Identity theft and Australian telecommunications:

Case analysis

Australian National University

IDcare

accan

Identity theft and Australian telecommunications: Case analysis

Victims, Attacks and Intervention Development

Sigi Goode

June 2017

Australian National University

NATURAM PRIMUM COGNOSCERE RERUM

accan

Identity theft and Australian telecommunications: Case analysis

Authored by Sigi Goode

Published in 2017

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

Australian National University
Website: www.anu.edu.au
Email: sigi.goode@anu.edu.au
Telephone: +61 2 6125 5048

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: 02 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au.

ISBN: 978-1-921974-51-9
Cover image: Design by Richard Van Der Male with image from Shutterstock

This work can be cited as: Goode, Sigi (2017) 'Identity theft and Australian telecommunications: Case analysis', Australian Communications Consumer Action Network, Sydney.

Table of Contents

List of Figures

Introduction

This report details the analysis of 4200 Australian cases of identity theft that have been supplied by IDCARE, Australia's identity protection service. The cases represent identity theft reports to the service over approximately a one-year period where clients have consented to their information being used for research purposes. The goal of the analysis provided in this report is to understand how identity theft is committed, and the processes behind an identity theft event, in order to develop some interventions that can be applied to identity theft management in Australia. This report is also intended as a foundation for the development of a set of identity theft awareness infographics that can be deployed via social media. The work is part of a larger research project, funded by the Australian Communications Consumer Action Network (ACCAN), aimed at better understanding the processes of identity theft, and to provide greater insight into the role of information and communication technology in identity theft attacks.

The rest of this report is structured as follows. In the first section, *Victim Demographics*, the report presents an overview of identity theft victims, including their age, gender and location effects. In the *Identity Theft Attack Demographics s*ection, the report examines the characteristics of identity theft attacks and associated victim response. In *Victim Recovery Demographics*, the report analyses the available evidence regarding the outcomes of identity theft and victim recovery, in order to inform the development of interventions. The section titled *Synthesis* provides graphical analysis of the relationships between variables when controlling for the dollar amount taken or the days elapsed since the identity theft began. The report then presents an overview of the two main *Interventions* developed as a result of the data analysis, and explains how these interventions will be applied practically. Finally, the report presents a set of *Recommendations* for businesses and consumers.

Victim Demographics

In order to present the main aspects of the data, we provide (mostly univariate) summary data of the identity theft cases in the data set. Our goal in this section is to summarise the data as it has been recorded from received identity theft reports. We provide more in-depth analysis of the data, incorporating appropriate graphical analyses, in a subsequent section of this report.

In total, there were 4239 raw cases, spread over a 600 day period between August 2014 and April 2016. This volume of cases includes only those cases where the victim has consented to allow their case to be used for research purposes – wider average case volume is approximately 45 new cases per day. Unless explicitly noted, the ensuing analysis in this report is based on the full set of cases.

Identity Theft Case Reports by Day and Time

This frequency equates to seven new potential identity theft cases each and every day. As shown in Figure 1, most new cases were reported on a Monday, with case reports slowly decreasing throughout the rest of the week; approximately 21% more cases are reported on a Monday than a Friday. As shown in Figure 2, most cases were reported in the afternoons and evenings (a slight dip in case reporting occurs at lunchtimes). While most cases are reported during business hours, identity theft cases are still reported online around the clock.

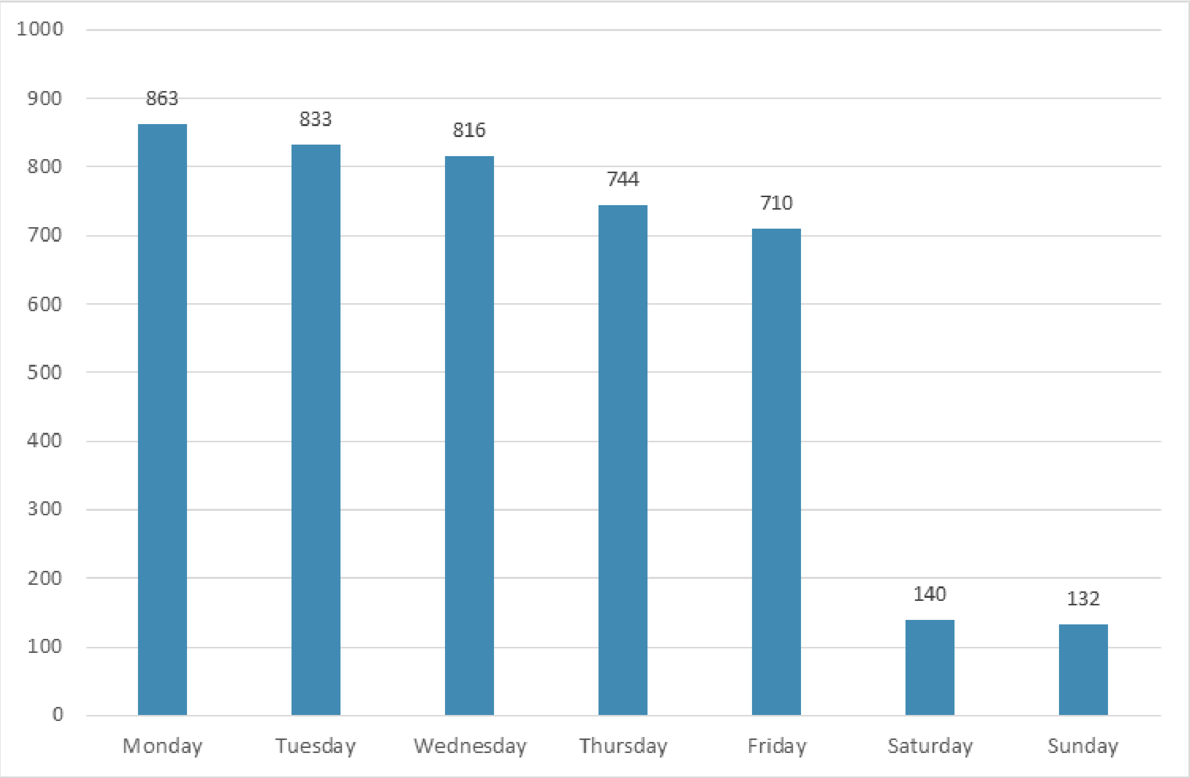

Figure 1 Identity Theft Case Reports by Day

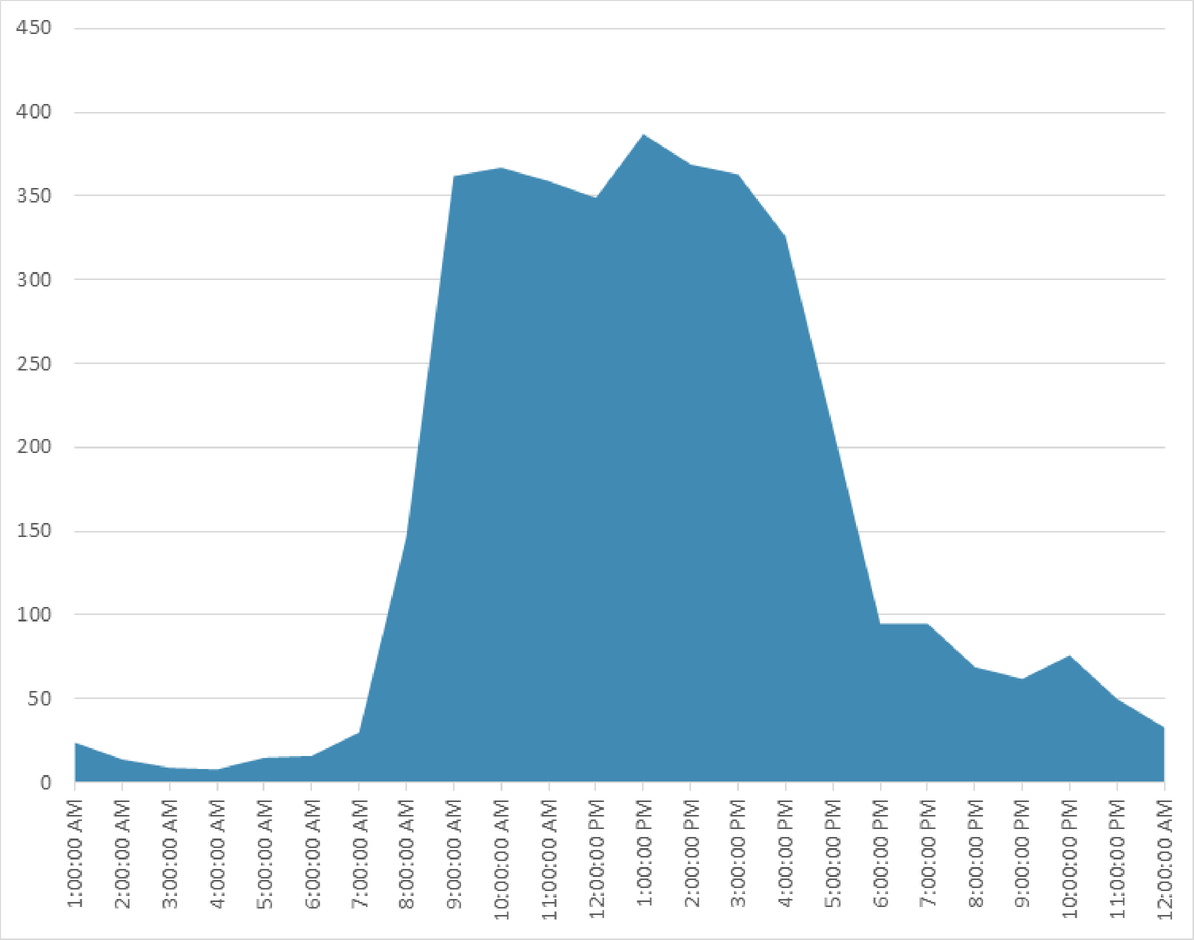

Figure 2 Identity Theft Case Reports by Time of Day

Identity Theft Cases by Victim Age

The 4239 raw data cases approximately corresponded to that many potential identity theft victims. Prior research has argued that a number of age groups are at greater risk of identity theft, however prior evidence has not been consistent. For instance, Anderson (2006) and Copes et al. (2010) argue that identity theft victims are likely to be younger. However, Reyns (2013) argues that identity theft victims are likely to be older. Our evidence shows that while some age groups appear at greater risk of identity theft, all ages can be potential identity theft targets.

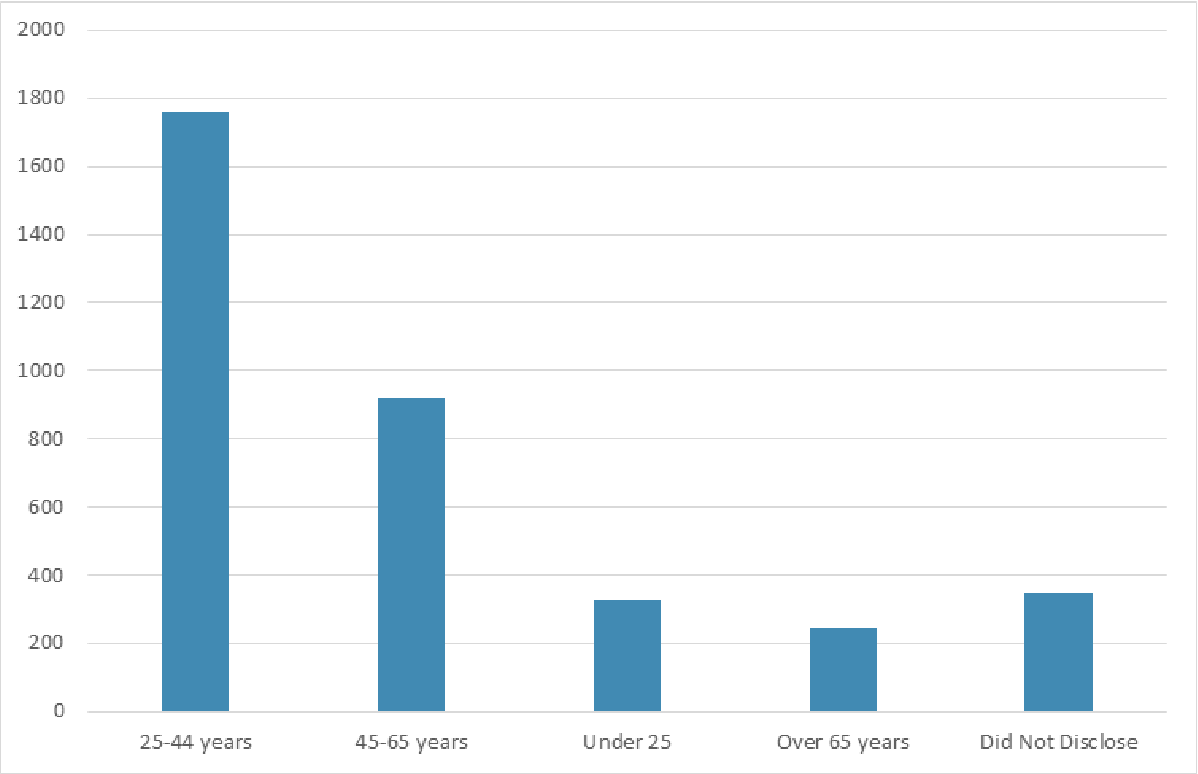

Figure 3 Identity Theft Cases by Victim Age Group

Figure 3 shows the age breakdown of reporting identity theft victims. The largest reporting group was in the 25–44 year bracket. Importantly, however, it must be noted that this age groups is not necessarily the most at-risk group, but rather the group most likely to feature in identity theft incident reports. There are several possible explanations for this finding. First, if this age group is likely to exhibit ownership of at least one piece of technology (more likely to own at least one smartphone, for instance) (Sensis 2016) and they are more likely to be heavy users of technology (Deloitte 2016a) then they may also be more likely to notice when something is wrong with their technology or communications device. This age group also shows strong tendencies toward adopting new services and product offerings (Deloitte 2016b) which therefore may require more frequent presentation of their identity credentials. They may also be more likely to have to provide their identity credentials to service providers with which they have little prior experience. Further, this behaviour means they may also be more likely to deliver their identity credentials to unproven companies, and to have this information shared among companies for the purposes of targeted advertising or service provision.

People under 25 years represented almost 10% of reporting cases. While individuals at this age may be unlikely to possess the financial resources that would ostensibly make them attractive identity theft targets, they might still possess 'clean' bank accounts that could be used for money laundering or other fraud (ALRC 2008). Some youth may also lack the experience to tell the difference between genuine, improper, incorrect and fake requests for identity credentials. Further, because they may possess low incomes, it may be easier to entice them into surrendering their identity credentials with a promise of financial or other incentives in return.

Almost one quarter of reported cases related to individuals between 45 and 65 years of age. Given that individuals in this age group may be more likely to hold numerous identity documents, and to have significant financial resources, it would seem that they are a viable target for identity thieves; that they represent only a quarter of cases suggests that this is not the case. Further work is needed here: in particular, further research is needed into this age group in order to determine whether they are under-reporting their identity theft victimhood, or whether they are legitimately resistant to such attacks.

The smallest group was over 65 years of age with approximately 250 reporting cases in this age group. Prior research has argued that older users are more at risk of online crimes and scams (Holtfreter et al. 2015; Reyns 2013) because they may lack online experience, may be unfamiliar with information technology products, and may be reluctant to report falling victim to a scam. Therefore, it could be argued that this reporting figure is also low.

Identity Theft Cases by Gender

Figure 4 shows the gender breakdown of the identity theft victim responses. The figure shows that approximately 51% of respondents were female, while only 34% of respondents were male (approximately 15% of cases did not disclose their gender). There are two countervailing explanations for this finding. The first is that this finding is consistent with evidence in popular literature that females are more likely to be targeted by identity thieves (Copes et al. 2010). There may be a number of reasons for this likelihood: first, perpetrators may feel that females can be more easily persuaded by a forceful caller (Caspi et al. 1994; Carli 2001); female identity documentation may be more useful than male documentation because females can claim that name changes are as a result of marriage, rather than system error (Herzog, Scheuren, and Winkler 2007); females are increasingly more likely to be guardians of family financial documentation (Westpac 2016); forged female identities may also be more useful in committing an identity theft attack (Wang et al. 2005), and the small amount of available evidence suggests that female identity thieves are more common than male identity thieves (Allison, Schuck, and Lersch 2005; Morris 2010) .

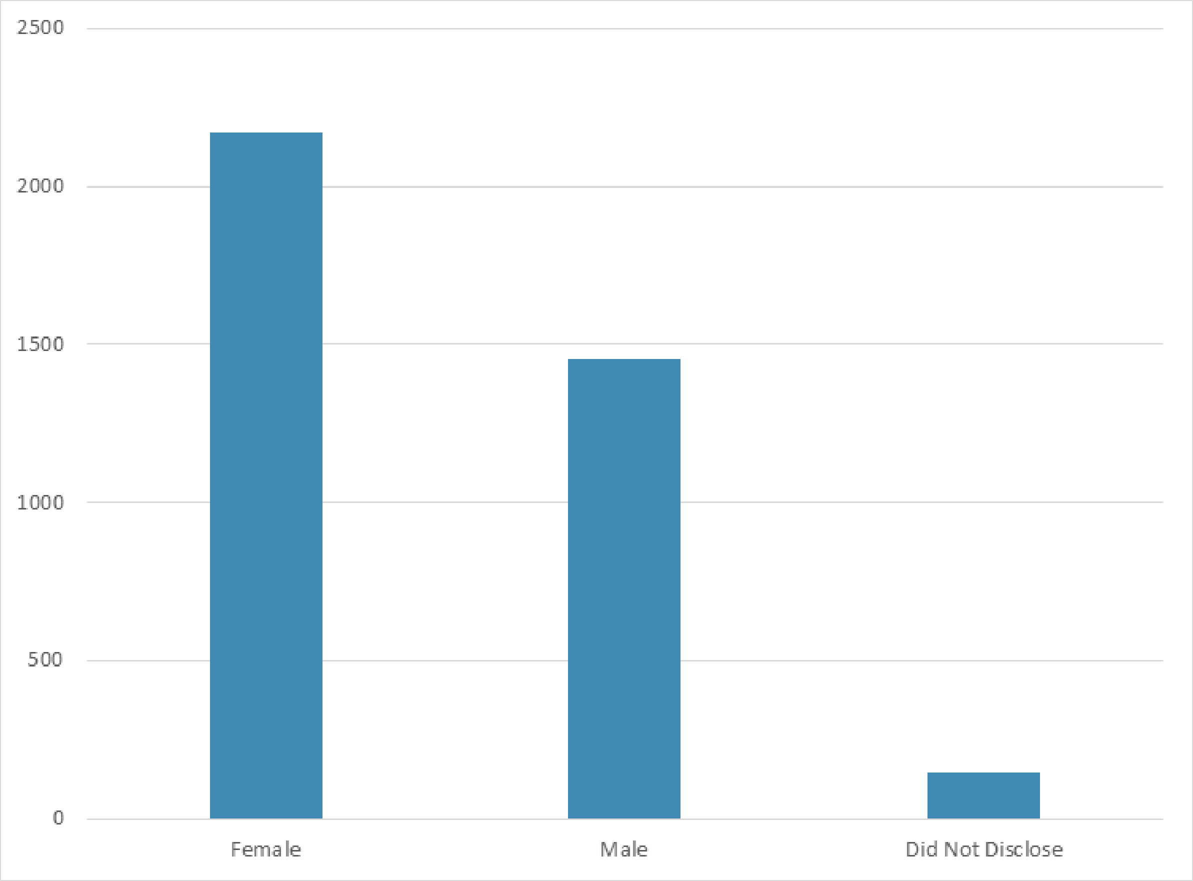

Figure 4 Identity Theft Cases by Gender

However, an alternative explanation may be that females are more likely to admit an identity theft attack, and to subsequently feel comfortable seeking assistance in recovering from the attack. Further, if Australian females in relationships are more likely than males to manage joint bank accounts, it may also be that females are also more likely to be able to detect an irregularity with the family's financial position or identity documentation. In this regard, sharing of financial news and information within the family may provide additional protection against identity theft because it can help to identify weaknesses or compromises in the family's identity portfolio.

