's primary aim, to capture empirical details about the identity theft response system, its interactions, and performance in terms of addressing the needs of victims.

Method

Data

To address this aim, the study has obtained unique access to a sample of 211 individual case studies of identity theft from IDCARE, Australia's national identity and cybercrime community support service. IDCARE provided the research team under an approved ethics research program (USC E/16/052), anonymised case records and notes, as well as interview content from follow-up engagement with individual victims over a 12-month period following the initial detection of their compromised identity information. These interviews were designed to uncover the needs of victim, who they engaged with, the tasks they had to perform with those organisations, and how effective these engagements had been in addressing their needs.

Complementing this data was further access to 120 organisational response plans that were obtained via IDCARE's independent testing of response system processes and requirements. This response planning information contained a rich source of data on the needs and requirements of organisations across the identity theft response system and complemented the anonymised capture from the actual experiences from victims in their traversing of the same system. Subject matter experts were also engaged from across industry, government and the victim support sector in testing thematic analyses and opinions formed as to performance enhancement opportunities.

Constructing the Identity Theft Networks

The study used Event Analysis of Systemic Teamwork (EAST; Stanton et al. 2008) to construct and analyse the identity theft response system. EAST was originally developed by Stanton et al. (2005, 2013) as an amalgamation of methods to form a framework for analysing command, communication, computers and intelligence (C4i) activities (Stanton et al. 2008: 49). Though novel to the context of an identity theft response system, the EAST methodology has been applied to a diverse range of research areas, such as air traffic control (Walker et al., 2010), military accidents (Stanton et al., 2012), road safety (Salmon et al., 2014), submarine control systems (Stanton, 2014), dark net carding markets (Lacey & Salmon, 2015), rescue systems (Plant & Stanton, 2016), and in sport ergonomics (Hulme et al., 2018).

There are three networks typically described in an EAST analysis: social, task, and information that are developed individually and combined to visualise a complete network diagram of links and informational currents (Stanton & Harvey, 2017: 222). These are described as:

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
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, or information nodes (e.g. financial institution, close bank account, identity credential, as each node type respectively). These were transcribed in an Excel spreadsheet, and the networks were constructed using Microsoft Visio. Once the nodes were identified, relationships were established between them to form a full network. Once the interview data and organisational response plans were analysed and represented as a network, SMEs from the identity security sector were engaged to confirm that the networks appeared representative of the reality of identity theft response, having already established its representation from an individual victim perspective.

Analysis

The analysis of the networks employed Social Network Analysis (SNA) metrics to demonstrate the structures and relationships between nodes in the EAST networks (Stanton & Harvey, 2017). These SNA 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 if an individual node's communications are more prominent than those of others within the network. Doing so enabled the analysis of the identity theft response system to examine the sociometric status key node influencers; that is, those nodes that influence the performance of the whole system in addressing the needs of victims (Stanton & Harvey, 2017: 224). These will indicate where the identity theft response system is most reliant.

Results and Discussion

In total, 211 individuals responded to the phone-interview survey. The sample selection occurred over a ten-month period and involved obtaining consent from individuals who had engaged IDCARE to participate in the 12-month study. Around two-thirds of individuals invited to participate in the study declined. In other words, approximately 600 individuals were invited to participate during that time period (211 agreed). These respondents were compared to the total data pool of IDCARE's case management centre for 2017 to demonstrate that the data collected was representative of the general clientele of IDCARE. Using a standard Chi-Squared Test, the data was found to be statistically representative of the 2017 IDCARE data. Of these 211 respondents, 52.8 per cent identified as female, and 40.4 per cent were between 25-45 years old. The majority of the respondents resided in New South Wales, Victoria and Queensland. These key statistics are indicative of IDCAREs general population, as well as being reflective of the general population spread of Australia. Thus, the results

from this can be considered generalisable to IDCARE's broader client population, as the only specialist identity theft victim support service operating in Australia.

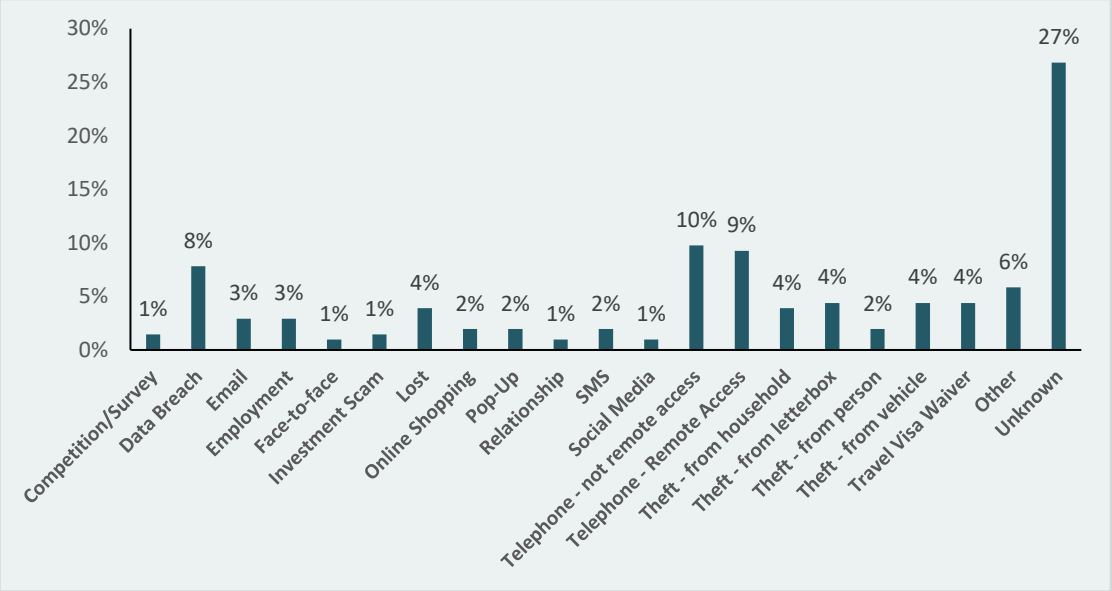
The data collection via survey and case information from IDCARE facilitated an examination of the identity compromise and misuse experiences of individuals over two distinct time periods: (1) 0-day to 3 months; (2) 3+ months to 12 months. The 0-day represents the day at which the criminal was known to have stolen the identity information, not the day upon which the individual became aware of the compromise. Three months was selected based on the majority of events having resulted in some awareness of the event by the individual victim. It also represented the period which the study was able to benefit from multiple engagements (on average 2.4 per participant) via the IDCARE National Case Management Centre. The study referred to this period as the Initial Detection & Response Phase. The second time period, 3+ months to 12 months, represented the nine-month period whereby key initial response measures were likely to have expired or established themselves, including any behavioural changes. In Australia under credit reporting codes, consumers are eligible to apply for a "credit ban" which allows them to prevent the misuse of their identity for credit-related identity misuse. These bans are only in place for 21 days unless a victim expressly requests an extension after having completed additional actions across the identity response system. It is likely, given the time period taken to detect an initial compromise, that the expiration of credit bans or their continuation will occur within this Consolidated Response Phase.

