Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 06

Identity crime and misuse in Australia:

Results of the 2016 online survey

Russell G Smith
Penny Jorna

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

Contents

Figures

Tables

Acknowledgements

This study was undertaken as part of the Commonwealth Attorney-General's Department's National Identification of Identity Crime and Misuse project, which is being 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 consultancy firm that provided a panel of individuals drawn from across Australia who were asked to complete the survey. 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 Commonwealth Government.

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACFT	Australasian Consumer Fraud Taskforce
ACORN	Australian Cybercrime Online Reporting Network
AGD	Attorney-General's Department (Commonwealth Government)
AIC	Australian Institute of Criminology
COAG	Council of Australian Governments
HIN	shareholder identification number
NCVS	National Crime Victimization Survey (US)
NFA	National Fraud Authority (UK)
NISS	National Identity Security Strategy
OAIC	Office of the Australian Information Commissioner
PIN	personal identification number
SD	standard deviation
TFN	tax file number

Executive summary

Background

Identity crime involving misuse of personal information is arguably one of the most prevalent criminal activities in Australia, affecting individuals, businesses and government agencies alike. It is estimated that identity crime affects hundreds of thousands of Australians each year (AGD 2016). In April 2007, the Council of Australian Governments (COAG) agreed to the National Identity Security Strategy to protect the identities of Australians in a more regulated and efficient way. This arose out of emerging evidence at the time that large numbers of Australians experience misuse of their personal information for criminal purposes each year (Cuganesan & Lacey 2003; OAIC 2007). The strategy sought to enhance identification and verification processes throughout Australia and to develop other measures to combat identity crime, including the creation of a national Document Verification Service to verify the authenticity of identity credentials and the development of reliable, consistent and nationally interoperable biometric security measures for use in all jurisdictions (AGD 2012).

The strategy also recognised the need to quantify the nature and extent of identity crime and misuse of personal information, particularly the victimisation experiences of Australians. It recommended the creation of an identity crime and misuse longitudinal measurement framework that could be used to measure the effectiveness of policy and practice throughout Australia. As part of the measurement framework, large-scale surveys have been conducted by the Australian Institute of Criminology (AIC) to determine respondents' 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.

This report presents the results of the latest identity crime and misuse survey, undertaken by the AIC in May 2016. It updates information obtained in earlier surveys, undertaken in 2013 and 2014, and provides an indication of how the identity crime and misuse of personal information environment has changed in Australia since 2013. Future surveys will continue to track not only changes in victimisation rates but also the economic impact of identity crime and misuse.

Definitions

The 2016 survey adopted the same definitions as the 2014 and 2013 surveys, and asked respondents about the misuse of various types of personal information. This included (but was not limited to) misuse of an individual's name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg fingerprint), 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, and student number. Respondents were also given the opportunity to 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.

