Australian Government

Australian Institute of Criminology

AIC reports
Statistical Report 11

Identity crime and misuse in Australia: Results of the 2017 online survey

Susan Goldsmid
Alexandra Gannoni
Russell G Smith

ISSN (Online) 2206-7930

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at aic.gov.au

Identity crime in Australia

Australian Government
Australian Institute of Criminology

1 in 4 of the Australians surveyed (25.2%) reported having been a victim at some point in their lives. This is an increase on the 21.5% reported in 2016.

13.1% of respondents reported having their **personal information misused in the last 12 months.** This is an increase on the 8.5% reported in 2016.

Victims of identity crime spend an average of **23 hours** repairing the damage caused.

Refusal of credit was the most common consequence of identity crime **(34.9%)**. This was followed by being refused government benefits, experiencing financial difficulties and suffering mental or emotional distress.

Names were the most misused type of personal information **(45.2%)**, along with credit/debit card information, address, date of birth and bank account information.

Average **out-of-pocket losses were over $3,000** per victim in 2017, with almost twice as many reporting being out-of-pocket in 2017 as in 2016.

The **most common misuse** of personal information was to obtain **money from a bank account**, although the number of incidents of filing fraudulent tax returns and obtaining superannuation monies has increased significantly.

Telephone scams were the most prevalent way in which personal information was obtained **(24.9%)**. This was followed by face-to-face, email, text message and theft or hacking.

In 2017, 1 in 10 victims (10.3%) did not report the misuse of their personal information in any way, which was less than the 14.3% who didn't report in 2016.

Contents

Figures

Tables

Acknowledgements

This study was undertaken as part of the Australian Government's National Identification of Identity Crime and Misuse project, which is conducted pursuant to the National Identity Security Strategy. The survey was developed with input and advice from the Attorney-General's Department. Data collection was undertaken professionally and efficiently by i-Link Research Solutions, a market research firm that provided a panel of individuals drawn from across Australia who were asked to complete an online questionnaire. The time and willingness of those who completed the survey are also gratefully acknowledged.

The opinions expressed are those of the authors alone and do not necessarily reflect the views or policies of the Australian Government.

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
AGD	Attorney-General's Department (Commonwealth Government)
AIC	Australian Institute of Criminology
APWG	Anti-Phishing Working Group
ATO	Australian Taxation Office
AusPayNet	Australian Payments Network
HIN	shareholder identification number
NCVS	National Crime Victimization Survey (US)
NFA	National Fraud Authority (UK)
PIN	personal identification number
SD	standard deviation
TFN	tax file number

Abstract

This report presents findings of the latest survey of identity crime and misuse undertaken by the Australian Institute of Criminology as part of the Australian Government's National Identity Security Strategy. Identity crime is one of the most prevalent forms of criminal activity in Australia and remains a persistent concern for many Australians. In 2017, a survey was conducted of 9,947 members of a national research panel concerning their experiences of victimisation—over their lifetime and during the preceding 12 months—and their perceptions of the risk of identity crime in the ensuing 12 months. The data for 2017 were compared with those of the similar survey conducted in 2016.

The survey found that 25 percent of respondents experienced misuse of their personal information at some time during their life, with 13 percent experiencing misuse of their personal information in the previous 12 months (both statistically significant increases on the findings for 2016). Almost twice as many respondents reported suffering out-of-pocket losses in 2017 as in 2016, with total out-of-pocket losses amounting to $2.9m in 2017 ($1.1m more than in 2016). The results from the 2017 survey should assist those designing awareness programs and prevention initiatives by indicating who may be most at risk of identity crime.

Executive summary

Background

Identity crime is one of the most prevalent crime types in Australia, with reports of prevalence and harm identifying rates far exceeding those of property crime and violent crime (Jorna & Smith 2018). This large-scale victimisation is mostly due to the extensive opportunities for misuse of personal information created by information and communications technologies. Identity crime has been defined by the United Nations Economic and Social Council (2007: 18) as 'crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes'. It covers a wide range of activities and offences in which a perpetrator makes use of information relating to another person by fabricating or manipulating credentials to obtain some economic or other benefit (Jorna & Smith 2018). It affects businesses, government entities and individuals alike, as criminals seek to misrepresent information that identifies both organisations and people for personal gain. Its extent in Australia is considerable, with the latest estimate of economic harm being approximately $2.65b for 2015–16 (Smith & Jorna 2018b).

Criminals obtain information for use in identity crime in a wide variety of ways, although the most extensive sources arise from data breaches involving large numbers of commercial or government records, or through acts of dishonesty conducted online or via telephone in which individuals are tricked into disclosing their personal details or through malware installed on their computers without their knowledge.

Data breaches and phishing attacks have continued to increase each year. The information industry experienced the heaviest business losses from data breaches in 2016, according to Verizon (2017), with numerous large entities releasing data by accident or through malicious activity. Equifax, a consumer credit reporting agency in the United States, lost personal data records belonging to an estimated 143m Americans, 400,000 Britons and many others between mid-May and July 2017. The data lost included social security numbers, birth dates, addresses and driving licence numbers (BBC 2017).

The fourth quarter of 2016 saw the highest number of phishing attacks recorded by the Anti-Phishing Working Group (APWG 2017) since data collection began in 2004. Phishing attacks seek to trick victims into providing personal identifying information in response to requests purporting to be from government or business organisations. Once obtained, the data can be used in a range of identity crimes, particularly online payment fraud.

In Australia, card-not-present fraud, which takes place when online purchases are paid for by disclosing credit card information, increased by 15 percent between 2015 and 2016, with fraudulent losses involving Australian-issued cards increasing from $363m in 2015 to $418m in 2016. Card skimming and counterfeiting of Australian-issued cards also increased during this period (AusPayNet 2017).

To address these problems, in April 2007 the Council of Australian Governments developed the National Identity Security Strategy. The strategy is designed to protect the identities of Australians in a more regulated and efficient way than in the past. The need for such a strategy arose from emerging evidence that large numbers of Australians had experienced misuse of their personal information for criminal purposes (Cuganesan & Lacey 2003; Office of the Australian Information Commissioner 2017). The strategy seeks to enhance identification and verification processes throughout Australia and to develop other measures to combat identity crime, including through the creation of a national Document Verification Service (AGD 2012).

The strategy also recognised the need to quantify the nature and extent of identity crime and recommended that an identity crime and misuse measurement framework be created to assess the effectiveness of policy and practice throughout Australia. As part of the measurement framework, each year a report is prepared on the current state of identity crime and misuse, the latest of which was for the 2016–17 year (Jorna & Smith 2018). A series of large-scale surveys have also been conducted to determine respondents' experiences of victimisation over their lifetime and during the preceding 12 months, as well as their perceptions of the risk of identity crime in the ensuing 12 months. This report presents results of the latest survey in the series, undertaken by the Australian Institute of Criminology in July 2017.

Methodology

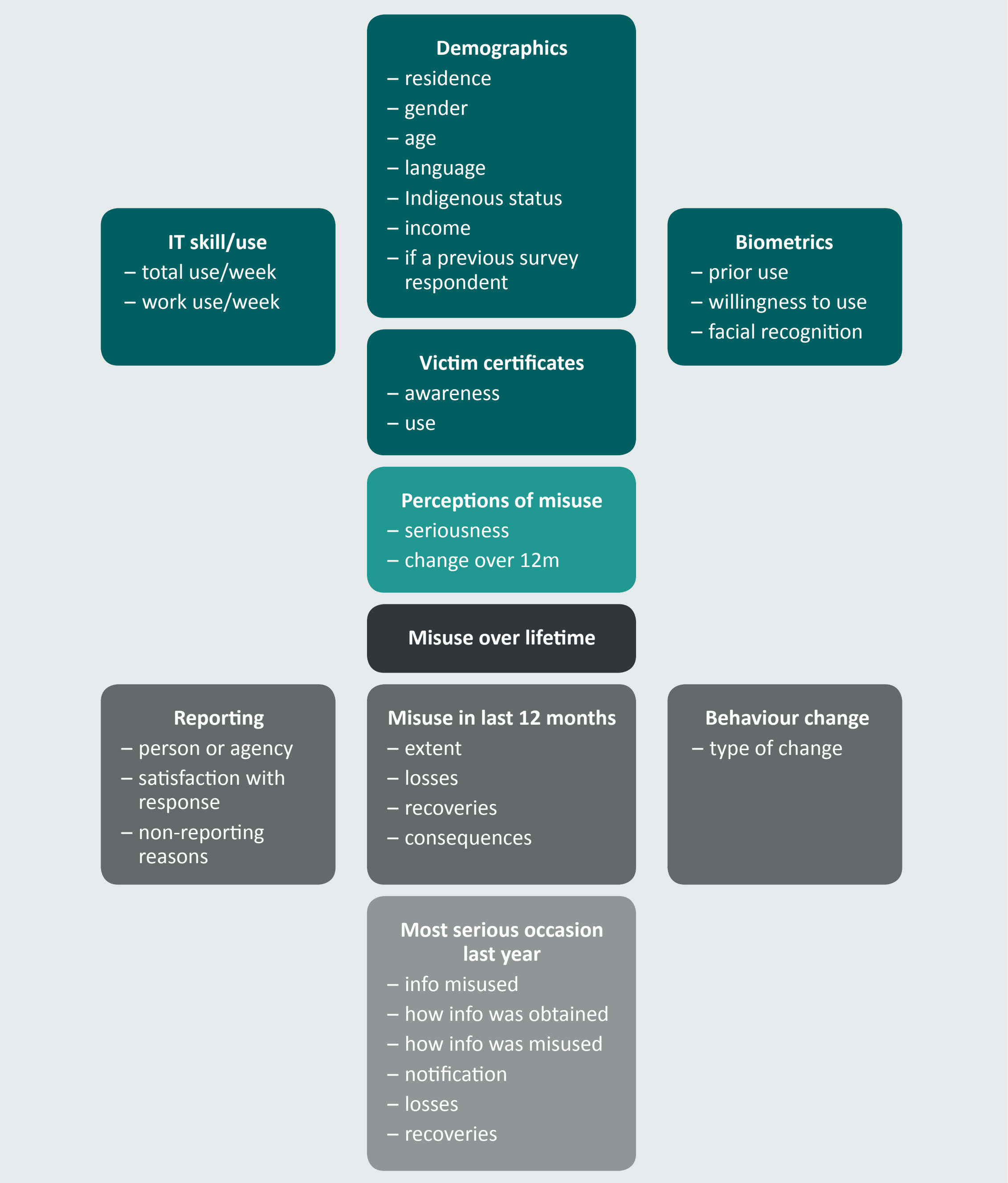
Consistent with previous surveys conducted in 2013, 2014 and 2016, the 2017 questionnaire asked respondents about the misuse of various types of personal information. These included misuse of an individual's name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (eg fingerprint and facial images), signature, bank account information, credit or debit card information, personal identification number, tax file number, shareholder identification number (HIN), usernames and passwords, and student number. Respondents could also provide details about other types of personal information that may have been misused.

Misuse of personal information was defined in the questionnaire as:

> obtaining or using your personal information without your permission, to pretend to be you, or to carry out a business in your name without your permission, or other types of activities and transactions. This does not include use of your personal information for direct marketing, even if this was done without your permission.

The questionnaire asked respondents about various dimensions of the problem, as illustrated in Figure 1.

Figure 1: Survey data collection structure



Demographics
- residence
- gender
- age
- language
- Indigenous status
- income
- if a previous survey respondent

IT skill/use
- total use/week
- work use/week

Biometrics
- prior use
- willingness to use
- facial recognition

Victim certificates
- awareness
- use

Perceptions of misuse
- seriousness
- change over 12m

Misuse over lifetime

Reporting
- person or agency
- satisfaction with response
- non-reporting reasons

Misuse in last 12 months
- extent
- losses
- recoveries
- consequences

Behaviour change
- type of change

Most serious occasion last year
- info misused
- how info was obtained
- how info was misused
- notification
- losses
- recoveries

In July 2017, a questionnaire comprising 37 main questions (see Appendix A) was administered online to a research panel of Australians drawn from all states and territories. The sampling frame of more than 300,000 individuals was provided by i-Link Research Solutions, a market research company, which then provided raw, de-identified data for the Australian Institute of Criminology to analyse.

Sampling was completed once a quota of 10,000 respondents had been satisfied. No other quotas were employed as the size of the sample was sufficiently large to ensure good representation from urban and regional areas across Australia.

Data were weighted by age and gender to represent the spread of the population in Australia. Australian Bureau of Statistics data from the 2016 Census were used to develop the weighting matrix for the sample data (Appendix B). The Census data did not provide population data for people who listed their gender as indeterminate/intersex or unspecified. Accordingly, responses from the 38 respondents in this group were excluded as weighting could not be undertaken using available data. A small number of respondents who did not specify their age were also excluded from the analysis (n=29). This resulted in a useable sample size of 9,947 respondents.

Prevalence of victimisation

Thirteen percent of respondents reported having had their personal information misused in the last 12 months. This was a statistically significant 4.6 percentage point rise in recent victimisation from results obtained in 2016. Driven by this rise in recent victimisation, there was also a statistically significant 3.7 percentage point increase between 2016 and 2017 in reports of lifetime personal information misuse. In 2017, one in four respondents reported that their personal information had been misused at some point in their lifetime. This is a reversal in trend, with declining victimisation observed since 2013.

An increase in misuse of personal information was reported across all geographic regions examined, with the exception of non-capital city residents of Western Australia and Tasmania, who experienced small reductions in reports of victimisation.

Male respondents between 25 and 34 years of age were the group most likely to report personal information misuse in the last 12 months. Across all age groups, men were more likely than women to report misuse of personal information in the last 12 months. When both men and women were considered together, the 25–34 age group was the most likely to report misuse of personal information.

The sample reported spending more time using a computer each week than has been reported in other studies of the Australian population. The impact that hours using computers each week had on victimisation was not as expected. Respondents who experienced misuse of personal information in the last 12 months reported using computers fewer hours per week than those who did not experience misuse. This finding held when total computer hours, computer hours for work purposes and computer hours for non-work purposes were considered. This may reflect a reduction in computer use after experiencing victimisation, although this cannot be explored using the current data.

The finding that misuse of personal information increased between the 2016 survey and the 2017 survey cannot be compared with the results of other international identity crime estimates, as most international estimates were published some years ago and were based on different samples and indicators of victimisation. The current rates are, however, generally comparable with rates reported in the most recent overseas and Australian studies (Jorna & Smith 2018).

Misuse of personal information in the last 12 months

About half of respondents who had experienced misuse of their personal information in the last 12 months had their information misused on only one occasion. However, the mean number of occasions was five, due to some respondents reporting multiple occasions of misuse.

Questions were also asked about victimisation on the most serious occasion of misuse, which was defined as the occasion that resulted in the largest financial or other harm to the respondent. Thirty-six percent of recent victims reported that only one type of information was misused. On average, three types of personal information were misused on the most serious occasion.

The type of information most commonly misused on the most serious occasion was a person's name, followed by credit/debit card information, address details, date of birth, bank account information and passwords. From 2016 to 2017, there was a notable increase in the number of respondents reporting misuse of address details, name and date of birth. There was also a 13.6 percentage point reduction in the proportion of respondents reporting misuse of credit/debit card details.

Respondents who had experienced misuse of their personal information in the last 12 months most commonly reported that their information had been obtained through face-to-face meetings, telephone, text message and email. All of these methods, with the exception of email, experienced an increase of at least 10 percentage points from 2016 to 2017.

The most common reason respondents gave for the misuse of their personal information was to obtain money from a bank account, the same as in 2016. The proportion of respondents reporting that their personal information had been used to file fraudulent tax returns or to obtain superannuation monies increased substantially. This finding is consistent with the reported increase in the misuse of names, address details and dates of birth, all of which could be used in taxation and superannuation fraud.

Consistent with the decrease in reported misuse of credit/debit card details, there was a substantial reduction in misuse of personal information to purchase something, down 13.3 percentage points from 2016.

Respondents most commonly became aware that their personal information had been misused when they were notified by a bank, financial institution or credit card company. This was followed by respondents noticing suspicious transactions in bank statements and notifications from police.

Police notifications rose significantly between 2016 and 2017, with almost one-third of respondents in 2017 reporting police notifications, compared with 11.9 percent in 2016. The reason for this increase is unclear. To examine whether it related to a change in practice of any one police service, the data were analysed across geographic regions. For almost all geographic regions, between 20 and 30 percent of respondents reported being notified by police, so the increase in police notifications cannot be attributed to any particular police agency.

Out-of-pocket, reimbursed and recovered losses

Almost twice as many respondents reported suffering out-of-pocket losses in 2017 as in 2016. Out-of-pocket losses are those experienced after deducting any amounts recovered. Total out-of-pocket losses were $1,141,893 higher in 2017 than in 2016. This was despite the out-of-pocket loss experienced per victim substantially reducing, to a median value of $150. In 2017, the number of victims reporting losses of between $100 and $199 increased. This appears to account for both the rise in the number of respondents experiencing out-of-pocket losses and the reduction in the mean amount lost.

There was considerable gender and age disparity in reported out-of-pocket losses. Men aged 65 years and over reported the highest mean financial losses, followed by men aged 24 years and under. In the 25–34 year age group, women reported higher losses than men. These findings may have been affected by large losses experienced by one or two participants within these categories, as the sample sizes in some categories were small. Alternatively, it may indicate that vulnerability to losses from the misuse of personal information varies by age and gender.

Total amounts recovered in 2017 were substantially lower than in 2016, despite increased victimisation rates. This was probably due to the 2016 data being unduly influenced by one multimillion dollar loss recovery. For this reason, caution should be taken when comparing 2016 and 2017 loss recovery data. Twenty-two percent of respondents reported recovering losses in 2017, with an increasing number of participants recovering small ($100–$199) and moderate ($300–$599) amounts. There was a notable reduction in recoveries of more than $1,000 in 2017 compared with 2016.

Trends for out-of-pocket and recovered losses for the most serious occasion of misuse mirrored the trends for total out-of-pocket and recovered losses.

Impact on victims

There was a statistically significant reduction in the proportion of victims of misuse of personal information in the last 12 months who reported no adverse consequences—from 55.9 percent in 2016 to 34.4 percent in 2017. The most common consequence of misuse of personal information was refusal of credit, with a statistically significant 18.7 percentage point increase in reports of this consequence in 2017. There were also considerable increases in reports of being refused government benefits (9.6 percentage point increase) and of experiencing financial difficulties resulting in repossession (8.1 percentage point increase).

Almost all respondents (93.5%) reported changing their behaviour in some way as a direct result of their personal information being misused. The most common behavioural change was changing passwords (37.5%), as one might expect in light of conventional cybersecurity advice.

In 2017, fewer respondents reported changing passwords (10.5 percentage point decrease) and changing banking details (8.8 percentage point decrease). Arguably, this corresponds with the finding that misuse of credit/debit card details decreased in 2017.

When method of access was considered, a number of differences in behavioural responses were identified. Of those who believed their personal information had been obtained via online banking, 53 percent reported changing passwords, 45.9 percent changed banking details and 45.6 percent reviewed financial statements more carefully—as one might expect.

Respondents who believed their personal information had been obtained via ATM transactions most commonly reported changing passwords (53.6%), followed by reviewing financial statements more carefully (45.8%), being more careful sharing personal information (43.5%), and changing banking details (42.5%).

Behavioural responses to having had personal information accessed through a website (excluding online shopping) included changing passwords (48.6%), being more careful when sharing personal information (44.1%), reviewing financial statements more carefully (40.7%) and not trusting people as much (40.0%).

Examining behavioural responses by the type of personal information misused provides insight into the appropriateness of these behavioural responses. Only 59 percent of respondents who reported their password had been misused changed their passwords and only 40 percent reported using better security for computers and computerised devices. Over 40 percent of respondents who had credit/debit card or bank account information misused reported changing banking details and reviewing financial statements more carefully.

Reporting misuse of personal information

Ten percent of respondents who had experienced misuse of their personal information in the last 12 months did not report the misuse at all. Fifty-seven percent told only a family member or friend, 7.4 percent reported it to a business, organisation or government agency, and 25.5 percent told family and friends as well as a business, organisation or government agency.

Most respondents who reported the misuse to a business, organisation or government agency were either satisfied or very satisfied with the response. All agencies either maintained or improved their satisfaction rating from 2016, with the exception of internet service providers, banks and credit unions, which experienced small reductions in levels of satisfaction. The Passport Office achieved the highest satisfaction rating in 2017, with 89.1 percent of respondents who reported misuse to that agency being either satisfied or very satisfied with the response.

ACORN experienced the largest increase in satisfaction rating from 2016 to 2017, with a 30.3 percentage point increase. There were also substantial increases in satisfaction with credit reporting agencies (27.8 percentage point increase), IDCARE (23.4 percentage point increase), utility companies (21.2 percentage point increase), and policing agencies (16.5 percentage point increase).

The most common reason respondents gave for not reporting misuse of personal information was that the bank or other financial institution had already resolved the issue, followed by respondents not thinking it was important enough to report.

The proportion of respondents who were unaware of Victims' Certificates decreased from 80.5 percent in 2016 to 71.8 percent in 2018. Victims' Certificates can be obtained from a court to prove occurred person has been the victim of identity crime. Geographic location was associated with awareness of Victims' Certificates, with respondents living in capital cities having the highest levels of awareness.

Risk and prevention of future personal information misuse

Almost one in five respondents reported believing the risk of their personal information being misused would increase greatly in the next 12 months. A further 46.4 percent reported their risk would increase 'somewhat.' Respondents who had experienced misuse of personal information in the last 12 months were more likely than other respondents to report that their level of risk would increase 'greatly' in the next 12 months. A small number of recent victims (n=16) reported that their level of risk would decrease greatly.