Regardless of the explanation, the data suggest that males seem under-represented in the identity theft reporting demographics. Much evidence shows that males are still likely to be earning more money than females (Vogler, Lyonette, and Wiggins 2008), and to retain much decision-making sovereignty even after entering a relationship or getting married (Bartley, Blanton, and Gilliard 2005; Smith, McArdle, and Willis 2010). These factors mean that male exposure to identity theft may be as high as that of females; therefore, it is necessary to better understand how and why there are substantial gender differences in the reporting of identity theft attacks. This data weakness is likely to undermine many analyses of the identity theft problem into the future because it effectively means that a significant but still unknown segment of the population is obscured from understanding.

Identity Theft Cases by Location

Figure 5 shows the breakdown of identity theft cases by Australian state[1], showing the raw number of cases per state. The chart shows that, in raw terms, New South Wales, Queensland and Victoria comprise the largest sources of cases: some 80% of cases come from these three states (a figure approximately reflecting the population figures in these states with respect to the rest of Australia).

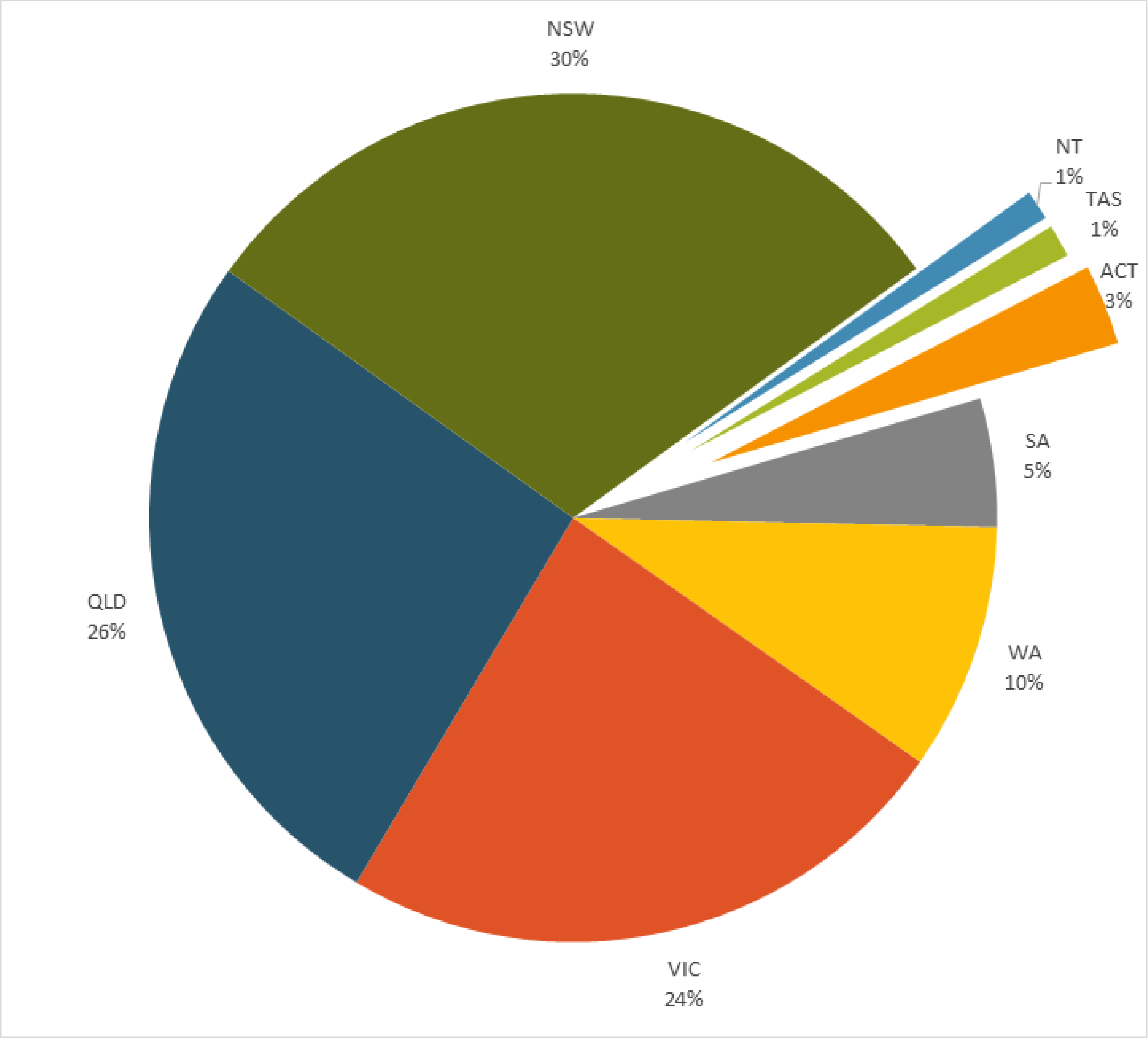

Figure 5 Identity Theft Cases by State

However, in order to understand the true rate of identity theft incidence by state, it is necessary to take the state's population into account, on the grounds that a more populous state is more likely to evidence greater rates of individual identity theft. Figure 6 discounts the number of identity theft cases by each state's population as at 2016 (Australian Bureau of Statistics 2016). This figure portrays a very different picture of identity theft incidence. Here, the two states with the largest incidence of identity theft reporting are Queensland (effectively 16%) and the Australian Capital Territory (ACT) (effectively 23%). Queensland remains well represented, even when taking the state's population into account.

[1] In total, 3352 respondents provided their state.

The ACT remains the largest single location of identity theft reporting, having taken population into account. However, it must be noted that with a population of just 400,000 (Australian Bureau of Statistics 2016), a small increase or decrease in the number of identity theft cases will skew these results somewhat because an increase in identity theft cases results in a larger proportional increase in per capita figures. The Northern Territory, with a population of approximately 244,000 (Australian Bureau of Statistics 2016), would likely see similar phenomena for the same reason.

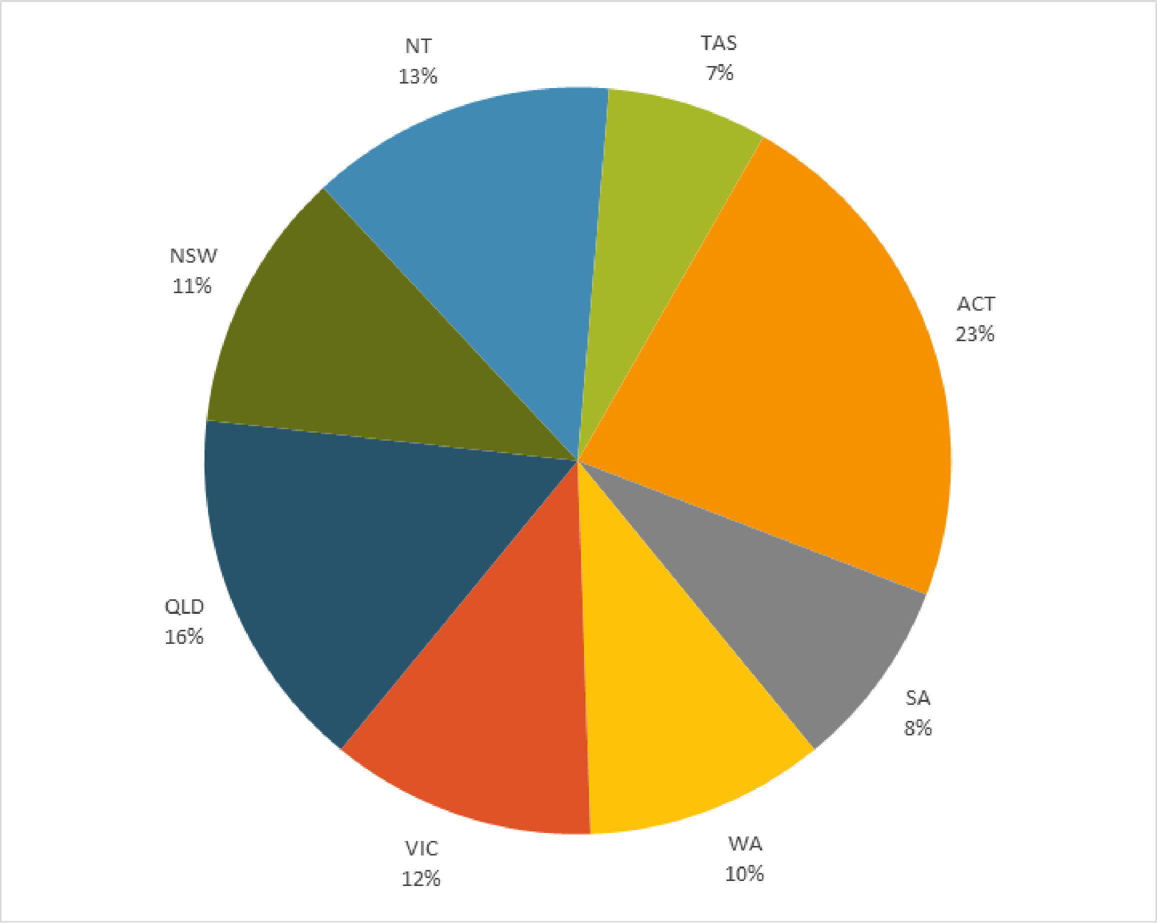

Figure 6 Identity Theft Cases by State (per Capita)

Interestingly, Tasmania and South Australia exhibit the lowest sources of identity theft reporting among the Australian states, when controlling for population. While these states hold similar reporting rates (7% for Tasmania, 8% for South Australia), their population levels are very different (519,000 for Tasmania and 1.7m for South Australia, according to Australian Bureau of Statistics figures).

Further research is needed in these states to understand the variance in identity theft reporting rates. There are a number of possible explanations. South Australia was the first state to enact identity theft laws in 2003 and South Australian government and law enforcement bodies maintain a strong online informational presence for its citizens. Until at least 2008, it was not an offense in most Australian states or territories to adopt or assume another person's identity (Steel 2010; ALRC 2008); as the first state to enact such legislation it could be that they are still reaping the rewards of such legislative control. It may also be that the state's established identity theft control mechanisms provide a suitable alternative avenue for identity theft reporting and redress. Alternatively, it may be that certain types of identity theft avoid this state. Further research is needed to understand this variance.

Identity Theft Victim Gender by Location

Figure 7 shows the breakdown of identity theft victims by gender, presented according to their state. Figure 8 shows a similar analysis controlling for state population. The analysis of gender by state produces a number of interesting findings.

First, in nominal terms, the largest single groups of victims are females in New South Wales, females in Victoria, females in Queensland, followed by males in New South Wales. In per capita terms, the ACT is again salient in having the largest number of female victim reports, followed by the Northern Territory and Queensland. The largest per capita male response is again from the ACT.

Second, it must be noted that in each state, female identity theft reports exceed male reports. Victim gender is most balanced in Victoria, however New South Wales and Western Australia are also quite close. Again, in per capita terms, female respondents outnumber male respondents by more than double (the only state or territory with this property).

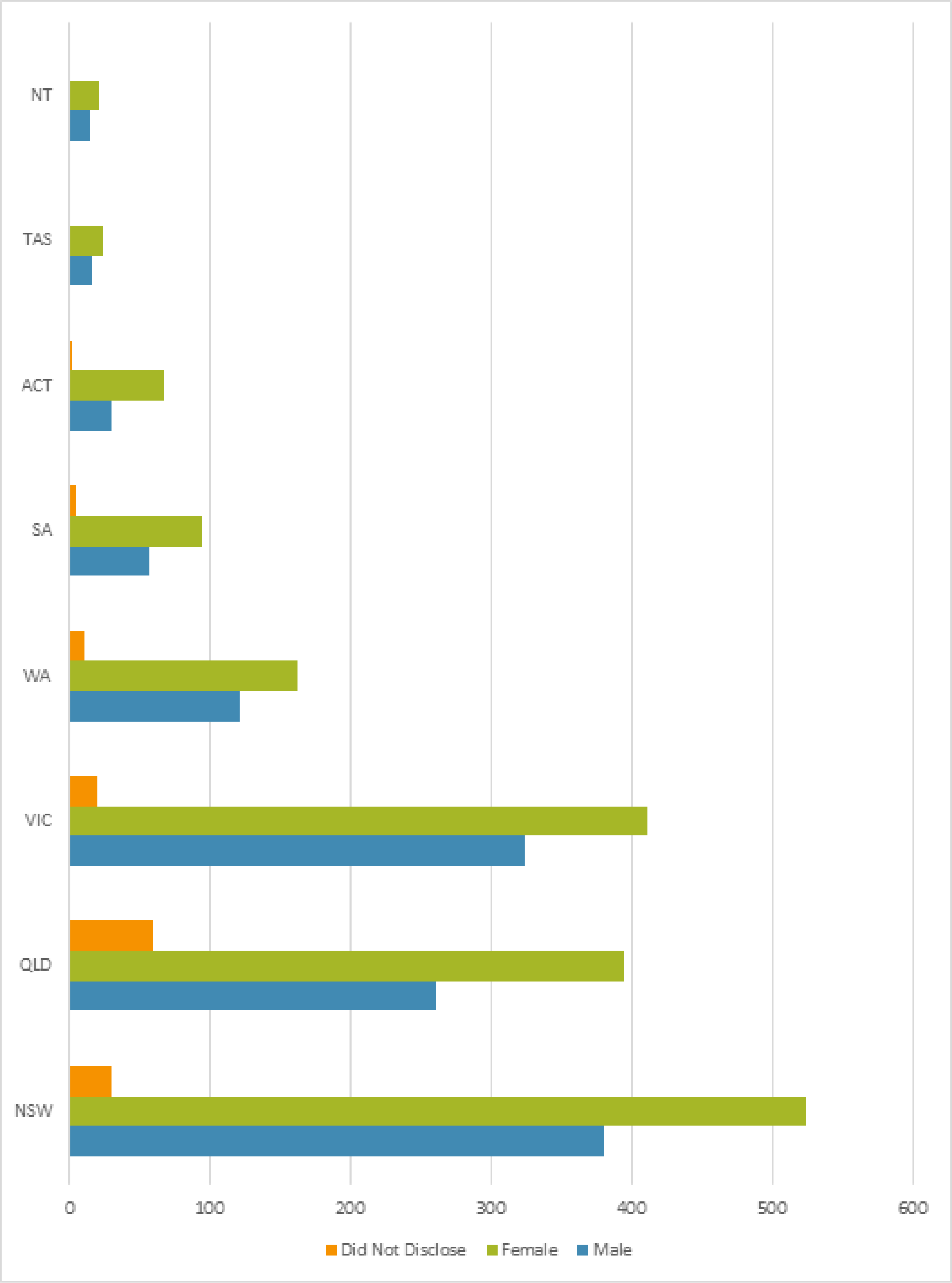

Figure 7 Identity Theft Victim Gender by State (n)

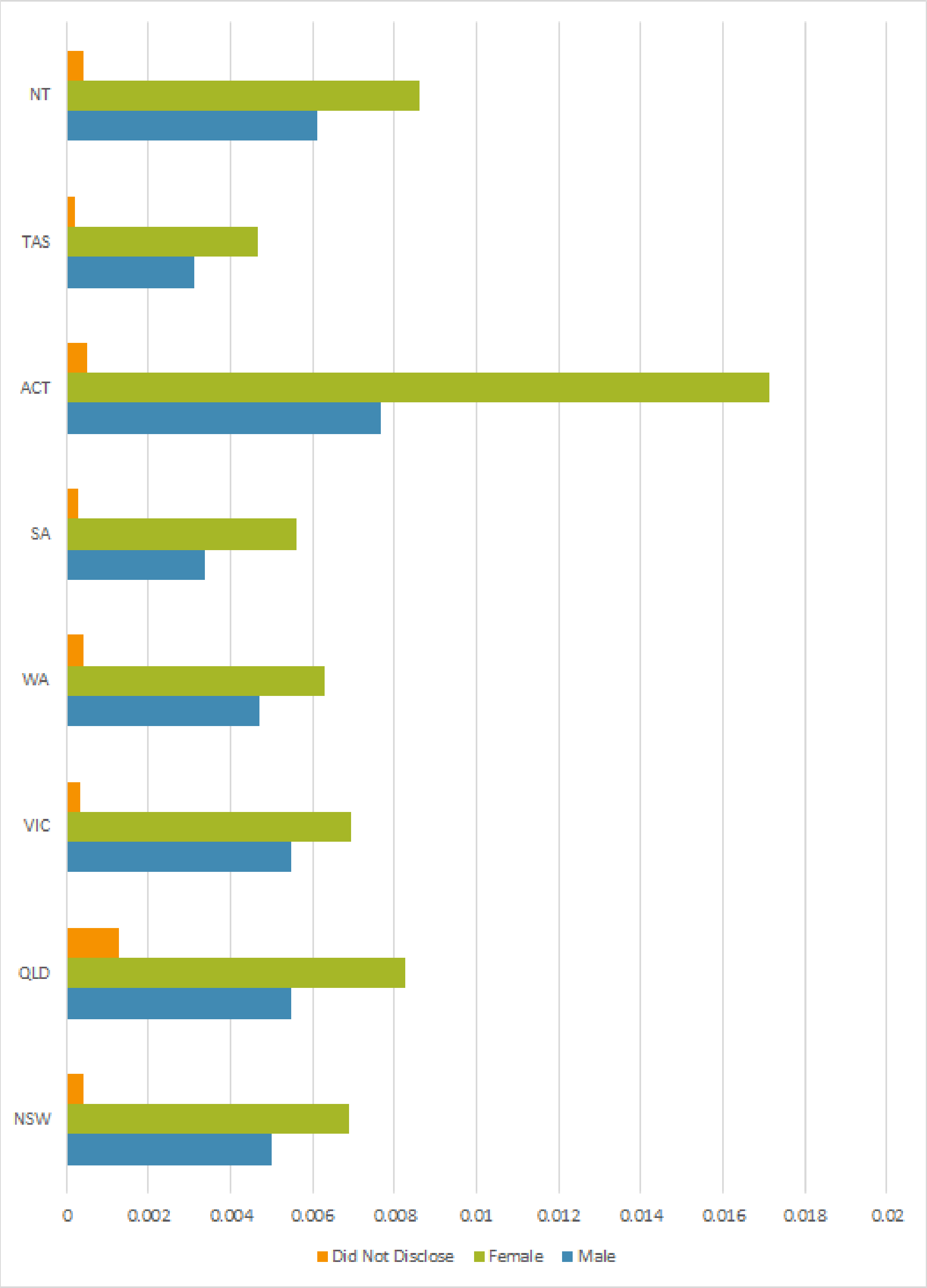

Figure 8 Identity Theft Victim Gender by State per Capita (%)

Identity Theft Victim Age by Location

Figure 9 shows the age breakdown of victims by each Australian state. The figure reveals a number of interesting observations. First, as noted earlier, respondents aged 25 to 44 years of age were the largest group of victims in the entire data set, regardless of state. However, this age group is most strongly represented in New South Wales, at more than double the size of the next largest group (45 to 65 years of age). Taken as a whole, the most frequently reporting groups are the 25–44 age group in New South Wales, followed by the 25–44 year age group in Victoria, and then the 25–44 year age group in Queensland.