Initial Detection and Response Phase (0-day to 3 months)

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 might commence engagement across the identity theft response system. It was found that approximately 68.2 per cent 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 intervening 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. It represents a period where "system" actors have no knowledge of the compromise or risk associated with an individual's identity credentials.

Their "compromise" events, statistically representative of the broader identity theft victim engagement with IDCARE, highlighted significant diversity. The combined telephone scam compromise experience was the most represented known compromise method; however, a significant portion of individuals had no knowledge of how the compromise of their identity information actually occurred (27% of respondents). Here the individual is most likely aware of the compromise of their identity information because they have become aware of its "misuse" but have no knowledge of how the criminal actually obtained their identity information in the first place. In such cases the individual may have had no involvement in the compromise at all. Criminals are known to sell identity credential information on dark net marketplaces following data breaches impacting organisations (events that have had no direct involvement of an individual, only their personal information entrusted with organisations).

Figure 1: Compromise types of survey respondents. The majority were unaware of how their details were compromised.

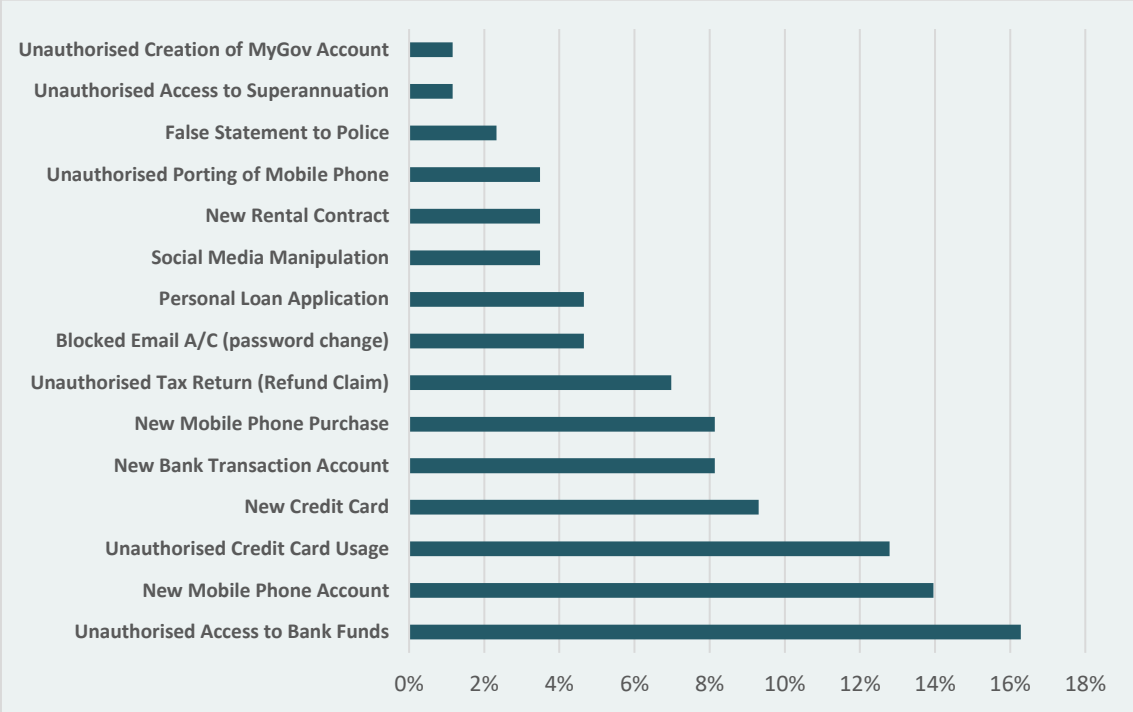


Of those that knew of the compromised information (63% of respondents), on average 3.97 credentials were compromised during the identity theft event. Of the Government credentials, the most common compromised were driver licences (32% of cases), passports (18% of cases), Tax File Numbers (17% of cases), Medicare cards (13% of cases), and Birth Certificates (6% of cases). Non-credential information also most commonly compromised included Full Name (33% of cases), Mobile number (31% of cases), Date of Birth (30% of cases), Address (28% of cases), and Email address (27% of cases). These attributes were identified by individuals as being additional information compromise attributes outside (or in addition to) those found on the credentials compromised.

Of the 211 cases studied, 29% during the Initial Detection and Response Phase experienced both the compromise and misuse of their identity information (i.e. multiple crimes). On average these individuals experience 1.6 misuse events in addition to their one compromise event (i.e. 2.6 alleged criminal identity crime events). This equated to 147 known individual criminal acts of compromising and misusing the identity information of individuals across the sample within the three-month period following the initial theft.

The most common misuse detected during Phase one resulted in criminals gaining unauthorised access of an individual's existing bank account funds (approximately 16% of misuse). The second highest represented misuse related to the establishment of a new mobile phone account, closely connected with the unauthorised usage of an existing credit card facility.

Figure 2: 0-day to 3 months Identity Misuse Profile.



Data was also collected on the cost victims accrued during their identity theft event. A total of $208,856 was lost from identity misuse, with an average loss of $9,081. Of this money, approximately $95,500 was recovered, however this does not account for possible further costs accrued during the recovery process, including the cost of changing behaviours.

Approximately 18% of individuals indicated that they had taken steps to change their behaviour during the first phase in an attempt to prevent further identity theft events in the future. Around 71% of these individuals ended the relationship with the organisation they attributed to the compromise or misuse event by closing the at-risk account or cancelling the identity credential (such as the passport). Around 16% indicated that they had stopped using online devices that were involved in the compromise / misuse event. Interestingly these cases did not feature one prominent form of compromise or misuse over another. Individuals that made a decision to stop engaging online experienced data breaches, “smishing” or SMS-based scams, social media scams, and employment scams. Around 40% of these cases observed a “misuse” event following the compromise prior to the decision to not engage online.