Questionnaire and sample

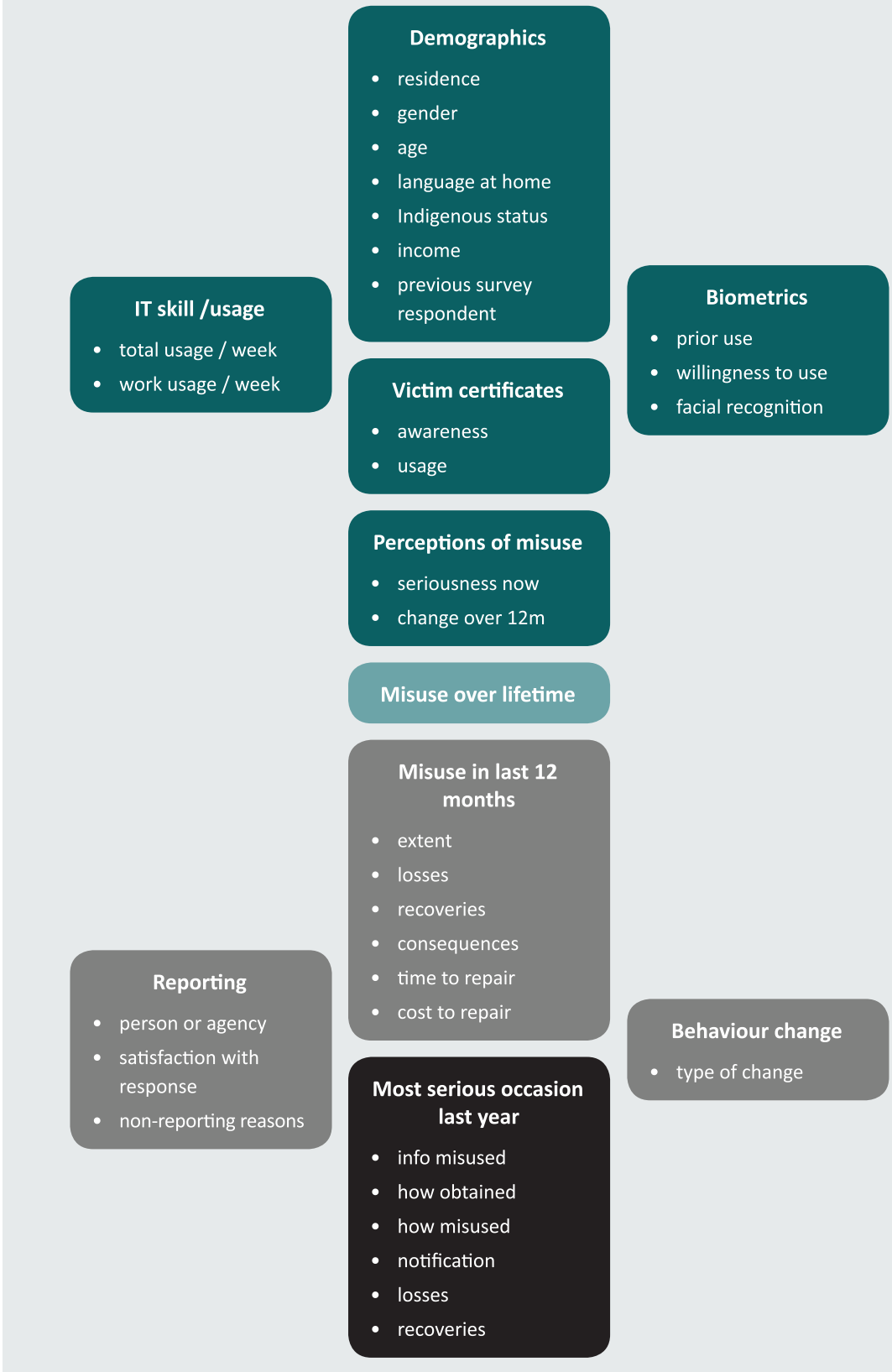
In May 2016, a questionnaire containing 24 main questions (see Appendix 1) was administered online to a research panel of Australians drawn from all states and territories. The sampling frame of more than 300,000 individuals and survey hosting were provided by i-Link Research Solutions, a commercial provider, in the form of raw de-identified data for the AIC to analyse.

The questionnaire sought information from respondents on various dimensions of the problem, as illustrated in Figure 1.

Data were weighted by age and gender to represent the spread of the population in Australia. ABS data estimating the age and gender population of Australians at 30 June 2015 (ABS 2016b,d) were used to develop the weighting matrix for the sample data (see Appendix 2). The sampling frame was insufficiently robust to permit the weighting of results to indicate estimates of national prevalence and financial loss—that is, the data which would have been obtained had the entire Australian population aged 15 years and over been surveyed.

Sampling was completed once a quota of 10,000 respondents had been reached. 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. The demographic data collected by the ABS (2016b,d) at 30 June 2015 did not provide population data for people who listed their gender as indeterminate/intersex or unspecified; accordingly, responses from these 19 respondents were excluded as weighting could not be undertaken. There were also a small number of respondents who did not specify their age who were also excluded from the analysis (n=25). Excluding these 44 responses left a sample size of 9,956 respondents for analysis.