Next, respondents aged 45 to 65 years were approximately equally represented in the three largest states of New South Wales, Queensland and Victoria, despite very different representations of respondents aged 25 to 44 years of age. In all states, respondents aged under 25 years are more strongly represented than respondents over 65 years of age. South Australia is the only state in which respondents aged under 25 are equal to respondents over 65 years old. Interestingly, values for the 45–65 year age group were very similar across the three largest states of New South Wales, Queensland and Victoria, suggesting that, as noted earlier, either this group is not reporting adequately, or they are more immune to identity theft attacks.

Figure 10 reveals the age breakdown of victims per capita in each state. Again, a number of interesting phenomena are evidenced. First, proportionally, respondents aged 25 to 44 years are approximately equally represented in the three most populous states, New South Wales, Queensland and Victoria. It is interesting to see this remarkably consistent pattern despite somewhat varied population figures in these states: 7.7 million in New South Wales, 6 million in Victoria and 4.8 million in Queensland (Australian Bureau of Statistics 2016). Western Australia shows a very similar pattern, albeit slightly lower, despite having a population of 2.6 million residents (approximately half that of Victoria).

Next, the figure shows the highest representation coming from the Australian Capital Territory. Here, the number of respondents from the 25 to 44 year age group is almost double that of the most populous states, mentioned above, and is proportionally the largest group in the entire data set. The ACT also shows the largest representation, proportionally speaking, of respondents aged below 25 years of age. This same pattern is also visible among respondents aged over 65 years. While respondents in the 45 to 65 year age bracket are also very well represented in this territory, they are still somewhat similar to Queensland and the Northern Territory.

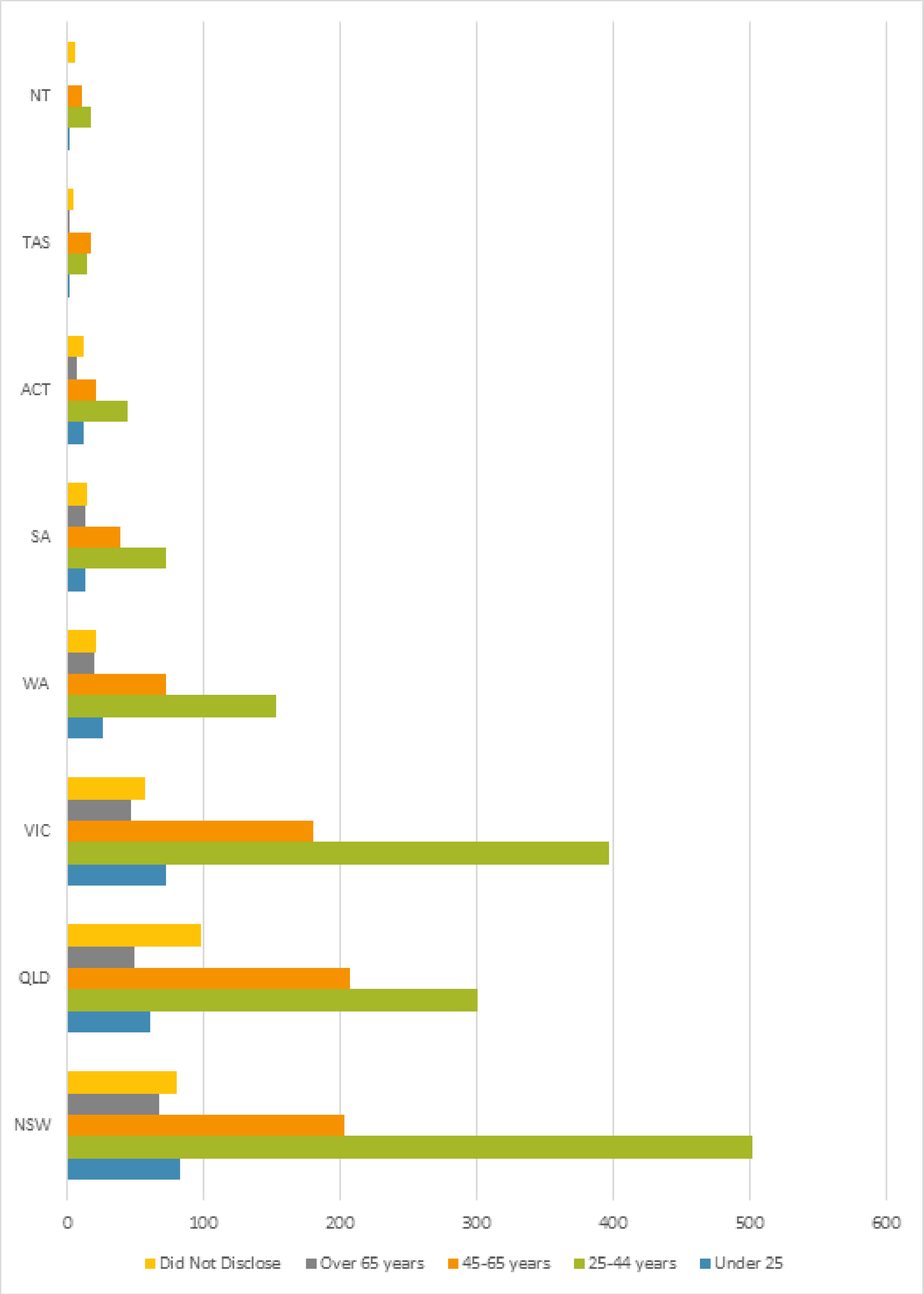

Figure 9 Identity Theft Victim Age by State (n)

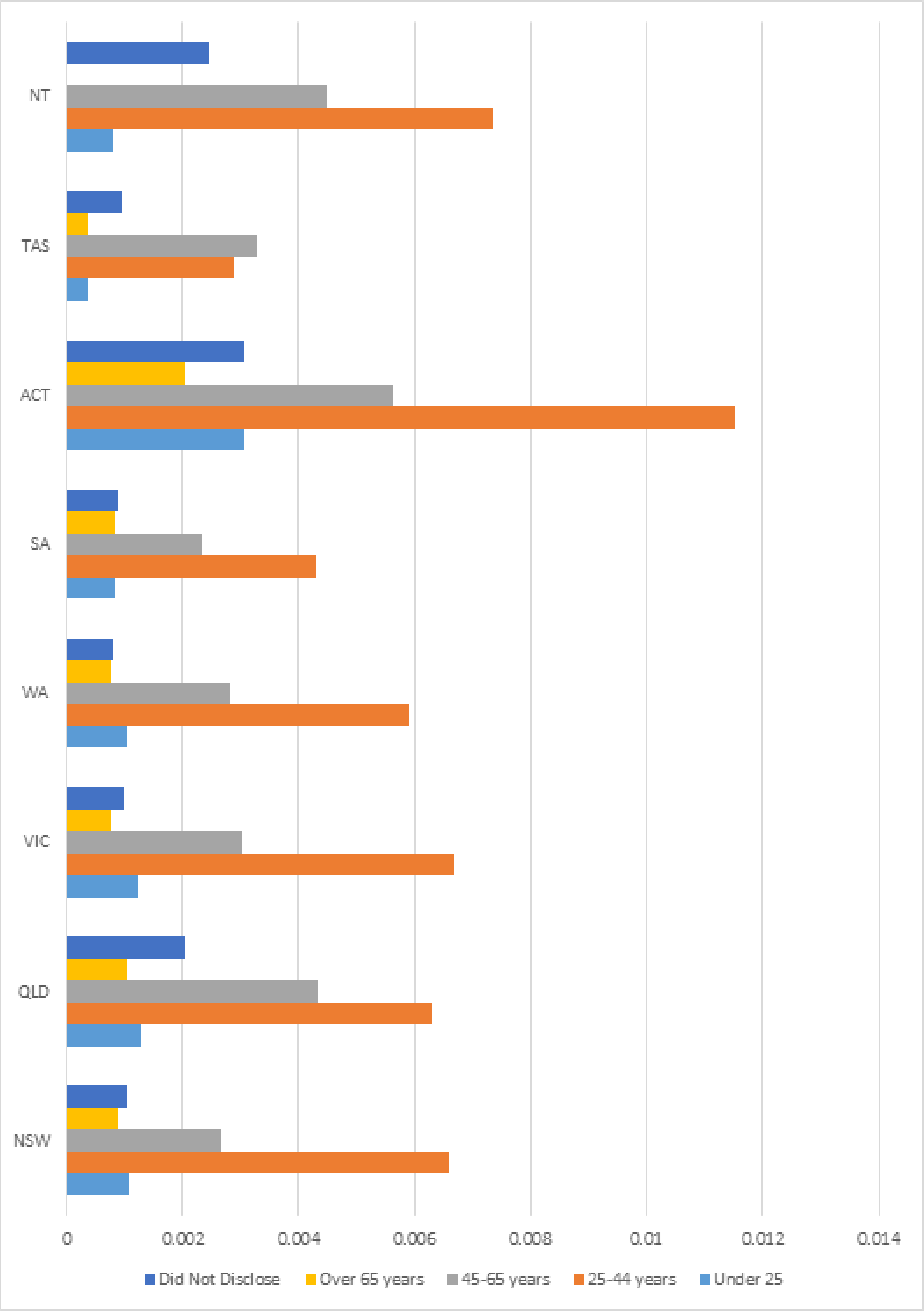

Figure 10 Identity Theft Victim Age by State per Capita (%)

Identity Theft Victim Cultural and Linguistic Diversity

The Cultural and Linguistic Diversity (CALD) category describes those respondents who originate from non-English speaking backgrounds (Sawrikar and Katz 2008). In prior literature, individuals from such backgrounds can be prominent targets for online crime because they may lack the linguistic ability or cultural background to explain and discuss their experiences in interacting online.

In total, 282 respondents (approximately 6%) identified as being from a culturally and linguistically diverse background. This number is quite low: it is likely that this number indicates under-reporting among these groups. There are three major reasons for this opinion. First, as noted above, some prior literature has noted that CALD individuals in Australia can be at greater risk of victimhood for some types of crime (Australian Institute of Criminology 2005; Willis 2011; Shepherd 2016) or may under-report incidences of crime (InTouch 2010; Bartels 2011; Dowse et al. 2016). Second, CALD respondents and other minority groups have historically under-reported in a variety of other surveys. Third, there is a lack of CALD support services in Australia, especially in the areas of online and identity crime and this lack of resources may contribute to confusion about how and where to report such incidents. Fourth, evidence from the Australian Institute of Family Studies notes that some 30% of Australians can be designated as CALD (Sawrikar and Katz 2008); following the state-based evidence presented earlier in this report, it would be reasonable to expect CALD responses to be significantly higher on these grounds.

Of the 282 CALD cases in the data set, 116 (41% of CALD respondents) were male, a slightly larger result than the overall percentage of males (34%) in the data set as a whole. However, 136 (48% of CALD respondents) were female, which is slightly less than the percentage of female respondents (51%) in the rest of the data set.

Figure 11 shows the breakdown of CALD respondents by state. As in previous panels, New South Wales, Queensland and Victoria had the largest representations of CALD identity theft callers. Non-CALD callers appear proportionally lower in Queensland. Figure 12 shows the breakdown of CALD respondents by state, adjusting for state population. Again, the ACT features the largest adjusted rate of CALD respondents in the data set at proportionally more than double the numbers from the next largest state or territory (in this case, the Northern Territory). Notwithstanding the proportional skewness faced by smaller states, the ACT seems over-represented in these CALD statistics, and further research is needed in order to understand the effects at play here.

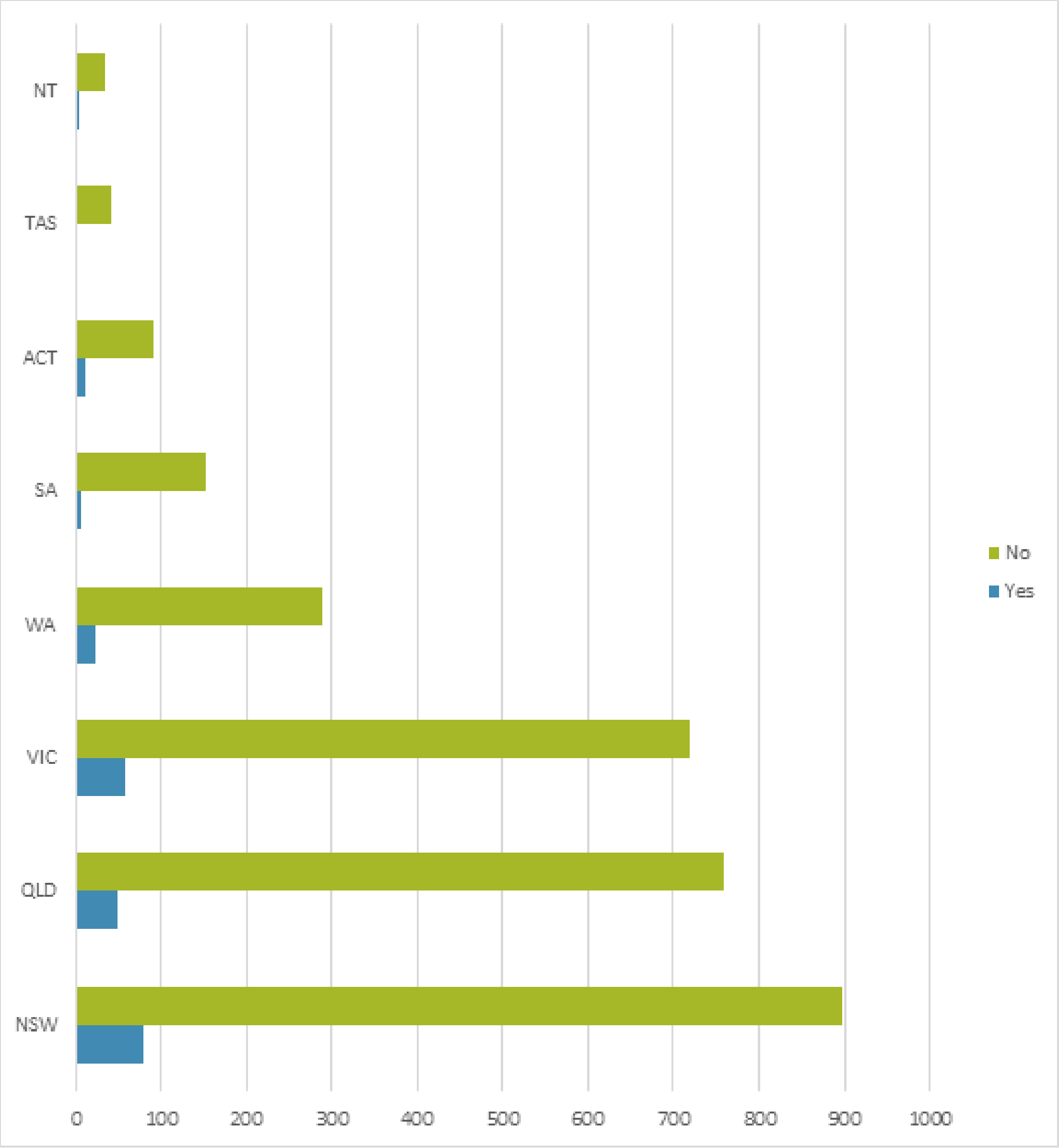

Figure 11 Culturally and Linguistically Diverse Respondents by State (n)

The results for South Australia again show proportionally lower incidences of identity theft reports. As noted earlier in this report, these results may be due to an early legislative lead and stronger governmental and law enforcement response. South Australia features the second lowest CALD reporting rate after Tasmania (despite having approximately three times the population).

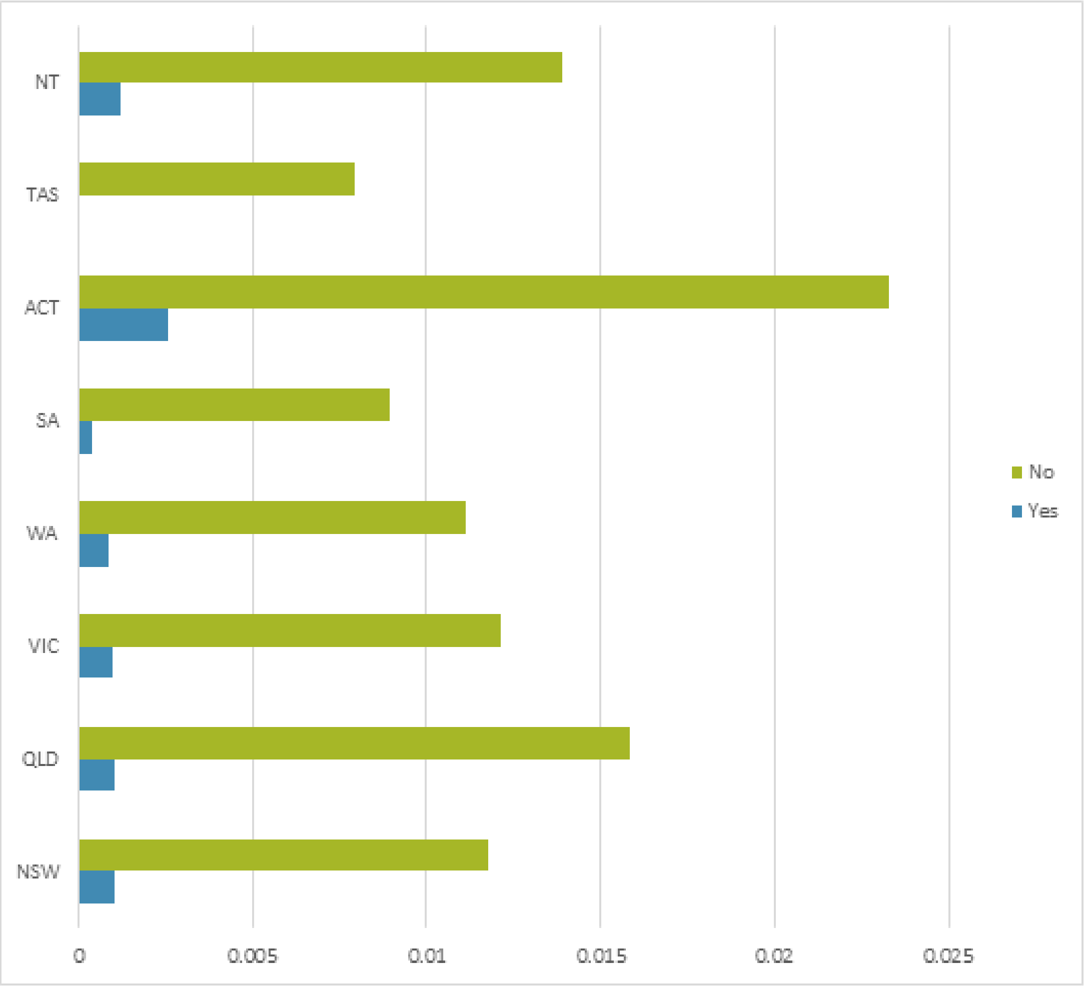

Figure 12 Culturally and Linguistically Diverse Respondents by State per Capita (%)

Identity Theft Attack Demographics

This section of the report analyses the characteristics of the reported identity theft incidents. Analysis in this section is based solely on what the victim volunteered to report during the investigation. Importantly, the victim may be under significant stress, confusion and anxiety following an attack, and may not be behaving rationally; this rationality extends to the quality, accuracy and veracity of the information they provide to an investigator. These effects must be borne in mind when examining these results.