Respondents were asked to describe their perceptions of the seriousness of misuse of personal information in terms of harm to the Australian community, regardless of their personal experience. Almost all respondents (96.9%) reported that misuse of personal information was 'very serious' or 'somewhat serious'. Respondents who had experienced misuse in the last 12 months were more likely to rate misuse as 'very serious' than respondents who had not experienced misuse. Respondents who had not experienced misuse were also more likely than recent victims to rate misuse as 'not at all serious'.

The survey also asked respondents about their willingness to use biometrics to protect personal information and to engage with government and business. To protect personal information in the future, respondents reported being most willing to use passwords and fingerprint scanning. Willingness to use passwords to protect personal information increased 56.4 percentage points from 2016. There is no clear explanation for this increase, other than concern about protecting information. Almost half of respondents (45.3%) were willing to use facial recognition in the future to protect personal information. When a number of security technology scenarios were posed, respondents were most willing to use facial recognition for airport security and to detect terrorists and criminals—all government activities as opposed to private sector ones.

Conclusions

This year's survey found an Australia-wide increase in reported misuse of personal information in the last 12 months, with 13 percent of survey respondents reporting such misuse. The most likely explanation for the rise in victimisation is the increase in phishing attacks reported globally (APWG 2017). In 2017, reports of personal information having been obtained via telephone, text message and face-to-face meetings substantially increased. The misuse of names, addresses and dates of birth also increased substantially. The growth in both of these measures could reflect an increase in personal information being compromised via phishing attacks.

Card-not-present fraud experienced unprecedented growth in 2016, according to the Australian Payments Network (2017). However, there is no evidence that card-not-present fraud underpinned the rise in misuse of personal information among this sample. There was a substantial reduction in respondents' reports of credit/debit card misuse and in misuse occurring in order to purchase something in 2017, compared with 2016. There was, however, a slight increase in personal information being obtained through ATM or EFTPOS transactions, or through online banking transactions, which would entail card-not-present fraud.

Misuse of personal information in connection with filing fraudulent taxation returns and obtaining access to superannuation monies increased substantially in 2017 compared with 2016. This finding is consistent with Australian Competition and Consumer Commission reports that taxation scams increased in 2016 and 2017 (ACCC 2018, 2017). It is also consistent with the findings of the Australian Criminal Intelligence Commission's (2017) report *Serious financial crime in Australia 2017*.

Consistent with the rise in the number of respondents experiencing misuse of personal information, almost double the number of victims reported out-of-pocket losses in 2017 compared with 2016. Perhaps due to differences in types of personal information obtained and the intended purpose of misuse, the median out-of-pocket loss per victim fell to $150, down from $300 in 2016. A commensurate reduction in the median amount recovered was also observed. Despite the reduction in the value of monetary losses, other financial, emotional and legal impacts all rose. In particular, there was an increase in the proportion of respondents reporting that they were refused government benefits, that they commenced legal action to clear debts or clear their name, and that they were wrongly accused of a crime. All of these impacts are potential consequences of the misuse of personal identifying details such as name, address and date of birth.

Behavioural changes that occurred as a consequence of experiencing misuse of personal information varied with the method of access and type of personal information misused. Misuse of credit/debit cards or banking details appeared to elicit the most uniform and appropriate responses, including changing passwords, changing banking details, and reviewing financial statements more carefully.

Satisfaction with government, business and organisational responses improved across almost all organisational types. The Passport Office received the highest satisfaction rating, and ACORN had the highest percentage point gain in satisfaction between 2016 and 2017. Satisfaction with police responses also increased substantially. This may have been in part due to a substantial increase between 2016 and 2017 in the number of respondents who were notified of the misuse of their personal information by police. The increase in police notifications appeared to occur across Australia and was not confined to any one region.

In sum, misuse of personal information was reported to have increased in the July 2016 to July 2017 period. This appears to be due largely to an increase in phishing attacks, but personal information was also obtained by telephone, text messages and face-to-face meetings. There is evidence that this information was used to obtain money from victims' bank accounts, as well as to commit taxation fraud and obtain access to superannuation monies. The survey also found an increase in victim satisfaction with the responses of government agencies, businesses and other organisations, and with the increase in police notifications of misuse.

Introduction

Identity crime is one of the most prevalent crime types in Australia. It has adapted and changed over time, from its beginnings in voter registration fraud (Smith 2002) to the data breaches, phishing attacks and scams of today. Identity crime involves exploiting vulnerabilities in systems, policies and procedures developed to identify individuals, businesses and government entities on enrolment and during authentication processes. It was defined by the United Nations Economic and Social Council (2007: 18) as 'crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes'.

The economic impact of identity crime and misuse in Australia was most recently estimated by the Australian Institute of Criminology (AIC) to be $2.65b in 2015–16 (Smith & Jorna 2018b). A substantial proportion of this, $239m, involved direct costs of identity crime suffered by individual members of the community via personal fraud (Smith & Jorna 2018b). The present study sought to assess the nature and extent of this crime type among a large sample of the Australian community in 2017.

Types of identity crime

In 2016, a consumer payments survey commissioned by the Reserve Bank of Australia found that credit and debit card use had, for the first time, surpassed cash as the most frequently used means of payment (Doyle, Fisher, Tellez & Yadav 2017). Cash payments now account for only 37 percent of consumer payments, down from 47 percent in 2013 (Doyle et al. 2017). Consumers' preference for card and online payments in part reflects an increase in online purchasing of goods and services. In 2016, Australians spent $714.5b using transaction cards, of which $534m was fraudulent. While fraud accounted for only a small proportion of overall card transactions (0.74%), it nevertheless had a large impact on individual victims and businesses, leading to declining trust in card payment systems.

Card-not-present fraud, in which valid card details are stolen and then used to make purchases or other payments without the card being physically present, mainly online or by phone, accounted for 78 percent of the value of all fraud on Australian cards in 2016 (Australian Payments Network (AusPayNet) 2017). The rise in this form of fraud may also be an unintended consequence of fraud control methods designed to make in-person fraud more difficult (AusPayNet 2017).

Another form of card fraud is counterfeit/skimming. This occurs when details are skimmed from a card's magnetic strip, usually at an ATM or point-of-sale terminal, and used to create a counterfeit, duplicate card (AusPayNet 2017: Glossary). Counterfeit/skimming has been substantially reduced by the introduction of chip and PIN cards and other fraud control measures. The practice has decreased 12 percentage points, from 23 percent of card fraud in 2011 to 11 percent in 2016 (AusPayNet 2017). Domestic counterfeit/skimming increased modestly, from $17m in 2015 to $21.4m in 2016, but remains at levels lower than those recorded in 2011.

Data breaches, or the disclosure of data to an unauthorised party (Verizon 2017), have increased in recent years. Such breaches can be accidental or caused by internal attacks or external hacking of corporate or government databases (Verizon 2017). Verizon has monitored data breaches since 2007 using voluntary reporting by organisations across the world. In 2016, the information industry experienced the heaviest losses from data breaches yet recorded (Verizon 2017). The information industry includes web portals and sites other than online retailers. These sites generally require users to provide names, addresses and other personal identification information when signing up for site access. Site access is usually secured by a single-factor authentication—that is, only one category of credentials—which makes the sites particularly vulnerable to attack. In 2016, 62 percent of data breaches featured hacking, 51 percent involved malware, and eight percent involved physical actions (Verizon 2017). Weak and/or stolen passwords were used in 81 percent of hacking-related breaches (Verizon 2017).

The most common method of attack recorded in 2016 was phishing via email (Verizon 2017). Phishing involves a blend of social engineering and technical subterfuge. Social engineering schemes seek to trick individual users into providing personal information or funds in response to a dishonest request in an email or cloned website that purports to be associated with a legitimate organisation (APWG 2017). Technical subterfuge schemes involve crimeware being installed on personal computers to intercept personal identity data, often by misdirecting victims to counterfeit websites or sending victims to legitimate websites via phisher-controller proxies that intercept the victims' keystrokes (APWG 2017). The Anti-Phishing Working Group (APWG) monitors phishing attacks on its member companies, global research partners and through email submissions. In the fourth quarter of 2016, APWG recorded the highest number of phishing attacks since data collection began in 2004. In 2016, 1,220,523 phishing attacks were recorded, a 65 percent increase on the number of attacks recorded in 2015 (APWG 2017). The most common industries targeted were retail/service (42%), financial (20%), internet service providers (13%) and payment services (11%).

An Australian example of phishing that occurred in 2016 involved the victim receiving a phone call or email advising that they were eligible for a pension or benefit from the Commonwealth Department of Human Services or Centrelink. The scammer either requested personal information or demanded money in order for the benefit to be paid. The Australian Competition and Consumer Commission (ACCC) received 2,200 reports of this scam in 2016, with $27,000 in losses recorded (ACCC 2017).

Phishing scams can also be used to commit taxation fraud. The Australian Taxation Office (ATO) estimated between January and August 2017, 29,000 people reported receiving phishing scams and lost a total of $1.6m (Robertson 2017). The losses arose from phishing scams in which criminals lodged false tax returns using a victim's personal identification details obtained via social media, data breaches or other sources. In June 2017, more than 1,000 taxpayers reported to the ATO that their personal information had been compromised. This constituted a 26 percent rise in reporting on the month before (ATO 2017). This substantial rise likely reflects an increase in scam activity around the end of the financial year.

Background to the survey

In April 2007, the Council of Australian Governments agreed to a National Identity Security Strategy. The aim of the strategy was to prevent identity crime and misuse, contribute to national security and facilitate the benefits of the digital economy, including by creating a national Document Verification Service to verify the authenticity of identity credentials (AGD 2012).

A review of the National Identity Security Strategy in 2012 recognised the need to quantify the nature and extent of identity crime and misuse, particularly the victimisation experiences of Australians. As a result, it recommended the creation of a longitudinal measure of identity crime and misuse to assess the effectiveness of policy and practice throughout Australia. To date, three *Identity crime and misuse in Australia* reports have been produced (AGD 2015; AGD 2016; Jorna & Smith 2018).

As part of the measurement framework, large-scale surveys have been conducted to determine respondents' experiences of victimisation over their lifetime and during the preceding 12 months. The surveys also assess their views concerning the risk of becoming a victim of identity crime in the ensuing 12 months. Further details of the survey are presented in the Methodology section, and the questionnaire is reproduced in *Appendix A*.

This survey is the fourth in the Identity Crime and Misuse in Australia series. The previous surveys were conducted by the AIC in 2013 (Smith & Hutchings 2014), 2014 (Smith, Brown & Harris-Hogan 2015) and 2016 (Smith & Jorna 2018a).

Purpose of this report

This report details the number, percentage and demographic characteristics of respondents who reported that their personal information was misused in the 12 months prior to July 2017. It also examines in more depth the most serious occasion of misuse of personal information in the last 12 months, and presents data on victim characteristics and how they changed their behaviour as a result of their personal information being misused. The report describes how crimes were detected, the financial and other impacts of misuse, the time and money victims spent dealing with the consequences, the reporting of misuse to private and public organisations, victims' subsequent satisfaction with responses to their reports, and perceptions of the risk of identity crime in the ensuing 12 months.

Methodology

Research design and definitions

This study employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information among a sample of Australian residents aged 15 to 96 years old. The methodology replicated three previous studies conducted by the AIC in 2013, 2014 and 2016 (see Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; and Smith & Jorna 2018a).

The definition of identity crime and misuse of personal information used in the survey was 'the use of personal information without permission'. This included obtaining personal information without permission, pretending to be someone else or carrying out a business in someone else's name without their permission. This definition excluded the use of personal information for direct marketing, even when this was done without permission.

Personal information was defined as including: name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (eg fingerprints), signature, bank account information, credit or debit card information, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), usernames and passwords, student identification numbers and similar types of personal information.

Survey questions

The questionnaire contained a mixture of closed-response and open-ended questions on the following topics:

- demographic and other characteristics of respondents including age, gender, usual place of residence, income, language spoken at home, Aboriginal and Torres Strait Islander status and computer usage;
- experience of misuse of personal information at any time in the past and over the preceding 12 months;
- method of victimisation on the most serious occasion in the preceding 12 months;
- actual financial losses, funds recovered, and other consequences of victimisation;
- whether and how respondents reported misuse of personal information and their satisfaction with the responses;
- behavioural changes arising from the misuse of personal information;
- awareness of the availability of court-issued Victims' Certificates;
- perceptions of the seriousness of misuse of personal information;
- perceptions of the risk of identity crime over the next 12 months; and
- use of security measures in the past and willingness to use them in the future to reduce the risk of identity crime victimisation.

These questions largely replicated those of the previous surveys so that direct comparisons could be made with earlier findings. The questions were originally developed in consultation with the Attorney-General's Department (AGD).

The questions spanned a number of reference periods. Demographic questions (eg usual place of residence, age and income) related to respondents' circumstances at the time of responding. Other questions asked about lifetime experience of identity crime and misuse, as well as identity crime and misuse experienced in the 12 months prior to completing the survey. The survey was available for completion during a two-week period at the beginning of July 2017.

The survey, which had 37 questions in total, took approximately 10 to 15 minutes to complete. No identifying information was requested from respondents. The questionnaire is presented in *Appendix A*.

Sampling

The survey was administered online by i-Link Research Solutions to members of its research panel of over 300,000 individual members throughout Australia. The de-identified data were then supplied to the AIC for analysis and reporting.

The non-probability sample consisted of 10,000 Australian residents aged 15 years and over (up to 96 years, the maximum age represented in the panel) who had internet access and who had registered with the panel provider. (Limitations associated with panel non-probability samples are discussed below.) Quotas were not employed at the point of recruitment.

Sampling was completed once the target sample size of 10,000 respondents had been obtained.

Respondents received incentives for completing the survey. They could select the type of reward they wished to receive from a range of incentives offered by the external provider. Examples of the incentives offered included:

- instant member reward points (accumulated to redeem gifts such as Caltex/Coles vouchers);
- chances to win $50,000 in a quarterly prize draw;
- donation of rewards to an affiliated charity; and
- chances to enter monthly competitions for prizes.

Weighting of data

Data were weighted by age and gender to represent the distribution of the Australian population. This is consistent with the approach to weighting undertaken in the 2016 survey. The Australian Bureau of Statistics (ABS) 2016 Census data for age and gender were used to develop the weighting matrix. The process of weighting involved applying a formula to data provided by each respondent who specified their gender and age category to make each response proportionate in relation to the broader population of Australians. Details of the weighting matrix are presented in Appendix B.

Comparisons with Census data show that respondents aged 15 to 24 years were under-represented in the 2017 survey (8.4% in the sample vs 15.7% in the Australian population. Male respondents were also under-represented in the sample (41.1%) in comparison with the Australian population (49.3%).

The 2016 Census did not provide an indeterminate/intersex/unspecified response or allow non-responses. This meant that the proportion of the Australian population not identifying as male or female is unknown. As a result, those not identifying as male or female were excluded from the survey analysis (n=13 indeterminate/intersex/unspecified; n=25 ‘I’d rather not say’), as the data for these groups could not be appropriately weighted. The 29 respondents who declined to indicate their age were also removed from the sample, as their data could not be appropriately weighted. This resulted in a final sample size of 9,947, noting that some participants declined to provide information on both gender and age. For further detail on the weighting of data, see Appendix B.

Analysis

Analysis undertaken was largely descriptive, centring on the characteristics of the sample and reported experiences of misuse of personal information. Bivariate analysis was undertaken to further examine the relationship between identity crime and the characteristics of the sample where a notable association was identified through descriptive analysis. Bivariate analyses undertaken and tests of statistical significance are described when used.

Where appropriate, 2016 and 2017 survey data were compared, with statistical significance of any difference calculated using MedCalc statistical software (https://www.medcalc.org/calc/comparison_of_proportions.php).

Ethical considerations

A number of ethical issues were considered when designing the study. These included:

- the need for research respondents to remain anonymous;
- the need to reach a large number of respondents;
- the need for informed consent;
- the presence of rewards for participation;
- the ability for respondents to withdraw from participation; and
- the potential for the research questions to cause psychological discomfort, particularly as they related to victimisation experiences.

To maintain the anonymity of participants, no identifying information was collected and results were presented in an aggregate form. The dataset was provided to the AIC in a de-identified format.

To ensure informed consent, respondents were given a plain language statement which detailed the nature of the research and the voluntary nature of participation. The statement also explained that individuals could withdraw from the study at any time, and that they could contact the external provider and have responses given prior to their withdrawal removed from the dataset. By commencing the survey, respondents indicated their consent to participate.

The risk of respondents experiencing psychological distress from participation was minimal, but could occur as the survey requested details of victimisation experiences. By describing the nature of the research in the plain language statement, some respondents who experienced distress on recalling identity crime victimisation may have opted not to participate. Details of support services were provided to all participants in the plain language statement. This included the telephone numbers and web addresses for Lifeline crisis support and IDCARE, which is a support centre for victims of identity crime funded by the Australian Government.

The research was approved by the AIC's Human Research Ethics Committee (approval no. P0265A).

Limitations

Because of resource constraints, the AIC's identity crime surveys use online non-probability panels to recruit respondents. Non-probability panels have consistently been identified as less accurate than probability panels and random digit dialling recruitment (Bethell et al. 2004; Malhotra and Krosnick 2007; Sanders et al. 2007; Yeager et al. 2011). This is most problematic when factors that determine a panel member's recruitment from the population are associated with the variables of interest. Problematic in this study is that the online panel required participants to have internet access, a variable which may be associated with an individual's chance of being a victim of identity crime. This limitation should be considered when interpreting the findings. It has the potential to limit the generalisability of the findings to the greater Australian population.

The limitations of human recall are also a factor in retrospective victimisation studies. Identity crime victimisation was identified via self-report. Given the nature of fraud, it can be difficult to determine when the crime occurred, as there may be a lapse in time between the individual's personal information being obtained, the misuse of that information and the victim finding out about the misuse. Another limitation is that some respondents may not identify themselves as a victim of identity crime despite having had their personal information breached if no financial loss was incurred.

In addition, the samples obtained in 2013, 2014 and 2016 were not entirely independent. Of the 9,947 respondents included in the 2017 sample, 153 respondents (1.5%) had completed the 2013 survey, 258 respondents (2.6%) had completed the 2014 survey, and 380 respondents (3.8%) had completed the 2016 survey. Less than one percent of respondents (n=21) reported having completed all three surveys (2013, 2014 and 2016). In total, 712 respondents (7%) had completed at least one previous identity crime and misuse survey. However, the 12-month reference period in 2017 was independent of those in previous years and so, for questions concerning victimisation over the preceding 12 months, the responses related to separate incidents. The total sample sizes were, in addition, large enough to provide adequate cell sizes for statistical analysis.

Despite these limitations, the 2017 identity crime survey results provide valuable information to inform policymakers and the public about the current extent and nature of identity crime and misuse of personal information in Australia.

Demographic characteristics of the sample

Place of residence

The distribution of survey responses and Census data by usual place of residence were closely aligned (see Table 1). South Australia was slightly over-represented in the survey data (8.8% vs 7.2%) and New South Wales slightly under-represented (28.8% vs 32.0%) compared with Census data. This discord in distributions is minor, however, with most residential location findings in the sample being within a few percent of the Australian population distribution.

Table 1: Respondents by usual place of residence

Source	ABS Census data	Survey sample data	
Location	%	n	%
Sydney	32.0	1,975	19.9
Other New South Wales		884	8.9
Melbourne	25.3	1,989	20.0
Other Victoria		705	7.1
Brisbane	20.1	1,122	11.3
Other Queensland		1,011	10.2
Perth	10.6	742	7.5
Other Western Australia		170	1.7
Adelaide	7.2	660	6.6
Other South Australia		221	2.2
Canberra (whole of ACT)	1.7	159	1.6
Hobart	2.2	102	1.0
Other Tasmania		152	1.5
Darwin	1.0	40	0.4
Other Northern Territory		15	0.2
Total	100.0	9,947	100.0

Note: Percentages may not total 100 due to rounding. ABS data are unweighted and identity crime survey data are weighted

Source: ABS 2017; Identity crime survey 2017 [AIC data file]

Language

Almost all survey respondents (94.3%) indicated that English was the language most often spoken at home (see Table 2). Two percent of survey respondents indicated that they spoke a language not listed. These responses included Vietnamese (n=18), Telugu (n=11), Tamil (n=11), Russian (n=11), Spanish (n=10), Greek (n=10) and Bengali (n=10).

Table 2: Respondents by language most often spoken at home (weighted data)

Language	n	%
English	9,383	94.3
Mandarin	81	0.8
Hindi	81	0.8
Cantonese	57	0.6
Italian	21	0.2
German	16	0.2
Arabic	16	0.2
Korean	16	0.2
Indonesian	14	0.1
Farsi	9	<0.1
French	8	<0.1
Japanese	4	<0.1
Other languages	218	2.2
I'd rather not say	25	0.3
Total	9,947	100.0

Note: Percentages may not total 100. Data are weighted and may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

Indigenous status

Five percent of survey respondents self-identified as being of Aboriginal, Torres Strait Islander or both Aboriginal and Torres Strait Islander descent (see Table 3). This is three percentage points higher than the proportion of Australians who self-identified as Indigenous in the 2016 Census. This suggests that Indigenous persons were over-represented in the 2017 identity crime survey. There was, however, a higher rate of non-response in the 2016 Census data than in the current survey. This may partially account for this difference, if it is assumed that Indigenous persons are less likely than non-Indigenous persons to take part in the Census.

Table 3: Respondents who identified as Aboriginal or Torres Strait Islander[a]

Source	ABS Census data	Survey sample data	
Indigenous status	%	n	%
Aboriginal		397	4.0
Torres Strait Islander		75	0.8
Both Aboriginal and Torres Strait Islander		55	0.6
All Indigenous	2.3	527	5.4
Non-Indigenous	91.5	9,327	93.8
I'd rather not say	6.2	93	0.9
Total	100.0	9,947	100.0

a: Survey data are weighted; ABS data are unweighted
Note: Percentages may not total 100 due to rounding
Source: ABS 2017; Identity crime survey 2017 [AIC data file]

Income

Respondents were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2016–17 (Table 4). Respondents most commonly reported having an income of between $37,001 and $80,000 (28.3%).