Around one in five (19%) of individuals reported psychosomatic impacts during the first Phase period. The most common impacts related to feelings of anxiousness about what could happen and a sense of frustration and dismay at a lack of information shared about the incident and its future risks by key response organisation. Both of these impact types reflect the express knowledge asymmetry between the individual that experiences identity theft and the organisations they engaged in seeking to determine more about the criminal event and/or their response needs.

It was common amongst this cohort during the first phase period to express "annoyance around not sharing information about how the event happened" or a sense that "the customer service officer seems disinterested in my situation". In fact, where individuals engaged Government document credential issuers, such as driver licence and passport issuing organisations, the general theme to emerge related to a sense from individuals that these agencies largely eschew responsibility for the misuse of their credentials.

Various respondents to the survey stated that when they wanted to change their document (e.g. by getting a new licence number), they were required to fulfil extensive requirements, if they were in a jurisdiction that allowed them to get a completely new document. These requirements included acquiring a court order, a letter from an investigating police officer, and evidence of the credential being misused across the system (not just compromised). In fact, clients highlighted that even this process was at times conflicting in terms of advice provided:

> *The police person told me that VicRoads will put a letter on the end of the licence number on the new licence to flag it if it gets used. When I spoke with VicRoads they told me this information was incorrect. (Respondent 56)*

Individuals repeatedly acknowledged impacts around the time and effort required to understand what's needed to respond and what the precise risks are to their identity information. This incurs further time and financial costs from the victim in order to apply for a change that could potentially prevent much of the possible misuse in their name.

Consolidated Response Phase (3+ months to 12 months)

The case information and repeated engagement between the 3 month and 12-month period of the data collection phase of the study contributed further to the expanded view of the identity theft response system. It also enabled the study to identify further instances of identity compromise and misuse across the sample and to examine comparatively changes in behaviours and response priorities.

Of the 29% to have experience both an identity compromise and misuse in during the first three-month period, a further 6% of this cohort experienced further misuse of their credentials over the proceeding 9-month period. Interestingly, of the cohort that did not experience any known misuse during the first three months (71% of the sample), a further 11% of this group did experience misuse over the proceeding 9-month period. In total this meant that across the entire sample, identity misuse occurred in 9% of occasions between month three and month 12 following the initial compromise event where this was known (i.e. where the individual knew when the initial compromise of their identity information occurred).

In fact, 13% of individuals during the consolidated response phase indicated that they have not been able to put the incident behind them and move on. This cohort felt as those the response was not adequate and that the initial compromise had not been "resolved" in addressing their needs. Insights into the reasons behind these feelings revealed that 35% of respondents in this cohort felt that they were a vulnerable person and that it could happen again. A further 32% acknowledged that despite their participation in the response system there was no-guarantee that misuse won't happen again. And 27% of individuals 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 from responding agencies.

In this cohort, there was an over-representation of misuse events occurring within the first 3-month period (48% of cases compared with 29% of the broader sample). This cohort also rated their experience across the response system actors during the first 3 months as being quite poor (averaged

3.9 out of ten in terms of overall satisfaction in addressing their needs). This compares to an average response system score across the residual cohort of 6.2 out of ten.

The majority of individuals that expressed that they had no residual needs or concerns (87% of the sample), revealed that this was primarily because there had been "no evidence of any ongoing misuse" (around 96% of these respondents) and that they knew they had "done everything I could to protect myself" (19% of these respondents). Interestingly, these views were largely absent of any specific act or response provided from within the identity response system itself.

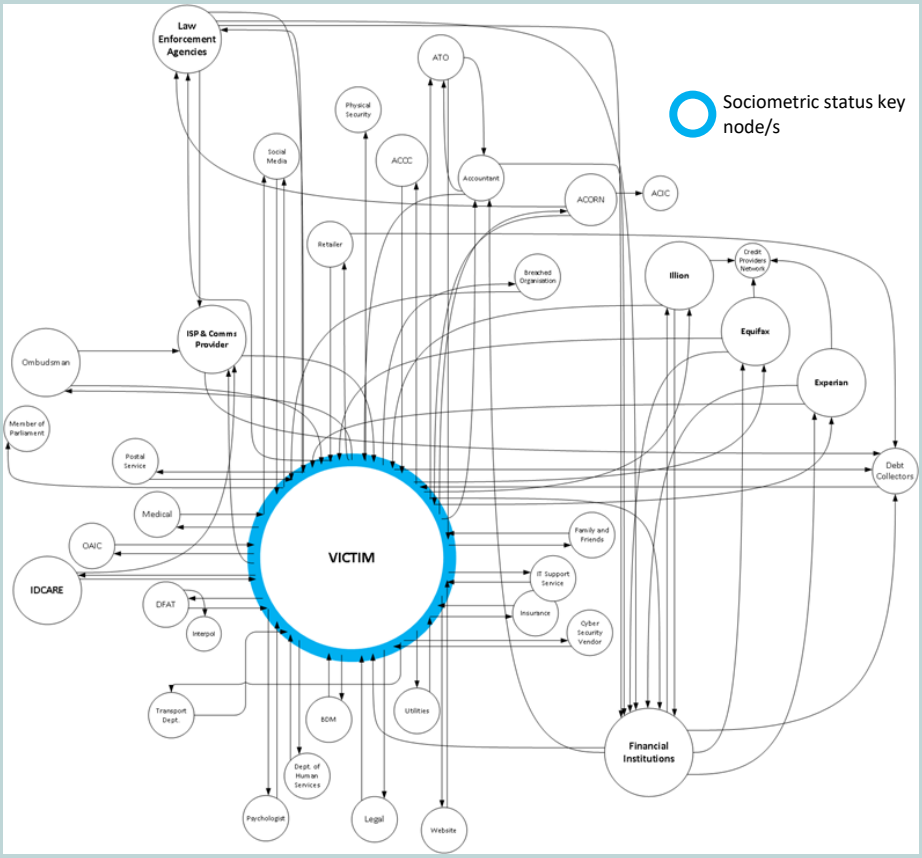
The two time-periods assisted the study in exploring changes in attitudes and behaviours. It also enhanced the ability to undertake the EAST analysis in directly capturing the key tasks (needs), the socialisation (the actors in the response system) and their information dependencies. The application of EAST captures the response system across the 12-month period. It was not useful to construct networks across the two time-periods as the actors, tasks and the information exchanged occurred pretty consistently across both periods. The order of engagement across the system is also not particularly consistent across the cohort, aside from the prioritisation of managing credit risk via engagement with credit reporting agencies (this assisted to define the initial two time periods), individuals and other actors within the system performed tasks rather inconsistently across the time period.