Identity Theft Victim's First Point of Organisation Contact

Figure 13 tabulates the organisations that were first contacted by the identity theft victim. First contact might come in two forms: first, the victim is seeking help and information on how to respond to a particular attack (for instance, in the case of law enforcement); second, the victim is responding directly to an information guardian in order to prevent further damage, or to assess the extent of the attack (for instance, in the case of a bank).

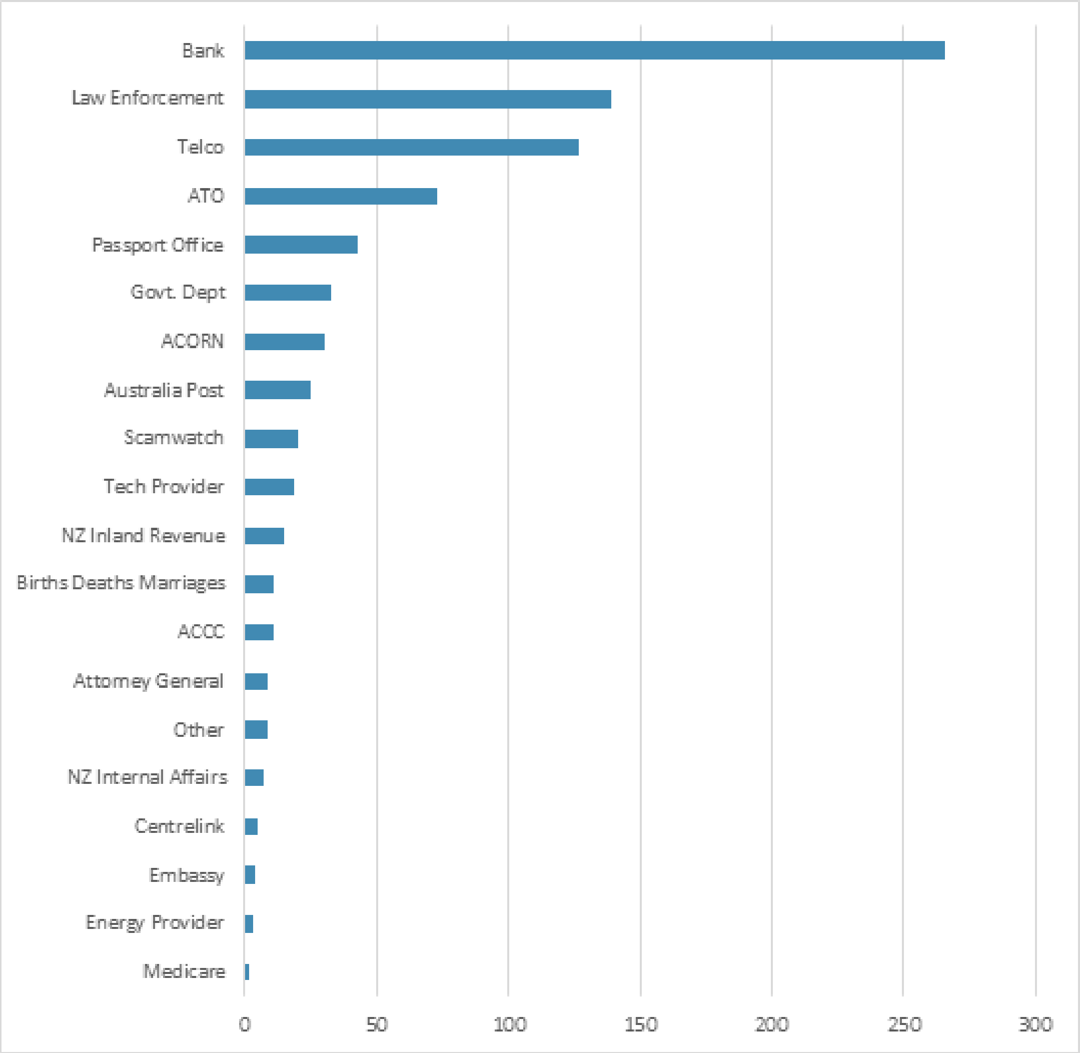

Figure 13 Organisation First Contacted by Victim

Across the data set, first contact was approximately evenly split between public and private organisations. By far the most common first contact was a bank, at almost double the incidence of law enforcement: this would make sense if the victim wishes to establish that their financial resources are safe. However, in these cases, only 113 (4% of customers who contacted a company first, 2.6% of the entire data set) were current customers of the affected organisation. Analysis of the accompanying case notes suggests that victims in these cases were usually calling the bank in order to determine the veracity of claims, evidence or representations, often for new bank accounts or for overdue loan repayments.

Telecommunications carriers were the second most common private sector organisations to be contacted first. Instances of this type of contact related principally to new post-paid smartphone accounts. Often, the stimulus for this first contact in these cases related to an overdue bill that had been sent to the victim's postal address. Again, the victim was often calling the organisation in order to establish the veracity of evidence they possessed.

However, of the top ten organisations contacted first, seven are governmental organisations. This public/private breakdown presents in stark contrast the nature of the institutions that produce and guard the identity documentation used by private citizens: privately, these are banks and telecommunications companies; publicly, they are law enforcement, the Australian Taxation Office and other government departments.

What Identity Documentation was Compromised

Next, the compromised identity documents were tabulated in order to understand what personal identity documents are at risk. In contrast to a physical theft, identity thefts are characterised by a difficulty in knowing exactly what identity documentation items have been compromised in an attack. In cases where a physical identity documentation artefact is missing, the victim may be able to identify the compromised material or indicate that it is missing. However, in the case of digital identity documentation, the victim may not know that the item has been compromised, or may never find out at all.

Figure 14 tabulates the compromised identity theft documents showing figures for the entire group and also dividing by victim gender. This figure shows only those identity documents that the victim has themselves reported as missing or compromised: as noted above, the victim may not know which items have been compromised or accessed. They may also not take into account the effective availability of identity-related information within each document. For example, a passport displays the holder's date of birth and full name, however this figure shows only that the passport itself has been compromised. The reason for this is to illustrate what identity documents are at risk, and not what items of information can be acquired in an identity attack. In addition, practically, analysis along these lines would skew the figure to show that name, address, and date of birth would be the most commonly compromised items of information.

A number of observations can be made. First, the figure shows more than 40 different types of personal identity documentation that have been compromised through the attacks in the data set. The sheer range of identity-related documentation is sobering. These items are at the heart of identity theft, and their acquisition constitutes the major goal of an identity thief. These information documents can be used to create new identities, or to assume another person's identity. Some items, such as a passport, are likely useful on their own for these purposes. However, others, such as an Australian Business Number (ABN) or a car registration number, may be more useful in combination with other types of information.

Second, it can be seen that females are almost always more likely than males to report compromised identity documents; in the case of each identity document, females are more commonly represented than males. As with earlier analysis presented in this report, it may be that females have more identity items compromised, or that females have a different (more, or less accurate) recall as to what items have been compromised (or in the case of physical artefacts, can better observe that a document is missing or has been tampered with). This finding also suggests that identity thieves may be better able to impersonate females when the time comes to apply this stolen identity documentation. Further research is needed here.

Third, the driver's licence is the most popular identity document to be compromised in an attack. A driver's licence is a very useful piece of identification because it features the holder's full name, address, date of birth, signature and a government-sanctioned photograph. Many businesses use the driver's licence as proof of identity, for instance to create an account, to receive a delivery, or to gain entry to a premises. As a result, drivers' licences can also be used to obtain other identity documentation. That this identity document is the most compromised item is hence somewhat remarkable, as the driver's licence requires physical access to the artefact in order to obtain it. The main reason for this finding is likely due to the frequent use of document scanning; subsequent ad hoc analysis of the case notes reveals a large number of victims in this group have kept a scan of their driver's licence on their personal computer, laptop or smartphone, thereby making it considerably easier for an identity thief to obtain this valuable document by targeting these devices directly. In other cases, the victim voluntarily scans the driver's licence and sends the image to an identity thief, who might be masquerading as a bank, utility or telecommunications employee. The gender breakdown for incidents involving this document is also the most even across all identity documents in the data set: males and females seem equally at risk of having their driver's licence stolen, and subsequently reporting it. The passport, the fourth most compromised identity document, is likely to be similar.

Fourth, the most distinct gender difference relates to accesses to bank accounts and credit cards. Here, as with other items, females are more likely than males to report a compromised bank account or credit/debit card. It is likely to be easier for a perpetrator to be able to use these identity items more quickly following an attack: a bank account can be liquidated through bank transfers or ATM withdrawals; a credit card can be used to purchase products online or in a physical retailer, or can be used to withdraw cash at an ATM or EFTPOS machine. Naturally, there is a preference for identity items that can be applied quickly as they afford the perpetrator a lower chance of apprehension.

Fifth, information and communications technology (ICT)-related documentation varied significantly in popularity. The most common ICT item (10th on the list) was login data, comprising a username and password typically for online services such as social media or other websites (but excluding email, which was recorded separately). This mechanism of attack appears to be the most significant ICT-related identity theft threat. Naturally, gaining access to online services can provide a great deal of other information for an identity thief. This access would be even more useful when coupled with access to the user’s own computer, which was listed twelfth. While a victim’s email address was featured high on the list (13th), actual access to an email account was considerably less frequent.

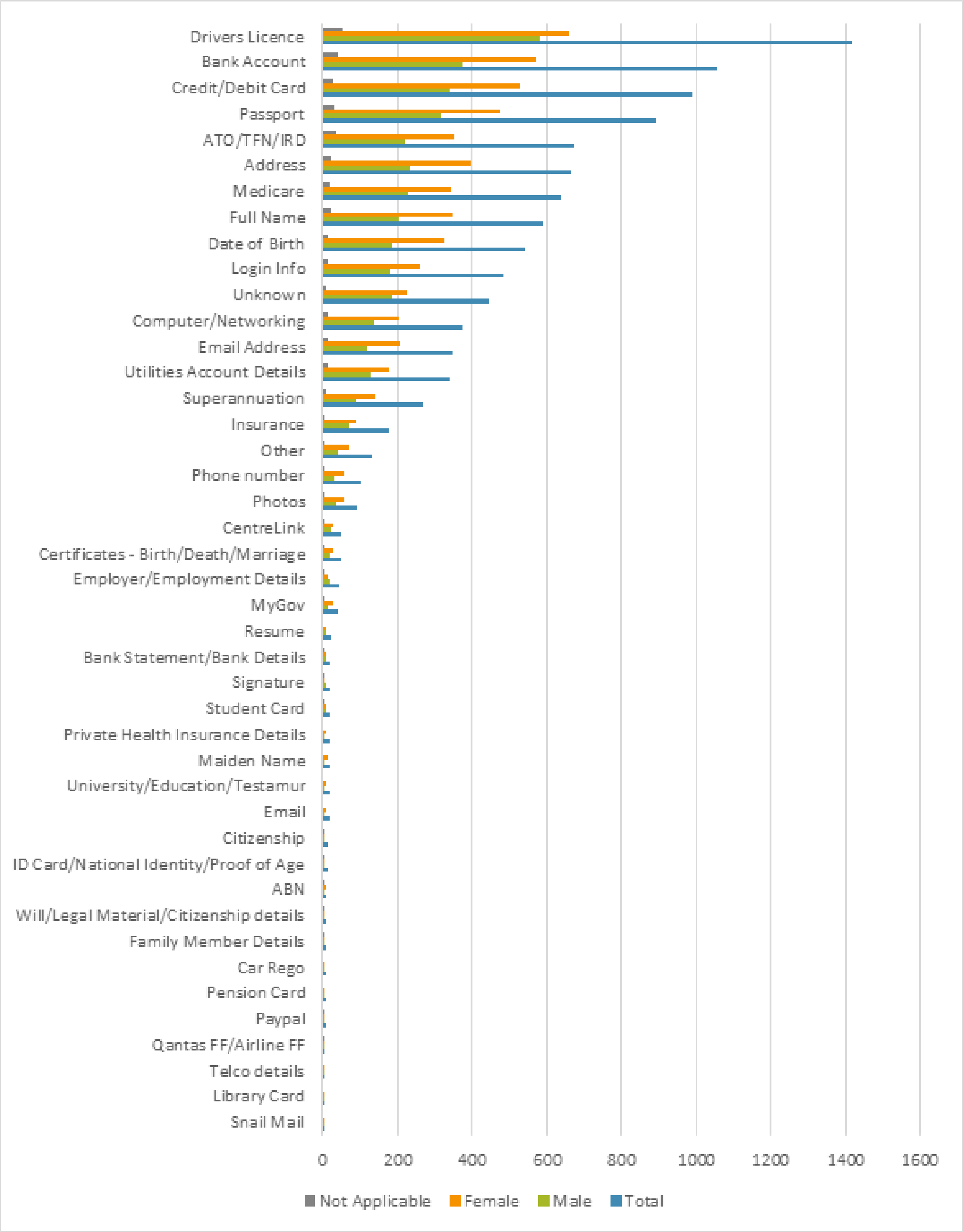

Figure 14 Reported Compromised Identity Theft Documents

Identity Theft Types

In this section, the report provides an overview of the physical method of the identity theft attack, and the logical method. The physical method describes the tools used to reach the victim — in other words, the mechanism of delivery that results in the attacker gaining privileged access to the victim or some aspect of the victim’s life.

Table 1 details the physical attack methods used to instigate an identity theft attack, from the cases in which the victim was able to explain or suggest an attack vector. It is important to note that these data originate from victim reports and recollections and may not be a complete indication of the method used to commence the attack. Further, in some cases, the victim is not able to completely or accurately describe the nature of the attack (especially for highly technical methods and approaches). For ease of reading, the methods have been grouped where appropriate.

The table raises a number of important implications. First, most attack methods involve an information technology or communications vector. To this end, the majority of cases involve communications technology regardless of the type of identity information obtained in the attack. A further 529 cases used a collection of complex identity theft vectors that the victim was not easily able to characterise. These have been classified as ‘Other’ at the time of producing this report while these attack types are under further analysis. A large number of victims did not know how the identity theft took place when submitting their investigation materials. Naturally, it is in the perpetrator's interests to obscure their own identity as much as possible, and it is not surprising that victims were unable to recall or identify the point of weakness.

The telephone ranked as the most common method of commencing an identity theft. While some of these attacks involved phishing (the use of social engineering and confidence techniques to sway the victim's trust and confidence), other attacks simply involved cold-calling without necessarily having prior knowledge of the victim. The telephone featured at approximately double the rate of the next most popular technique, physical document theft. Here, the perpetrator must physically present in order to obtain the victim's identity material for the purposes of later use. Of these, the theft from the household was the most common type of physical theft.

Email, social media (including profile information) and websites were the next most common mechanisms of identity theft. This finding means that of the five most common identity theft attack vectors, four involved communications or information technology. Only physical theft did not depend on ICT use to complete the attack.

Interestingly, computer viruses and data breaches did not feature heavily in the identity theft reports, despite their media popularity. This finding may suggest that common safeguards against these vectors may be working (e.g. anti-virus software, strong passwords, etc.).

Table 1 Types of Identity Theft Attack

Category	Method	n	Total
Other			***529***
Unknown			***476***
Telephone	Telephone	428	***462***
	Telephone - Phishing	34	
Theft	Theft - from unknown source	140	***252***
	Theft - from household	48	
	Theft - from letterbox	25	
	Theft - from person	21	
	Theft - from vehicle	18	
Email	Email	147	***185***
	Email - Phishing	38	
Social Media			***179***
Website	Website - Shopping	77	***169***
	Website - Scam	63	
	Website - Job Application	13	
	Website - Travel Visa	7	
	Website - Romance/Dating Scam	4	
	Website - Competition/Survey	3	
	Website - Auction	1	
	Website - Pop-up	1	
Lost documents			***128***
Face-to-face	Face to face – known to victim	23	***89***
	Face to Face – unknown to victim	66	
Job Application			***38***
Cyber Stalking	Cyber Stalking - known to me	13	***26***
	Cyber Stalking - not known to me	10	
Virus			***22***
SMS	SMS/Text Message	15	***19***
	SMS/Text Message - Phishing	4	
Data Breach			***19***

The Purpose of the Attack

In this section, the report presents analysis of what identity thieves did once they had acquired the identity documentation. After securing access to the victim's identity, the attacker undertakes a variety of attacks. Table 2 shows the number of these attacks cited by victims. The table reveals that financial gain, while among the most common, is most definitely not the only purpose of an identity theft attack; also among the attack types are impersonation attacks, often targeting the victim's reputation either via telephone or online, and account attacks, whereby the victim's online or telecommunications accounts are accessed.

Broadly, of the 4240 cases in the data set, 373 cases (8%) reported not knowing of any adverse outcomes following the attack. Explanations for this finding include the possibility that some instances were cases of false alarm, or that the perpetrator had second thoughts or was apprehended prior to executing a subsequent attack, or that the perpetrator was unsuccessful in using the identity credentials (possibly because they were prevented from doing so at the intended site of the crime, e.g. a bank or telecommunications company). It is also possible that the perpetrator had simply not yet had the opportunity to commit further crimes, or was waiting on acquiring further information, or had somehow successfully gone undetected. An implicit result of this finding is that approximately almost two thirds of suspected identity theft cases result in identifiable adverse outcomes for the victim.

Of the remaining cases, the adverse events which subsequently took place ranged from access to bank accounts, taking control of investments (including superannuation), obtaining social services via government providers and a variety of other outcomes. For ease of summary, we initially classified these outcomes into three broad groupings. First, 'financial' cases related to the acquisition or control of financial outcomes, such as banking and credit cards. Second, reputational cases related to undermining the victim's character by compromising, controlling or otherwise influencing the victim's relationship with other people. Third, technological cases related to compromising, controlling or destroying the victim's information and communication technology tools or services such as passwords, computer login details or smartphone accesses (it is important to note that most technology-related cases involving technological outcomes included a communications component.

Table 2 Purpose of the Attack

Attack Purpose	n
Accessed bank account	562
Credit card	447
Mobile	407
Stolen money	382
Don't know	373
Asked for money	270
Created bank account	254
Created a telecommunications account	194
Opened online account (incl. social media)	192
Acquired personal loan	171
Impersonated email	165
Impersonated to others to damage reputation	163
Manipulated social media	109
Tax return	102
Used telecommunications account	102
Ported mobile phone	82
Locked victim out of accounts	79
Redirected mail	69

Attack Purpose	**n**
Accessed superannuation	46
Falsify police information	41
Obtained investments	40
Rent house	39
Medical benefits	31
Obtained social services	27
Injected malware	17
Energy utility account	16
Injected virus	13
Accessed online payment account	12
Injected keylogger	11
Impersonated for non-monetary purposes	8
Accessed government accounts	6
Injected ransomware	3
Contacted business clients	1
Established a business entity	1

Identity Theft Detection

Table 3 shows the frequencies of methods used to detect the identity theft attack. The majority of identity theft cases were detected by the victim themselves: most identity thefts are still discovered by the victim, usually as the crime is in progress, or afterwards. This means that the victim really only becomes aware of the crime when other services or service providers are disrupted or encounter an anomalous event (such as being unable to place a call from their smartphone, or receiving a visit from an asset repossessor. Hence the direction of investigative effort is usually from the victim towards other services or service providers.