Almost 10 percent of respondents preferred not to divulge their income details.

Table 4: Respondents by individual gross income, 2016–17

Income	n	%
$0–$18,200	1,866	18.8
$18,201–$37,000	2,329	23.4
$37,001–$80,000	2,818	28.3
$80,001–$180,000	1,684	16.9
$180,001 and over	281	2.8
I'd rather not say	970	9.8
Total	9,947	100.0

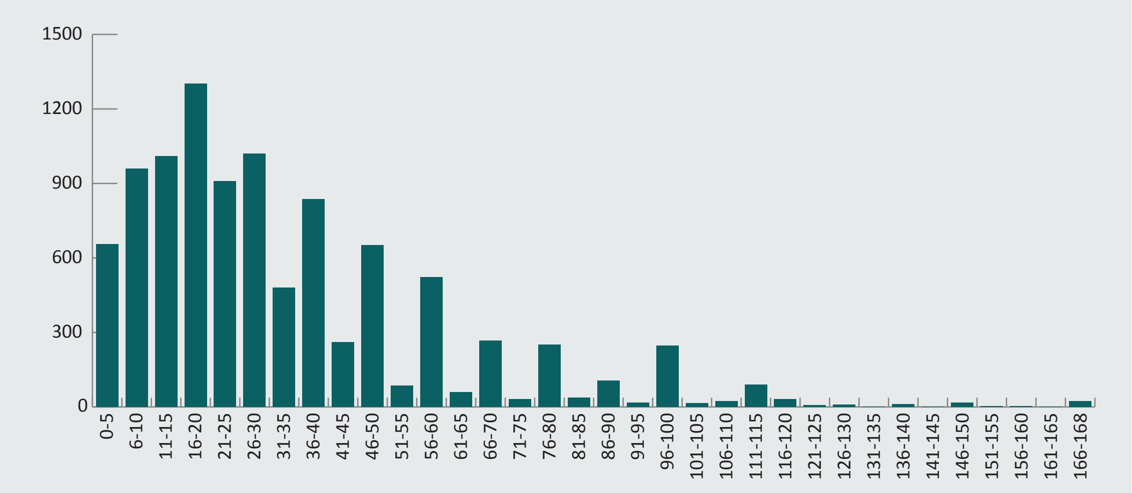
Note: Weighted figures may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

Computer use

Respondents were asked how many hours in the previous week they had spent using a computer or computerised device (including desktop computers, laptops, smartphones and tablets; see Figure 2). Responses (after weighting) ranged from zero to 168 hours (mean=34.6, SD=27.1, n=9,947). Sixty-four respondents indicated that they used a computer 136 or more hours per week, equating to less than five hours of sleep and other non-computing activities each day. Of these, 19 participants reported using computers or computerised devices for 168 hours per week (24 hours a day). Despite this being improbable, consistent with data analysis of previous surveys, participants were retained.

There was a modest increase of 7.7 hours in the average reported hours spent using a computer or computerised device between 2016 (mean=26.9) and 2017. There was also a larger standard deviation in 2017 than in 2016 (SD=19.8), indicating a greater spread of respondents across levels of computer use. This was due to a higher number of respondents in 2017 reporting that they spent more than 40 hours on devices per week (26.2% in 2017 vs 17.2% in 2016).

Figure 2: Hours spent using a computer or computerised device in the previous week (n)

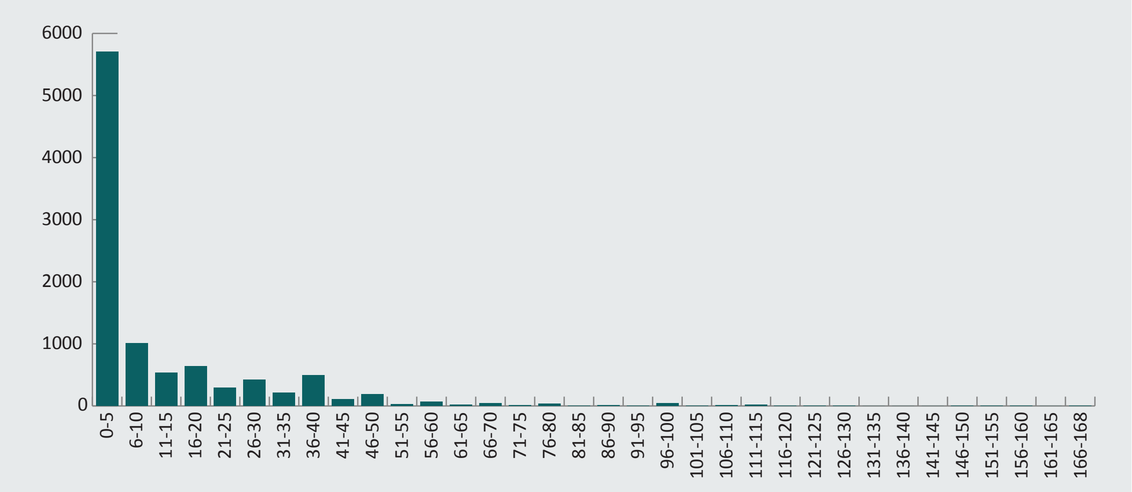


Note: Weighted figures may not total 9,947 due to rounding

Source: Identity crime survey 2017 [AIC data file]

Respondents were also asked how many hours in the previous week they had spent using a computer or computerised device for work-related activities. Responses ranged from zero to 168 hours (mean=12.18, SD=18.9, n=9,947). As shown in Figure 3, the majority of respondents (94.3%) reported spending 40 hours or less on computers or computerised devices in the previous week, with 74 percent of respondents reporting 15 hours or less. This represents a slight increase from the 2016 survey, in which the average number of hours using a computer or computerised device for work-related activities was 10 hours.

Figure 3: Hours spent using a computer or computerised device for work-related activities in the previous week (n)

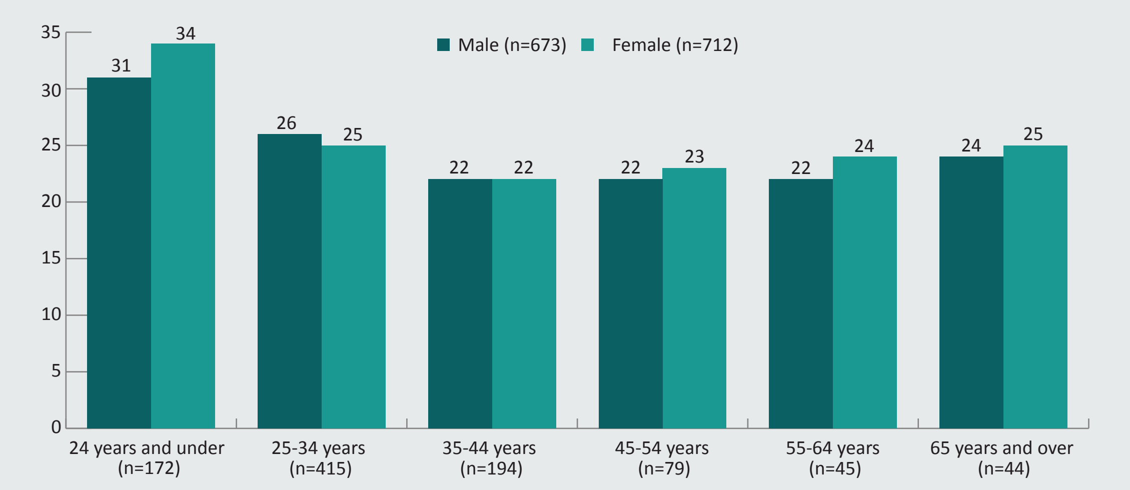


Note: Weighted figures may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

The number of hours spent on computerised devices for work were deducted from the total hours on computerised devices to determine the number of hours using devices for non-work related activities (see Figure 4). Respondents, on average, reported spending 22.4 hours on devices per week for non-work related activities (SD=21.8, n=9947). This is more than double the average number of hours per week spent on the internet for personal use reported in ABS data for 2014–15 (ABS 2016a). This difference may partially reflect growing internet use among Australians since 2015. It is, however, more likely a product of the recruitment of survey participants through an online survey panel. All participants were required to have internet access to join the panel.

Respondents aged 24 years or under reported a significantly greater number of non-work related computer hours per week than all other age groups: F(5,9101)=21.85, *p*<0.001 (log transformation of computer hours). This difference remained when total computer hours were examined by age: F(5,9942)=40.65, *p*<0.001. There were no statistically significant gender differences in the number of non-work related hours spent using a computer per week.

Figure 4: Mean number of non-work related hours on computer per week by age and gender (weighted data) (%)



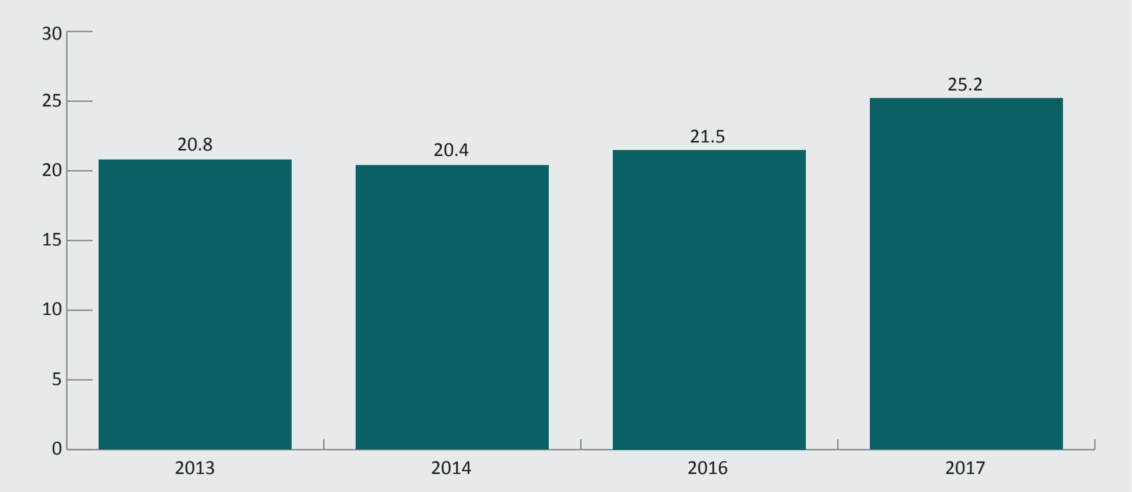
Source: Identity crime survey 2017 [AIC data file]

Prevalence of victimisation

Lifetime prevalence of victimisation

One in four respondents (25% of 9,947) reported that they had experienced misuse of their personal information at some point in their lifetime (see Figure 5). This was a statistically significant 3.7 percentage point rise in lifetime victimisation from 2016, when 21.5 percent of respondents (of n=9,956) reported lifetime victimisation: N-1 $\chi^2(1)=38.06$, $p<0.001$. This increase was driven by a rise in 2017 of reports of recent victimisation (see Figure 6).

Figure 5: Lifetime victimisation rates of respondents (weighted data) (%)

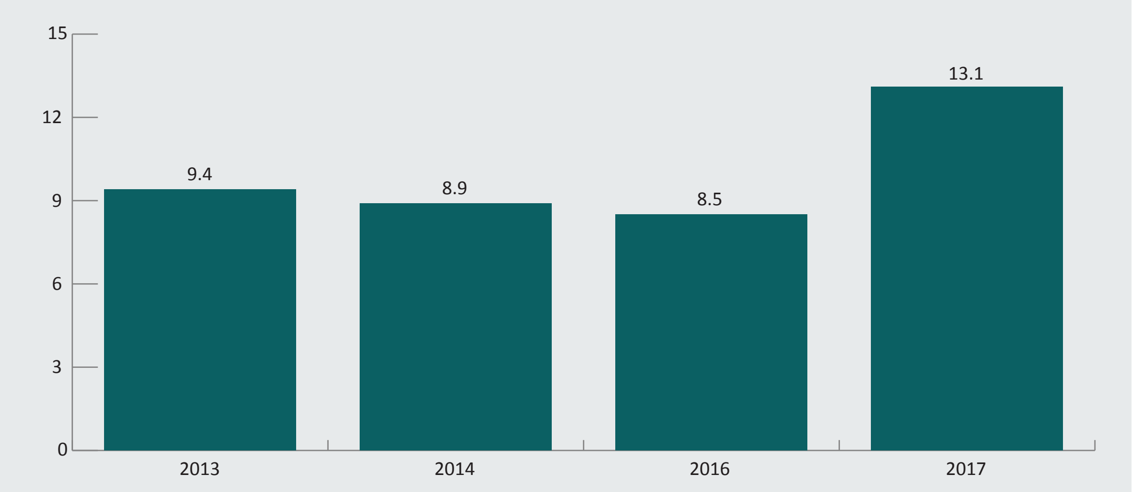


Source: Identity crime surveys 2013, 2014, 2016 and 2017 [AIC data file]

Victimisation in the last 12 months

Thirteen percent of respondents (n=1,307) reported that they had experienced misuse of their personal information in the last 12 months (hereafter referred to as recent victimisation). This was a statistically significant 4.6 percentage point increase from 2016, when 8.5 percent of respondents (n=848) reported recent victimisation: N-1 $\chi^2(1)=109.30$, $p<0.001$.

Figure 6: Respondents experiencing misuse of personal information in last 12 months, 2013, 2014, 2016 and 2017 (weighted data) (%)



Source: Identity Crime Survey 2013, 2014, 2016 and 2017 [AIC data file]

Recent victimisation and geographic location

The 2017 recent victimisation data were examined against geographic location to identify whether the observed rise in recent victimisation was confined to particular geographic locations (see Table 5). Comparing 2017 data with 2016 data, all regions recorded a rise in recent victimisation, with the exception of ‘other Western Australia’, which had a 3.8 percentage point decrease, and ‘other Tasmania’, which had a small decrease of one half of a percentage point.

The most notable rise in recent victimisation occurred in the Northern Territory. There was an 11.7 percentage point rise in recent victimisation in Darwin and a 7.7 percentage point rise in ‘other Northern Territory’ locations. The same number of Northern Territory respondents completed the survey in 2016 (n=49) and 2017 (n=49), minimising the influence of sample size on victimisation rate; however, the small sample size negatively impacts the finding’s reliability.

Hobart also recorded a seven percentage point increase in recent victimisation and Sydney recorded a 6.4 percentage point increase.

In sum, while some states reported greater fluctuations in recent victimisation than others, the overall 4.6 percentage point increase in recent victimisation cannot be attributed to any one state. It appears to represent an Australia-wide increase in recent victimisation.

Table 5: Respondents who experienced misuse of their personal information in the last 12 months by usual place of residence (unweighted data)

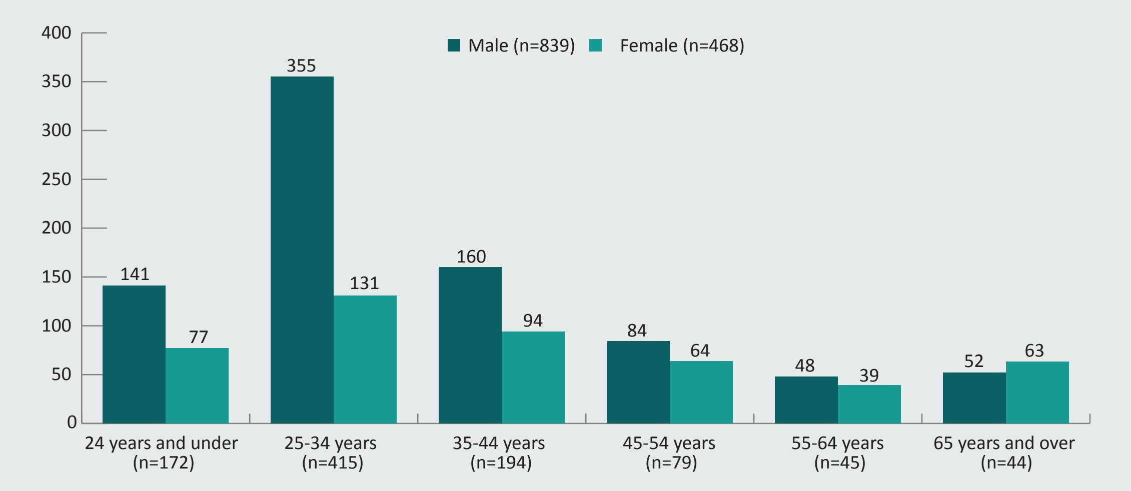
Location	2016	2017		% change
	%	%	n	
Sydney (n=1,890)	8.8	15.2	288	+6.4***
Other New South Wales (n=905)	9.4	12.6	114	+3.2***
Melbourne (n=1,979)	8.3	10.8	214	+2.5***
Other Victoria (n=708)	8.8	14.3	101	+5.5***
Brisbane (n=1,137)	7.3	10.6	120	+3.3***
Other Queensland (n=1,050)	8.1	9.1	95	+1.0*
Perth (n=719)	10.6	11.3	81	+0.7
Other Western Australia (n=183)	15.3	11.5	21	–3.8***
Adelaide (n=680)	6.8	8.5	58	+1.7***
Other South Australia (n=229)	5.8	10.0	23	+4.2***
Canberra (whole of ACT) (n=153)	9.9	10.5	16	+0.6
Hobart (n=107)	3.3	10.3	11	+7.0***
Other Tasmania (n=158)	10.0	9.5	15	–0.5
Darwin (n=36)	16.1	27.8	10	+11.7***
Other Northern Territory (n=13)	0.0	7.7	1	+7.7***
National (n=9,947)	8.5	11.7	1,168	+3.2***

***statistically significant at *p*<0.001, *statistically significant at *p*<0.05
Source: Identity crime survey 2017 [AIC data file]

Recent victimisation, age and gender

Males between 25 and 34 years of age were the group most likely to report having had their personal information misused in the last 12 months (see Figure 7). Consequently, males were significantly more likely than females to report having experienced personal information misuse in the last 12 months: $\chi^2(1, n=9{,}947)=86.90$, $p<0.001$ (see Table 6). Respondents between 25 and 34 years of age were also more likely to experience personal information misuse than other age groups: $\chi^2(5, n=9947)=504.96$, $p<0.001$ (see Table 7).

Figure 7: Recent victimisation by age and gender (weighted data) (n)



Source: Identity crime survey 2017 [AIC data file]

Table 6: Recent victimisation by gender (weighted data) (n)

Gender	Recent victimisation		
	Yes	No	Total
Males	629***	3,473	4,102
Females	539	5,306	5,845
Total	1,168	8,779	9,947

***statistically significant at *p*<0.001
Source: Identity crime survey 2017 [AIC data file]

Table 7: Recent victimisation by age (weighted data) (n)

Age group	Recent victimisation		
	Yes	No	Total
24 years and under	218	1,343	1,561
25–34 years	486***	1,274	1,760
35–44 years	254	1,389	1,643
45–54 years	147	1,475	1,622
55–64 years	87	1,352	1,439
65 years and over	115	1,806	1,921
Total	1,307	8,640	9,947

***statistically significant at *p*<0.001
Source: Identity crime survey 2017 [AIC data file]

Recent victimisation and Indigenous status

Respondents who self-identified as Aboriginal or Torres Strait Islander were more likely to report having had their personal information misused in the previous 12 months. Respondents who identified as non-Indigenous were significantly less likely to have reported recent victimisation: $\chi^2(4, n=9,946)=1,287.43$, *p*<0.001 (see Table 8).

Table 8: Recent victimisation by Indigenous status (weighted data) (n)

Indigenous status	Recent victimisation		
	Yes	No	Total
Aboriginal	267***	131	397
Torres Strait Islander	40	36	75
Both Aboriginal and Torres Strait Islander	32	24	55
Non-Indigenous	961	8,366***	9,327
Total	1,300	8,557	9,854

***statistically significant at *p*<0.001
Source: Identity crime survey 2017 [AIC data file]

Recent victimisation and computer use

There was a significant association between victimisation and computer use, but not in the direction expected. Respondents who had experienced personal information misuse reported using a computer fewer hours per week than those who did not experience misuse. This finding held when total computer hours (t(9,894)=–7.51, *p*<0.001), computer hours for work purposes (t(5,726)=–3.82, *p*<0.001) and computer hours for non-work purposes were compared (t(9,104)=–1.82, *p*<0.05). The unweighted mean number of hours per week victims spent using a computer for non-work purposes was 19.58 (SD=23.59), while non-victims reported an unweighted mean of 22.38 (SD=20.82).

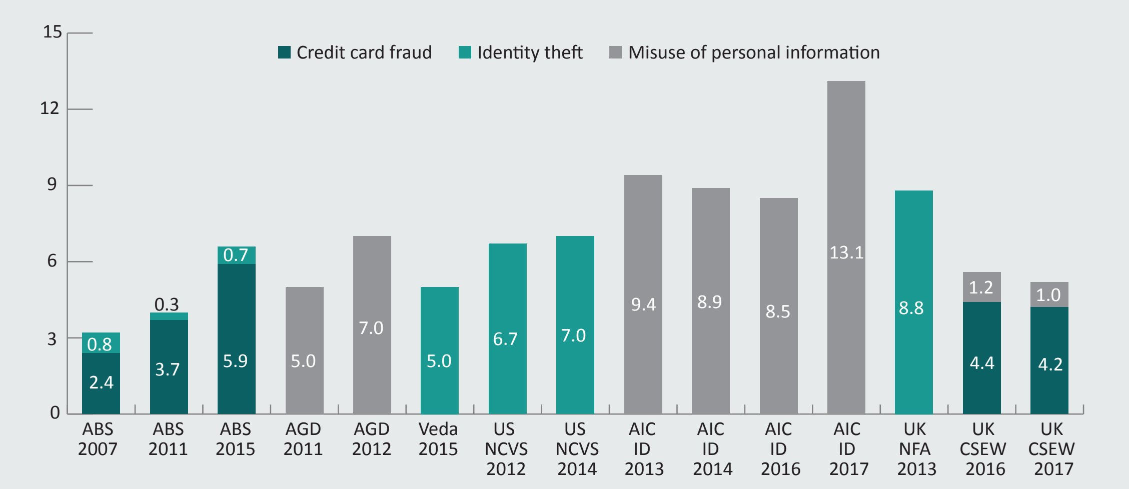
International prevalence of identity crime

International estimates of identity crime prevalence are of limited value in determining whether the rise in recent victimisation reported here reflects trends in other locations (see Figure 8). This is due to the different questions asked in other surveys and the age of some international estimates.