Figure 1: Survey data collection structure



Perceptions of misuse of personal information

Respondents were asked how serious they thought misuse of personal information was in terms of harm to the Australian economy. A high proportion (63.7%) of respondents believed that misuse of personal information was very serious and a further 32 percent believed it was somewhat serious (95.7% combined). When asked if they thought the risk of someone misusing their personal information would change over the next 12 months, 16.4 percent believed it would increase greatly (slightly lower than 22% in 2014) and 45.3 percent believed it would increase somewhat (almost identical to the findings in 2014). Less than one percent (0.6%) believed the risk would decrease greatly, and 1.2 percent believed it would decrease somewhat. These responses were similar to those recorded in 2014. However, these perceived levels of concern about the changed risk of misuse of personal information are not reflective of the reported rates of victimisation, which were similar in 2014 and 2016.

Victimisation and misuse of personal information

The present survey found that 21.5 percent of the 9,956 respondents reported misuse of their personal information at some time during their life, with 8.5 percent reporting misuse of their personal information in the previous 12 months (compared with 8.9% in 2014).

The number of separate occasions on which respondents believed that their personal information had been misused ranged from one to 255 occasions. More than half of respondents (51.4%) believed that their personal information had been misused on a single occasion only—a slightly lower percentage than in 2014 (53.3%).

The proportion of respondents experiencing victimisation in the 12 months prior to the survey was 8.5 percent. This was slightly lower than results reported in the two previous AIC surveys (8.9% in 2014, and 9.4% in 2013), although higher than the seven percent of respondents who reported victimisation in the 12 months prior to a survey in the United States (Harrell 2015). Research by Veda (2015a) also found a lower percentage of victimisation (5%) in the 12 months prior to their survey, and the ABS (2016) found only 0.7 percent of respondents experienced an incident of identity theft in the 12 months prior to the survey period, with a further 5.9 percent experiencing card fraud. The overall victimisation rate reported in 2016 for the previous 12 months is lower than the rate reported in the UK National Fraud Authority's (2013) survey of 8.8 percent. These variations are most likely due to the use of different sampling frames and data collection techniques, and to the focus of questions asked of respondents. Nonetheless, these rates of victimisation are much higher than those for other criminal offence types. For example, in Australia in 2014–15, the victimisation rate for household break-ins was 2.6 percent; assault, 2.3 percent; motor vehicle theft, 0.6 percent; and robbery, 0.4 percent—compared with the 6.6 percent victimisation rate for identity fraud, including both identity theft and card fraud (ABS 2016a,e).

The most serious occasion of misuse of personal information in the previous 12 months

Respondents who experienced misuse of their personal information in the previous 12 months were asked further questions about the most serious occasion on which misuse had occurred during that time. The most serious occasion was defined as the occasion that had resulted in the largest financial impact or other harm to the individual.

The top three types of personal information that had been misused were credit/debit card information (49.8%), name (34.6%) and bank account information (27.0%). These were the same top three categories identified in both the 2014 and 2013 surveys; however, the proportion of people who had their credit/debit card misused in 2016 had decreased (51.8% in 2014). Respondents indicated between one and 18 different types of personal information had been misused, although half (50.7%) of respondents believed only one type of personal information had been misused.

For the most serious occasion of identity crime in the previous 12 months, respondents were asked how they believed their personal information had been obtained. Twenty-two percent (n=182) of respondents did not know how their information had been obtained. For those who knew how their personal information had been obtained, the top five sources reported were: through theft or hacking of a computer or other computerised device (20.0%); by email (18.4%); through an online banking transaction (15.8%); through information placed on a website other than social media, such as online shopping (14.3%); and by telephone (11.7%). The top four of these sources of information were the same as in 2014. In 2016, reports of information lost or stolen from a business or other organisation (ie data breach) declined slightly to under 10 percent, and reports of information obtained by telephone (known as vishing—phishing via telephone) were the fifth-most common.

Respondents were also asked how they believed their personal information had been misused on the most serious occasion in the previous 12 months. The top three categories of misuse were: to obtain money from a bank account, excluding superannuation (31.1%); to purchase something (29.7%); and to file a fraudulent tax return (8.6%). These top three categories were the same as in 2014, although the second of these (to purchase something) declined by 6.1 percentage points between 2014 and 2016.