In 84% of cases, the individual victim was the first person to discover the potential compromise. The remaining 16% of cases were detected by another business (131 cases), a bank (253 cases), a public utility (45 cases), a credit bureau or debt collection agency (60 cases), law enforcement (47 cases), or a friend or family member (12 cases).

However, the mechanism of this detection is still unknown. Further work is needed to understand how victims detect such threats, and then the mechanisms that they use to determine whether a threat is worth reporting.

In some cases, self-detection may involve the victim being aware of anomalous activity through vigilant checking of their accounts or services. In other cases, the self-detection is more passive (and might be better termed 'discovered'). The fact that self-detection is so popular increases the importance of understanding how victims recover from identity theft attacks, particularly given that these victims may have very intimate understanding and knowledge of how the identity theft was carried out. A deeper understanding of this knowledge is likely to improve future detection methods.

Because service disruption is a key detection event in most identity thefts, it is possible that service providers are unable to detect an identity theft event because they cannot tell a legitimate service disruption from an illegitimate service disruption. One explanation for this observation relates to how service providers deal with customer profiles: if they are used to seeing each customer as a portfolio of potential actions and activities, then it becomes difficult to determine a real activity from a fabricated activity.

Table 3 Methods of Identity Theft Detection

Detection Method	n
Self	3592
Bank or Financial Institution	253
Another Business/Agency	131
Police and Law Enforcement	47
Utility	45
Debt Collection	43
Member Organisation	20
Credit Bureau	17
Family member/Friend/Acquaintance	14
Media Data Breach Alert	13
Other	5

Duration of the Identity Theft Attack

It is difficult to assess the duration of the attack, for various reasons. First, analysis of the time taken to detect and act on a suspected identity theft compromise is challenging. On average, 43 days elapsed between when the victim first discovered the suspected identity theft, and when they called IDCARE for assistance. However, this figure is not necessarily a true indication of the contact events. First, in 2439 cases (57%), the victim contacted IDCARE on the same day that they noticed the potential compromise. A further 613 cases (14%) contacted IDCARE within two days of discovering the potential compromise. In total, approximately 84% of cases contacted IDCARE within a week of the potential compromise.

Inconsistent detection methods, and the fact that most detection is by victims themselves, mean that identity theft reports do not always clearly identify the time at which the attack took place. Second, some identity thefts require a long time to enact and it can be difficult for a victim to correctly recall the date at which the attack first began. Third, identity thefts may proceed along non-linear lines, such that a successful first attack may eventually give rise to successful subsequent attacks: an attacker may come to better know their victim and may subsequently enact the specific attack types that are likely to be most successful. An attacker may also later identify a use for earlier identity documentation.

The date data were split into three categories. These were the elapsed time between when the fraud was thought to have begun, and when it was discovered; the elapsed time between when the fraud was discovered and when the victim called IDCARE; and the elapsed time between when the theft was thought to have begun and when the victim called IDCARE. Table 4 shows the relative frequencies of these three time periods.

We first examined the time elapsed between when the theft was thought to have begun and when it was discovered. In approximately 47% of cases in this category, the victim discovered the theft on the day it occurred. Unsurprisingly, approximately 84% of victims then also reported the identity theft on that same day. However, only 20% of victims both discovered the theft and reported it on the same day. In 80% of cases, there was a delay in either detecting or reporting the theft. The intervening period can be explained through various factors: the customer didn't know that IDCARE existed, the customer was still entertaining alternative explanations for the potential compromise, the first point of contact was tardy in their response, and others.

A substantial number of cases took longer than a year to detect, and some 96 cases (approximately 3% of cases) took over a year to report the theft once detected. The longest observed period was 16 years. These delays emphasize the issue that identity theft is not a straightforward fraud: victims may yet doubt their own evidence, or may have other reasons for not wishing to disclose the nature of the theft, thus hampering investigations. As a result of these figures, the overall calculation of reaction times could be heavily skewed.

Table 4 Duration of the Identity Theft Attack

Days	**From Began To Discover**	**From Discover to Call**	**From Began To Call**
0	1371	2442	571
1	316	418	447
2	123	193	195
3	78	142	157
4-7	206	281	374
8-14	142	151	226
15-21	97	84	131
22-36	126	88	161
37-72	110	79	161
73-100	61	42	92
101-200	96	72	148
201-300	41	39	68
301-400	39	26	47
400+	110	70	185

Perpetrator Relationships Involved

In some cases, the data provided some insight into the nature of the perpetrator of the identity theft. Importantly, it must be noted that not all cases yielded sufficient insight into the identity of the attackers; further, it is possible that there is an inherent bias among those cases that were able to identify the attacker. It must be noted that the analysis below is tentative, and may not provide a complete picture of identity theft perpetrators in all cases.

Clearly, in many cases, the victim has little to no understanding of, or insight into, who committed the identity theft. Table 5 illustrates the expressed relationships when the victim was able to explain them. The table shows that 268 reporting victims were able to identify a relationship with the perpetrator. This table hence provides a view that is a subset of the identity theft cases where the victim had sufficient understanding of the case that they could identify the attacker.

Table 5 Perpetrator Relation to Victim

Relation	n
Employer/co-worker/colleague	178
Ex-partner	40
Relative	19
Friend	17
Partner	9
Individual related to ex-partner	5

In only 26 cases, the victim knew the perpetrator. In the vast majority of the rest of the cases, there was no prior relationship between the victim and the perpetrator. Of those cases where a prior relationship had existed, 12 cases involved a partner or ex-partner, two cases involved a work colleague and four involved a family member. The message from this finding is clear: in almost all cases, the perpetrator does not need to know who the victim is in order to steal their identity.

As shown in the table, the most commonly cited relationships to the victim were the victim's employer or co-worker. Some 66% of victims who knew their attacker were also employed by or with them. The workplace can provide an environmental intimacy where staff relax their vigilance over their identity documents or information. Further, the workplace is also a venue where employee identity information may be recorded and frequently accessed (e.g. for the purpose of payroll or emergency contact reasons). Some workplaces may lack the governance to correctly and effectively prevent co-workers from accessing each other's sensitive identity information or documentation (e.g. support documents, payslips, places of residence, dates of birth, etc.). The nature of identity theft in the workplace is not well understood in the wider research literature.

The rest of the identified relations were of a social or family nature, the most common being the ex-partner. This finding highlights the potential damage arising from identity theft as a weapon of revenge or domestic violence.

In all cases, the recorded data regarding known relationships highlights the importance of familiarity with the attacker. This is not to say that identity theft requires a close relation between the thief and the victim; rather, identity theft attacks can come from a range of attack sources, and an effective counter-attack strategy must take this into account, at the victim and attack theatre levels.

Impersonations to the Victim

Table 6 illustrates the entities that were impersonated to the client in order to convince them to relinquish their identity documentation. The table features 878 cases. In a number of cases, the attack was ‘unsupervised’, in that the victim did not need to be present or complicit in order for the attack to proceed.

The most common identity represented to the victim was that of a government officer. Government officers comprised approximately half of the cases where a victim could recall the impersonation and the theft was reported. Government officers are likely to be an effective cover for a perpetrator because of the ubiquity of certain government services making it easier for a perpetrator to discover and exploit weaknesses in a potential victim.

The second most common impersonation vector was a telecommunications provider. These cases often involved a perpetrator calling regarding an existing telephone account or a payment to an account. Technology providers were also well represented in this group. These callers often highlighted a fabricated problem or security issue with the potential victim's device or computer, and then compelled them to grant the perpetrator access (either remotely or physically) in order to repair the problem.

Table 6 Identities Impersonated to the Victim

Impersonation Vector	n
Government department	309
Telecommunications provider	209
Technology provider	98
Other financial institution	86
Bank	63
Australian Taxation Office (ATO)	53
Employer/co-worker	20
Business other than employer/contractor/co-worker	15
Utility	15
Friend	6
Relative	4

Impersonations of the Victim

Table 7 shows the breakdown of whom the perpetrator subsequently impersonated the victim to, once the perpetrator had acquired the identity details. The table shows that the perpetrator most commonly impersonated the victim towards a bank. This impersonation vector is likely to give the perpetrator the fastest access to the victim's financial resources, thus resulting in a quicker payoff.

The second most popular impersonation vector was the telecommunications carrier. This type of impersonation might relate to acquiring a new account or device (e.g. a new smartphone), or it might form part of a mobile number porting scheme where the victim's smartphone account credentials are transferred to another provider and device thereby granting the perpetrator access to mobile banking and other services, such as two-factor authentication (2FA) which in turn is used to access a range of other services.

Interestingly, while a government officer was the most common impersonation vector to a victim at the outset of the attack, the same position featured in only 11% of victims who knew or could report to whom they had been impersonated.

In total, the three most common impersonations of the victim were the government officer, the telecommunications provider, and the bank. In sum, these three vectors accounted for 94% of cases where a victim was subsequently impersonated to another party (and was able to identify the fact).

Table 7 Identity Impersonations of the Victim

Impersonation Target	**n**
Bank	506
Telecommunications carrier	427
Government department	134
Utility	21
Other financial institution	19
Friend	12
Social media	8
Relative	4
Co-worker	3

Victim Recovery Demographics

In this section, the report analyses the available evidence regarding the victim's ability to recover. The most pressing issues in an identity theft are to prevent further damage and restore financial reality as quickly as possible: clearly, investigative resources must be devoted to these ends. However, longer-term emotional damage is likely to be more challenging to repair. There is very little insight in the wider research literature regarding the restitutional processes. Hence, in this section, the report will detail the initial victim responses regarding the identity theft attack, possibly providing a foundation for further work in this area.

Victim Justification Responses

The data yielded insight on 160 identity theft victims and their reactions to the identity theft attack. Figure 15 shows the breakdown of these justification responses. Of these 160 victim statements, the most common reaction was the expression that they were normally so careful in managing their personal, financial or communications affairs. The second most popular reaction was that the request for identity documentation appeared to be completely genuine (to this end, approximately 78% of responses related to the concept of sounding or appearing official). Clearly, the appearance of authority is likely to compel a potential victim to follow a perpetrator's instructions, and to willingly surrender their identity documentation.

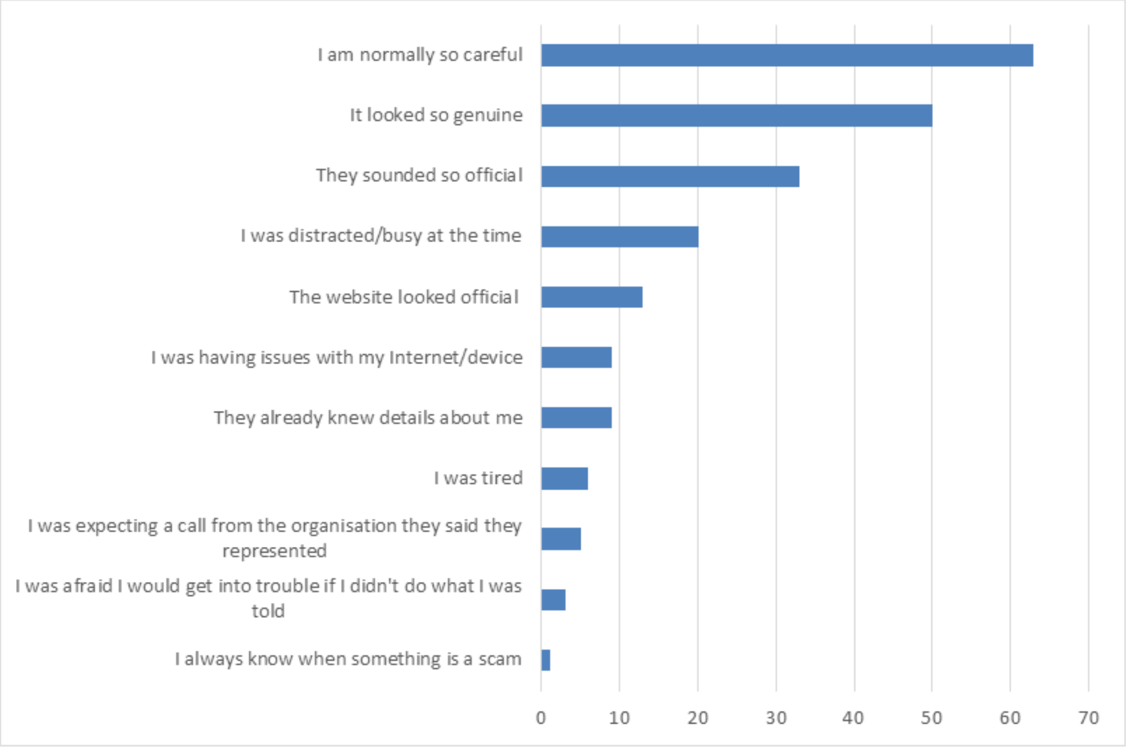

Figure 15 Classification of Victimhood Justification Responses

Victim Emotional Responses

In total, 272 victims provided emotional responses, and some signalled more than one emotional response. Figure 16 shows the breakdown of these emotional response signals. The most common emotional response was the feeling of 'stupidity', mentioned in 28% (approximately one quarter of cases in this group). Respondents also signalled that they felt 'silly' or 'angry'. Taken in sum, these results show the overwhelming negative emotional effect brought about by an identity theft attack.

The feeling of stupidity may come from the victim's perception that the attack itself was either not complex (in other words, there were clear or obvious warning signs that were not merely visible in hindsight) or that the attack exhibited some complexity, but that the victim themselves aided the perpetrator in completing the attack.

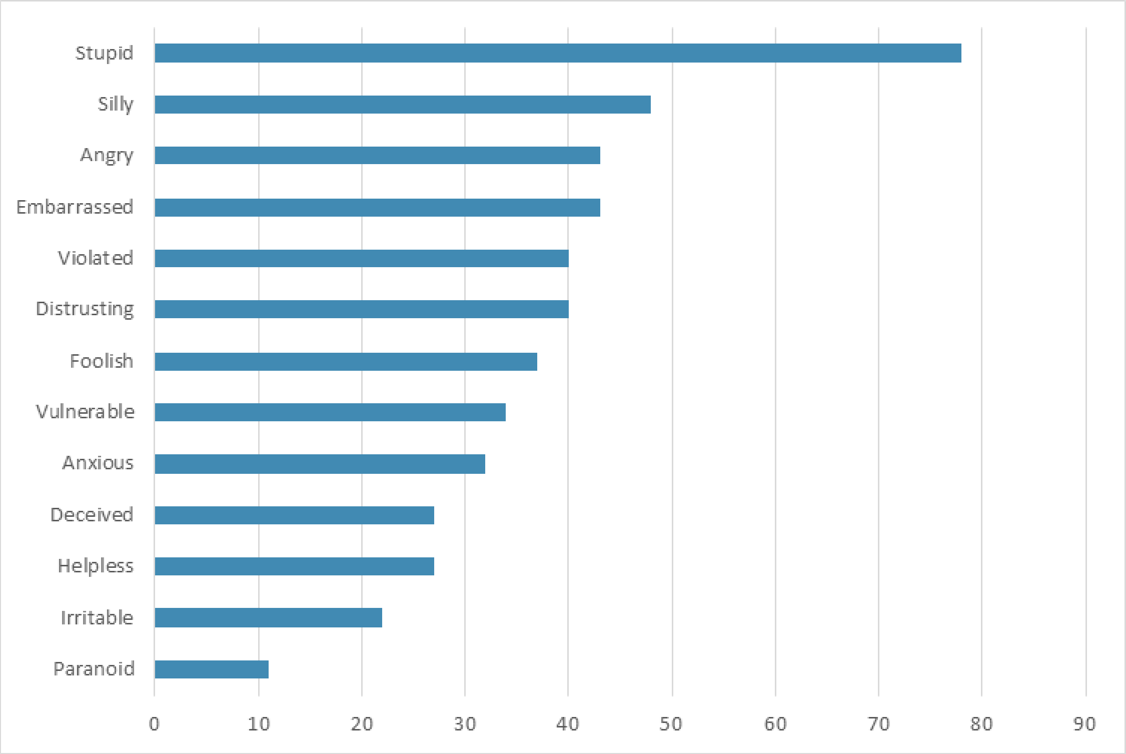

Figure 16 Classification of Victim Emotional Response Signals

Steps Taken to Recover

The available evidence provides some insight into those steps that the victim had already taken to begin restitution of the identity theft attack. These initial steps are tabulated in Table 8. The most common step was to report the attack to law enforcement, with a slightly smaller number reporting the attack to their bank or another government agency. Approximately half (44%) of those cases that cited an initial step fell into this grouping.

Only 7% of victims volunteered that they had since changed their computing practices as a result of the attack. This figure may indicate that victims believe that their computing practices are already sufficiently secure, that they do not know how to improve the security arrangements of their computing environment, or are otherwise unaware that the attack was facilitated through these measures.

As noted previously, the relative effectiveness of these initial steps remains uncertain. There is likely to be some benefit to further educating and supporting both actual and potential victims of identity theft, with further research into the effectiveness of these actions.

Table 8 Initial Victim Recovery Steps

Recovery Procedure	**n**
Reported to police	367
Reported to bank	316
Reported to other government agency	284
Cancelled credit/debit cards	161
Reported to telecom	119
Reported to credit report agency	118
Changed computer practices in some way	112
Reported to other victim / impersonated entity	26
Obtained counselling	17
Cancelled scheme	1

Synthesis

To this point in the report, the analysis has illustrated raw frequencies. However, solely focusing on raw frequencies does not give a complete picture of the effective incidence of identity theft. For this to occur, we need to take the damage of the identity theft attack into account. Also, analysis so far has focused on univariate analyses of the data. However, in order to understand identity theft processes, it is necessary to understand the relationships between variables.

In this section, the report graphically models the relationships between a number of key variables in the data set, in order to shine additional light on identity theft processes.

The following visualisations are represented using alluvial diagrams. This visualisation technique was selected because it favours ease of data presentation and interpretation. In contrast to more traditional data classification techniques, such as a decision tree, the alluvial diagram supports ‘many to many’ relationships that might appear naturally in the data. The technique is also well suited to visualising structural relationships in large, unstructured data sets (Rosvall and Bergstrom 2010).

In an alluvial diagram, groups of data are represented in blocks, and the magnitude of the relationship between these groups of data is represented using streams or flows; the 'stream' of data in this sense is analogous to the flow of water in a river as it splits and merges. The size of the block indicates the magnitude of the relevant relationship in the data.

Each graphic controls for a particular scalar variable (in this case, the dollar amount taken, or the days taken to detect the attack). Each graphic models only the data that has been reported by the victim in its raw form. Further, in order to improve ease of interpretation, missing variables have been omitted in most cases.

Identity Theft Type, Notification and Attack Purpose by Amount Taken

Figure 17 shows the relationship between the types of identity theft attack, the way in which the victim discovered or was notified about the attack, and the purpose of the attack, controlling for the dollar amount taken in the attack. The figure shows a number of relationships.

First, a substantial number of victims do not know or cannot explain how the attack first took place. It is in the attacker's interest to conceal their mechanism of exploitation, and for this reason many victims do not discover that they are under threat. In most cases where the victim does not know the route of the attack, they themselves detect the attack. Further, most such self-detections involve accessing the victim's bank account. This relationship hence means that banks have little information, from the victim's perspective, for diagnosing the cause and flow of events in the attack.