The Crime Survey for England and Wales (CSEW) (ONS 2018) provides the most recent estimate of identity-related computer crime and fraud from October 2015 to December 2017. CSEW data indicate that incidents of computer misuse showed a statistically significant (*p*<0.05) decrease from 1.917m incidents in 2016 to 1.374m incidents in 2017. Unauthorised access to personal information (including hacking) showed a non-statistically significant decrease over the same period, from 642,000 to 534,000 incidents. Declining victimisation rates are shown in Figure 7.

The magnitude of victimisation estimates vary between surveys due to differences in the definition of identity crime and the data collection methodologies used. For example, the ABS Personal Fraud Survey (ABS 2016b) reports separately on card fraud (which 31% of respondents reportedly experienced in the 12 months prior to interview in 2014–15) and identity theft (experienced by an estimated 126,300 Australians in 2014–15). The current survey, however, reports all misuse of personal information without permission. Therefore, while it may be expected that all victimisation estimates will rise if the current data reflect a wider trend, the magnitude of that rise will be unique to each dataset. The Identity Crime and Misuse in Australia Survey estimates have consistently been higher than those reported by others. Because of this, the magnitude of the recent rise in victimisation reported by this survey (4.6 percentage points) is likely to be greater than would be expected in subsequent studies.

Figure 8: Respondents reporting identity crime victimisation over the preceding 12 months, by survey and year (%)



Note: The AGD surveys asked about victimisation in the previous six months, whereas the reference period in the other surveys was 12 months prior to survey completion. AIC surveys used weighted data

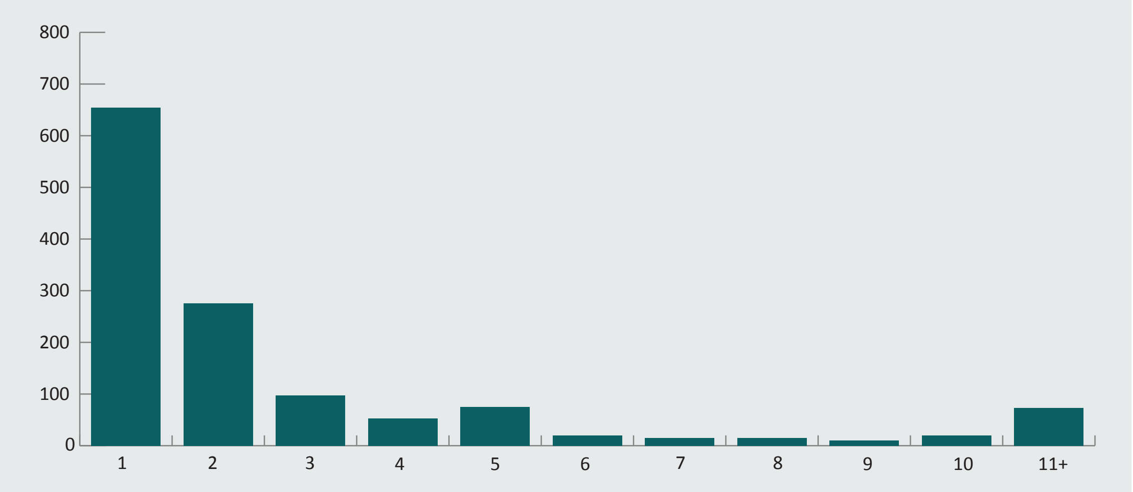
Sources: ABS *Personal fraud*, 2007 (ABS 2008); ABS *Personal fraud*, 2010–11 (ABS 2012); ABS *Personal fraud*, 2014–15 (ABS 2016b); AGD 2011 survey (Di Marzio Research 2011); AGD 2012 survey (Di Marzio Research 2012); Veda 2015; US National Crime Victimization Survey (NCVS) 2012 (Harrell & Langton 2013); US NCVS 2014 (Harrell 2015); AIC survey 2013 (Smith & Hutchings 2014); AIC survey 2014 (Smith, Brown & Harris-Hogan 2015); AIC survey 2016 (Smith & Jorna 2018a); AIC survey 2017 (current study); UK NFA 2013; UK CSEW 2016 (ONS 2017); UK CSEW 2017 (ONS 2018)

Misuse of personal information in the last 12 months

Number of occasions of personal information misuse

Fifty percent (n=654) of recent victims reported that their personal information had been misused on one occasion (see Figure 9). Another 21.1 percent (n=276) reported misuse of personal information had occurred on two separate occasions. On average, recent victims reported misuse of their personal information on five separate occasions (mean=5.13, SD=23.28).

Figure 9: Number of separate occasions on which respondents believed their personal information had been misused (weighted data) (n)



Source: Identity crime survey 2017 [AIC data file]

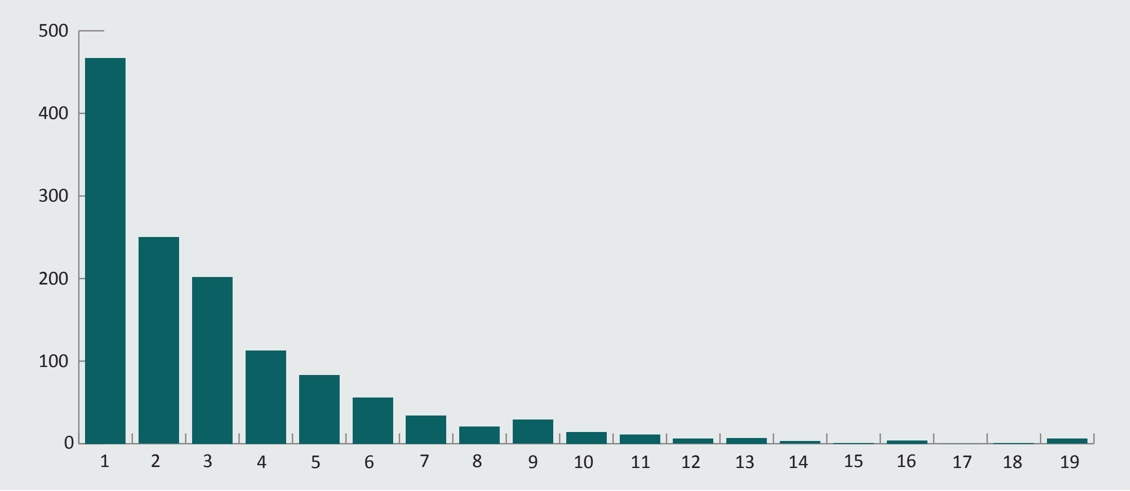
Number of types of personal information misused on most serious occasion

Respondents who had experienced misuse of their personal information in the last 12 months were asked to identify the most serious occasion of misuse. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the respondent. This occasion was selected based on respondents' subjective assessments of harms experienced.

Recent victims reported that between one and 19 different types of personal information had been misused on the most serious occasion of victimisation in the last 12 months (see Figure 10). On average, recent victims reported that three types of information had been misused (SD=2.87, n=1,307). Only four percent of victims reported 10 or more types of personal information were misused.

Of the 35.7 percent of recent victims who reported misuse of only one type of personal information, 36.8 percent (n=172) reported that the information misused was credit/debit card details. The second most common response was misuse of a name (15.1%, n=70), followed by bank account information (9.5%, n=45).

Figure 10: Number of types of personal information misused on the most serious occasion in the last 12 months (weighted data) (n)



Source: Identity crime survey 2017 [AIC data file]

Type of information misused on most serious occasion

Among all recent victims, a person's name (45.2%) was the most common type of personal information reported by recent victims to have been misused on the most serious occasion of misuse (see Table 9). This was followed by credit/debit card information (36.2%), then address details (35.8%), date of birth (32.2%), bank account information (26.1%), and password (20.3%). Comparing 2016 and 2017 data, there was a significant increase in reported misuse of address details (13 percentage points), name (10.6 percentage points), and date of birth (10.1 percentage points).

For the first time, name overtook credit/debit card information as the most common type of personal information to be misused. There was a 13.6 percentage point decrease in misuse of credit/debit card information from 2016 to 2017. This finding cannot be explained by a decrease in credit/debit card use, as the Reserve Bank's 2016 Consumer Payments Survey showed that debit and credit card use increased over this period (Doyle et al. 2017).

Table 9: Types of personal information respondents believed were misused in the most serious occasion of misuse in the previous 12 months (weighted data)

Type of personal information	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
Name	34.6	45.2	590	+10.6***
Credit/debit card information	49.8	36.2	474	–13.6***
Address	22.8	35.8	468	+13.0***
Date of birth	22.1	32.2	421	+10.1***
Bank account information	27.0	26.1	340	–0.9
Password	19.6	20.3	265	+0.7
Gender	14.3	18.1	237	+3.8*
Place of birth	9.2	14.6	191	+5.4**
Driver licence information	8.9	14.4	188	+5.5***
Online account username	13.3	10.3	135	–3.0*
Personal identification number (PIN)	7.0	8.8	116	+1.8
Passport information	4.1	8.5	111	+4.4***
Computer username	10.6	8.4	109	–2.2
Signature	6.8	8.2	107	+1.4
Tax file number	4.0	7.9	104	+3.9**
Medicare information	6.0	7.5	98	+1.5
Biometric information (eg fingerprint)	0.6	2.8	36	+2.2**
Shareholder information number (HIN)	1.3	2.8	36	+1.5**
Student number	0.4	2.5	33	+2.1**
Other	7.4	4.5	58	–2.9**

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

How personal information was obtained on most serious occasion of misuse

Recent victims were asked to indicate how they believed their personal information had been obtained on the most serious occasion of identity crime experienced in the last 12 months (see Table 10). Respondents could select multiple options.

The forms of access that experienced the greatest increases between 2016 and 2017 were face-to-face meetings (13.6 percentage points), telephone (excluding text messages—13.2 percentage points), and text message (10.3 percentage points). They were also the most common forms of access reported, along with email (21.4%). The number of respondents reporting that they did not know how their personal information was obtained declined notably (7.1 percentage points) from 2016 to 2017.

There was a small decrease (2.8 percentage points) in the proportion of recent victims reporting their personal information had been obtained from information placed on a website other than social media (eg online shopping). This does not represent a statistically significant decrease.

Table 10: How personal information was obtained on the most serious occasion of misuse in the previous 12 months (weighted data)

Way of obtaining personal information	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
Telephone (excluding text message)	11.7	24.9	325	+13.2***
Face-to-face (eg a job interview or a doorknock appeal)	9.6	23.2	303	+13.6***
Email	18.4	21.4	279	+3
Text message	8.5	18.8	246	+10.3***
Theft or hacking of a computer or other device	20.0	18.2	237	–1.8
Online banking transaction	15.8	17.1	224	+1.3
ATM or EFTPOS transaction	6.9	11.6	151	+4.7**
Website other than social media (eg online shopping)	14.3	11.5	150	–2.8
Social media (eg Facebook, Linked-In)	9.2	9.9	130	+0.7
Information lost or stolen from a business or other organisation (ie data breach)	9.2	8.9	116	–0.3
From a person I know[a]	–	4.0	53	4.0
Theft of mail	3.3	3.4	45	+0.1
Theft of an identity or other personal document	2.1	1.8	24	–0.3
Theft of a copy of an identity or other personal document	1.2	0.7	10	–0.5
Other	6.1	2.9	38	–3.2**
Don't know[a]	21.8	14.7	192	–7.1***

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01
a: Included in 2017 survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Intended use of personal information on most serious occasion of misuse

The most common reason personal information had been misused on the most serious occasion of misuse, according to respondents, was to obtain money from a bank account (37.5%; see Table 11). This was also the most common use reported in 2016 (31.1%). There was a 16.3 percentage point rise in recent victims reporting that their personal information had been used in multiple ways (18.5% in 2016 vs 34.8% in 2017). Recent victims reported, on average, having their personal information used in two ways (mean=1.70, SD=1.29).

There were statistically significant increases between 2016 and 2017 in the use of personal information to file fraudulent tax returns (13.2 percentage points; N-1 $\chi^2(1)=64.68$, $p<0.001$) and to obtain superannuation monies (12.0 percentage points; N-1 $\chi^2(1)=68.25$, $p<0.001$).

There was also a statistically significant 13.3 percentage point decrease in the misuse of personal information to purchase something: N-1 $\chi^2(1)=53.64$, $p<0.001$. This finding, considered with the reported decrease in misuse of credit/debit card information (see Table 9), suggests a lower level of card-not-present fraud in this sample than in the 2016 sample. This is despite card-not-present fraud being the most prevalent type of fraud on Australian cards (Australian Payments Network 2017).

Table 11: How personal information was misused on the most serious occasion in the previous 12 months (weighted data)

Category of misuse	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
To obtain money from a bank account (excluding superannuation)	31.1	37.5	490	+6.4**
To file a fraudulent tax return	8.6	21.8	284	+13.2***
To obtain superannuation monies	5.1	17.1	224	+12.0***
To purchase something	29.7	16.4	214	–13.3***
To obtain money from an investment (eg shares)	7.5	10.6	139	+3.1*
To apply for a loan or obtain credit	6.1	9.9	129	+3.8**
To apply for a job	3.9	8.8	115	+4.9***
To open a mobile phone account	4.7	7.7	101	+3.0**
To apply for government benefits	3.3	6.7	87	+3.4**
To provide false information to police	3.1	4.0	52	+0.9
To open an online account (eg Facebook, eBay)	4.9	3.0	39	–1.9*
To rent a property	1.8	2.0	26	+0.2
Other	9.4	5.5	72	–3.9**
Don’t know	13.6	11.5	150	–2.1

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Detection of most serious occasion of misuse

Recent victims of identity crime were asked how they became aware of the misuse of their personal information on the most serious occasion of misuse in the last 12 months (Table 12). Again, multiple responses could be selected.

As in 2016, victims were most commonly notified of the misuse of their personal information by a bank, financial institution or credit card company (40.8%). The majority of respondents (74.1%) reported detection of the misuse of their personal information via one method, 14.8 percent reported two detection methods, and 11.2 percent detection via three or more methods (mean=1.43; SD=0.87).

Table 12: How misuse of personal information was detected on the most serious occasion in the last 12 months (weighted data)

Detection method	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
Notified by a bank, financial institution or credit card company	42.9	40.8	534	–2.1
Noticed suspicious transactions in bank statements or accounts	30.6	33.0	431	+2.4
Notified by police	11.9	27.5	360	+15.6***
Received a bill for which they were not responsible	5.8	11.1	145	+5.3***
Was unsuccessful in applying for credit	8.4	10.1	132	+1.7
Contacted by debt collectors	3.0	4.4	57	+1.4
Notified by another company	6.4	3.5	45	–2.9**
Notified by a government agency other than police	1.1	1.8	24	+0.7
Other	14.9	10.5	137	–4.4**

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01
Source: Identity crime survey 2017 [AIC data file]

There was a statistically significant 15.6 percentage point increase in police notifications of personal information misuse from 2016 to 2017: N-1 $\chi^2(1)=74.47$, $p<0.001$. To explore this finding further, the percentage of recent victims who were notified by police was calculated for each geographic region (see Table 13). There were no notable differences in police notifications by geographic region in 2017, with between 20 and 30 percent of recent victims in most regions reporting they were notified by police. When 2016 and 2017 data were compared, there were increases in the proportion of victims in each region reporting notification of misuse by police, with the exception of Canberra, Perth and Adelaide. Regional areas reported the largest percentage point increases in police notifications.

Table 13: Recent victims in each region who were notified by police (weighted data)

Location	2016	2017		% change
	%	%	n	
Sydney	13.1	30.1	100	+17.0
Other New South Wales	3.2	22.5	30	+19.3
Melbourne	8.1	30.8	75	+22.7
Other Victoria	6.1	38.5	45	+32.4
Brisbane	18.8	23.4	31	+4.6
Other Queensland	7.0	21.3	21	+14.3
Perth	23.3	21.6	19	–1.7
Other Western Australia	13.1	33.5	7	+20.4
Adelaide	21.4	18.5	11	–2.9
Other South Australia	7.4	30.4	7	+23.0
Canberra (whole of ACT)	36.4	22.6	4	–13.8
Hobart	0.0	35.3	4	+35.3
Other Tasmania	0.0	0.0	0	0.0
Darwin	0.0	31.4	4	+31.4
Other Northern Territory	0.0	100.0	1	100.0

Source: Identity crime survey 2017 [AIC data file]

Out-of-pocket, reimbursed and recovered losses

Total out-of-pocket losses for all personal information misuse experienced in last 12 months

Respondents were asked to provide an estimate of the total out-of-pocket losses from all occasions of misuse of personal information experienced in the last 12 months (see Table 14). Respondents were instructed to exclude from this estimate any money recovered or reimbursed and any costs associated with repairing what occurred.

Total out-of-pocket losses suffered by victims rose by $1,141,893 between 2016 and 2017. This was due to almost double the number of respondents reporting out-of-pocket losses in 2017 (n=950) compared with 2016 (n=488). The mean amount of out-of-pocket losses per victim fell from $3,696 in 2016 to $3,101 in 2017. The median, which is the midpoint on a frequency distribution of all losses reported, halved from $300 in 2016 to $150 in 2017. Therefore, although more victims reported a financial loss, the impact on each victim tended to be lower.

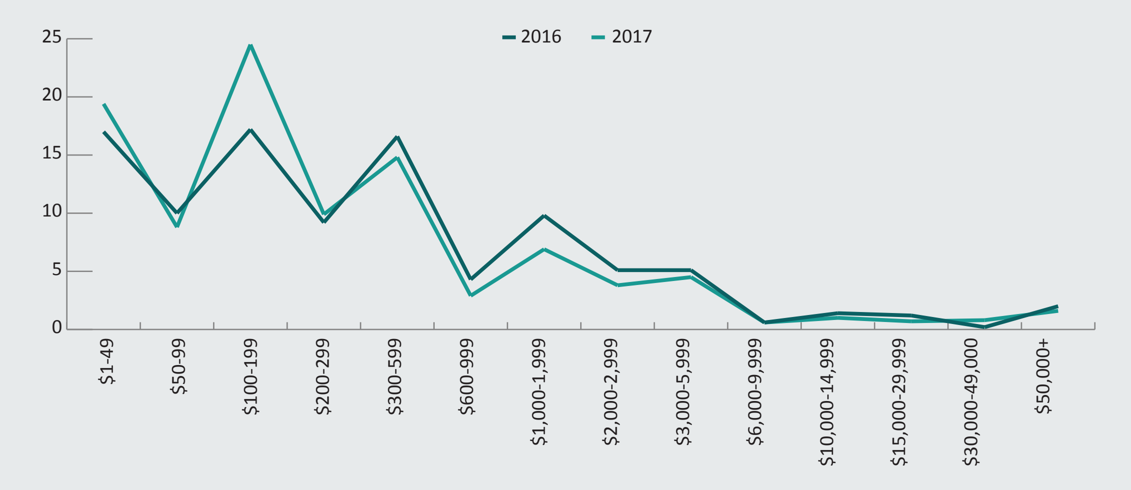
Table 14: Summary statistics for out-of-pocket losses for all personal information misuse experienced in the last 12 months

Statistic	2016	2017
Number of respondents	488	950
Minimum ($)	1	1
Maximum ($)	500,000	341,541
Mean ($)	3,696	3,101
Median ($)	300	150
Standard deviation ($)	28,680	20,199
25% quartile ($)	100	65
75% quartile ($)	1,000	498
Total ($)	1,802,893	2,944,786

Note: Median and quartiles calculated using unweighted data; all other statistics calculated using weighted data
Source: Identity crime survey 2017 [AIC data file]

The distribution of out-of-pocket losses as a percentage of the number of respondents (see Figure 11) shows a spike in reports of small, $100–$199, losses in 2017. The distribution of out-of-pocket losses otherwise closely mirrors the 2016 distribution. This suggests that a substantial proportion of the additional victims reporting losses in 2017, compared to 2016, reported losses in the $100–$199 range.

Figure 11: Distribution of total financial out-of-pocket losses, 2016 and 2017 (weighted data) (%)

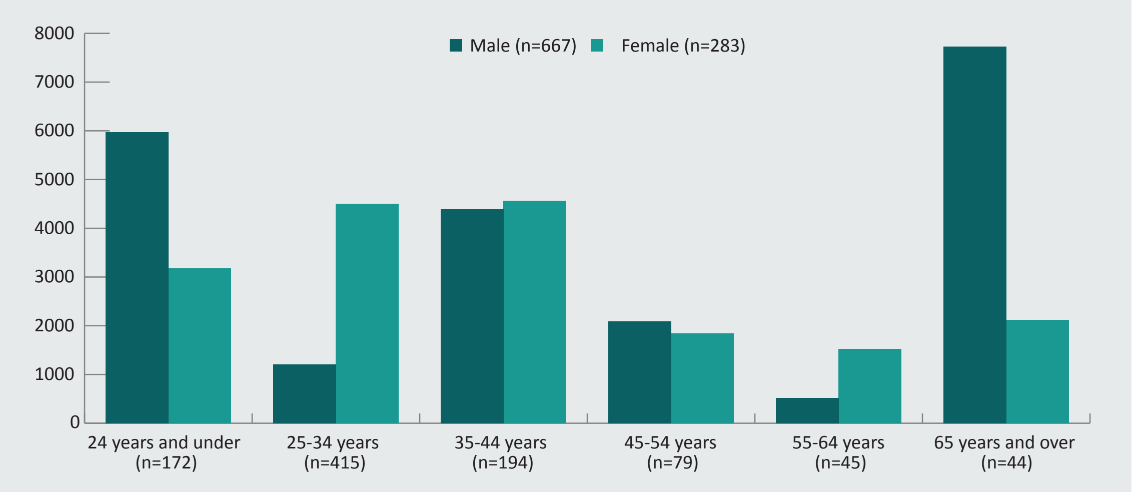


Source: Identity crime survey 2017 [AIC data file]

Male respondents aged 65 years and over reported the highest mean financial losses in 2017 ($7,729; see Figure 12). This was followed by males aged 24 years and under (mean=$5,967). Females aged 25 to 34 years reported higher losses ($4,501) than their male counterparts ($1,209). Gender disparity reduced among those 35 to 54 years of age, with male and female respondents in this age range reporting similar levels of loss.