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 that information was exchanged between social actors during their responses to the survey. The analysis identified 37 social actors, including the victim, within the identity theft response system. These are represented in Figure 3. These nodes were further tested by Subject Matter Experts recruited by the researchers from IDCARE and its identity theft response system partners as a reasonable representation of the main actors within this system.

The 'victim' node was identified as the key actor within the identity theft response system, based on sociometric status. Of the 37 nodes in the social network for the identity theft response system, the victim node communicates with 33 other nodes within the system. As such, this node also scored the highest on emission and reception, as the victim is receiving and providing information to nearly all of the other social actors. The victim also acts as the in-between point for the majority of the identity response system, as it provides an information conduit between several organisations (e.g. reporting to police and then taking that report to various organisations as proof of the identity theft), with information passing through the victim to reach other areas of the network.

Figure 3: Social nodes and their links within the identity theft response system



These results strongly indicate that the victim is vital in the social structure of the identity theft response system. It is evident based on the preliminary survey data, and the social network, that the victim is providing the largest amount of feedback to other actors. There appears to be little to no communication between other actors in the network without information passing through the victim. The second most influential node within the system was the 'financial institutions' node, which experienced a much lower sociometric status, and largely only interacted with financially orientated organisations. 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.

This network also highlights the variety of organisations and agencies that the victim will engage during their journey. The social network's critical dependence on the individual victim reinforces the view of many participants that there seemed a "disinterest" in their needs by organisations and a complete focus on only the "specific risks to the organisation" and not the individual (including broader risks to other identity credential relying parties). The Subject Matter Experts presented an ironic position relating to the social network results, that is, whilst the individual appears to be central to Australia's identity theft response system, any future misuse is likely to be a risk owned by the relying parties of the identity (such as financial institutions, mobile phone providers, and Government service providers). Put simply, individual victims appear to be performing a considerable amount of

socialisation, ultimately to protect government and industry that may rely upon their compromised credentials when providing products and services.

It also highlights the overly complicated expectations placed on the victim regarding how they can best respond to their identity theft. The network demonstrates that the victim must report to all three credit reporting agencies (Illion, Equifax and Experian). However, all three credit reporting agencies do not communicate to each other, despite reporting to the Credit Providers Network. This is an example of a communication breakdown that is requiring the victim to act as the intermediary, again to protect the interests of credit providers. Multiple respondents were distressed that they had to reach out to all three agencies and stated that having a central reporting figure would make more sense. Furthermore, many respondents were unaware that it was necessary to contact all three agencies, and only discovered this after seeking advice at other nodes such as IDCARE. This further delayed response time and pro-longed the period of time where criminals were best placed to commit credit-related misuse (prior to a credit ban being placed).

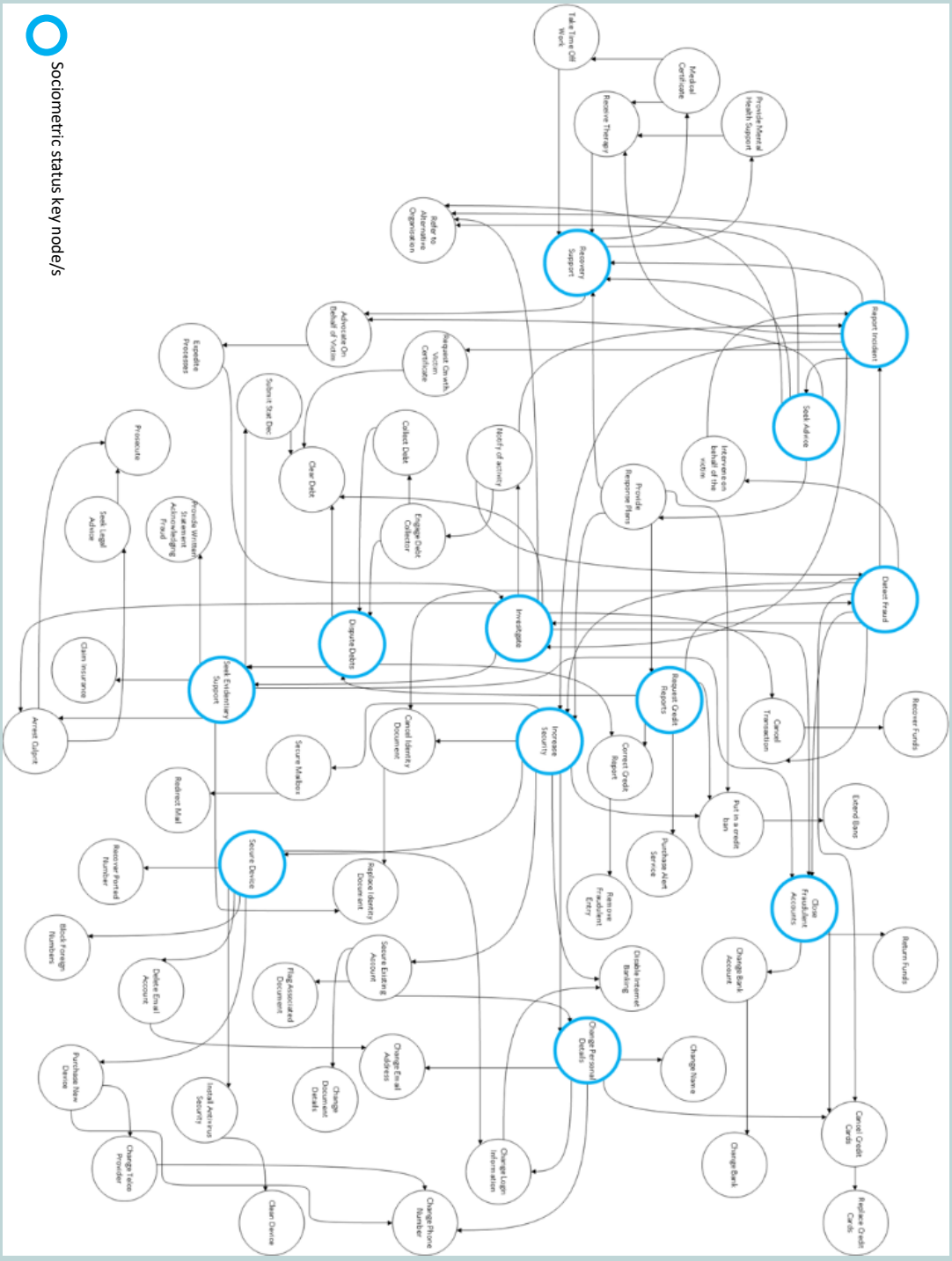
Task Network

Figure 4 shows that 67 task nodes and their connections were identified from the survey responses, as well as SME input. The task network was constructed by identifying the different tasks that each survey respondent indicated that they pursued when contacting each social node. These tasks were then linked using SME input, and background understanding of the various processes associated with each major task branch. In the task network, 12 key nodes with high sociometric status were identified. These, as well as their respective reception and emission values are outlined in Table 2:

Table 2: Key task nodes identified in the task network and their associated reception and emission values

Node	Reception	Emission	Total
Report Incident	3	7	10
Detect Fraud	2	8	10
Investigate	3	7	10
Increase Security	3	7	10
Recovery Support	5	3	8
Seek Evidentiary Support	2	5	7
Secure Device	1	6	7
Change Personal details	2	5	7
Seek Advice	1	5	6
Dispute Debts	4	2	6
Request Credit Reports	1	5	6
Close Fraudulent Accounts	3	3	6

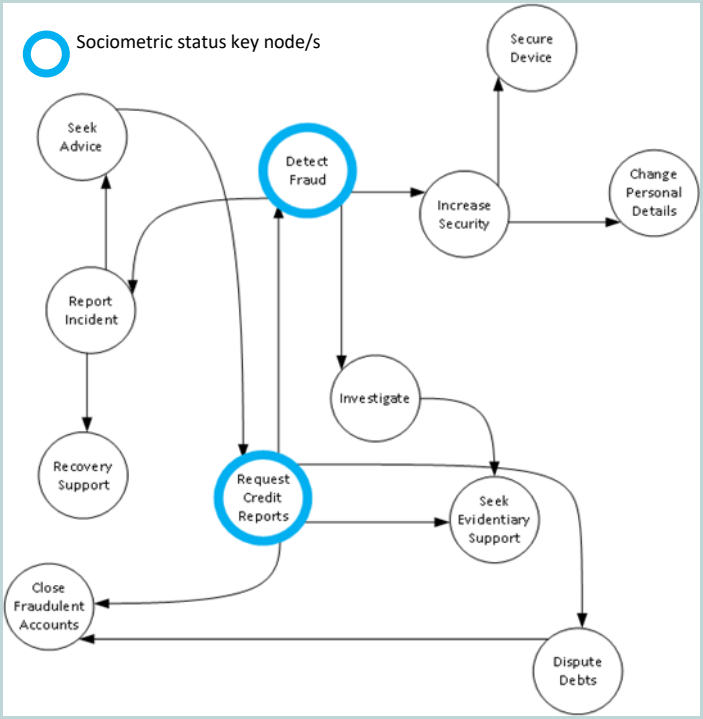
Figure 4: Task nodes and their links within the identity theft response system



It is clear that this network demonstrates a higher number of nodes than the social network but does not possess one centralised node such as the victim. Instead there are several spread out key nodes that are interrelated and correspond to different key tasks that act as ultimate goals that the victim is

trying to achieve during their response journey. The interconnected nature of the nodes indicates the reliance that the tasks nodes have on the rest of the network. For ease of understanding, the key tasks were further condensed into an abridged task network, as shown in Figure 5, in order to visualise the main goals of the victim.

Figure 5: The abridged task network, showing goal tasks pursued by the victim



The abridged task network identified two key nodes, which demonstrate a reliance on the victim to request their credit reports, and by extension, to detect their identity misuse (ie fraud). This further demonstrates that there is little notification by the wider organisational network of the individual of their compromise or misuse, which is further supported by the number of victims who self-detect their identity theft event(s). Other key tasks include investigating, increasing security, reporting, and addressing various fraudulent activities by disputing debts or closing accounts. It is important to note that this task network highlights the need for the victim to seek evidentiary support on their own behalf, despite the social network demonstrating that law enforcement agencies are involved to a certain extent. All these tasks rely on each other in some respect in order to be accomplished.

It is surprising that ultimately less focus is given to putting more proactive protective measures in place, such as establishing a credit ban. A credit ban with all three agencies effectively prevents a criminal from accessing any lines of credit in the victim's name, or purchasing products on payment plans in any fashion, and prevents the more common types of misuse. This may be attributed to a lack of knowledge about the credit reporting agencies in the general public. Most clients who were surveyed indicated that they were unclear about the procedures around credit reports. Since the main three credit reporting agencies are also business working for profit, many clients had been told that they were expected to pay for the myriad of services that credit reporting agencies provide.

There also appears to be less focus given to actions around replacing the actual identity credential. This may be reflective of the inability to change credential numbers (presently only three Australian States allow for this to occur only after various complex tasks have been completed). This may be due to many of these cases involving online compromises of a credential copy, thus the victim retains the original document and it does not require physical replacement.

Focus appears to be on reporting the incident, detecting the fraud, investigating the event, and increasing security on accounts, based on the nodes with the highest sociometric status scores. This may indicate that the identity theft response system has most of its limited focus on address a specific event or transaction, rather than the enduring risk a compromised credential may have for the rest of the system.