Next, social media is the next largest source of attacks, when factoring the dollar amount stolen. The majority of these cases are detected by another business—in some cases, the social media provider itself, however this may be another business that the victim or the perpetrator has done business with. Again, the vast majority of cases detected by another business involve the perpetrator accessing the victim's bank account. In cases where an identity theft attack was undertaken by way of the victim's lost documents or through a cyber stalking incident, most such cases were detected by the victim's bank or other financial institution. Controlling for the dollar amount taken in the attack, incidents involving the telephone were almost universally detected by the victim themselves. In cases where the victim lost money, these typically involved access to the bank account or a credit card, and came from attacks involving social media, cyber-stalking and the telephone.

Attacks involving other types of dollar loss, such as manipulating social media, acquiring a personal loan, or obtaining investments were significantly less frequent.

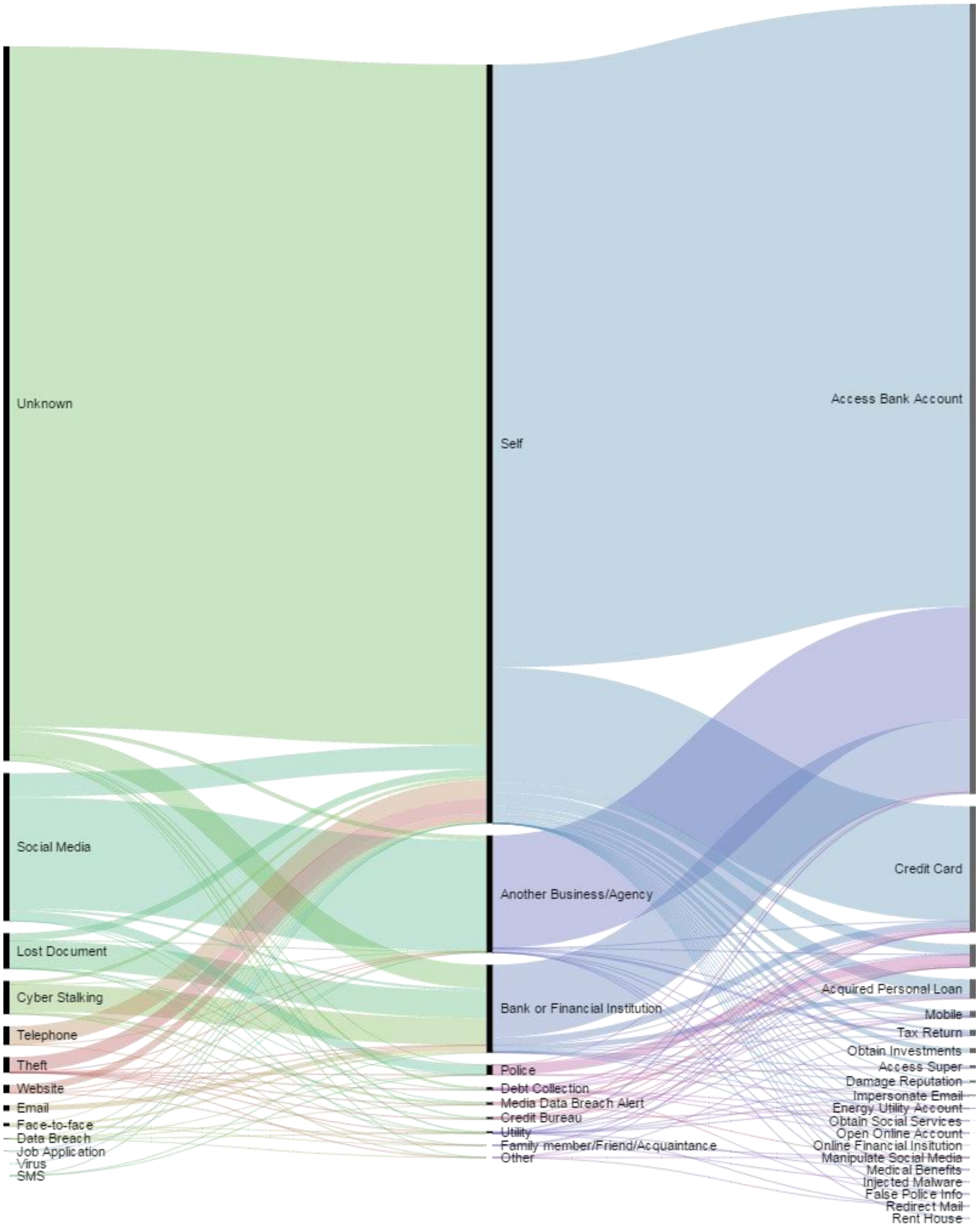

Figure 17 Identity Theft Type, Notification and Attack Purpose by Amount Taken (n=1336)

Identity Theft Type, Gender and Attack Purpose by Amount Taken

Figure 18 shows the relationship between the type of identity theft attack, the victim's gender, and the purpose of the attack, controlling for the dollar amount taken in the attack. The figure shows several important relationships. As shown in the figure, a large number of victims could not explain the source of the attack. However, male victims were more likely to be unable to recall or identify the source of the attack. Only slightly more than half of female victims were unable to identify the source of the attack, when controlling for the dollar amount lost.

The vast majority of social media attacks were conducted on female victims. A comparatively small number of social media attacks were undertaken on male victims. This does not necessarily mean that females are at greater risk than males of such attacks, however there does appear to be a systematic gender bias in these social media results. The figures for lost documents also illustrate an interesting gender difference, in that the majority of lost document cases are reported by female victims.

By contrast, incidents of cyber stalking are more likely to be reported by males (it is important to note that the data does not provide a complete picture of the gender of the stalker, nor, in most cases, other identity details regarding such perpetrators).

While theft of documents appears reasonably evenly spread between both genders, gender differences manifest again with regard to the subsequent purpose of the attack. Both genders are reasonably evenly distributed when the case involves accessing a bank account. However, controlling for the dollar amount taken, females are substantially more strongly represented in the case of credit card fraud.

Identity Theft Type, Number of Attacks and Attack Purpose by Amount Taken

Perpetrators do not always execute only one attack, however for the purposes of the analysis in this report, we have taken the first attack made by the perpetrator. Figure 19 shows the relationship between the type of identity theft attack, the number of attacks undertaken by the perpetrator, and the purpose of the attack, controlling for the dollar amount taken in the attack.

The data shows that a substantial number of victims who cannot identify the source of the attack are likely to witness at least one attack (and likely two attacks). The bulk of these attacks, as suggested by previous analysis, result in bank account accesses and credit card use.

The bulk of attacks arising from social media, cyber-stalking and the telephone result in only one reported attack. A small number of cases result in up to six different types of attack.

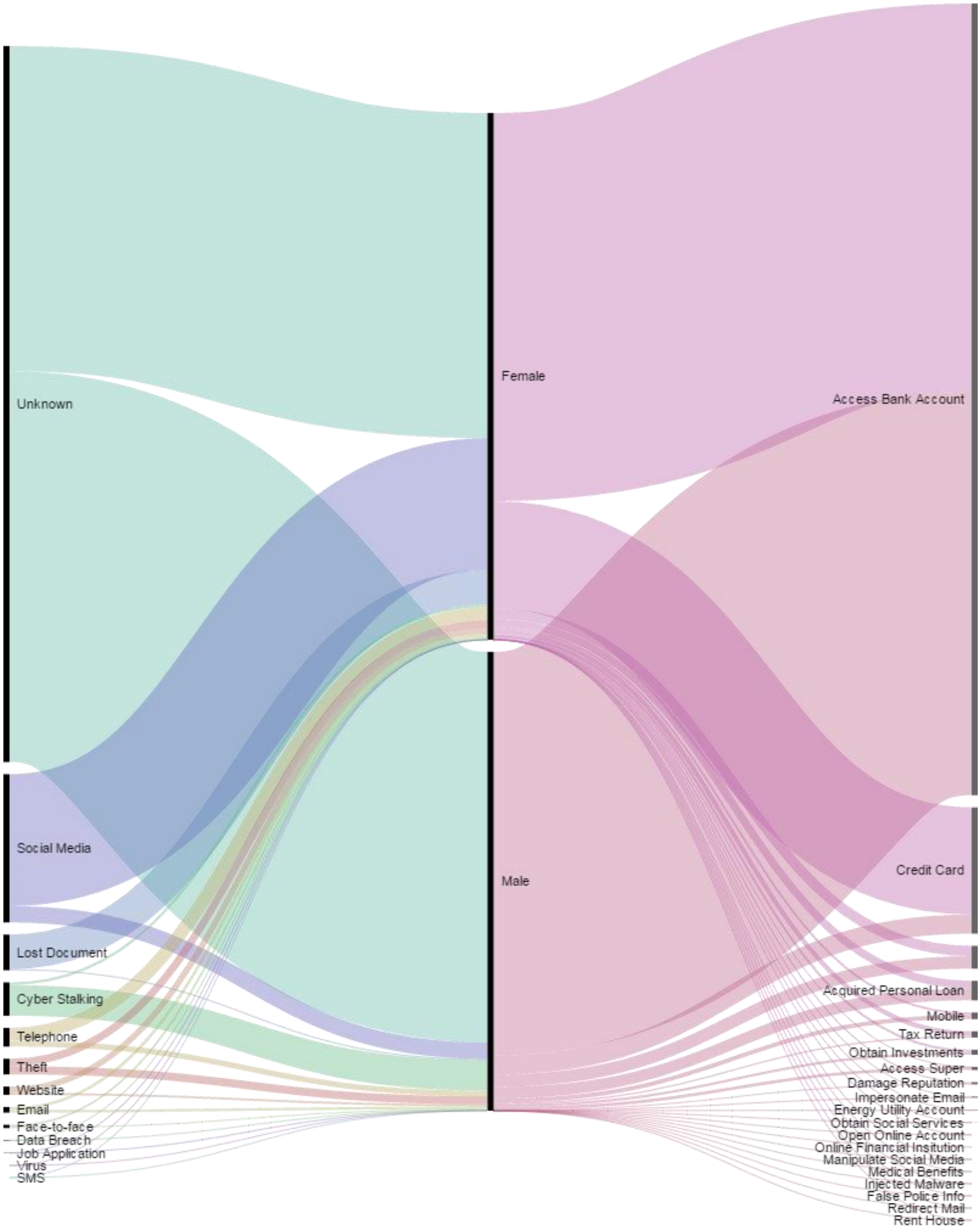

Figure 18 Identity Theft Type, Gender and Attack Purpose by Amount Taken

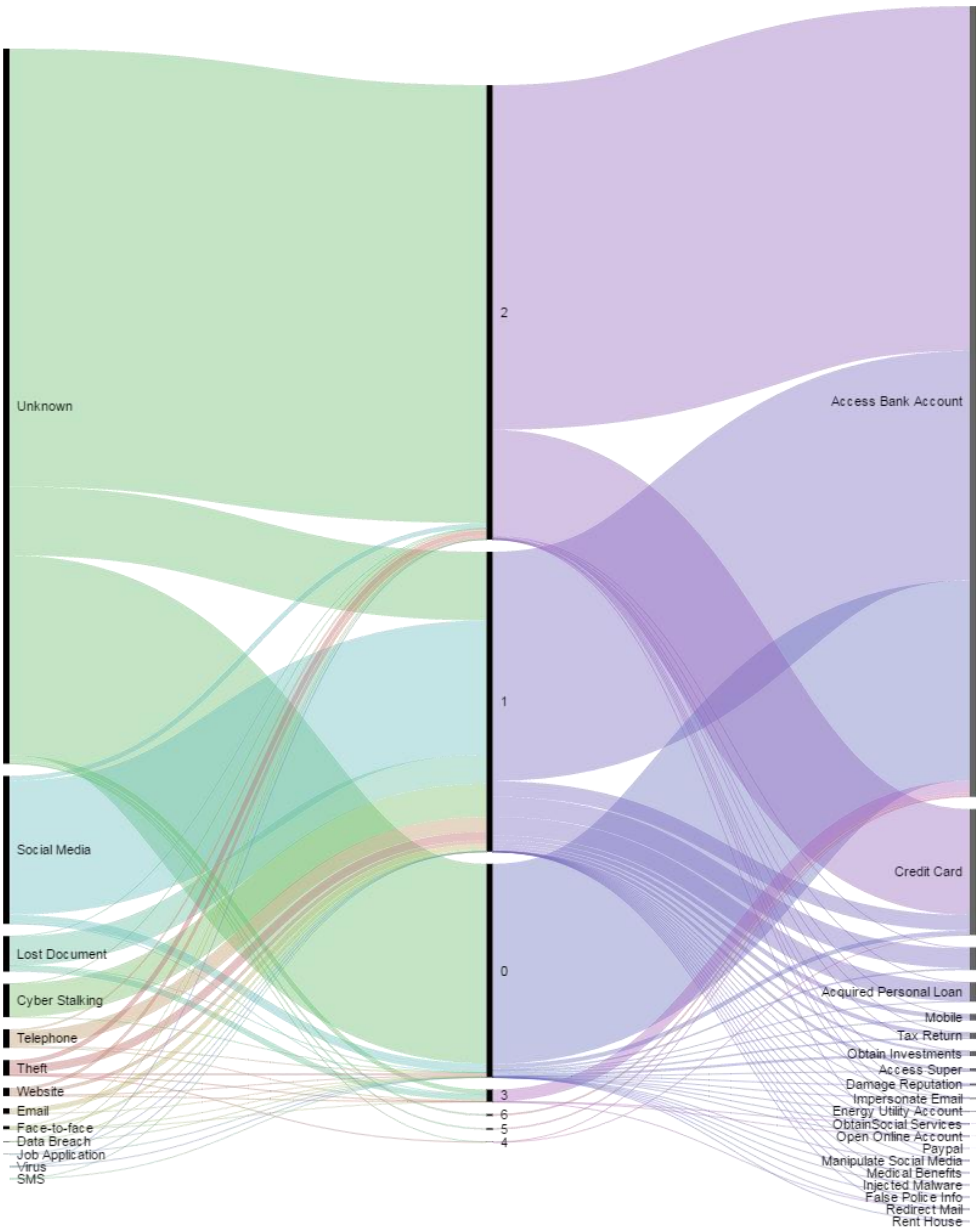

Figure 19 Identity Theft Type, Number of Attacks and Attack Purpose by Amount Taken

Gender, Age Range and Notification by Amount Taken

Figure 20 shows the relationship between the victim's gender, their age group and how the attack was detected, controlling for the dollar amount taken in the attack. The figure shows several main relationships.

First, male victims comprise the majority of victims in the 45 to 65 years and under 25 years brackets, when controlling for dollar loss. However, females comprise almost the entirety of the over 65 years bracket and a substantial portion of the 25 to 44 years bracket, controlling for dollar loss. This finding reinforces the notion that gender plays an important but not fully understood role in the identity theft problem. Females may be more vulnerable in the over 65 years bracket, or are more likely to be able to report a loss.

With regard to detection, the bulk of cases were detected by the victim, however, attacks that were detected by another business or agency were almost solely for victims in the 45 to 65 years age bracket. This element is in contrast to detections by a bank or financial institution, which was approximately evenly split between genders, when controlling for dollar loss. One possible explanation for this finding is that older individuals cease patronage of some businesses as they age: as this happens, businesses stop being able to detect fraudulent access of their accounts. This finding reinforces the idea that older individuals face a greater threat of identity theft than younger individuals because they are less integrated in other commercial systems (and hence do not experience the benefit of a third party monitoring their affairs).

Finally, victims over 65 years were almost entirely detected by themselves. Only a small number of these cases were detected by other means. It is likely that the social engagement concerns affecting older individuals also extend to threats from identity theft. Further research is needed in order to understand whether programs to boost social engagement among older individuals also in turn yield benefits to ameliorating that identity theft threat.

Notification, Number of Attacks and Attack Purpose by Days Elapsed

Figure 21 shows the relationship between the method by which the identity theft was discovered, the number of attacks and the purpose of the attack, controlling for the number of days elapsed between when the victim believed the attack to begin and when the attack was discovered. For ease of understanding, this figure focuses only on those cases where the identity theft was not detected by the victim themselves. The figure shows a number of relationships.

The figure shows that a little more than half of instances of identity theft involved only one attack (or, at least, the identity theft was discovered before a subsequent attack could be carried out). The bulk of cases involving only one attack were detected by a debt collection agency, another business or agency, and a bank or financial institution. Almost all cases detected by a utility and approximately half of cases detected by a credit bureau also fell into this category. The most common attack purpose arising from that single attack targeted the victim's mobile device, when controlling for the days elapsed since the attack began. It is possible that the perpetrator intended to target the victim's mobile device for the purposes of mobile number porting, in preparation for other subsequent frauds.

The figure shows that a small number of cases involved no perceptible attack - in other words, the victim's identity details had been apprehended by a perpetrator, but the perpetrator had not yet been able to mount a successful attack (of which the victim was aware by the time they had reported the case to IDCARE). While these cases may exhibit different prophylaxis properties to other cases, it would be necessary to conduct further investigation into these cases to determine whether a later identity theft attack eventually took place (and nature of the ensuing outcomes).

The next largest group of numbers of attack were detected by debt collection agencies and other businesses. In the main, these attacks involved accessing a bank account, credit card, impersonating via email and obtaining other social services.

A number of cases involved more complex attack profiles, comprising multiple attacks. Interestingly, cases detected by credit bureaus exhibited a degree of polarity: the analysis shows that cases detected by credit bureaus either involved only one attack, or seven attacks (most of which involved accessing a bank account). Similarly, in cases when a perpetrator was able to access a victim's superannuation account, between six and eight attacks took place, and most such cases were detected by the police.