As the number of respondents in some categories is relatively low, the mean financial loss reported may have been affected by outliers reporting large losses.

Figure 12: Mean total financial loss in the last 12 months by age and gender (weighted data) ($)



Note: Weighted figures may not total 950 due to rounding
Source: Identity crime survey 2017 [AIC data file]

Out-of-pocket losses for the most serious occasion of personal information misuse in the last 12 months

Respondents were also asked to report out-of-pocket losses for the most serious occasion of misuse of personal information in the last 12 months (excluding any money that they were able to recover from banks and any costs associated with repairing what occurred). The mean out-of-pocket loss reported was $2,711, which was almost $10,000 lower than the mean reported in 2016 (see Table 15). The maximum loss reported in 2017, $350,000, was considerably lower than that reported in 2016 ($654,646). This would have contributed to the reduction in mean losses. The data again suggest that losses associated with the most serious occasion of misuse in 2017, as with total losses, were, on average, lower per victim than those reported in 2016.

Table 15: Summary statistics for out-of-pocket losses for the most serious occasion of misuse in the last 12 months (weighted data) ($)

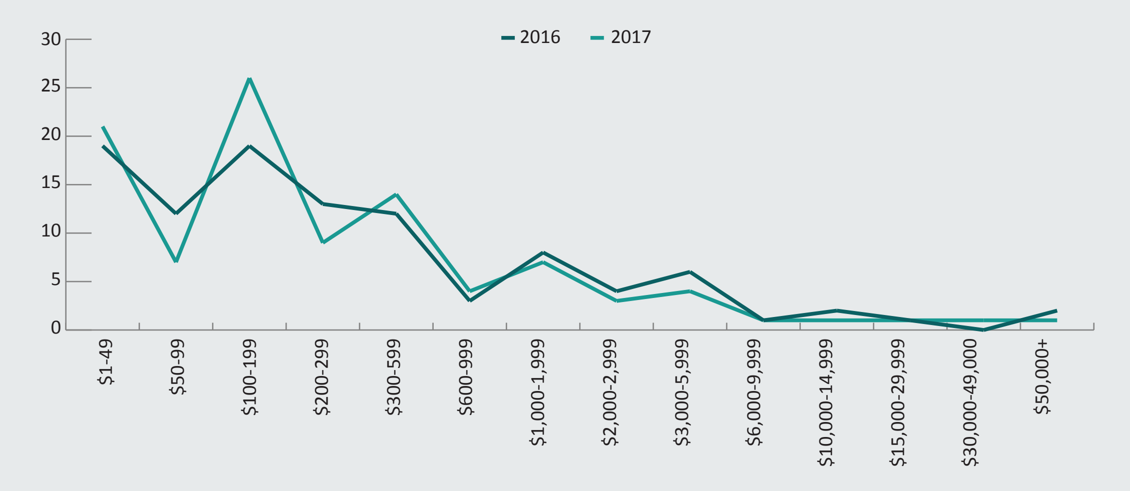
Statistic	2016	2017
Number of respondents	460	893
Minimum ($)	1	1
Maximum ($)	654,646	350,000
Mean ($)	12,466	2,711
Median ($)	199	136
Standard deviation ($)	82,856	18,474
25% quartile ($)	77	69
75% quartile ($)	1483	555
Total ($)	5,726,706	2,421,433

Source: Identity crime survey 2017 [AIC data file]

Note: Median and quartiles calculated using unweighted data; all other statistics calculated using weighted data

The distribution of out-of-pocket losses for the most serious occasion of misuse as a percentage of the number of respondents (see Figure 13) closely mirrors the 2016 distribution, with the exception of a spike in reports of small losses ($100–$199). There was also a reduction from 2017 to 2016 in reports of $50–$99 and $200–$299 losses for the most serious occasion of misuse.

Figure 13: Distribution of financial losses experienced on the most serious occasion of misuse in the last 12 months (weighted data) (%)



Source: Identity crime survey 2017 [AIC data file]

Total losses recovered in the last 12 months

The total amount of monies recovered fell substantially, from $7,725,761 in 2016 to $3,419,039 in 2017 (see Table 16). This reduction was also reflected in mean ($3,350 in 2017 vs $14,026 in 2016) and median ($200 in 2017 vs $400 in 2016) losses recovered. It is likely that the 2016 data were unduly influenced by a $4,500,000 loss recovered. The maximum loss recovered in 2017 was substantially lower, at $700,000. Caution should therefore be taken when comparing 2016 and 2017 recovered losses.

Twenty-two percent of respondents (n=286) who had experienced personal information misuse in the last 12 months reported recovering no money. Noting that, some losses experienced in 2017 and captured by the survey may have been recovered after the completion of the survey. For this reason, out-of-pocket losses captured by the survey and amounts recovered cannot be directly compared.

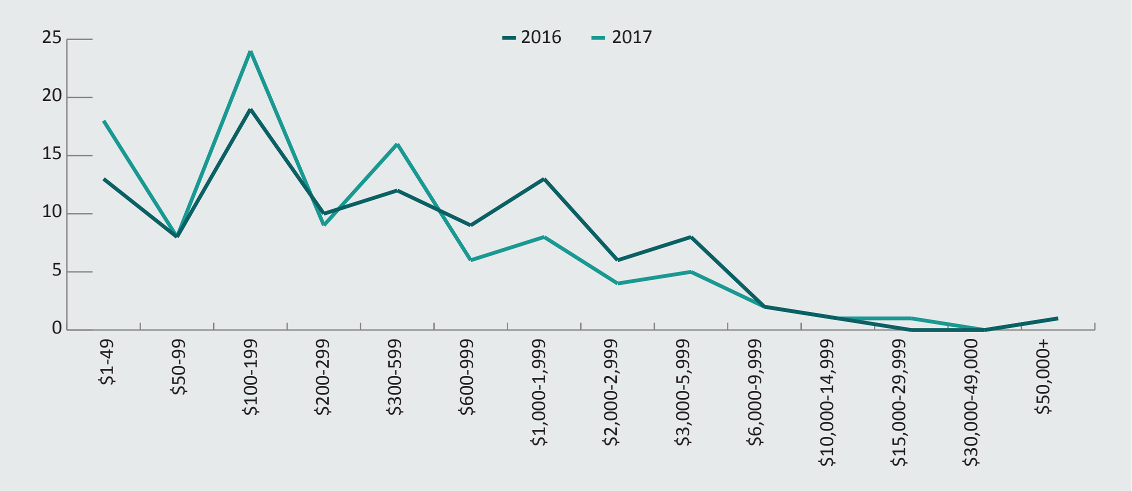
Table 16: Summary statistics for total losses recovered in the last 12 months ($)

Statistic	2016	2017
Number of respondents	550	1,021
Minimum ($)	1	1
Maximum ($)	4,500,000	700,000
Mean ($)	14,026	3,350
Median ($)	400	200
Standard deviation ($)	215,586	36,882
25% quartile ($)	100	86
75% quartile ($)	1,022	700
Total ($)	7,725,761	3,419,039

Source: Identity crime survey 2017 [AIC data file]

The distribution of total losses recovered in the last 12 months as a percentage of the number of respondents suggests that a higher proportion of respondents in 2017 received small ($100–$199) and modest ($300–$599) reimbursement amounts than in 2016 (see Figure 14). A smaller proportion of 2017 respondents than 2016 respondents had losses of over $600 recovered, with the 2017 distribution much flatter than the 2016 distribution after this value.

Figure 14: Distribution of total losses recovered in the last 12 months (weighted data) (%)



Source: Identity crime survey 2017 [AIC data file]

Recovered losses for the most serious occasion of misuse in the last 12 months

Total losses recovered for the most serious occasion of misuse in the last 12 months remained relatively stable between 2016 ($1,610,730) and 2017 ($1,500,352; see Table 17). However, as with total losses recovered for all misuse in the last 12 months, between 2016 and 2017 mean and median losses recovered for the most serious occasion of misuse decreased. In 2017, the mean amount recovered was $1,526 (down from $3,067 in 2016) and the median loss was $200 (down from $340). Almost twice as many respondents reported recovering money in 2017 (n=983) compared to 2016 (n=525). Consistent with earlier data, this suggests that more victims are recovering amounts lost, but the amount recovered per victim was, on average, lower than in 2016.

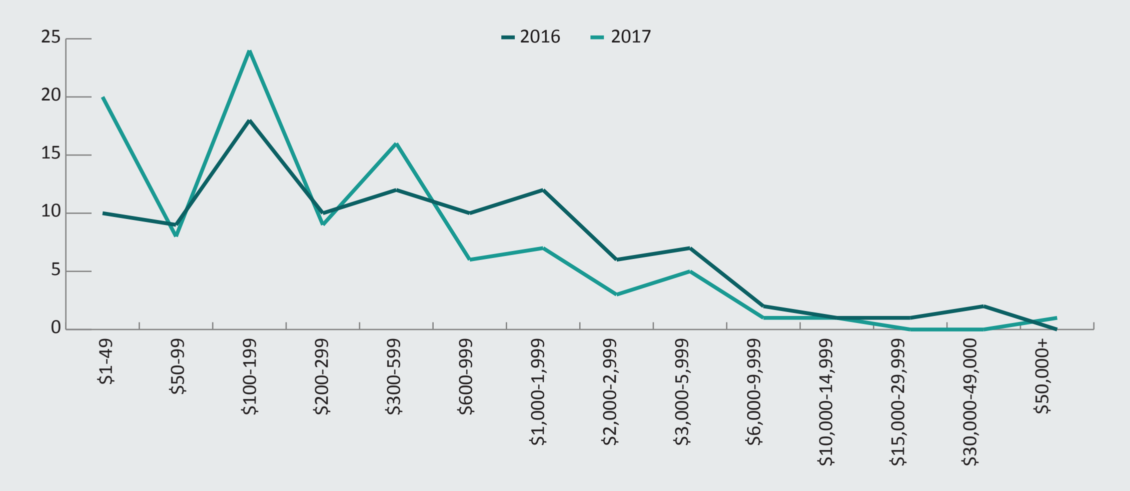
Table 17: Summary statistics for recovered losses relating to the most serious occasion of misuse in the last 12 months (weighted data) ($)

Statistic	2016	2017
Number of respondents	525	983
Minimum ($)	1	1
Maximum ($)	480,000	160,000
Mean ($)	3,067	1,526
Median ($)	340	200
Standard deviation ($)	25,552	9,719
25% quartile ($)	100	80
75% quartile ($)	1,200	600
Total ($)	1,610,730	1,500,352

Source: Identity crime survey 2017 [AIC data file]

The distribution of losses recovered for the most serious occasion of misuse in the last 12 months as a percentage of the number of respondents shows that substantially more respondents in 2017 than in 2016 reported recovering losses below $600 (see Figure 15). In particular, there were more reported recoveries of minor losses ($1–$49) and small losses ($100–$199). The number of respondents who reported recovering losses of between $300 and $599 also rose, although this increase was not as pronounced as at lower values. Consistent with findings for total losses recovered, a smaller proportion of 2017 participants than 2016 participants reported recovering losses of more than $600.

Figure 15: Distribution of losses recovered for the most serious occasion of misuse in the last 12 months (weighted data) (%)



Source: Identity crime survey 2017 [AIC data file]

Impact on victims

Consequences of personal information misuse

Respondents who reported experiencing misuse of their personal information in the last 12 months were asked to indicate any other consequences they experienced as a result of that misuse.

About a third of recent victims (35%, n=457) reported being refused credit as a consequence of their personal information being misused (see Table 18). This was a statistically significant increase on the proportion of victims reporting credit refusal (16.2%) in 2016: N-1 $\chi^2(1)=90.08$, $p<0.001$.

Another third of recent victims (34%, n=449) reported experiencing no negative consequences as a result of their personal information having been misused. This was a statistically significant reduction from the 55.9 percent of recent victims who reported the same in 2016: N-1 $\chi^2(1)=97.03$, $p<0.001$.

There were also 9.6 and 8.1 percentage point increases in the proportion of recent victims reporting refusal of government benefits and financial difficulties resulting in repossession, respectively.

Ninety-three respondents (7.1% of recent victims) reported experiencing consequences other than those listed. Of those respondents, 21 participants referred to experiencing a level of distress that did not require treatment.

Table 18: Consequences experienced as the result of personal information being misused in the previous 12 months (weighted data)

Consequence	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
I was refused credit	16.2	34.9	457	+18.7***
I experienced mental or emotional distress requiring counselling or other treatment	9.8	12.3	161	+2.5
I was wrongly accused of a crime	6.6	10.6	139	+4.0**
I experienced physical health problems requiring medical treatment by a doctor	3.0	5.6	73	+2.6**
I had to commence legal action to clear debts and/or to clear my name	4.3	11.2	147	+6.9***
I experienced financial difficulties resulting in the repossession of a house, land, motor vehicle or other items	5.2	13.3	173	+8.1***
I experienced other reputational damage	3.4	1.9	25	–1.5*
I was refused government benefits	5.3	14.9	195	+9.6***
I was refused other services	1.4	1.3	17	–0.1
I experienced other consequences not mentioned above	8.6	7.1	93	–1.5
I did not experience any consequences as a result of the misuse of my personal information	55.9	34.4	449	–21.5***

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Behavioural changes arising from the misuse of personal information

Respondents were asked how their behaviour had changed as a direct result of their personal information being misused (Table 19). Almost all respondents (93.5%) reported having changed their behaviour in some way.

The most common behaviour reported in 2017 was changing passwords after experiencing misuse of personal information (37.6%). This was, however, 10.5 percentage points lower than in 2016, when 48.1 percent of respondents reported changing passwords.

In comparison with the 2016 sample, there was an 8.8 percentage point decrease in reports of changing banking details after experiencing misuse. This concurs with earlier findings of a decrease in credit/debit card fraud among the 2017 sample.

Also in line with earlier findings indicating an increase in misuse of personal/address details, there were modest percentage point increases in reports of changing telephone numbers, redirecting mail, using a registered post office box and changing place of residence.

Table 19: Behavioural changes resulting from the misuse of personal information (weighted data)

Behavioural change	2016 (n=848)	2017 (n=1,307)		% change
	%	%	n	
Changed passwords	48.1	37.6	491	–10.5***
More careful when using or sharing personal information	34.5	31.8	416	–2.7
Changed banking details	36.2	27.4	357	–8.8***
Review financial statements more carefully	32.7	29.7	388	–3.0
Don’t trust people as much	24.2	25.1	327	+0.9
Use better security for computer and other computerised devices	23.5	23.4	306	–0.1
Shred personal documents before disposing of them	19.0	17.3	226	–1.7
Changed email address(es)	14.2	15.2	199	+1.0
Changed social media account(s)	11.5	13.5	176	+2.0
Ceased all social media use[a]	–	8.7	114	–
Lock mailbox	11.1	13.4	175	+2.3
Redirect mail when away or moving residence	7.3	11.2	147	+3.9**
Changed telephone numbers	7.1	11.6	152	+4.5**
Applied for a credit report	9.0	12.1	158	+3.1*
Use a registered post box	7.3	10.0	131	+2.7*
Changed place of residence	5.8	8.7	113	+2.9*
Signed up for a commercial identity theft alert/ protection service	6.5	7.4	96	+0.9
Avoid using the internet for banking and purchasing goods and services[a]	–	7.8	102	–
Other	5.8	3.9	51	–1.9*
Behaviour has not changed	8.9	6.5	85	–2.4*

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05
a: Included in 2017 identity crime survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Relationship between behavioural change and method used to obtain personal information

To examine how the method used to access personal information affected behaviour, the behavioural changes of those who experienced each of the most common methods of access were compared (see Table 20). This analysis examined the eight methods of obtaining personal information reported by 10 percent of victims or more.

More than half of all respondents who believed their personal information had been obtained via hacking reported changing passwords (63.4%) and being more careful when sharing personal information (57.7%). Nearly half of the same group reported using better security for their computer and other computerised devices (48.9%) and reviewing financial statements more carefully (47.4%), and 41.2 percent reported changing banking details.

Fifty-three percent of respondents who believed their personal information had been obtained via online banking reported changing passwords, and almost half reported changing banking details (45.9%) and reviewing financial statements more carefully (45.6%).

Respondents who believed their personal information had been obtained via ATM transactions most commonly reported changing passwords (53.6%), followed by reviewing financial statements more carefully (45.8%), being more careful sharing personal information (43.5%), and changing banking details (42.5%).

Behavioural responses to personal information being accessed via a website (excluding online shopping) included changing passwords (48.6%), being more careful when sharing personal information (44.1%), reviewing financial statements more carefully (40.7%), and not trusting people as much (40.0%).

Behavioural responses to personal information being obtained by telephone, in a face-to-face meeting, email or text message were more variable.

Table 20: Behavioural changes by method of obtaining personal information (weighted data) (%)

Behavioural change	Method by which personal information was obtained							
	Telephone (n=325)	Face to face (n=303)	Email (n=279)	Text message (n=246)	Theft or hacking (n=237)	Online banking (n=224)	ATM (n=83)	Other website[a] (n=150)
Changed passwords	30.0	27.3	38.2	28.4	63.4	52.5	53.6	48.6
More careful when using or sharing personal information	26.3	24.2	34.1	26.6	57.7	39.1	43.5	44.1
Changed banking details	25.2	21	23.6	24.1	41.2	45.9	42.5	34.3
Review financial statements more carefully	23.0	21.6	24.7	26.9	47.4	45.6	45.8	40.7
Don’t trust people as much	20.4	19.4	29.0	21.4	44.4	36.0	30.2	40.0
Use better security for computer and other computerised devices	24.2	18.0	27.0	23.8	48.9	33.1	31.1	33.1

Table 20: Behavioural changes by method of obtaining personal information (weighted data) (%)

Behavioural change	Method by which personal information was obtained							
	Telephone (n=325)	Face to face (n=303)	Email (n=279)	Text message (n=246)	Theft or hacking (n=237)	Online banking (n=224)	ATM (n=83)	Other website[a] (n=150)
Shred personal documents before disposing of them	19.0	18.4	18.4	24.1	23.5	23.9	18.8	25.2
Changed email address(es)	23.6	18.4	24.4	24.9	24.7	21.7	34.3	28.9
Changed social media account(s)	21.8	21.7	20.0	21.6	21.4	20.7	29.3	26.0
Ceased all social media use[b]	15.4	16.5	13.6	18.2	10.3	8.9	18.4	18.4
Lock mailbox	22.1	21.0	20.4	27.4	17.4	15.9	27.5	17.2
Redirect mail when away or move residence	15.7	17.9	12.6	19.1	15.4	18.6	22.6	14.1
Changed telephone numbers	17.5	16.0	21.5	21.4	20.2	19.2	19.4	22.3
Applied for a credit report	18.1	18.3	20.6	25.2	13.7	19.0	22.8	23.8
Use a registered post box	19.7	19.6	19.0	24.6	12.0	17.9	24.7	23.0
Changed place of residence	19.7	16.0	18.2	21.6	10.7	14.4	21.1	17.3
Signed up for a commercial identity theft alert/protection service	14.0	13.6	14.5	15.2	12.5	14.9	22.1	17.2
Avoid using the internet for banking and purchasing goods and services[b]	6.0	3.0	9.8	3.2	17.9	16.4	15.6	16.6
Other	1.1	1.0	4.0	0.3	5.5	6.0	0.0	7.3
Behaviour has not changed	0.9	2.0	1.3	0.5	2.5	2.0	3.6	2.9

a: 'Other website' category excludes online shopping websites

b: Included in 2017 identity crime survey only

Note: Respondents could select multiple responses

Source: Identity crime survey 2017 [AIC data file]

Relationship between behavioural change and type of personal information misused

Behavioural responses to the misuse of different types of personal information were compared. This analysis examined all types of personal information that at least 20 percent of victims reported as having been misused (see Table 21).

Fifty-nine percent of respondents who reported having had a password misused changed their password, followed by being more careful when using or sharing personal information (44.2%), and using better security for computers and computerised devices (40.0%).

Fifty percent of respondents who had their credit/debit card information misused reported changing passwords, and nearly half reported changing banking details (46.6%), reviewing financial statements more carefully (47.8%) and being more careful when sharing personal information (46.8%). Behavioural changes among respondents whose bank account details were misused were similar.

Respondents whose name had been misused reported changing passwords (42.5%), being more careful when using and sharing personal information (35.2%), reviewing financial statements more carefully (31.4%) and not trusting people as much (30.2%).

The most common response to having a date of birth or address misused was changing passwords (41.7% and 34.9% respectively).