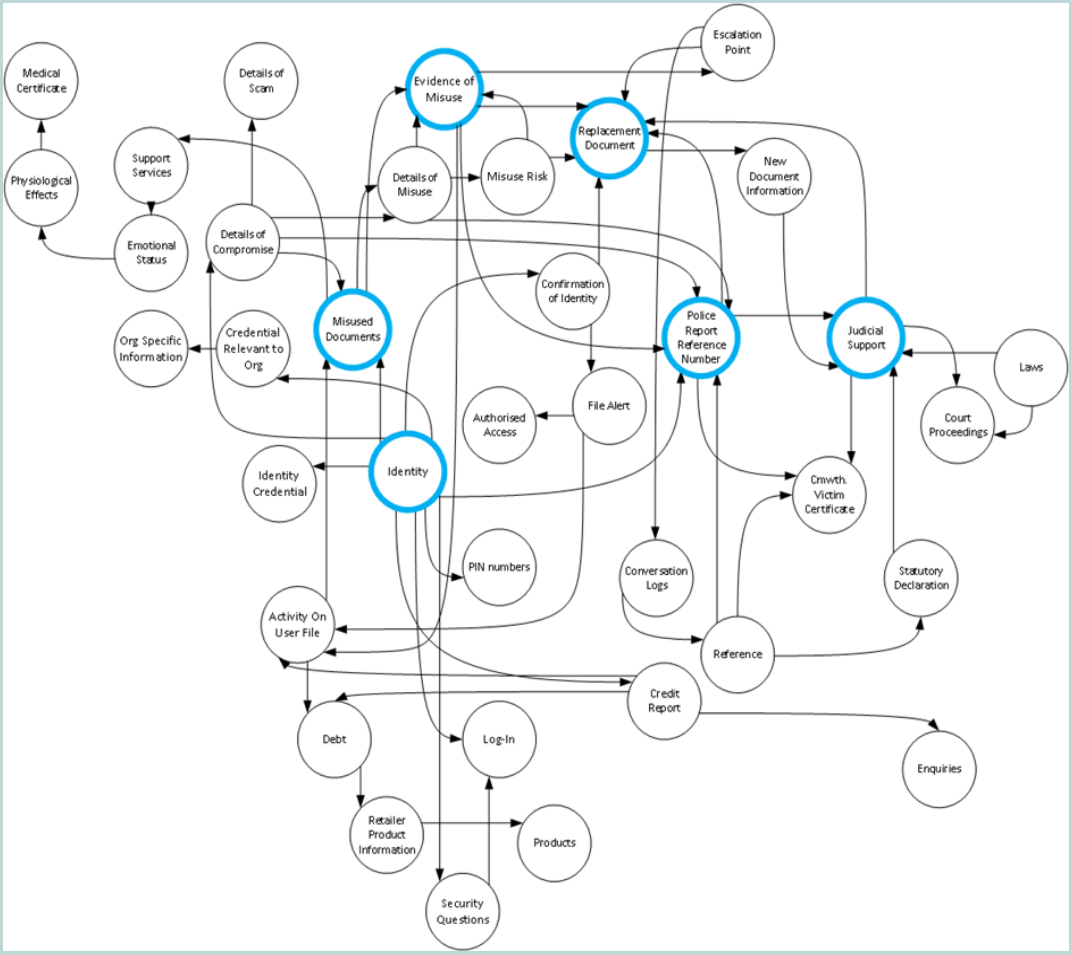
Information Network

EAST identified 37 information nodes and their corresponding connections based on surveys conducted on organisational procedures and response plans across the organisations identified as actors in the Social Network. These surveys were further supported by engagement with Subject Matter Experts to collect further details relating to the precise information requirements of each task. This network is demonstrated in Figure 5.

Six key nodes were identified. 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, thus reinforcing the importance of advancing information about the compromised or misused identity information in order to complete the tasks identified. 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 actually been stolen.

Based on this network, one can conclude that the majority of information being transmitted involves demonstrating that misuse has happened by gathering information about the individual victim (their identity credential information). This underscores the experience of many victims of identity theft in that they are often expected to restore their identity by repeatedly re-exposing their identity information to various organisations across the system in order to address their needs. There was a sense amongst the respondents, that they felt re-victimised by the process of having to continually reproduce the very credential information that had been stolen. For example, for cases that involved the compromise or misuse of identity information online, it was common for law enforcement to request individuals submit the very same information via online police reporting forms (such as the Australian Cybercrime Online Reporting Network). Dissatisfaction with this particular process was high across this cohort of the sample (averaging an overall satisfaction level of 3.42 out of ten).

Figure 5: Information nodes and their links within the identity theft response system



Policy Implications

Over a million Australians a year experience the compromise and misuse of their identity information. Individuals need to respond to the crime, which often includes building sufficient knowledge about what it means and what to do, as well as put in place mitigation strategies that seek to address enduring risks that these crimes present. The research has identified that individual victims are central to initiating and performing tasks critical to the response of identity crime. Despite these efforts, the nature of most identity theft crimes means that there is little guarantee that the identity will not be misused at some point in the future. Whilst the misuse of the identity information following its compromise or theft may be limited only to a perpetrator's imagination, the most common forms of misuse include the accessing of existing account services, such as bank balances, email accounts and tax entitlements, as well as the creation of relationships with government and business that are unfamiliar with the identity and allow access to their products and services, such as new personal loans, social media accounts, credit cards or mobile phone services.

The variability of an individual's response capacity coupled with a focus on organisations to prioritise their own response protection tasks represents an environment of disjointed response efforts and responsibilities. It is largely reliant on the individual victim to traverse industry and government, and in will lead to enduring risks, in some cases further criminal offending, and significant financial and non-financial harms. These impacts can go beyond the individual concerned and can have permanent and lasting negative consequences for families and communities.

Despite this trend, engagement across industry and Government subject matter experts revealed that whilst this was the victim's experience, it is quite likely that a portion of these individuals would have had their identity theft event detected by organisations across the system earlier but not communicated to them. This is a particular point of interest in relation to policies that aim to prevent future identity misuse and the timeliness of the response efforts. The growing number of identity data matching and cleansing initiatives being performed by Government and businesses across the identity system is likely to exacerbate this development. Put simply, organisations are increasingly likely to be in a position to know of the suspected compromise and/or misuse of identity information before the consumer. Whilst the recently introduced notifiable data breach legislation under the Commonwealth privacy regime will likely address these instances where the identity credential information is captured in breach events by regulated entities, this legislation does not cover instances where legitimate data matching and cleansing activities uncover the potential compromise or misuse of identity credentials and related information in the ordinary course of business transactions. Furthermore, most States and Territories do not have notifiable data breach schemes that would result in a mandatory notification to the individual consumer. Policy development is required to examine the roles and responsibilities of organisations to address systemic weaknesses in the communication and notification at risk credentials on behalf of citizens – rather than leave this for individuals to do on behalf of these organisations.

Our research found that there is a great potential capacity for the identity system to enhance the timeliness of its detection, and more importantly, the efficiency of its communication to impacted individuals. A cornerstone to unlocking this potential is a shift in approach by organisations to the management of compromised of identity information. The research observed that the decision to not communicate the detection of an identity theft event was not necessarily constrained by legislation, but a limited view on the benefits of doing so to the impacted consumer and the likely target organisations of identity thieves.

Even without being the initial point of identity theft detection, victims are often placed in a disadvantaged position in responding to the enduring risks identity theft present. The nature of the identity theft risk, particularly relating to the future misuse of the compromised credentials, in large part reflects a combination of the type of credentials compromised, the capacity of the impacted individual to respond, and the reporting and notification requirements of the relevant organisations they must engage.