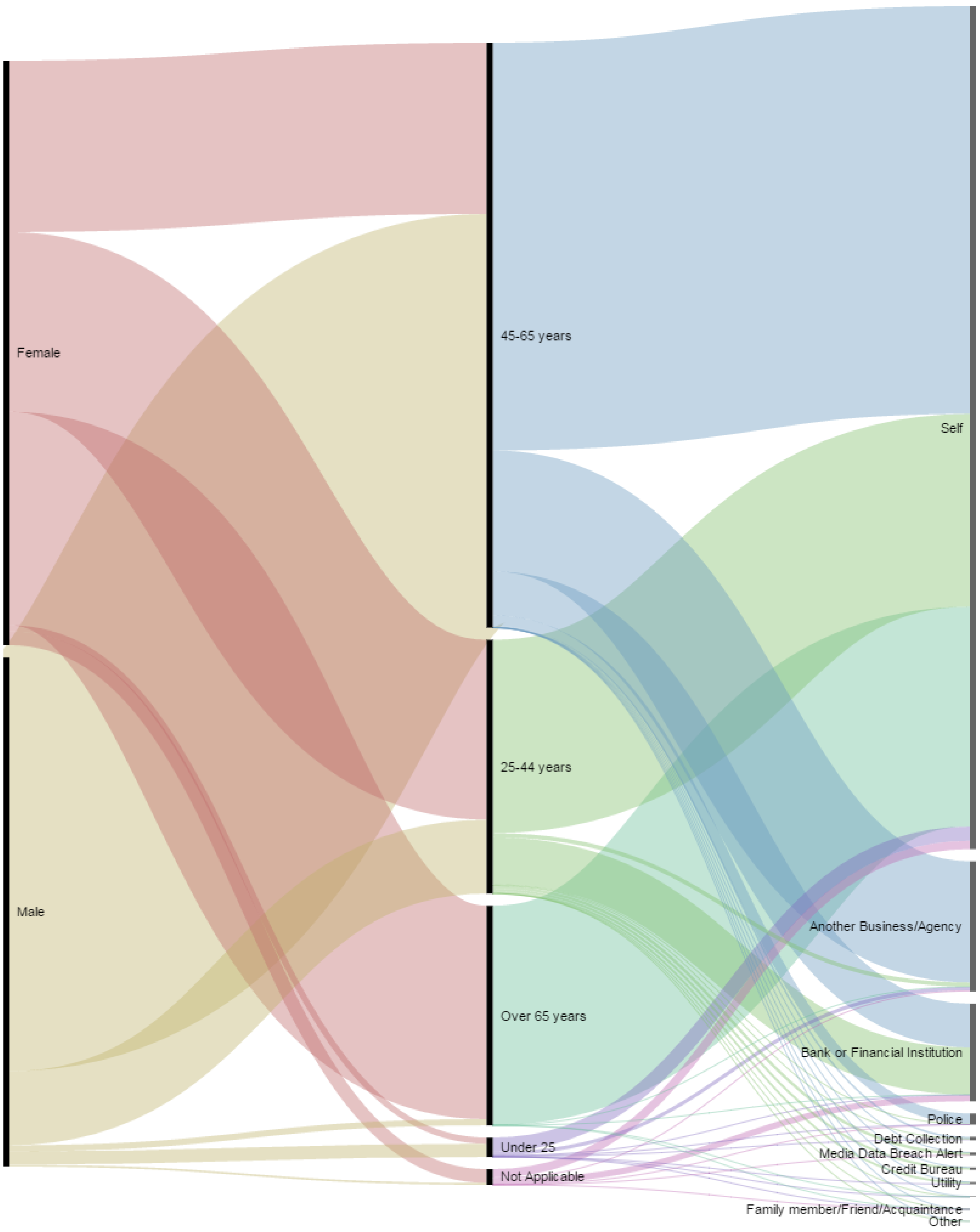

Figure 20 Gender, Age Range and Notification by Amount Taken

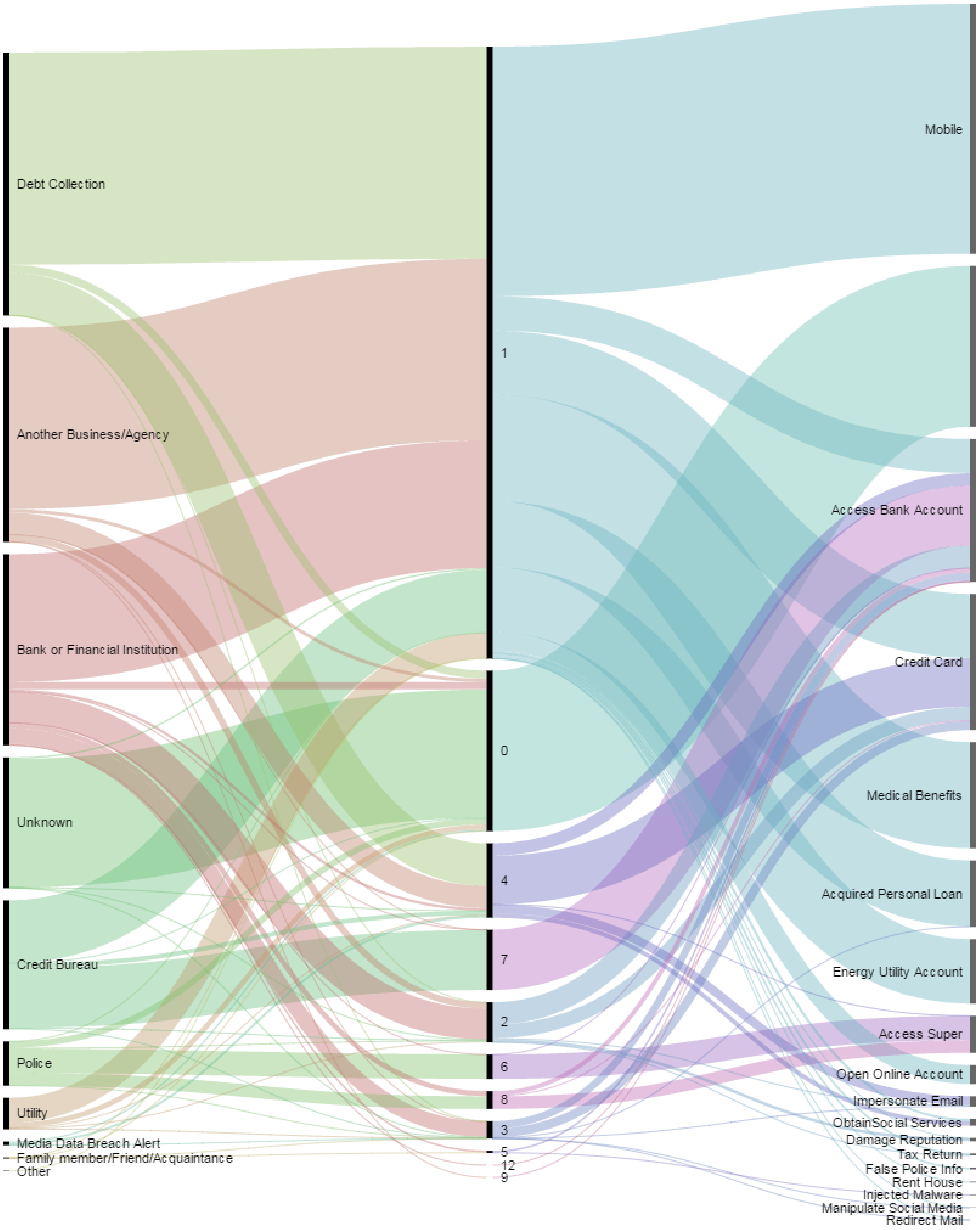

Figure 21 Notification, Number of Attacks and Attack Purpose by Days Elapsed (n=283)

Relationship to Perpetrator, Client Impersonated To and Notification by Days Elapsed

Figure 22 shows the relationship between the victim's relationship to the perpetrator, whom the victim was subsequently impersonated to, and the method by which the identity theft was discovered, controlling for the number of days elapsed between when the victim believed the attack to begin and when the attack was discovered. For ease of understanding, this figure includes only those cases where the victim was able to identify the perpetrator.

First, in many cases, the victim cannot identify whom they were impersonated to (in other words, they do not know how their personal credentials were used or represented to another party). For example, the largest group of identity frauds in this grouping were perpetrated by the victim's employer or a work colleague. In most of these cases, the victim was subsequently unable to determine who they had been represented to; further, in approximately half of those cases, the victim was not able to identify how the identity theft had been detected. The majority of the remainder of cases when the victim couldn't identify the target of the impersonation were perpetrated wither by an ex-partner or an associate of their ex-partner. This finding highlights the identity damage that an intimate acquaintance can do.

Identity theft cases involving a relative typically involved representations to a bank (which also comprised the bulk of attacks instigated by a current partner). Interestingly, approximately half of these cases were detected by the victim, but the other half were detected by the bank. The figure also shows that the bulk of attacks enacted by an ex-partner involved subsequent impersonation of the victim to a telecommunications provider. However, the majority of these cases were either detected by the victim themselves, or a debt collection agency, and not the provider.

Finally, it is interesting to note that, when controlling for the number of days between commission and detection, the most common known target of any impersonation is the telecommunications provider. As noted above, however, the bulk of these cases were detected by the victim.

Impersonated To Client, Impersonated of Client and Attack Purpose by Amount Taken

Figure 23 shows the relationship between who was impersonated to the victim, whom the victim was subsequently impersonated to, and the purpose of the attack, controlling for the dollar amount taken. For ease of understanding, this figure includes only those cases where the victim was able to identify who had been impersonated to them. The figure shows a number of relationships.

The figure shows that, controlling for the dollar amount taken, the telecommunications provider is most likely to be impersonated to the victim (for example, by way of a phone call to the victim in order to discuss their account or device). In only a comparatively small number of cases was the victim then impersonated to a telecommunications provider (that the victim knows of).

Of the cases in which the victim knew who they had been impersonated to, following the identity theft attack, the bank was the most common target when controlling for the dollar amount taken. The other two targets, of a considerably smaller representation, were telecommunications providers and government departments.

As in previous analyses, the attack purpose for the majority of these cases involved accessing bank accounts, credit cards or tax returns. This outcome is to be expected when controlling for the dollar amount taken; however, it does raise the possibility that not all identity thefts directly target a financial benefit in the first instance. While some perpetrators are clearly seeking a direct or immediate financial benefit, others are prepared to either wait for an opportunity to acquire a financial benefit (that may never come), or are more concerned with reputational, psychological or emotional harm. However, there are few measures for such outcomes in current literature and it is hence difficult to capture such alternative goals in these analyses.

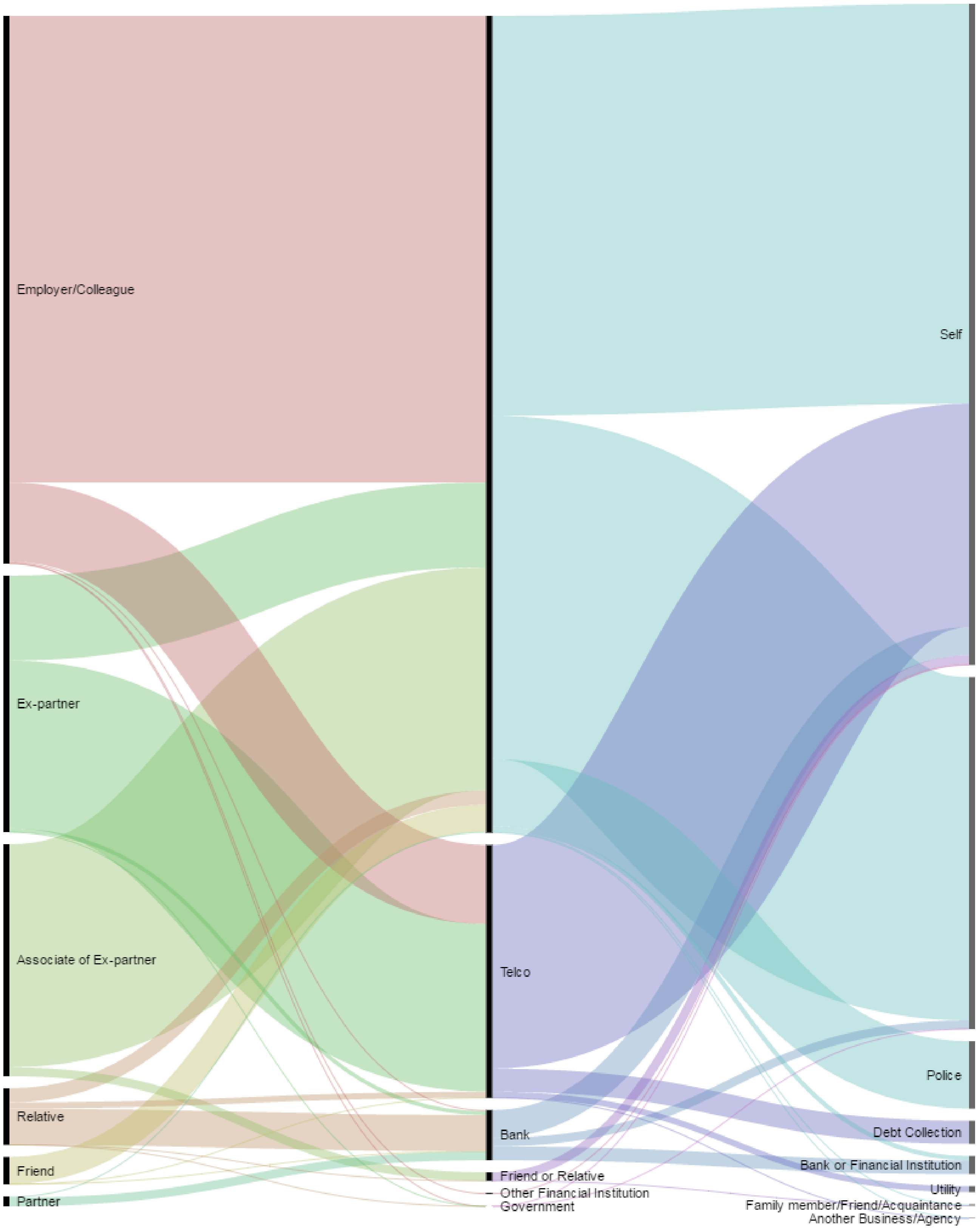

Figure 22 Relationship to Perpetrator, Client Impersonated To and Notification by Days Elapsed (n=123)

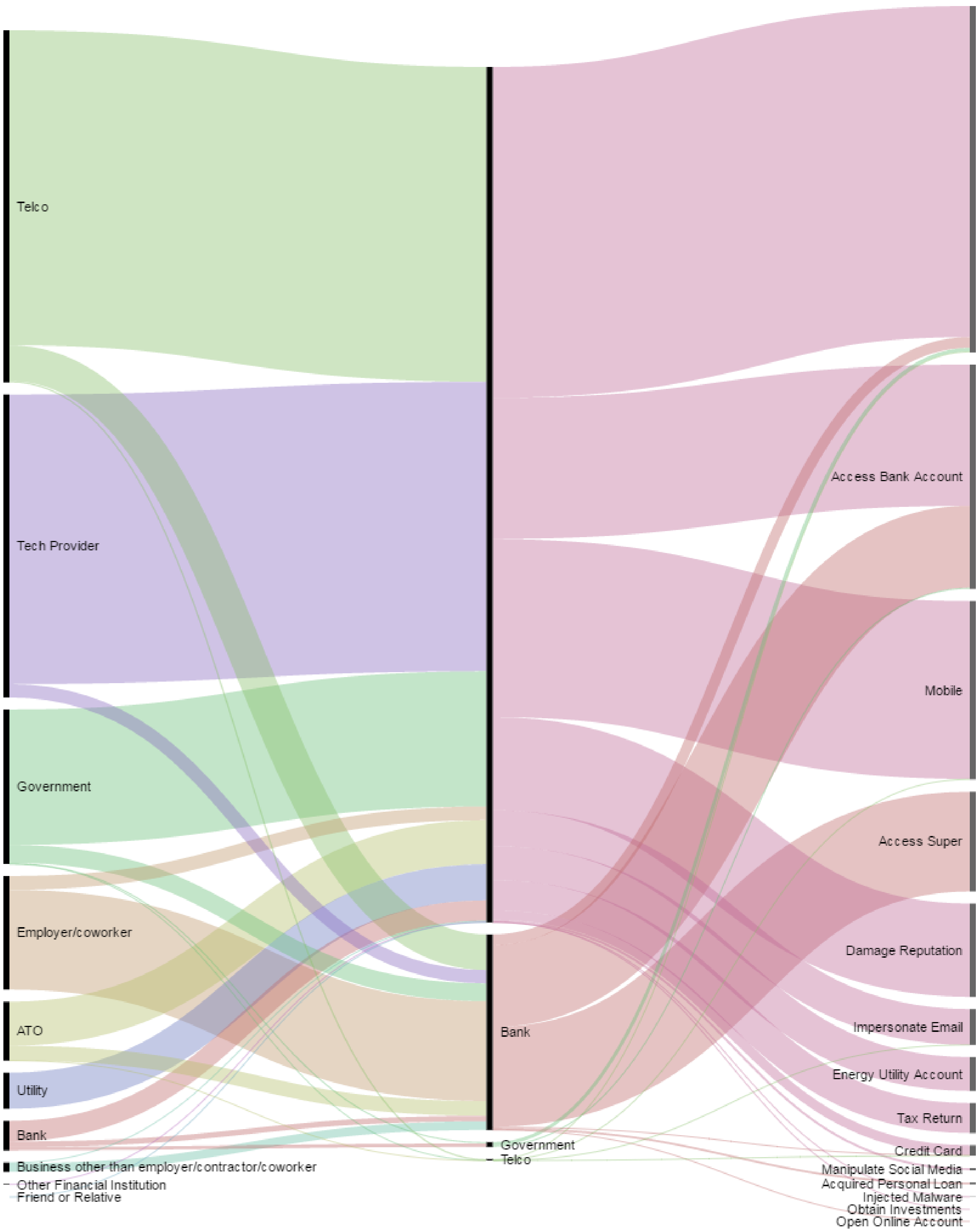

Figure 23 Impersonated To Client, Impersonations of Client and Attack Purpose by Amount Taken (n=232)

Summary Findings

In this section, we present some summary interpretation of the findings from this report.

Identity theft is a complex ongoing problem. The rate of new cases featured in this report is approximately seven new reports each and every day, with approximately 21% more cases reported on a Monday than a Friday. However, the cases in this report feature only those cases that have consented to participate in research - IDCARE receives the equivalent of approximately 30 to 50 new identity theft cases every day. Identity theft attacks occurred throughout Australia. In terms of raw report figures, Queensland, New South Wales and Victoria comprised 80% of reported identity theft attacks. State-based identity theft legislation may have an effect on the number and type of identity thefts committed and reported. South Australia appears to have the lowest incidence of identity theft reporting per capita.

While all age groups were targeted, individuals in the age group of 25-44 years were found most likely to report an identity theft. The fewest reports were received from individuals over 65 years of age, and the evidence suggests under-reporting in this age group: to this end, victims aged under 25 years are more strongly represented than individuals over 65 years of age, suggesting that a clean victim without financial resources is more useful to an identity thief than an experienced victim with financial resources. Subsequent analysis revealed that identity thefts involving older individuals are less likely to be detected by a third party, so that almost all identity thefts involving older individuals must be detected by the victim themselves.

By a rate of almost three to two, more identity theft reports were received from females than males. There may be a gender effect with regard to either reporting, detection, admission or victimisation, but the effect is still unclear. The largest single groups of victims are females in New South Wales, females in Victoria, females in Queensland, followed by males in New South Wales. Females are more likely to be able to identify the source of their identity theft attack, while males are substantially more likely to be unable to identify the source. Controlling for dollar loss, females represent almost the entirety of identity theft reports in the over 65 years age group, and the majority of the 25-44 years age group; males represent the majority of identity theft cases in the 45-65 years age group, controlling for dollar loss.

Victims from Culturally and Linguistically Diverse (CALD) backgrounds were likely under-represented in the identity theft reports. It is difficult to estimate the degree of under-reporting in this context, but previous state-based figures approximately accorded with general population levels. Only 282 respondents identified as culturally or linguistically diverse at the time of reporting.

In the vast majority of cases — some 84% — it was the victim themselves who detected the identity theft, and usually after reputational or financial damage had already been done. Other detections were afforded by banks and third party businesses in particular. Where a victim could identify the relationship with the perpetrator, most cases involved the victim’s employer or a work colleague.

Most victims of identity theft called their bank first, followed by law enforcement and a telecommunications provider, in that order. Subsequent analysis revealed that these three organisation groups represent the key battleground in the identity theft war, with most identity theft attacks involving at least two of these organisations in either a commission or detection capacity.

The most common item of identity documentation that was compromised in an attack was the drivers licence. Bank account details, credit card details and the passport were the next three most common items. Subsequent analysis of the case data revealed numerous instances of victims keeping electronic scans of these types of documents either on their smartphone or personal computer.