Table 21: Behavioural changes by type of personal information misused (weighted data) (%)

Behavioural change	Type of personal information misused					
	Name (n=590)	Credit/ debit card (n=474)	Address (n=468)	Date of birth (n=421)	Bank account (n=340)	Password (n=265)
Changed passwords	42.5	50.4	34.9	41.7	49.6	58.6
More careful when using or sharing personal information	35.2	46.8	30.3	29.9	44.0	44.2
Changed banking details	28.4	46.6	25.2	26.4	47.5	36.0
Review financial statements more carefully	31.4	47.8	27.7	29.2	44.3	38.7
Don’t trust people as much	30.2	32.7	26.2	27.8	37.0	39.6
Use better security for computer and other computerised devices	28.6	34.2	26.4	27.0	38.2	40.0
Shred documents before disposing of them	19.3	22.5	17.5	20.9	23.0	22.6

Table 21: Behavioural changes by type of personal information misused (weighted data) (%)

Behavioural change	Type of personal information misused					
	Name (n=590)	Credit/ debit card (n=474)	Address (n=468)	Date of birth (n=421)	Bank account (n=340)	Password (n=265)
Changed email address(es)	21.9	17.0	20.3	22.5	21.5	28.7
Changed social media account(s)	19.3	14.5	18.4	20.5	19.3	21.1
Ceased all social media use[a]	13.1	8.0	11.2	11.4	11.0	17.8
Lock mailbox	17.6	12.0	18.2	19.6	15.0	18.6
Redirect mail when away or move residence	15.3	11.3	15.3	16.7	14.6	16.9
Changed telephone numbers	14.9	14.1	14.5	18.5	17.2	23.3
Applied for a credit report	15.9	13.1	18.0	18.6	17.6	21.3
Use a registered post box	13.6	10.2	13.4	17.7	15.2	18.7
Changed place of residence	12.4	9.1	15.3	15.2	13.1	17.9
Signed up for a commercial identity theft alert/protection service	11.6	6.8	12.5	13.2	10.4	14.8
Avoid using the internet for banking and purchasing goods and services[a]	9.2	14.8	8.1	8.4	14.7	12.9
Other	2.6	7.8	1.6	1.9	4.2	4.8
Behaviour has not changed	4.0	5.4	2.3	2.7	6.7	3.0

a: Included in 2017 identity crime survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Reporting the misuse of personal information

Of the 1,307 respondents who experienced misuse of their personal information in the previous 12 months, 10.3 percent (n=134) did not report the misuse in any way. This was almost the same proportion as in 2014 (10.1%), but lower than the 14.3 percent who failed to report in 2016. Fifty-seven percent of victims (n=743) told only a family member or friend; 7.4 percent of victims (n=97) told only a government agency, business or organisation; and 25.5 percent (n=333) told an agency and a family member or friend. In 2016, 50.8 percent of victims reported the misuse to family or friends only, 8.3 percent to an agency or organisation only, and 26.7 percent to both an agency and family or friends.

Satisfaction with reporting

Respondents who reported personal information misuse to a government agency, business or organisation were asked to specify who they reported the misuse to and how satisfied they were with the response (see Table 22). The majority of respondents were satisfied or very satisfied with the response, regardless of the agency to whom the misuse was reported.

Table 22: Government agencies, businesses and organisations reported to and satisfaction with responses, 2017 (weighted data)

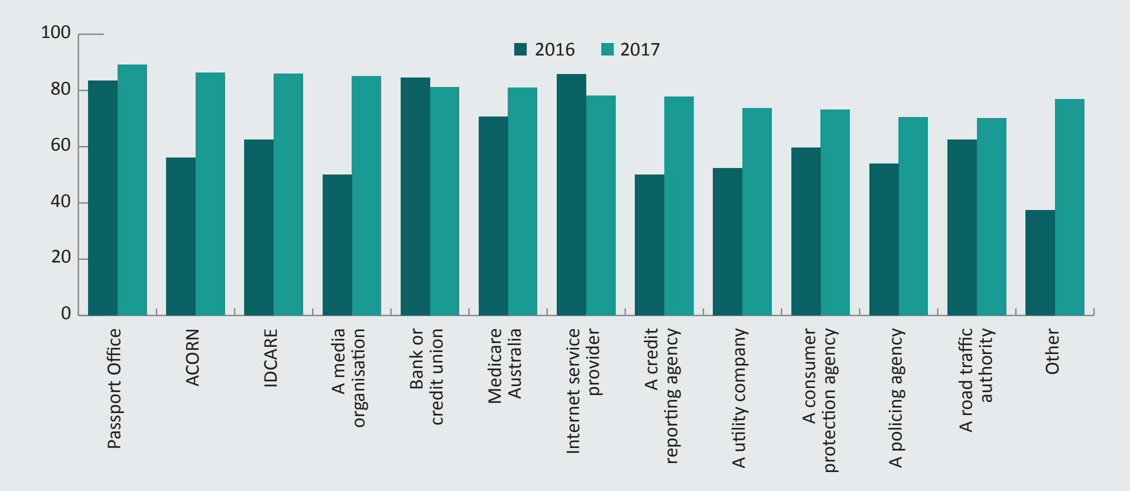
Agency/organisation reported to		Level of satisfaction			
		Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
Bank, credit union, credit/debit card company (eg Visa or MasterCard) or e-commerce provider (eg PayPal) (n=270)	n	112	107	30	21
	%	41.4	39.8	11.0	7.8
Police (n=141)	n	44	55	23	19
	%	31.3	39.2	16.4	13.1
Consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading) (n=74)	n	22	32	13	6
	%	29.5	43.6	18.2	8.8
Internet service provider (n=80)	n	15	48	13	4
	%	18.3	59.9	16.7	5.1
Credit reporting agency (eg Veda, Dun & Bradstreet) (n=56)	n	21	23	10	3
	%	37.1	40.8	17.1	5.1
Utility company (eg gas, electricity, telephone, water) (n=46)	n	12	22	7	5
	%	25.5	48.1	15.5	11.0
Medicare Australia (n=52)	n	19	23	7	3
	%	36.7	44.3	13.6	5.4
Media organisation (n=39)	n	10	22	4	2
	%	26.9	58.2	10.8	4.1
Passport Office (n=45)	n	14	25	4	1
	%	32.5	56.6	7.9	3.0
Road traffic authority (n=37)	n	10	16	9	2
	%	27.1	43.1	23.9	5.9
Australian Cybercrime Online Reporting Network (n=59)	n	25	26	4	4
	%	41.6	44.7	7.2	6.5
IDCARE (n=39)	n	18	16	4	2
	%	44.7	41.1	10.2	4.0
Other (n=42)	n	14	18	5	5
	%	32.8	44.0	11.3	11.9

Note: Percentages may not total 100 and weighted figures may not add up to totals due to rounding
Source: Identity crime survey 2017 [AIC data file]

Figure 16 shows the percentage of respondents who were satisfied or very satisfied with the response of each type of agency in 2016 and 2017. The Passport Office achieved the highest satisfaction rating, with 89.1 percent of respondents in 2017 stating they were either satisfied or very satisfied with the response. All categories of agencies either improved their satisfaction ratings or remained relatively stable, with the exception of internet service providers, whose satisfaction rating decreased by 7.5 percentage points, and banks and credit unions, whose rating decreased by 3.3 percentage points, noting that both types of entities retained high satisfaction ratings.

ACORN experienced the largest increase in satisfaction rating, with a 30.3 percentage point increase in the proportion of respondents who were satisfied or very satisfied (86.3% in 2017 vs 56.0% in 2016). There were also substantial increases in satisfaction with credit reporting agencies (a 27.8 percentage point increase), IDCARE (a 23.4 percentage point increase), utility companies (a 21.2 percentage point increase), and police (a 16.5 percentage point increase).

Figure 16: Respondents who were satisfied or very satisfied with the response, by agency (weighted data) (%)



Source: Identity crime survey 2016 and 2017 [AIC data files]

Respondents who indicated they had not reported the misuse of their personal information to a government agency, organisation or business were asked why they had not (Table 23). Multiple reasons could be given.

The most common reason given for not reporting the misuse was that the bank or other financial institution had already resolved the issue (32.5% of respondents who did not report). The second most common reason given was that the respondent did not think it was important enough to report (25.0%). These two response options were introduced in 2017 and so these responses cannot be compared with those of previous years. All other reasons for non-reporting showed a decrease in respondent endorsement. This was most likely due to the introduction of the two new response options. Nonetheless, the 12 percentage point decrease in the proportion of respondents saying they did not believe the police or any other authority could do anything and the 7.2 percentage point decease in respondents not knowing how or where to report the matter are encouraging.

Table 23: Reasons for not reporting misuse of personal information (weighted data)

Reason for not reporting	2016 (n=121)	2017 (n=877)		% change
	%	%	n	
Bank, credit union or credit card company had already resolved the issue[a]	–	32.5	285	–
Not important enough to report[a]	–	25.0	220	–
I did not believe the police or other authority would be able to do anything	33.9	21.9	192	–12.0
I did not know how or where to report the matter	28.1	20.9	183	–7.2
I was too embarrassed to report it	23.3	16.8	147	–6.5
I did not believe it was a crime	19.0	15.6	137	–3.4
Other	10.7	5.5	49	–5.2

a: Included in 2017 identity crime survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Victims' Certificates

All respondents, regardless of recent or lifetime victimisation, were asked if they were aware that a person whose personal information has been misused can apply to a court to obtain a Victims' Certificate to prove they are a victim of identity crime (see Table 24). The proportion of respondents unaware of Victims' Certificates significantly decreased from 2016 (80.5%) to 2017 (71.8%): N-1 $\chi^2(1)=207.4$, $p<0.001$.

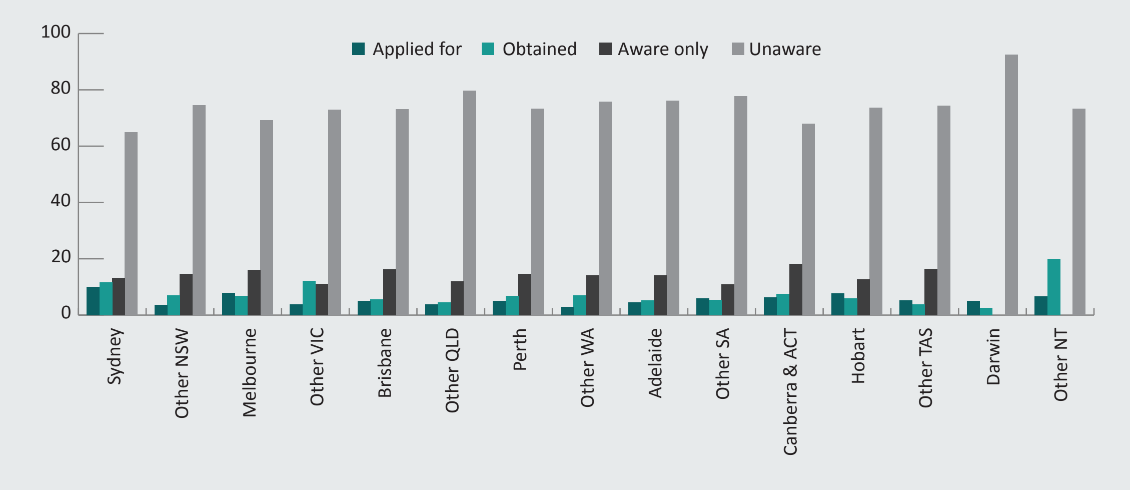
Table 24: Respondents' awareness of Victims' Certificates (weighted data)

	2016	2017	
	%	%	n
I am aware of such certificates, and have obtained one or more in the past[a]	–	7.6	759
I am aware of such certificates, and have applied for one in the past	5.0	6.3	625
I am aware of such certificates, but have not applied for any	14.5	14.3	1,421
I am unaware of such certificates	80.5	71.8	7,142
Total	100.0	100.0	9,947

a: Included in 2017 identity crime survey only
Source: Identity crime survey 2016 and 2017 [AIC data files]

For all states and the ACT other than the Northern Territory, a higher proportion of respondents living in capital cities reported being aware of Victims' Certificates, compared to respondents residing outside of a capital city (see Figure 17). The highest proportion of respondents who had applied for or obtained a Victims' Certificate in the past lived in Sydney and Melbourne.

Figure 17: Usual place of residence by awareness of Victims' Certificates (weighted data) (%)



Source: Identity crime survey 2016 and 2017 [AIC data files]

Notes: Only respondents in 2017 were asked if they had actually obtained a Victims' Certificate. Percentages are the number of respondents indicating awareness, or otherwise out of the total number of respondents in each category of usual place of residence. Percentages may not total 100 due to rounding

Risk and prevention of future misuse of personal information

Perceived risk of victimisation in the next 12 months

Respondents were asked whether they thought the risk of someone misusing their personal information would change over the next 12 months. Almost one in five respondents (19.7%) reported that their risk of being a victim of identity crime would 'increase greatly' in the next 12 months (see Table 25). A further 46.4 percent of respondents reported that they believed the risk would 'increase somewhat'.

Table 25: Respondents' perceptions about the risk of misuse of their personal information in the next 12 months (weighted data)

Change in risk of misuse of personal information	2016	2017	
	%	%	n
Risk will increase greatly	16.4	19.7	1,959
Risk will increase somewhat	45.3	46.4	4,613
Risk will not change	36.6	32.2	3,201
Risk will decrease somewhat	1.2	0.9	92
Risk will decrease greatly	0.6	0.8	83
Total	100.0	100.0	9,947

Note: Percentages may not total 100 and weighted figures may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

Additional analysis was conducted to examine whether being a recent victim of identity crime was associated with a perception that the risk of victimisation would increase. A significant relationship was identified between recent identity crime victimisation and predicted change in risk of victimisation in the next 12 months: (χ^2(4, n=9,947)=432.18, *p*<0.001). Recent victims were significantly more likely than non-victims to predict the risk of identity crime would 'increase greatly' in the next 12 months (see Table 26). Respondents who had not experienced identity crime in the previous 12 months were significantly more likely than recent victims to predict no change in risk in the next 12 months.

A small number of recent victims (n=16) reported that the risk of their personal information being misused would 'decrease greatly' in the next 12 months. The proportion of victims who reported reduced risk was greater than the proportion of non-victims who reported the same. This finding suggests that some victims, either because they had been a victim or perhaps because of steps taken after victimisation, believed themselves to be at a greatly decreased risk of identity crime in the future. When behavioural changes made after victimisation were examined, there were no notable differences between changes made by this group and other victims that would explain their perception of reduced risk.

Table 26: Contingency table for misuse of personal information in the previous 12 months and perceptions about the risk of misuse of personal information in the next 12 months (weighted data) (n)

Risk of misuse of personal information	Misuse of personal information in previous 12 months		
	Yes	No	Total
Risk will increase greatly	497***	1,462	1,959
Risk will increase somewhat	610	4,003	4,613
Risk will not change	170	3,031***	3,201
Risk will decrease somewhat	14	77	92
Risk will decrease greatly	16*	67	83
Total	1,307	8,640	9,947

***statistically significant at *p*<0.001, *statistically significant at *p*<0.05
Source: Identity crime survey 2017 [AIC data file]

Perceived seriousness of personal information misuse

Respondents were asked to give their opinion as to the seriousness of misuse of personal information in terms of harm to the Australian community. The respondents were not considered experts in identity crime, and as such the findings should be interpreted as indicating their personal opinions. Almost all respondents (96.9%) believed that misuse of personal information was a 'very serious' or 'somewhat serious' issue (see Table 27). This is a 1.2 percentage point increase from 2016.

Table 27: Respondents' perceptions about the seriousness of misuse of personal information (weighted data)

Seriousness	2016	2017	
	%	%	n
Very serious	63.7	65.2	6,483
Somewhat serious	32.0	31.7	3,152
Not very serious	3.6	2.8	278
Not at all serious	0.7	0.3	34
Total	100.0	100.0	9,947

Source: Identity crime survey 2017 [AIC data file]

Additional analysis was conducted to examine whether the rise in perceived seriousness related to experiences of personal information misuse. Perceptions of seriousness of personal information misuse were associated with having experienced victimisation in the last 12 months: $\chi^2(3, n=9,947)=32.15$, $p<0.001$ (see Table 28). That is, respondents who reported recent victimisation were more likely to rate personal information misuse as 'very serious' than those who had not experienced victimisation. Non-victims were also more likely than victims to rate personal information misuse as 'not at all serious'.

Table 28: Contingency table for misuse of personal information in the previous 12 months and perceptions of the seriousness of misuse of personal information (weighted data) (n)

Seriousness	Misuse of personal information in previous 12 months		
	Yes	No	Total
Very serious	891***	5,592	6,483
Somewhat serious	407	2,746	3,152
Not very serious	6	272	278
Not at all serious	3	31***	34
Total	1,307	8,640	9,947

***statistically significant at *p*<0.001
Note: Weighted figures may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

Willingness to use security measures to protect personal information

Respondents were asked whether they had ever used particular security measures in the past—that is, in any way, not just to prevent misuse of personal information. Consistent with 2016, most respondents (93.3%) reported using at least one of the measures listed (see Table 29).

Passwords were the most common security measure respondents had used in the past (90.8%). This was followed by signatures (41.4%) and fingerprint recognition (35%). The least common type of technology used in the past was a computer chip implanted under the skin (2.6%), followed by iris recognition (5.2%).

Comparing 2016 and 2017 data, there were considerable increases in the use of fingerprints (8.3 percentage points) and voice recognition (6.4 percentage points), and modest increases in the use of facial recognition (3.8 percentage points) and iris recognition (3.3 percentage points). The option 'computer chip implanted under the skin' was introduced in 2017 and so responses cannot be compared with those of previous years.

Table 29: Use of security measures in the past (weighted data)

Security measure	2016 (n=9,956)	2017 (n=9,947)		% change
	%	%	n	
Passwords	90.8	90.8	9,029	0.0
Signatures	41.8	41.4	4,117	–0.4
Voice recognition	11.5	17.9	1,784	+6.4***
Fingerprint recognition	26.7	35.0	3,476	+8.3***
Facial recognition	6.6	10.4	1,033	+3.8***
Iris recognition	1.9	5.2	514	+3.3***
Computer chip implanted under your skin[a]	–	2.6	254	–
Any of the above	92.8	93.3	9,280	+0.5
None of the above	7.2	6.7	667	–0.5

***statistically significant at $p<0.001$
a: Included in 2017 identity crime survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Respondents were then asked whether they would be willing to use these measures in the future to protect personal information—for example, at ATMs, at airports, or when using a computer or entering a building. Consistent with 2016, almost all respondents (94.3%) reported a willingness to use at least one of these technologies to protect personal information in the future (see Table 30).

The measure respondents most often said they were willing to use in the future was passwords (78.6%), followed by fingerprint recognition (63.8%). The measure respondents were least willing to use in the future was a computer chip implanted under the skin (9.4%).

When 2016 and 2017 data were compared, there was a statistically significant 56.4 percentage point increase in the willingness to use passwords. There were modest increases in willingness to use voice recognition (5.2 percentage points), signatures (2.9 percentage points), facial recognition (2.7 percentage points) and iris recognition (2.7 percentage points).

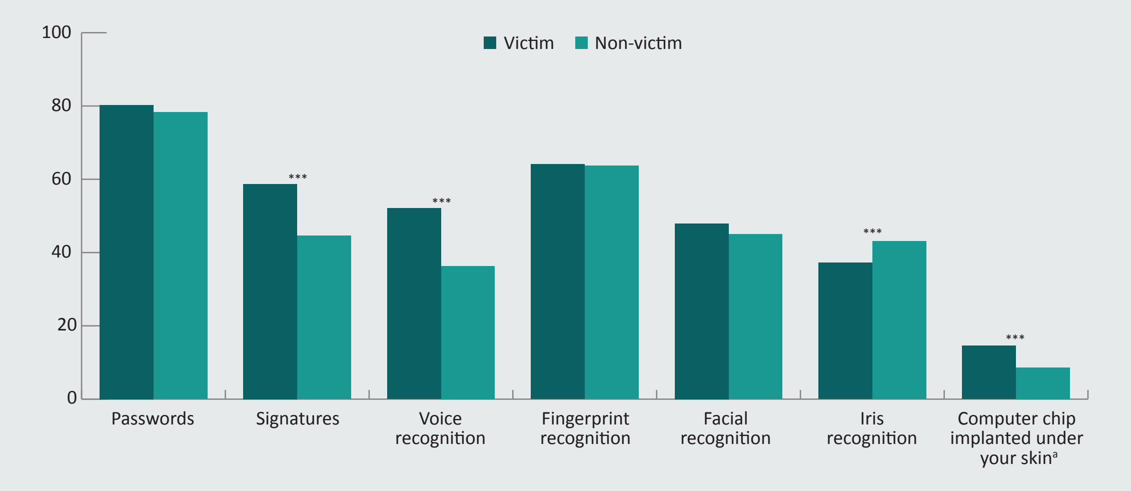
Table 30: Willingness to use security measures to protect personal information in the future (weighted data)

Security measure	2016 (n=9,956)	2017 (n=9,947)		% change
	%	%	n	
Passwords	22.2	78.6	7,816	+56.4***
Signatures	43.6	46.5	4,620	+2.9***
Voice recognition	33.2	38.4	3,815	+5.2***
Fingerprint recognition	62.9	63.8	6,342	+0.9
Facial recognition	42.6	45.3	4,509	+2.7***
Iris recognition	39.6	42.3	4,210	+2.7***
Computer chip implanted under your skin[a]	–	9.4	937	–
Any of the above	93.8	94.3	9,381	+0.5
None of the above	6.2	5.7	566	–0.5

***statistically significant at $p<0.001$
a: Included in 2017 identity crime survey only
Note: Respondents could select multiple responses
Source: Identity crime survey 2017 [AIC data file]

Additional analysis was conducted to examine whether willingness to use security measures in the future to protect personal information related to experiences of personal information misuse in the previous 12 months. Respondents who reported recent victimisation were significantly more likely than non-victims to report a willingness to use signatures (58.7% vs 44.6%; χ^2(1, n=9,947)=90.97, $p<0.001$, V=0.1), voice recognition (52.1% vs 36.3%; χ^2(1, n=9,947)=119.35, $p<0.001$, V=0.1) and a computer chip implanted under the skin (14.6% vs 8.6%; χ^2(1, n=9,947)=46.91, $p<0.001$, V=0.1; see Figure 18).