A major contributing factor to the inefficiencies associated with identity theft response from a consumer perspective related to the efforts required to manage credit risk. Whilst only recently reviewed, the Credit Code regulated by the Office of the Australian Privacy Commissioner, does not in any meaningful way acknowledge the difficulties or inefficiencies associated with placing credit bans when an identity is compromised. This risk relates to the misuse of identity credentials by criminals in order to obtain credit in a victim's name, such as a new credit card, personal loan or mobile phone account. These risks are heightened for individuals if the credentials compromised consist of either a driver licence, passport or Medicare card or a combination thereof. Criminals in most instances do not need access to the physical credentials. The online and related arm's length nature of most

applications facilitate a clear preference by identity criminals to pursue misuse events where the mere information on the credential is enough to submit applications or access existing account privileges.

The primary method by which consumers that respond to identity theft address these credit misuse risks is through the application of a credit ban on their credit report. Under the Privacy Act 1988 (Cwth) Privacy (Credit Reporting) Code 2014 (Version 2), each Australian is eligible to request a credit ban which has the effect of denying a credit provider's ability to check the individual credit report. The Code has practical limitations and impediments for victims of identity theft.

The engagement with victims found that interactions with Credit Bureaus are highly problematic. The experiences of some were reinforced by a recent finding of the Federal Court in relation to action taken by the Australian Competition & Consumer Commission (ACCC) against Equifax, one of Australia's Credit Bureaus. Equifax admitted it breached the Australian Consumer Law (ACL) in 2016 and 2017, when its representatives made false or misleading representations when it told consumers that its paid credit reports were more comprehensive than free reports it had to provide under the law, when in fact they contained the same information.

Despite recent efforts to review the underpinning Privacy Act 1988 (Cwth) Privacy (Credit Reporting) Code 2014 (Version 2), the Review has found that little attention to the exact journey of identity theft victims in seeking to protect against credit risks was considered in producing Version 2. In a number of other Western democracies, consumers have a right to place an indefinite credit ban on their Credit Reports. This is not on the basis of a consumer "request", rather a requirement place on the Credit Bureau should a consumer apply. Section 20K(3) of the Privacy Act 1988 provides that bans be initially provided for 21 days. In the United States, a citizen may request that their credit report is banned indefinitely and until such time as they request the credit report to be reactivated. Our research observed a response system that presents a strong case for Australia to consider adopting a similar approach to the United States. The consequences of an indefinite ban should be explored, particularly in relation to accessing contemporaneous credit worthiness information should bans be lifted by consumers as an attempt to initiate a new credit application.

Our research has been mindful that any future moves or recommendations to improve identity theft victim response may create risks or opportunities for criminals to exploit identity information repositories. The interdependent nature of the identity system and a lack of common ownership of the risks that present when an individual's identity credentials have been stolen also presents opportunities for criminals to access and exploit other identity information repositories. Prior policy attempts have been made to introduce processes and mechanisms for the identity response system to adapt and rebuild compromised and misused information. The identity theft victim certificate regime introduced in 2009 is one such response that has not resulted in the desired policy outcome. Certificates are difficult to obtain, and in some States applications are not accepted by local Magistrates (for example, Commonwealth Identity Theft Victim Certificate applications are not currently accepted by Queensland Magistrates). Engagement with our case victims found that it is likely that the broader identity system has no real knowledge of their existence. This undermines the original policy intent of providing individuals with a formal acknowledgement of their experience and the risk to their identity does not result in any rapid transfer of such information to industry and government organisations that interact with criminals that impersonate these victims – it is merely a physical certificate issued to the individual. Notwithstanding this, the underpinning policy priority remains – the formal acknowledgement to individuals that they have been victimised and the rapid transfer of this information or its accessibility across the identity system.

Certain needs are the same for individual victims and organisations across the identity system when an identity is compromised and at risk of further misuse. Individuals require confidence and assurance that their personal information and identity credentials will not be misused at some point in the future. Organisations that rely upon such information need access to information that will enable them to make appropriate risk-based decisions about the identity credentials submitted. These represent a common information transfer need which at present is almost entirely up to the individual victim to pursue, adding to the time, cost and risk that a person's identity information will not be adequately prevented from future misuse.

Several recommendations are made to respond to this finding:

R1. Allowing the Document Verification Service and Facial Verification Service to acknowledge that an individual's credential is at risk of misuse. Guidelines on interpreting these acknowledgements should be developed and agreed by users of the services. This will allow service users to make appropriate risk-based decisions about the identity credential and support individuals in rapidly transferring information across the identity system.

R2. Designing agreed victim acknowledgement and reporting standards and processes across the identity system that:

a) Provide individuals with an agreed mechanism of formal acknowledgement that they have experienced the compromise of their identity and are at risk of identity misuse. This will replace the victim certificate regime and allow individuals to determine what organisations or classes of organisations across the identity system they wish to notify;
b) Facilitate the rapid transfer of identity compromise information and reporting across the identity system by embedding reporting services through key community hubs, such as Police Stations (physical), online reporting mechanisms (online), such as ACORN, and via national victim support services (telephone and online).

R3. The Commonwealth should establish industry and government Codes of Practice in consultation with key stakeholders, including individuals and organisations impacted by identity compromise and misuse, to advance the efficient operational protection, response and overall integrity of the identity system.

R5. That the 21 day credit report ban period under section 20K(3) of the Privacy Act 1988 as a key current measure to prevent identity misuse involving fraudulent credit applications be reviewed. The review should also consider mechanisms to enhance the efficiency of credit report access and ban applications on behalf of individuals that experience identity credential compromise and misuse. In doing so, such a review should examine the responsibilities of Credit Providers in notifying individuals of detected identity misuse, including the precise nature of the credentials suspected of being compromised.

Conclusions

This study has presented a representation of Australia's identity theft response system through the application of EAST. This novel approached allowed for the identification of the key actors, tasks and information flows performed in addressing the needs of individual victims and others when responding to the compromised and misuse of identity information. The engagement and re-engagement of individual victims over a 12-month period was critical in extracting relevant data on the nature and performance of the system (particularly from the victim's perspective). Qualitatively victims at large seem to reach a point through navigating the system that they believe that have

responded and share little residual concerns of future misuse. In large part this was found to be because they had “done everything possible” to prevent future misuse. But the smaller cohort (13% of the sample), that held residual concerns following several months of response, carried an equally valid observation – no one can guarantee that future misuse will not occur. This is but one of the dichotomies observed by the researchers when examining the identity theft response system.