A number of mechanisms were used to commence an identity theft. However, the most common method was the telephone. To this end, of the four most common methods for a perpetrator to obtain a victim's identity details, three – email, social media and websites – related to electronic communication media. However, it must be noted also that communications technology plays a vital role in speeding recovery from an identity theft attack, in a number of different ways. First, initial IDCARE reports are made either by direct phone call, direct email message or by form submission on the IDCARE website (these cases are subsequently followed up via phone call). The use of communications technology to provide initial investigative information represents a fast and effective first step in beginning to determine the parameters of the identity theft event. Further case diagnosis, and discussions with third party service providers for the purposes of account recovery or information gathering is also conducted via telephone call or email. In summary, while communications technology may pose an initial threat to increased incidence of identity theft attack, this technology also serves to improve identity theft investigations and, hence, recovery.

In analysing evidence of the identity theft attack, it must be noted that usually scant information is available regarding the dynamics of the attack. In particular, there is very little prior insight into the behavioural identity of attackers and perpetrators. Further, the variety of identity theft attack types and the fact that identity theft in all its forms itself aims to evade identification makes it difficult to characterise perpetrator identities, activities and processes. Though there were more than 30 different subsequent attack types, the available evidence revealed that the most common attacks undertaken after obtaining the victim's identity theft was to access their bank account or credit card. Subsequent analysis revealed that, taking the dollar loss into account, while most identity thefts were detected by the victim, the most common impersonation to the victim was as a telecommunications or technology provider; when the victim knew the subsequent impersonation of the victim, it was usually to a bank. Approximately two thirds of cases, the victim contacted IDCARE within two days of discovering the attack.

Data regarding long-term recovery is scant. Where victims volunteer emotional descriptions of their state of mind, most victims describe highly negative views of themselves, including feelings of disbelief, stupidity and anger.

Interventions

The analysis provided in this report raises a number of areas that require further research in order to better understand identity theft, its mitigation and management. Based on the findings arising from the data analysis, the following interventions have been designed.

Intervention 1: Understanding Consumer Experience Pathways and Impacts

An outcome of the analysis provided in this report is that the journey of consumers in response to identity theft involving communications is complex and harmful. Response measures take time and involve multiple stakeholders to cater for unique consumer response requirements. IDCARE does not know whether the response measures advised are followed and create more or less harm to the consumer. To date the ability to undertake targeted follow-up on clients that have experienced a communication-enabled event has been constrained by resources and competing priorities.

Exploring the post-IDCARE engagement journey for consumers is critical in understanding the effectiveness of IDCARE service delivery as well as highlighting any unforeseen challenges. The initial data analysis reveals the complexity of identity theft events and the depth of IDCARE's response advice. To date there has been little opportunity to explore what the impacts of following IDCARE's response planning has meant for individuals that utilize this service and whether such insights could serve to improve response strategies. In order to address this gap, we need to better understand how victims respond long-term to identity theft attacks, resolution measures, and industry stakeholder response.

Under this intervention, IDCARE will sample a number of former clients (the target will be >100) that have experienced the exploitation of their identity involving communications and explore their response experiences and impacts. Following this analysis, IDCARE has budgeted under the ACCAN project a specific resource to undertake interviews with past clients in examining their journey and impacts following response planning and behavioural support provided initially by IDCARE's Identity Security Counsellors. Each client will participate in a semi-structured engagement with IDCARE. There will need to be a degree of flexibility in the questions asked, however indicative questions relate to the identity ecosystem engagement experience and performance, resolution and blame attribution, subsequent direct impacts, and emotional outcomes.

Intervention 2: Understanding the Threat Picture

A key observation from the data analysis phase was that identity theft events are often complex systems involving many participatory and response actors that possess incomplete information and rarely possess total knowledge of each event and its intricate parts. Communications media have emerged in this report as a key mechanism for perpetrating identity theft. However, it remains unknown whether the transnational crime communications dependencies are also as complex or diverse, or whether perpetrators have evolved to exploit these communications media in order to obscure their activity (in other words, do criminals that exploit communications spread their risk by engaging and utilising many telecommunications actors, or do they instead preference specific actors?). To better manage identity theft response, we need to understand how perpetrators initially target victims via communications media.

Under this intervention, IDCARE will specifically ask clients that experience engagement via telephone channels for the number used by the criminal and the time/date of engagement in order to determine whether any common communication service providers used. Client data processes at IDCARE will broaden to include these variables. An IDCARE analyst will then identify what service provider is hosting each number.

If it is found that telephone scammers are utilising only few service providers, a relatively quick analysis can be undertaken by IDCARE on what it takes to establish a new service connection (domestically and from offshore). The results will look to potentially inform regulatory and industry standards and responses as a means to disrupt transnational crime. This intervention would directly improve diagnosis and improving empirical insights on the nature of the threat and the opportunity to shape key stakeholders.

Recommendations

For Agencies and Providers

Based on the analysis conducted in this report, we make a number of recommendations for commercial businesses and providers, and for regulatory bodies.

Recommendation 1: Encourage your staff and customers to report identity theft. In particular, older individuals, males and individuals from culturally or linguistically diverse backgrounds should be further encouraged to report identity theft. Reporting fluctuates between states. Therefore, any report initiative must reach beyond state borders.

Recommendation 2: Work to increase awareness of the role of communications technologies in initiating and executing identity theft attacks. Communications media represented the majority of identity theft inception mechanisms. Therefore, this awareness should be undertaken at key contact points of communications devices and services: with telecommunications providers, ISPs and on social media.

Recommendation 3: Take gender into account. It is likely that females and males respond differently to identity theft attacks and reporting. Future prevention and awareness mechanisms must take this gender difference into account.

Recommendation 4: Work to improve threat information sharing. The majority of identity theft attacks involve banks, telecommunications providers and law enforcement. However, most identity thefts are still detected by the victim themselves. Therefore, it will be necessary to improve the degree of threat information sharing between these bodies, regarding both identity theft vectors and recovery processes.

Recommendation 5: Support and engage with victims long-term. Long-term recovery outcomes of identity theft victims is still not well understood. To understand which recovery pathways work the best, it will be necessary to understand long-term victim recovery processes and experiences. A program is needed to capture this information from victims, preferably as part of a conventional victim management plan.

Recommendation 6: Don’t just take money into account. Analytically, researchers need measures of distress other than purely dollar indicators. A goal is to prevent identity theft before it can wreak havoc on a victim's telecommunications or financial situation, so alternative measures of the relative success of safeguards and prevention tactics will be required.

Recommendation 7: Identity theft awareness material should be developed with CALD individuals in mind. This includes publishing awareness literature in accessible forms, and across multiple languages.

For Commercial Providers

Businesses emerged in two key roles in the analysis provided in this report: as detectors of identity theft, and as theatres for identity theft commission. Based on the findings in this paper, we provide a number of recommendations.

Recommendation 8: Places of work are key theatres for identity theft. Businesses need to maintain strong and workable governance mechanisms surrounding the storage, access and disposal of employee information. Ensure that these governance mechanisms are widely publicised throughout the business' workforce.

Recommendation 9: Treat cases of employee information snooping seriously. This type of activity, which might involve employees, managers or customers, could have strong, long-term consequences for those adversely affected.

Recommendation 10: Educate staff members regarding the signs of an identity theft, and what to do if they suspect an attack is in progress. Identity theft works because a perpetrator can apply their new identity at another venue, such as a business.

Recommendation 11: Be vigilant about the type of identity documentation you are willing to accept during a transaction. This report revealed the most commonly compromised items of identity, the most common being a drivers licence.

Recommendation 12: Carefully assess the possibility of missing documentation following a burglary. As with consumer premises, burglaries at commercial sites can result in identity theft. Hence, ensure customer and employee documentation is securely stored when not in use.

Recommendation 13: Ensure robust processes are in place. Most identity thefts are still detected by the victim, possibly resulting in years of financial and personal trauma. An effective identity theft detection plan and procedure can help your customers, employees and business partners.

For Consumers

The analysis of the case investigation material provides the foundation for a number of recommendations for individual consumers. These recommendations are designed to be read in concert with and in addition to wider recommendations regarding online and personal safety, published by law enforcement and other interest groups. The recommendations are as follows.

- Be careful with your communications device. The vast majority of identity thefts involve your telephone or another communications device. The evidence in this report has shown that individuals from all ages and age groups are targeted, but a communications device is common to many attacks.

- Burglaries can result in identity thefts. If your place of residence or work has been burgled, checking your personal documentation should be just as important as verifying lost possessions. Keep your personal documentation in a specific place, so you can tell whether this material has been disturbed.

- Be vigilant about keeping your personal information secure while you are at work. Become familiar with your employer's policy regarding access to employee information. In cases when a victim could identify the relationship with their identity theft attacker, the majority involved an employer or work colleague.

- Secure your personal documents at home and at work, especially if these items are rarely accessed. Shred old documents that you aren't using, and shred any documents you're disposing of. If you must keep a copy, then scan the document and keep it in an encrypted form, preferably away from your computer or smartphone.

- Have a specific policy for giving information over the phone or online, and make sure the policy is well known among members of your family or household. Do not verify who you are to someone who has called you: always call them back on an official phone number. Always ask a caller to fully identify themselves, where they are calling from, and the purpose of the call. The onus is on the caller to prove their identity, and not on you to prove yours.

- Resist any attempt to pressure you into surrendering information about yourself over the telephone or online. If you feel that you are being pressured to make a decision over the telephone or social media, or to provide documentation about yourself, this is a sign that the call is not above board. If you are too tired or busy to vet such calls at that particular moment, request the caller to call back later. Most legitimate businesses will be happy to do this.

- Only keep copies of documents on your PC or smartphone for as long as you absolutely need them. Examples of these documents include your driver's licence or passport. Do not store copies of personally identifiable information in a cloud storage system for any length of time, and do not store them in an unencrypted form.

- Understand that identity thieves work hard to appear or sound legitimate. They may use the conventional business language and expressions with which you are familiar (e.g. 'This call will be recorded for training and quality purposes') in order to seem genuine.

- Re-evaluate your personal computing security practices regularly. This includes changing your passwords and refreshing your anti-virus definitions. Many identity thefts, especially those involving online vulnerability, depend on routine activity.

- Periodically re-evaluate the extent and type of information you keep online about yourself – including personal information in social media profiles. A careful identity thief wants to know as much about who you are as possible.

- Use a separate signature just for courier or postal deliveries. There is no legal requirement for you to use your full legal signature for this purpose.

- Be suspicious of supplying your name, address and other details when the purpose is not clear (e.g. when entering competitions at a shopping mall, or completing surveys on the street). You don't know how this information is stored, how it will be disposed of, and it could be used as a pretext for a later fraud.

- Be suspicious of supplying your date of birth to anyone for any reason (including in-store loyalty cards). Most businesses do not need to use your date of birth to verify you.

- Talk to friends and family about identity theft. Most identity thefts are still detected by the victim themselves, often when they notice something strange or irregular.

Limitations

The analyses presented in this report are subject to a number of important limitations. These limitations must be borne in mind when examining the results. The following is a brief discussion of some of these limitations.

First, our analysis is based on data received for analysis purposes from IDCARE, Australia's only identity theft support organisation. The data comprises those cases wherein the victim consented to having their case admitted for research purposes. There may be some unseen or hidden properties of these data that are not reflective of wider cases of identity theft. However, given the number of observations and the variety of cases seen in this report, we believe this risk to be very low.

Second, as with all criminal activity, identity theft is likely to be under-reported. The data that forms the basis of the analysis in this report consists of identity theft victims that have identified their victimhood, identified IDCARE, and made contact. It would not be unreasonable to assume that the 4000 cases of identity theft described in this report would be complemented by a much larger number of victims that have not come forward, either because they did not know they were compromised, did not want to identify the perpetrator, did not feel that there was any effective solution, did not feel that the problem was significant enough, did not know of IDCARE or did not wish to call. These victims remain unknown, and may possess properties that are different to those discussed in this report.

Next, IDCARE is based in Queensland, and it is possible that this state provides greater advertising and marketing to the initiative. If this is the case, then this greater exposure might also lead to greater awareness - which in turn means a larger number of respondents from Queensland. While the per capita analyses provided in the report are consistent across the largest Australian states, this over-representation may still be a possibility.

There are also several important points to note about data quality. As law enforcement, public and private understanding of identity theft changes, so have the mechanisms for detecting and defeating it. Accordingly, IDCARE has also made changes to its procedures and data collection methods over the period reflected in this data set. As a result, some data items only became available part-way through the analysis period. This has been noted in the report in those cases where this has affected the data analysis. However, for this reason, some analyses do not extend for the whole period covered by the data set.

Second, it must be remembered that victims usually present in a highly anxious state. Initial interviews, as a result, can be emotionally charged, with much consternation as the client and investigator attempt to determine what has happened and how to repair the situation. Therefore, there is likely to be some level of error in the data. While the magnitude of this error is unknown on a case by case basis, it is hoped that most errors would be randomised out over the entire data set. However, the effect of this variance remains unknown.

Next, while it would be useful, from an analytical point of view, to have deeper insight into victim behaviour (notably with respect to emotional responses, event recollection and behavioural descriptions) it must be noted that client welfare is the primary goal of the interview exercise, and robust research is fundamentally a secondary outcome. Recording of emotional responses, in particular, depends on the investigator being able to code the response as it is being received, or in the subsequent case review stage. We feel that the data presented in this report represents a unique opportunity to understand identity theft, and we are not aware of many other such large-scale analyses of the phenomenon.

Authors

Sigi Goode is an associate professor of information systems in the Research School of Management at the College of Business and Economics, Australian National University (ANU). He received his Ph.D. from the Australian National University. His research interests lie in information security behaviour, services and technology adoption, policy and use. He has published papers in journals such as Journal of Management Information Systems, European Journal of Information Systems, Decision Support Systems, Journal of Business Ethics, Information & Management, and European Journal of Operational Research. He has more than fifteen years' experience designing and managing online information platforms. Dr. Goode received the ANU Vice-Chancellor's Award for Excellence in Education in 2005, and a Carrick Institute National Award for Teaching Excellence in 2006. He is an associate editor of *Information and Management*, the International Journal of Information Systems Theories and Applications.

References

Allison, S. F. H., A. M. Schuck, and K. M. Lersch. 2005. 'Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/Offender Characteristics.' *Journal of Criminal Justice* 33: 19–29.

ALRC. 2008. *Australian Privacy Law and Practice (ALRC Report 108)*. Sydney, Australia: Australian Law Reform Commission.

Anderson, K. B. 2006. 'Who Are the Victims of Identity Theft? The Effect of Demographics.' *Journal of Public Policy and Marketing* 25: 160–171.

Australian Bureau of Statistics. 2016. *3101.0 - Australian Demographic Statistics, Mar 2016*. 3101.0. Canberra, Australia: Australian Bureau of Statistics.

Australian Institute of Criminology. 2005. *Crime Victimisation in Two Selected Migrant Communities*. 107. Crime Facts Info. Australian Institute of Criminology.

Bartels, Lorana. 2011. *Crime Prevention Programs for Culturally and Linguistically Diverse Communities in Australia*. Research in Practice 18. Canberra, Australia: Australian Institute of Criminology.

Bartley, Sharon J., Priscilla W. Blanton, and Jennifer L. Gilliard. 2005. 'Husbands and Wives in Dual-Earner Marriages: Decision-Making, Gender Role Attitudes, Division of Household Labor, and Equity.' *Marriage & Family Review* 37 (4): 69–94.

Carli, Linda L. 2001. 'Gender and Social Influence.' *Journal of Social Issues* 57 (4): 725–741. doi:10.1111/0022-4537.00238.

Caspi, Avshalom, Terrie E. Moffitt, Phil A. Silva, MAGDA Stouthamer-Loeber, Robert F. Krueger, and Pamela S. Schmutte. 1994. 'Are Some People Crime-Prone? Replications of the Personality-Crime Relationship across Countries, Genders, Races, and Methods.' *Criminology* 32 (2): 163–196.

Copes, H., K. R. Kerley, R. Huff, and J. Kane. 2010. 'Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey.' *Journal of Criminal Justice* 38: 1045–1052.

Deloitte. 2016a. *Mobile Consumer Survey 2016 The Australian Cut*. Sydney, Australia: Deloitte Consulting.

Deloitte. 2016b. *Media Consumer Survey 2016*. Sydney, Australia: Deloitte Consulting.

Dowse, Leanne, Karen Soldatic, Jo Spangaro, and Georgia van Toorn. 2016. 'Mind the Gap: The Extent of Violence against Women with Disabilities in Australia.' *Australian Journal of Social Issues; Sydney* 51 (3): 341-359,383-385.

Herzog, Thomas N., Fritz J. Scheuren, and William E. Winkler. 2007. 'Social Security and Related Topics.' In *Data Quality and Record Linkage Techniques*, 169–177. Springer. http://link.springer.com/content/pdf/10.1007/0-387-69505-2_17.pdf.

Holtfreter, K., M. D. Reisig, T. C. Pratt, and R. E. Holtfreter. 2015. 'Risky Remote Purchasing and Identity Theft Victimization among Older Internet Users.' *Psychology, Crime and Law* 21: 681–698.

InTouch. 2010. *'I Lived in Fear Because I Knew Nothing': Barriers to the Justice System Faced by CALD Women Experiencing Family Violence*. Melbourne, Victoria: InTouch.

Morris, R. G. 2010. 'Identity Thieves and Levels of Sophistication: Findings from a National Probability Sample of American Newspaper Articles 1995-2005.' *Deviant Behavior* 31: 184–207.

Reyns, B. W. 2013. 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses.' *Journal of Research in Crime and Delinquency* 50: 216–238.

Rosvall, Martin, and Carl T. Bergstrom. 2010. ‘Mapping Change in Large Networks.’ *PLOS ONE* 5 (1): e8694. doi:10.1371/journal.pone.0008694.

Sawrikar, P, and I Katz. 2008. *Enhancing Family and Relationship Service Accessibility and Delivery to Culturally and Linguistically Diverse Families in Australia*. 3. AFRC Issues. Canberra, Australia: Australian Institute of Family Studies.

Sensis. 2016. *Sensis Social Media Report 2016*. Melbourne, Victoria: Sensis.

Shepherd, Stephane. 2016. ‘Criminal Engagement and Australian Culturally and Linguistically Diverse Populations: Challenges and Implications for Forensic Risk Assessment.’ *Psychiatry, Psychology and Law* 23 (2): 256–274. doi:10.1080/13218719.2015.1053164.

Smith, James P., John J. McArdle, and Robert Willis. 2010. ‘Financial Decision Making and Cognition in a Family Context*.’ *The Economic Journal* 120 (548): F363–F380. doi:10.1111/j.1468-0297.2010.02394.x.

Steel, Alex. 2010. ‘The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence?’ *University of New South Wales Law Journal* 33: 503–531.

Vogler, Carolyn, Clare Lyonette, and Richard D. Wiggins. 2008. ‘Money, Power and Spending Decisions in Intimate Relationships1.’ *The Sociological Review* 56 (1): 117–143. doi:10.1111/j.1467-954X.2008.00779.x.

Wang, Alan G., Homa Atabakhsh, Tim Petersen, and Hsinchun Chen. 2005. ‘Discovering Identity Problems: A Case Study.’ In *International Conference on Intelligence and Security Informatics*, 368–373. Springer. http://link.springer.com/chapter/10.1007/11427995_30.

Westpac. 2016. *Westpac Women’s Markets Women & Money Survey*. Westpac Women’s Markets White Paper. Westpac.

Willis, Matthew. 2011. *Non-Disclosure of Violence in Australian Indigenous Communities*. 405. Trends & Issues in Crime and Criminal Justice. Canberra, Australia: Australian Institute of Criminology.

Identity theft and Australian telecommunications:

Case analysis