Figure 18: Willingness of recent victims and non-victims of misuse of personal information to use security measures to protect personal information in the future (weighted data) (n=9,947) (%)



***statistically significant at *p*<0.001

a: Included in 2017 identity crime survey only

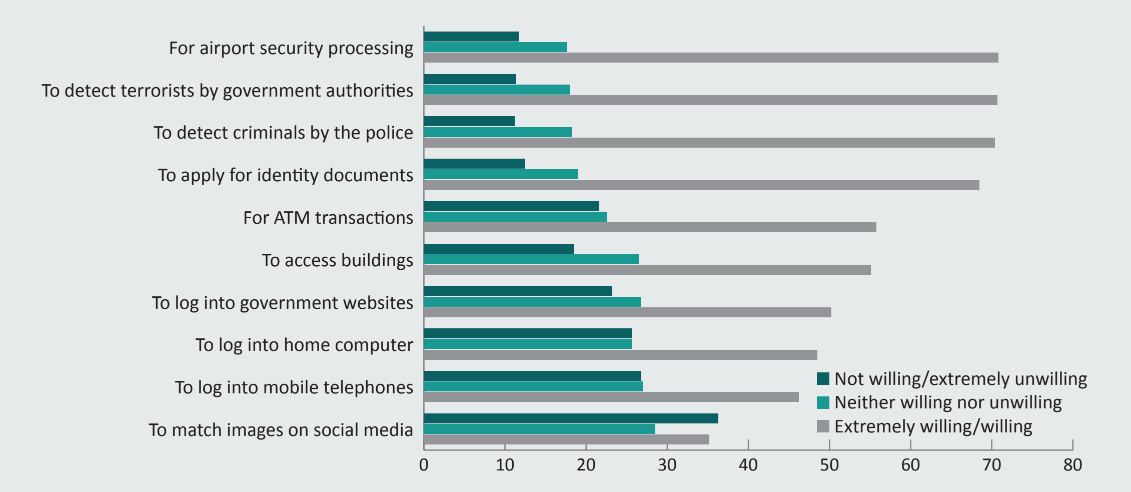
Note: Respondents could select multiple responses

Source: Identity crime survey 2017 [AIC data file]

Facial recognition

To further explore perceptions of facial recognition, respondents were asked how willing they would be to use facial recognition technologies in various scenarios. Respondents were asked to respond to 11 facial recognition scenarios using a five-point Likert scale with response options ranging from extremely unwilling (1) to extremely willing (5). Figure 19 shows the results grouped into three categories: willing or extremely willing; neither willing nor unwilling; and not willing or extremely unwilling.

Figure 19: Willingness of respondents to use facial recognition technologies for specific purposes (weighted data) (n=9,947) (%)



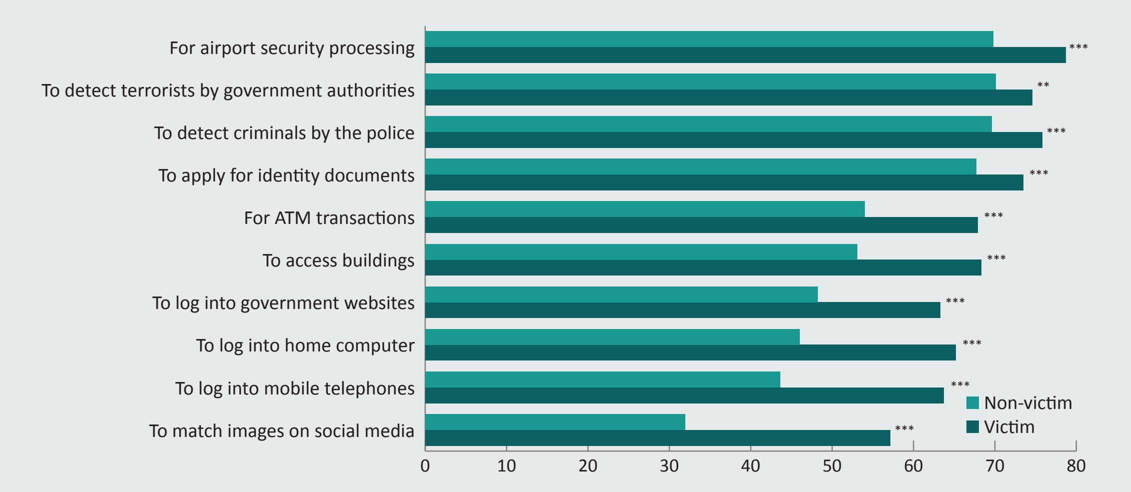
Source: Identity crime survey 2017 [AIC data file]

Respondents indicated that they would be most willing (ie willing & extremely willing combined) to use facial recognition technologies for government authorised purposes: airport security (70.8%), detection of terrorists by government authorities (70.7%), detection of criminals by the police (70.4%) and to apply for identity credentials (eg driver licence, passport) (68.5%; see Figure 18). About half of respondents indicated they would be willing to use facial recognition technologies for ATM transactions (55.8%), accessing buildings (55.1%), logging onto government websites (50.2%), and logging onto mobile phones (46.2%). Respondents were least willing to use facial recognition technologies for matching images on social media (35.2%) and logging onto home computers (20.3%). Apart from the use of facial recognition for logging onto government websites, there was less willingness for private sector purposes than official government purposes.

Comparing 2016 and 2017 data, there was a statistically significant 22.8 percentage point increase in willingness (ie willing and extremely willing combined) to use facial recognition for logging onto computers at home. There were modest increases in willingness to use facial recognition in all other scenarios: logging onto mobile phones (6.2 percentage points), accessing buildings (4.8 percentage points), detecting terrorists by government authorities (4.4 percentage points), matching images on social media (4 percentage points), airport security (3.8 percentage points), ATM transactions (3.7 percentage points), detecting criminals by police (3.5 percentage points), applying for identity credentials (3.1 percentage points), and logging onto government websites (2.4 percentage points).

Figure 20 explores the differences between recent victims and non-victims in their willingness to use facial recognition in various scenarios. Recent victims were significantly more willing than non-victims to use facial recognition for ATM transactions (67.9% vs 54%; χ^2(1, n=9,947)=89.94, *p*<0.001, V=0.1); accessing buildings (68.3% vs 53.1%; χ^2(1, n=9,947)=107.24, *p*<0.001, V=0.1); logging onto government websites (63.3% vs 48.2%; χ^2(1, n=9,947)=103.84, *p*<0.001, V=0.1); logging onto the home computer (65.2% vs 46%; χ^2(1, n=9,947)=168.06, *p*<0.001, V=0.1); logging onto mobile phones (63.7% vs 43.6%; χ^2(1, n=9,947)=185.18, *p*<0.001, V=0.1); and matching images on social media (57.1% vs 31.9%; χ^2(1, n=9,947)=315.61, *p*<0.001, V=0.2).

Figure 20: Willingness[a] of recent victims and non-victims of misuse of personal information to use facial recognition technologies for specific purposes (weighted data) (n=9,947) (%)



***statistically significant at *p*<0.001, **statistically significant at p<0.01
a: ‘Willing’ and ‘extremely willing’ responses combined
Source: Identity crime survey 2017 [AIC data file]

Discussion

On the basis of the findings of this survey, the prevalence of misuse of personal information in Australia has risen, with 13.1 percent of respondents reporting that their personal information had been misused in the 12 months prior to July 2017. This was a 4.6 percentage point increase in the proportion of respondents who reported victimisation in the 12 months prior to May 2016. The increase in personal information misuse appeared to be Australia-wide, with an increase in victimisation reported in almost all metropolitan and rural regions. Males were more likely than females to report having experienced misuse of personal information. Male respondents aged 25 to 34 years reported the highest rates of victimisation. If the increase in misuse of personal information identified in this survey is indicative of a widespread domestic or international increase in identity crime, then the increase occurred after June 2016, as there was no indication of increased prevalence in previous AIC identity crime surveys.

International indicators of identity crime prevalence are not available to explain the increased prevalence in Australia, as overseas studies have not been conducted since 2016. However, a number of fraud and scam indicators have reported a rise in activity in the latter half of 2016. As discussed earlier, in the fourth quarter of 2016 APWG reported the highest number of phishing attacks since data collection commenced in 2004 (APWG 2017). Verizon data holdings also indicated that the information industry experienced the heaviest losses from data breaches in 2016, and the data obtained were often personal details provided when signing up to websites (Verizon 2017). AusPayNet also reported that card-not-present fraud experienced unprecedented growth in 2016, accounting for 78 percent of all fraud on Australian cards (AusPayNet 2017). In addition, Australian Competition and Consumer Commission reports on scam activity found a 23.3 percent increase in identity theft reports between 2016 and 2017 and a 5.9 percent increase in phishing reports over the same time frame (ACCC 2018, 2017). The findings of this survey will be examined in light of these other indicators of victimisation.

A compelling argument can be made that a substantial proportion of the misuse of personal information reported in the 2017 survey is attributable to unsolicited cold-calling and online phishing. The survey found a significant increase in reports of personal information being obtained via telephone, face-to-face meetings and text messages. Email phishing was also a commonly reported method of obtaining personal information. It appears that offenders are moving away from purely online techniques to landline telephones and more personal strategies, probably due to the enhanced security and fraud prevention measures incorporated into digital technologies. Interestingly, few respondents thought their information had been obtained via a data breach (8.9 percent).

Reports of name, address and date of birth details being obtained and misused increased substantially in 2017 compared with 2016. These high-value details are of greatest use in monetising online fraud, as they are a means of obtaining other credentials for use in committing identity crimes (Jorna & Smith 2018).

There was no evidence that card-not-present fraud was responsible for the increase in misuse of personal information observed in 2017. The proportion of respondents reporting misuse of their credit/debit card information reduced by 13.6 percentage points between 2016 and 2017. The proportion of recent victims who said their personal information had been misused for the purpose of purchasing something also substantially reduced (13.3 percentage points). If card-not-present fraud in this sample had increased over the 2016 to 2017 period, both of these measures would have increased.

The reduction in card-not-present fraud can be explained by the increased use of credit card security measures, including multi-factor authentication, in online transactions. Reports of personal information being obtained through ATM, EFTPOS or online banking transactions, however, increased slightly on previous years. This could be due to multi-factor authentication not being used, and an increase in contactless card transactions at point of sale.

There was a notable increase in misuse of personal information to file fraudulent tax returns and to access superannuation monies. Data to interpret this finding are not publicly available, although the risks of superannuation fraud are well known (Freiberg 1996). The increased misuse of name, address and date of birth details in 2017 could associated with these forms of fraud. There was also a 9.6 percentage point increase from 2016 in the number of identity crime victims reporting that they were refused government benefits. This could be a consequence of a fraudulent tax return being lodged, resulting in reassessment of an individual’s entitlement to benefits. Whether the increase in misuse to support fraudulent tax returns relates to an increase in phishing attacks where the fraudulent communication purports to come from the ATO or another government agency is conjectural. The ACCC, however, stated in July 2016 that more than $1m in losses related to tax scams had been reported in the first half of 2016. This was a substantial increase on the $1.6m lost in total in 2015 (ACCC 2017). In 2018 an ACCC report on scams noted that in 2017:

> The ATO received 81 250 scam reports with $2 396 178 in reported losses. Of these, 58 054 reports were for threat-based impersonation scams for which $2.3 million was reported lost. (ACCC 2018: 9)

Almost double the number of victims in 2017 reported out-of-pocket losses compared with 2016. The cost per victim, however, was much lower than those reported in previous years. The median loss reported for all personal information misuse in the last 12 months was $150, down from $300 in 2016. This finding appears to be a product of a substantial increase in the number of victims reporting small out-of-pocket losses ($100–$199). When out-of-pocket losses from the most serious occasion of misuse were considered, the same pattern was observed. Commensurate with the reduction in the median out-of-pocket loss per victim, the median amount recovered per victim also fell. The median amount recovered for all misuse experienced in the last 12 months halved, from $400 in 2016 to $200 in 2017. This was due to a higher proportion of victims recovering small ($100–$199) and modest ($300–$599) losses. The recovery of losses greater than $600 reduced notably from 2016 to 2017. These findings may have been unduly influenced by one exceptionally large amount recovered in 2016, which was more than six times the largest loss recovered in 2017. The rise in the number of victims reporting losses, and in the number of small losses, however, would not have been influenced by this outlier. These findings may instead reflect differences between 2016 and 2017 in the types of personal information obtained and the intended purpose of the information misuse.

Almost all respondents assessed misuse of personal information as being somewhat or very serious in terms of harm to the Australian community, with victims more likely than non-victims to report it as being very serious. Impacts other than financial losses were reported by 65.6 percent of respondents who had experienced personal information misuse in the last 12 months. Financial, emotional and legal consequences all rose in 2017, due to a 21.5 percentage point reduction in the proportion of respondents who reported experiencing no consequences from the misuse of their personal information. It is plausible that the rise in reports of commencing legal action to clear a name or clear debts, being wrongly accused of a crime and being refused government benefits relate to the reported increase in the misuse of personal identifying details such as name, address and date of birth.

Almost all respondents who had experienced personal information misuse in the last 12 months reported making behavioural changes as a consequence. Examination of behavioural changes by method of access and type of information misused showed that behavioural changes were not uniform across victims, but related to the type of information misused and the method of access. Behavioural changes made after experiencing credit/debit card fraud were well defined, with almost half of victims reporting changing passwords, changing banking details, and reviewing financial statements more carefully. Concerningly, only 58.6 percent of respondents who had their password information misused reported changing their passwords. The highest percentage of respondents who implemented better security for computer and other computerised devices were those whose information was obtained via theft or hacking of a computer or other device. Those who experienced theft or hacking were also the ones who most commonly reported not trusting people as much as a consequence of that experience.

The security measure that respondents were most willing to use to protect their personal information in the future was password authentication, followed by fingerprint recognition, signature and facial and iris recognition. Despite their willingness to use such technologies, only 23.4 percent of respondents who experienced personal information misuse in the last 12 months reported using better security for computer or other devices after becoming a victim. Arguably, the use of fingerprint and voice recognition technologies would have been captured in this behavioural change. Given that these technologies are now features that can be enabled on most computers and mobile devices, it can reasonably be concluded that willingness to use such technologies is not translating into actual use, even among those who have experienced misuse of personal information.

Satisfaction with government agency, organisation and business responses to reports of personal information misuse rose across almost all entities. The highest levels of satisfaction were reported for Passport Office responses, followed by ACORN, IDCARE and media organisations. ACORN experienced the greatest increase in satisfaction levels, with a 30.3 percentage point increase in satisfaction from 2016 to 2017. Satisfaction with credit reporting agencies and IDCARE also increased substantially.

Satisfaction with police responses also increased in 2017. This may have been driven in part by a significant increase in the number of respondents who were notified by police that their personal information had been misused. When police notifications were examined by geographic region, no single police force could be identified as responsible for the reported increase in notifications. It appears that the increase in satisfaction with police responses and notifications by police is the result of efforts across all Australian law enforcement agencies to improve how they respond to victims of identity crime.

In sum, misuse of personal information increased from 2016 to 2017. This appears to be due to an increase in phishing attacks and information being obtained by telephone and in face-to-face meetings. There is evidence that this information is being used to obtain money from victims' bank accounts, as well as to commit taxation fraud and access superannuation monies. There was some evidence that card-not-present fraud decreased from 2016 to 2017, with the misuse of credit/debit card information decreasing over this period. Despite almost double the number of victims reporting out-of-pocket losses in 2017 compared with 2016, out-of-pocket loss per victim fell. This may indicate earlier detection of the misuse, preventing further losses, or that taking money from individual victims may not have been the primary aim of offenders. Instead, they have been seeking to obtain personal information for use in other forms of identity crime and fraud. An increase in satisfaction with the responses provided by government agencies, organisations and businesses, as well as an increase in police notifications of misuse, suggested that industry and government responses are easing, somewhat, the impact of identity crime suffered by victims in Australia. Nonetheless, with almost $3b in economic harm caused by identity crime in Australia at present (Smith & Jorna 2018b), the community and government cannot be complacent.

References

URLs correct as at August 2018

Anti-Phishing Working Group (APWG) 2017. *Phishing activity trends report: 4th quarter 2016.* https://www.antiphishing.org/resources/apwg-reports/

Attorney-General's Department (AGD) 2016. *Identity crime and misuse in Australia 2016.* Canberra: AGD. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime

Attorney-General's Department (AGD) 2015. *Identity crime and misuse in Australia 2013–14.* Canberra: AGD

Attorney-General's Department (AGD) 2012. *National Identity Security Strategy 2012.* Canberra: AGD. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Australian Bureau of Statistics (ABS) 2017. *Australian demographic statistics, Sep 2017.* ABS cat. no. 3101.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0/

Australian Bureau of Statistics (ABS) 2016a. *Household use of information technology, Australia, 2014–15.* ABS cat. no. 8146.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0

Australian Bureau of Statistics (ABS) 2016b. *Personal fraud, 2014–15.* ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/

Australian Bureau of Statistics (ABS) 2012. *Personal fraud, 2010–11.* ABS cat. no. 4528.0. Canberra: ABS

Australian Bureau of Statistics (ABS) 2008. *Personal fraud, 2007.* ABS cat. no. 4528.0. Canberra: ABS

Australian Competition and Consumer Commission (ACCC) 2018. *Targeting scams: Report of the ACCC on scams activity 2017.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2017

Australian Competition and Consumer Commission 2017. *Targeting scams: Report of the ACCC on scams activity 2016.* Canberra: ACCC

Australian Criminal Intelligence Commission (ACIC) 2017. *Serious financial crime in Australia 2017.* Canberra: ACIC. https://acic.govcms.gov.au/publications/intelligence-products/serious-financial-crime-australia-2017

Australian Payments Network (AusPayNet) 2017. *Australian payments fraud 2017: Jan–Dec 2016 data.* Sydney: AusPayNet. https://www.auspaynet.com.au/resources/fraud-statistics/2016-Calendar-year

Australian Taxation Office (ATO) 2017. *Don't be the next scam victim. Media release 26 Jul.* https://www.ato.gov.au/Media-centre/Media-releases/Don-t-be-the-next-scam-victim/

Bethell C, Fiorillo J, Lansky D, Hendryx M & Knickman J 2004. Online Consumer surveys as a methodology for assessing the quality of the United States health care system. *Journal of Medical Internet Research* 6(1):e2

British Broadcasting Corporation (BBC) 2017. Equifax data breach: Credit rating firm replaces key staff. *BBC News* 16 Sep. http://www.bbc.co.uk/news/technology-41291643

Chang L & Krosnick JA 2009. National surveys via RDD telephone interviewing versus the internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly* 73(4): 641–678

Cuganesan S & Lacey D 2003. *Identity fraud in Australia: An evaluation of its nature, cost and extent.* Sydney: Securities Industry Research Centre of Asia-Pacific

Di Marzio Research 2012. *Identity theft concerns and experiences.* Report prepared for the Attorney-General's Department. Melbourne: Di Marzio Research. https://www.homeaffairs.gov.au/criminal-justice/files/identity-theft-data-survey-report-2012.pdf

Di Marzio Research 2011. *Identity theft concerns and experiences.* Report prepared for the Attorney-General's Department. Melbourne: Di Marzio Research

Doyle M-A, Fisher C, Tellez E & Yadav A 2017. How Australians pay: New survey evidence. *Reserve Bank of Australia Bulletin* March 2017: 59–66. http://www.rba.gov.au/publications/bulletin/2017/mar/

Freiberg A 1996. Superannuation crime. *Trends & issues in crime and criminal justice* no. 56. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi56

Harrell E 2015. *Victims of identity theft,* 2014. Bureau of Justice Statistics bulletin. NCJ 248991. Washington, DC: US Department of Justice. https://www.bjs.gov/content/pub/pdf/vit14.pdf

Harrell E & Langton L 2013. *Victims of identity theft, 2012.* Bureau of Justice Statistics bulletin. NCJ 243779. Washington, DC: US Department of Justice. https://www.bjs.gov/content/pub/pdf/vit12.pdf

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

Malhotra N & Krosnick JA 2007. The effect of survey mode and sampling on inferences about political attitudes and behavior: Comparing the 2000 and 2004 ANES to internet surveys with nonprobability samples. *Political Analysis* 15(3): 286–324

National Fraud Authority (NFA) 2013. *Annual fraud indicator 2013*. London: NFA

Office for National Statistics (ONS) 2018. *Crime in England and Wales: Year ending December 2017: Additional tables on fraud and cybercrime.* London: ONS. https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingdecember2017

Office for National Statistics (ONS) 2017. *Crime in England and Wales: Year ending December 2016: Additional tables on fraud and cybercrime.* London: ONS. https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingdecember2016

Office of the Australian Information Commissioner (OAIC) 2017. *Australian community attitudes to privacy survey 2017.* Canberra: OAIC. https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017

Robertson A 2017. Tax: Be careful with that big return, it could be a costly scam. *ABC News* 11 Aug. http://www.abc.net.au/news/2017-08-11/new-cyber-scams-worry-ato/8795520

Sanders D, Clarke HD, Stewart MC & Whiteley P 2007. Does mode matter for modelling political choice? Evidence from the 2005 British Election Study. *Political Analysis* 15(3): 257–285. DOI: 10.1093/pan/mpl010

Smith RG 2002. Electronic voting: Benefits and risks. *Trends & issues in crime and criminal justice* no. 224. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi224

Smith RG, Brown R & Harris-Hogan S 2015. *Identity crime and misuse in Australia: Results of the 2014 online survey.* Research and public policy series no. 30. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp130

Smith RG & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey.* Research and public policy series no. 128. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp128

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

Smith RG & Jorna P 2018b. *Counting the costs of identity crime and misuse in Australia, 2015–16*. Statistical Bulletin no. 15. Canberra: Australian Institute of Criminology

United Nations Economic and Social Council 2007. *International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.* Vienna: United Nations

Veda 2015. *Veda 2015 cybercrime and fraud report.* Sydney: Veda Advantage Information Services & Solutions Ltd. https://www.equifax.com.au/sites/default/files/008_veda_2015_cybercrime_and_fraud_report.pdf

Verizon 2017. *2017 Data breach investigations report.* https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Yeager DS, Krosnick JA, Chang L, Javitz HS, Levindusky MS, Simpser A & Wang R 2011. Comparing the accuracy of RDD telephone surveys and internet surveys conducted with probability and non-probability samples. *Public Opinion Quarterly* 75(4): 709–747

Appendix A: Identity Crime and Misuse in Australia Survey 2017

About the identity crime and misuse survey

This survey examines your attitudes to, and experience of, identity crime and misuse. Identity crime is a critical issue in Australia and overseas and your answers will provide information that can be used to prevent crimes of this kind in the future.