It is a defined system, but one that is complex and highly leveraged on the performance of tasks and resultant socialisation of individual victims. The tasks performed, and information shared amongst actors documented a conflicting overall purpose, where individuals were pursuing response and resilience measures at their own cost that ultimately protect industry and government actors from the consequences of identity misuse but were often doing so believing they were protecting themselves. The performance of the system also indicates that responding actors, despite relying on identity information and identity credential providers, almost exclusively respond in a manner that is oriented towards protecting their own products and services and not other actors across the system – again this appeared to be the role of the individual victim on behalf of the system. The system also displayed evidence of disjointed and at times conflicting response communications, where industry and government actors would create response loops in requiring individuals to perform functions that were contrary or opposite to those required of other actors. Interviews highlighted these experiences and the rather inefficient circularity of response efforts.

Perhaps the most significant finding was the observation that the risk from the compromise and/or misuse of an individual's identity in large part endures. Put simply, there appears no present means for most individuals who confront identity theft to mitigate future risks of identity misuse across the system. Response measures, albeit largely leveraged on the actions of individual victims, appear quite temporary in addressing risks. This was consistent with a general view from identity theft victims engaged in the study that because they hadn't noticed further identity misuse, then they must be alright.

References

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

Australian Bureau of Statistics (ABS) 2016. Personal fraud, 2014-15. Canberra: ABS.

Australasian Centre for Policing Research (ACPR), (2006), Standardisation of definitions of identity crime terms: A step towards consistency, Report Series No. 145.3

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.

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.

Brosi, M. W., & Rolling, E. S. (2010). A narrative journey for intimate partner violence: From victim to survivor. The American Journal of Family Therapy, 38(3), 237-250.

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. Trends & Issues in Crime and Criminal Justice, 474, 1-6

Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to online fraud victims: An examination of reporting and support. Criminology Research Grant Final Report

Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. Security Journal, 30(1), 74-88.

Englebrecht, C., Mason, D. T., & Adams, M. J. (2014). The experiences of homicide victims' families with the criminal justice system: an exploratory study. Violence Vict, 29(3), 407-421.

Fuller G (2015). The Database of Victimisation Experiences. Australian Institute of Criminology Technical and Background Paper no 60 Canberra: AIC

Ganzini, L., McFarland, B. and Bloom, J. (1990) Victims of fraud: Comparing victims of white collar and violent crime. Bulletin of the American Academy of Psychiatry and Law 18 (1): 55–63.

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. Victims & Offenders, 12(5), 741-760.

Harrell, E., & Langton, L. (2015). Victims of identity theft, 2014. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Hulme, A., Thompson, J., Plant, K. L., Read, G. J., Mclean, S., Clacy, A., & Salmon, P. M. (2018). Applying systems ergonomics methods in sport: A systematic review. *Applied ergonomics*.

Jamieson, R., Land, L., Sarre, R., Steel, A., Stephens, G., & Winchester, D. (2008). Defining identity crimes. ACIS 2008 Proceedings, 107, 442-451

Jordan, J. (2013). From victim to survivor-and from survivor to victim: Reconceptualising the survivor journey. Sexual Abuse in Australia and New Zealand, 5(2), 48

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows?. Technological Forecasting and Social Change, 80(3), 541-555.

Koops, B. J., & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. Datenschutz und Datensicherheit-DuD, 30(9), 553-556

Lacey, D., & Cuganesan, S. (2004). The Role of Organizations in Identity Theft Response: The Organization–Individual Victim Dynamic. Journal of Consumer Affairs, 38(2), 244-261.

Lacey, D., and 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, 117-128.

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

New South Wales Police Service (NSWPOL). Charter of Victims' Rights. (Unknown). Retrieved from https://www.police.nsw.gov.au/safety_and_prevention/victims_of_crime/more_information/charter_of_victims_rights

Queensland Police Service (QPS). Charter of Victims' Rights for agencies. (2018, February 15). Retrieved from https://www.qld.gov.au/law/crime-and-police/victims-and-witnesses-of-crime/agency-training-funding-and-research/rights-of-victims

Plant, K. L., & Stanton, N. A. (2016). Distributed cognition in Search and Rescue: loosely coupled tasks and tightly coupled roles. *Ergonomics*, 59(10), 1353-1376.

Salmon, P. M., Lenne, M. G., Walker, G. H., Stanton, N. A., & 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), 1628-1642.

Saunders, K. M., & 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), 183-192

Smith, R. G. (2008). Coordinating individual and organisational responses to fraud. Crime, Law and Social Change, 49(5), 379-396.

Smith, R. G., Brown, R., Harris-Hogan, S. (2015). Identity crime and misuse in Australia: Results of the 2014 online survey. AIC reports. Research and Public Policy series

Smith, R. G & Jorna, P. (2018). Identity crime and misuse in Australia: Results of the 2016 online survey. AIC reports. Statistical Reports No. 6

Song, H., Lynch, M. J., & Cochran, J. K. (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): 213–230.

Stanton, N., Harris, D., & Baber, C. (2008). Modelling Command and Control : Event Analysis of Systemic Teamwork. Aldershot, Hampshire, England: CRC Press.

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

Stanton, N. A., P. M. Salmon, L. A. Rafferty, G. H. Walker, C. Baber, and D. P. Jenkins. (2013). Human Factors Methods: A Practical Guide for Engineering and Design. 2nd ed. Aldershot: Ashgate.

Stanton, N. A., & 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), 221-233.

Standing Council on Law and Justice (SCLJ) 2013. Annual report 2012–13. http://www.sclj.gov.au/agdbasev7wr/sclj/sclj_annual_report.pdf

Tapley. J., Stark. A., Watkins, M. and Peneva, B. (2014), A Strategic Assessment of Support Services for Victims of Crime in the South East, Portsmouth: University of Portsmouth.

Taylor-Dunn, H., Bowen, E. and Gilchrist, E. (2017) The Victim Journey: A Participatory Research Project Seeking the Views and Experiences of Victims of Stalking and Harassment. Project Report. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, London.

Walker, G. H., Stanton, N. A., 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), 184-197.

Wall, D. S. (2013). Policing identity crimes. Policing and Society, 23(4), 437-460

Wedlock, E., & Tapley, J. (2016). What works in supporting victims of crime: A rapid evidence assessment. University of Portsmouth, Victims' Commissioner.

Wemmers, J. A. (2013). Victims' experiences in the criminal justice system and their recovery from crime. International review of victimology, 19(3), 221-233.

White, M. D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. Criminal Justice Policy Review, 19(1), 3-24.

Whitson, J. R., & Haggerty, K. D. (2008). Identity theft and the care of the virtual self. Economy and Society, 37(4), 572-594.

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48.