Identity crime and misuse involves someone using your personal information without your permission.

'Personal Information' includes your:

name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (e.g. fingerprint, voice, facial, iris recognition), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, or other types of personal information.

You will be asked to answer questions about:

- Your experience of identity crime and misuse;
- How your information was obtained and used;
- Any financial loss and other impact;
- Your reporting and response activities;
- If you changed your behaviour in any way as a result of what happened;
- Whether you think this type of crime will change over the next 12 months;
- How serious you think this is;
- Whether you know about, have applied for, or received an identity crime victim certificate;
- Some information about your: age, gender, residence, income, language at home, Indigenous background, computer usage and experience of, and willingness to use biometric technologies to protect your personal information.

The survey will take approximately 10 minutes of your time, and you will be offered a selection of rewards to choose from. Your answers will be completely anonymous and the results will not be able to identify you personally. You may withdraw from the survey at any time and participation is entirely voluntary.

If you feel uncomfortable about answering any questions you can choose not to reply and you may withdraw at any stage. If you decide to withdraw, you may request that any information you have already provided not be used in the research by contacting ______________________.

If you would like to speak to someone after the research has been completed to obtain advice or support, Lifeline provides crisis support by telephone 24 hours a day on 13 11 14 (at the cost of a local call), or online at https://www.lifeline.org.au/Get-Help/Online-Services/crisis-chat between 8pm and midnight. You should contact your local police if you suspect that your identity has been stolen or misused. More information on how to report identity theft and how to protect your identity can be found at www.ag.gov.au/identitysecurity. Other advice and support is available from IDCARE on 1300 432 273 or www.idcare.org.

The results of the survey will be available from the Australian Institute of Criminology's website at www.aic.gov.au. You can obtain further information from [email] who is in charge of the study. You can also obtain further information or make a complaint about the study by contacting [email] or [phone number].

Thank you for participating in this research, your involvement is greatly appreciated.

Please now answer the following questions.

Background information

Q1) Please indicate the postcode and place of your usual place of residence?

Postcode in Australia ______________________

State or Territory (please specify) ______________________

I do not normally reside in Australia □ Yes □ No

Q2) What is your gender? (select one only)

□ Male

□ Female

□ Indeterminate □ Intersex □ Unspecified

□ I'd rather not say

Q3) Which age group do you belong to? (select one only)

□ 17 years and under

□ 18–24 years

□ 25–34 years

□ 35–44 years

□ 45–54 years

□ 55–64 years

□ 65 years and over

□ I'd rather not say

Q4) What language is most often spoken at your home? (select one only)

□ English

□ Mandarin

□ Cantonese

□ Korean

□ Indonesian

□ Japanese

□ French

□ German

□ Hindi

□ Italian

□ Farsi

□ Arabic

□ Swahili

□ Other (please specify) ____

□ I'd rather not say

Q5) Do you identify as an Aboriginal or Torres Strait Islander? (select one only)

□ Yes—Aboriginal

□ Yes—Torres Strait Islander

□ Yes—both Aboriginal and Torres Strait Islander

□ No

□ I'd rather not say

Q6) What is the highest educational level you have completed?

□ Postgraduate degree

□ Graduate Diploma or Graduate Certificate

□ Bachelor's Degree

□ Advanced Diploma or Diploma

□ Professional qualification without a degree

□ Certificate III or IV

□ Year 12

□ Year 11 or below

□ Other ______________________________

Q7) What was your individual gross income from all sources for the year 2016–17 (ie before tax has been deducted)?

□ $0–$18,200

□ $18,201–$37,000

□ $37,001–$80,000

□ $80,001–$180,000

□ $180,001 and over

□ I'd rather not say

Q8) Last week, how many hours did you spend using a computer or computerised devices including a desktop, laptop, smartphone and tablet?

Insert number of whole hours only ______________________________

(there are only 168 hours in a week, or 112 usual waking hours in a week)

Q9) Of these hours spent using a computer (including a desktop, laptop, smartphone and tablet), how many hours were spent on work-related activities only?

Insert number of whole hours only ______________________________

Q10) Have you ever used any of the following technologies in the past (in any way, not just to prevent misuse of personal information) (Select all that apply)

Q11) In order to prevent misuse of personal information in the future, would you be willing to use any of the following technologies?

Value ranges	(Q10) Select if you have ever used this technology in the past, in any way	(Q11) Select if you would be willing to use this technology in the future to protect personal information (e.g. at ATMs, at airports, for computers, building access etc.)
Passwords	□	□
Signatures	□	□
Voice recognition	□	□
Fingerprint recognition	□	□
Facial recognition	□	□
Iris recognition	□	□
Computer chip implanted under your skin	□	□

Q12) How willing would you be to use facial recognition technologies for each of the following purposes?

Use of facial recognition technology for:	(select one rating for each purpose)				
Purposes	Extremely unwilling	Not willing	Neither willing nor unwilling	Willing	Extremely willing
Purposes	□	□	□	□	□
Mobile Phone	□	□	□	□	□
ATM transactions	□	□	□	□	□
Matching images on social media	□	□	□	□	□
Airport security processing	□	□	□	□	□
Logging onto mobile phones	□	□	□	□	□
Logging onto computers at home	□	□	□	□	□
Logging onto government websites	□	□	□	□	□
Applying for evidence of identity documents (e.g. driver's licence, passport)	□	□	□	□	□
Access to buildings	□	□	□	□	□
Detecting criminals by the police	□	□	□	□	□
Detecting terrorists by government authorities	□	□	□	□	□

Misuse of personal information

The following questions ask about various types of 'personal information'. This could include information such as your name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (e.g. fingerprint, voice, facial, iris recognition), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, or other types of personal information.

The following questions also ask about the misuse of your personal information. This includes obtaining or using your personal information without your permission to pretend to be you or to carry out a business in your name without your permission, or other types of activities and transactions. This does not include use of your personal information for direct marketing, even if this was done without your permission.

Q13) In terms of harm to the Australian community, do you think that misuse of personal information is:

□ Very serious

□ Somewhat serious

□ Not very serious

□ Not at all serious

Q14) Over the next 12 months do you think that the risk of someone misusing your personal information will:

□ Increase greatly

□ Increase somewhat

□ Not change

□ Decrease somewhat

□ Decrease greatly

Q15) Are you aware that a person who has had their personal information misused may be able to apply to a court to obtain a victim certificate to prove what occurred? (select one only)

□ Yes, I am aware of such certificates, and have obtained one or more in the past

□ Yes, I am aware of such certificates, and have applied to a court for one or more in the past

□ Yes, I am aware of such certificates, but have not applied for any

□ No, I am unaware of such certificates

Q16) Please indicate if you have had your personal information misused at any time in the past

□ Yes, I have had my personal information misused in the past

□ No, I have not had my personal information misused in the past

Misuse of personal information over the last 12 months

The following questions ask about misuse of your personal information that took place during the last 12 months only. You should count all these occasions for each of the following questions.

Q17) In the last 12 months have you experienced misuse of your personal information?

(This could include use of your information without your permission for business or personal transactions, opening accounts, taking out loans or making claims to the government, but not for direct marketing).

□ Yes

□ No

□ Don’t know

Q18) If you answered Yes, on how many separate occasions do you believe that your personal information was misused?

(insert number) ______________________________

Q19) Over the last 12 months, how much did you pay out as a result of the misuse of your personal information on all occasions?

$ ______________________________

(insert your best estimate of the total amount you paid or was accessed from your bank or credit card account) over the 12 months in whole dollars, including any money that you were later able to recover from banks etc. and also including any costs associated with repairing what occurred)

Q20) Over the last 12 months, how much were you left out-of-pocket as a result of the misuse of your personal information on all occasions?

$ ______________________________

(insert your best estimate of the total losses over the 12 months in whole dollars excluding any money that you were able to recover from banks etc. and also excluding any costs associated with repairing what occurred)

Q21) Over the last 12 months, how much money was reimbursed to you by banks or other organisations, or recovered in other ways, as a result of the misuse of your personal information on all occasions?

$ ______________________________

Q22) Over the last 12 months, did you experience any other consequences as a result of your personal information being misused? (select all that apply)

□ I was refused credit

□ I was refused government benefits

□ I was refused other services (please specify) ________________

□ I experienced financial difficulties resulting in the repossession of a house or land, motor vehicle or other items

□ I had to commence legal action to clear debts and/or to clear my name

□ I was wrongly accused of a crime

□ I experienced other reputational damage (please specify) ________________

□ I experienced mental or emotional distress requiring counselling or other treatment

□ I experienced physical health problems requiring medical treatment by a doctor

□ Other (please specify) ________________

or

□ I didn't experience any consequences

Q23) Over the last 12 months, approximately how many hours did you spend dealing with the consequences of having had your personal information misused? (This might include time taken to have your credit rating fixed, get new cards issued, accounts changed etc)

Please indicate how many whole hours were spent ________________

Q24) Over the last 12 months, approximately how much money did you spend dealing with the consequences of having had your personal information misused? (This might include cost of getting legal advice, lost income, telephone charges, postage and fees etc)

Please insert your best estimate (in whole dollars only) ________________

Q25) Over the last 12 months, did you tell anyone about the misuse of your personal information? (Select all that apply)

□ No, I told no-one

□ Yes, I told a friend or family member

□ Yes, I told a government agency or a business organisation

Q26) If you made a report to a government agency or a business organisation, which of the following did you make a report to? (Select all that apply)

Q27): If you made a report to a government agency or a business organisation, how satisfied are you with the outcome?

Organisation	Select if a report was made to:				
Purposes	Select if no report was made to	Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
The police	□	□	□	□	□
ACORN (Australian Cybercrime Online Reporting Network)	□	□	□	□	□
A consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading)	□	□	□	□	□
A Road Traffic Authority	□	□	□	□	□
The Passport Office	□	□	□	□	□
Medicare Australia	□	□	□	□	□
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)	□	□	□	□	□
A credit reporting agency (eg Veda or Dun and Bradstreet)	□	□	□	□	□
Your internet service provider	□	□	□	□	□
A utility company (eg gas, electricity, telephone, water etc.)	□	□	□	□	□
A media organisation	□	□	□	□	□
IDCARE (www.idcare.org)	□	□	□	□	□
Others (please specify)					
1. ____________________	□	□	□	□	□
2. ____________________	□	□	□	□	□
3. ____________________	□	□	□	□	□

Q28) If you did NOT report the misuse of your personal information to a government agency or a business organisation, please indicate why (select all that apply)

□ I did not know how or where to report the matter

□ I was too embarrassed to report it

□ I did not believe it was a crime

□ I did not believe the police or any other authority would be able to do anything

□ Bank or credit union or credit card company (eg. Visa, MasterCard, etc.) had already notified me and issue resolved

□ Not important enough to report

□ Other (please specify) ______

Q29) As a direct result of having had your personal information misused, in what ways has your behaviour changed? (select all that apply)

□ I am more careful when I use or share personal information

□ I changed my password(s)

□ I changed my social media account(s)

□ I ceased all social media use

□ I changed my email address(es)

□ I changed my banking details

□ I changed my telephone number(s)

□ I changed my place of residence

□ I use better security for my computer or other computerised devices

□ I lock my mailbox

□ I redirect my mail when I am away or move residence

□ I use a registered post box

□ I shred personal documents before disposing of them

□ I review my financial statements more carefully

□ I applied for a copy of my credit report

□ I signed up for a commercial identity theft alert/protection service

□ I don't trust people as much

□ I avoid using the internet for banking and purchasing goods and services

□ Other (please specify) ______

□ My behaviour has not changed ______

Most serious occasion of misuse of personal information in the last 12 months

The following questions ask about the most serious occasion on which your personal information was used without your permission in the last 12 months (this is the occasion that resulted in the largest financial or other harm to you).

Q30) On this most serious occasion, please indicate which of the following types of personal information you believe were misused.

□ Name

□ Address

□ Date of birth

□ Place of birth

□ Gender

□ Driver’s licence information

□ Passport information

□ Medicare information

□ Biometric information (e.g. fingerprint, voice, facial, iris recognition)

□ Signature

□ Bank account information

□ Credit/debit card information

□ Password

□ Personal Identification Number (PIN)

□ Tax File Number (TFN)

□ Shareholder Identification Number (HIN)

□ Computer username

□ Online account username

□ Student number

□ Other (please specify) ______________________________

Q31) On this most serious occasion, how do you believe that your personal information was obtained? (select all that apply)

□ In a face-to-face meeting (e.g. a job interview or a doorknock appeal)

□ By telephone (excluding SMS)

□ By text message (SMS)

□ By email

□ From theft or hacking of a computer or other computerised device (eg smartphone)

□ Theft of an identity or other personal document (please specify type)

____

□ Theft of a copy of an identity or other personal document (please specify type)

____

□ Theft of your mail

□ From information lost or stolen from a business or other organisation (i.e. a data breach)

□ From an online banking transaction

□ From information you placed on social media (eg Facebook, Linked-In etc.)

□ From information you placed on a website (other than social media, eg online shopping)

□ From an ATM transaction

□ From an EFTPOS transaction

□ From a person that I know

□ Other (please specify) ____ or

□ I don’t know how my information was obtained

Q32) On this most serious occasion, in which of the following ways do you believe that your personal information was misused (select all that apply)

□ To file a fraudulent tax return

□ To obtain money from a bank account (excluding superannuation)

□ To obtain superannuation monies

□ To obtain money from an investment (eg shares)

□ To apply for a job

□ To provide false information to police

□ To rent a property

□ To purchase something—(please specify what was purchased) ____________________

____

□ To apply for government benefits

□ To apply for a loan or obtain credit

□ To open a mobile phone account

□ To open an online account, such as Facebook, eBay (please specify)

□ Other (please specify) ____________________

□ Don't know

Q33) On this most serious occasion, how did you become aware that your personal information had been misused? (select all that apply)

□ Received a notification from a bank or financial institution and/or credit card company

□ Received a notification from another company (please specify) ____________________

____

□ Received a notification from the police

□ Received a notification from a government agency or authority other than the police (please specify) ____________________

□ Noticed suspicious transactions in bank statements or accounts

□ Was unsuccessful in applying for credit

□ Received a bill from a business or company for which you were not responsible

□ Was contacted by debt collectors

□ Other (please specify) ____________________

Q34) On this most serious occasion, how much did you pay out as a result of the misuse of your personal information?

$ ____________________

(insert your best estimate of the total amount you paid or was accessed from your bank or credit card account) in whole dollars, including any money that you were later able to recover from banks etc. and also including any costs associated with repairing what occurred)

Q35) On this most serious occasion, how much were you left out-of-pocket as a result of the misuse of your personal information?

$ ____________________

(insert your best estimate of the total losses in whole dollars excluding any money that you were able to recover from banks etc. and also excluding any costs associated with repairing what occurred)

Q36) On this most serious occasion, how much money was reimbursed to you by banks or other organisations, or recovered in other ways, as a result of the misuse of your personal information?

$ ____________________

Q37) Have you participated in our Identity Crime Surveys in the past?

□ Yes – in 2013

□ Yes – in 2014

□ Yes – in 2016

□ No

□ Don’t know

Appendix B: Weighting of the data

Survey data were weighted to reflect the distribution of the Australian population in terms of age and gender (either male or female only) based on population data from the 2016 Census (ABS 2017).

Tables B1 and B2 show the 2016 Census data and the unweighted distribution of survey respondents by age and gender.

Table B1: Respondents by age (unweighted data)

	ABS 2016 Census	2017 Survey	
Age	**%**	**%**	**n**
15–24 years	15.7	8.4	832
25–34 years	17.7	17.4	1,738
35–44 years	16.5	17.7	1,769
45–54 years	16.3	18.0	1,803
55–64 years	14.5	19.3	1,930
65 years and over	19.3	19.0	1,899
I'd rather not say	–	0.3	29
Total	100.0	100.0	10,000

Source: ABS 2017; Identity crime survey 2017 [AIC data file]
Note: Percentages may not total 100 due to rounding

Table B2: Respondents by gender (unweighted data)

	ABS 2016 Census	2017 Survey	
Gender	%	%	n
Male	49.3	41.1	4,113
Female	50.7	58.5	5,849
Indeterminate/intersex/unspecified	–	0.1	13
I'd rather not say	–	0.3	25
Total	100.0	100.0	10,000

Source: ABS 2017; Identity crime survey 2017 [AIC data file]

Consistent with the approach taken in the 2016 Identity Crime and Misuse in Australia Survey (Smith and Jorna 2018a), the 2017 survey responses were aligned with the Australian population gender and age distributions via data weighting (see Table B3). Under-represented categories were assigned a multiplier larger than 1, and over-represented categories were assigned a multiplier smaller than 1, as determined by a mathematical formula.

The assumption behind data weighting is that responses given by respondents from under-represented groups are consistent with the responses that would be provided by other members of the under-represented group, were they to be surveyed. Weighting of demographic variables for non-probability online samples, such as the one in this study, has been found to reduce accuracy through increased error (Chang & Krosnick 2009; Yeager et al. 2011). Where the current findings differ substantially from those identified in samples derived by other recruitment methods, this limitation should be considered.

Table B3: Respondents by age and gender (unweighted and weighted data)

Age/gender	Unweighted	Multiplier	Weighted	
	n		n	%
24 years and under				
Male	299	2.662	796	8.0
Female	525	1.458	766	7.7
25–34 years				
Male	652	1.333	869	8.7
Female	1,080	0.825	891	9.0
35–44 years				
Male	633	1.280	810	8.2
Female	1,134	0.734	833	8.4
45–54 years				
Male	629	1.264	795	8.0
Female	1,169	0.707	827	8.3
55–64 years				
Male	850	0.825	701	7.1
Female	1,080	0.683	738	7.4
65 years and over				
Male	1,039	0.857	891	9.0
Female	857	1.203	1031	10.4
Total	9,947		9,947	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,947 due to rounding
Source: Identity crime survey 2017 [AIC data file]

The number of respondents by age and gender is shown in Table B4. Because the 2016 Census did not include ‘indeterminate, intersex or unspecified’ as a gender category, respondents to the current survey who responded with this designation or declined to respond (n=38) were removed from analysis as it was not possible to weight their data. A small number of respondents who did not specify their age were also removed from the analysis (n=29). Accordingly, the final sample size used for weighting and analysis was 9,947.

Table B4: Age and gender of respondents, 2017 identity crime survey (n)

Gender	Age category						
	15–24	25–34	35–44	45–54	55–64	65+	Total
Male	299	652	633	629	850	1,039	4,102
Female	525	1,080	1,134	1,169	1,080	857	5,845
Total	824	1,732	1,767	1,798	1,930	1,896	9,947

Source: Source: Identity crime survey 2017 [AIC data file]

Table B5 presents the nationally representative age and gender distribution of the Australian population. As shown, the number of Australians in the age category 25–34 years is similar to the number of Australians aged 65–94, but in the survey those aged 65–94 years represent double the number of those aged 24–34 years. The AIC data were over-represented by older respondents and females when compared with the ABS data, therefore weighting of the AIC data from the non-probability sample, was deemed appropriate to provide data that reflected the national distribution of age and gender throughout Australia.

Table B5: ABS age and gender data at 30 June 2015

Gender	Age category						
	15–24	25–34	35–44	45–54	55–64	65+	Total
Male	1,523,100	1,663,905	1,550,834	1,522,124	1,341,472	1,704,373	9,305,808
Female	1,465,284	1,704,551	1,594,099	1,582,883	1,412,262	1,972,396	9,731,475
Total	2,988,384	3,368,456	3,144,933	3,105,007	2,753,734	3,676,769	19,037,283

Source: ABS 2017

The method used to calculate weights involved finding the percentage of the population for each age and gender category using ABS data and then performing the same calculations on the AIC data, and then dividing the ABS data percentages by the survey data percentages for each of the age and gender categories. Table B6 presents the weights applied to the survey data to generate the altered distribution of age and gender ratios using the survey results. These weights were then applied across the entire sample for each respondent's data.

Table B6: Multipliers used for 2017 survey sample to reflect the age/gender distribution of the Australian population

Gender	Age category						
	15–24	25–34	35–44	45–54	55–64	65+	Total
Male	2.6616098	1.3334234	1.2801143	1.2644060	0.8246124	0.8571094	1.1853472
Female	1.4583093	0.8246571	0.7344959	0.7074919	0.6832485	1.2025425	0.8699240
Total	1.8949438	1.0161788	0.9299551	0.9023189	0.7455072	1.0132466	1.0000000

Although the results used for analysis reflect the Australian population in age and gender, they cannot be used to estimate national prevalence of identity crime and associated losses. Accordingly, the data presented in this report are only indicative of the experiences of the 9,947 respondents included in the analysis.

Dr Susan Goldsmid is a former Principal Research Analyst at the Australian Institute of Criminology.

Ms Alexandra Gannoni is a Senior Research Analyst at the Institute.

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology and Professor in the College of Business, Government and Law at Flinders University.

AIC reports
Statistical Report

Australia’s national research and
knowledge centre on crime and justice

aic.gov.au