Finally, respondents were asked how they had become aware of the misuse of their personal information on the most serious occasion in the previous 12 months. The top three ways of becoming aware of misuse were: receiving notification from a financial institution (42.9%); noticing suspicious transactions in a bank statement or account (30.6%); and receiving notification from the police (11.9%, an increase from 8.4% in 2014). Between 2014 and 2016, the number of respondents who became aware of misuse due to an unsuccessful application for credit doubled from 4.9 percent in 2014 to 8.4 percent in 2016.

Financial impact and other consequences resulting from misuse of personal information

Financial impact

Respondents who had experienced misuse of their personal information in the past 12 months were asked about their losses—that is, how much they were left out of pocket as a result, excluding any money that they were able to recover from banks and any costs associated with repairing what had occurred. Just over half (57.5%) were left out of pocket (n=488), which was more than in 2014 (53.8%). These respondents experienced losses that ranged from $1 to $500,000 when weighted (mean=$3,696, median=$300, SD=$28,680). Although the median was the same as in 2014, the mean and standard deviation were slightly higher than in 2014, indicating a wider range of losses in 2016.

The majority of respondents experienced losses of up to $1,000, with only a few reporting out-of-pocket losses of much larger amounts. Total out-of-pocket losses in 2016 amounted to $1,802,893. The latest estimate by the Attorney-General's Department of the total economic impact of identity crime for Australia is $2.6b for 2014–15, including both direct and indirect costs (AGD 2016). As with the rates of victimisation, the costs of identity crime exceed those of other individual crime types in Australia (Smith et al. 2014).

Financial impact and most serious occasion of misuse of personal information

In relation to respondents who were left out of pocket due to the misuse of their personal information on the most serious occasion in the past 12 months (excluding any money they were able to recover from banks and any costs associated with repairing what had occurred), just over half (54.2%) reported out-of-pocket losses (n=460). These respondents experienced losses ranging from $1 to $654,646. When these data were weighted, for those who suffered a loss, the mean financial loss was $12,466, and the median loss was $199 (SD=$82,856). Slightly more than three quarters (77%) of respondents experienced losses of up to $1,000. In 2016, the total out-of-pocket losses suffered as a result of the most serious occasion in the previous 12 months were $5,726,706.

Reimbursement

Respondents who had been reimbursed by banks or other organisations or who had recovered their losses in other ways after the misuse of their personal information in the previous 12 months recovered between $1 and $4.5m in total. When the data were weighted, the mean amount reimbursed or recovered was $14,026 and the median amount was $400 (SD=$215,586, n=550). The mean amount reimbursed or recovered in 2016 was lower than in 2014 ($14,026); however, the median amount and standard deviation were much higher, mostly owing to the much higher maximum recovered ($4.5m compared with $2m in 2014). As with the out-of-pocket losses recorded by respondents, the amounts reimbursed or recovered tended to be small, with only a few respondents receiving much larger amounts. The total amount reimbursed or recovered during the previous 12 months was $7.7m. The remaining 298 respondents (35.1%) did not receive any reimbursement or recover any losses. As the amounts recovered in the 12 months preceding the 2016 survey did not necessarily relate to losses experienced during the same period, it is not possible to state a percentage of losses recovered during the 12 months in question.

Reimbursement and most serious occasion of misuse of personal information

Respondents who had been reimbursed by banks or other organisations or who had recovered their losses in other ways in respect of the most serious occasion recovered between $1 and $480,000. When weighted, the mean amount recovered was $3,067, and the median amount recovered was $340 (SD=$25,552, n=525). As in previous years, most respondents received reimbursement of or recovered only small amounts, and a few received much larger amounts. The total recovered was $1,610,730. The remaining 323 respondents (38%) did not receive any reimbursement or recover any losses relating to the most serious occasion of misuse in the previous 12 months.

Other consequences of misuse of personal information

In addition to suffering out-of-pocket losses, some respondents experienced other consequences as a result of having their personal information misused; most commonly, being refused credit (16.2% compared to 14.9% in 2014). Respondents also reported experiencing mental or emotional stress requiring counselling or other treatment (9.8%), and being wrongly accused of a crime (6.6%). These findings were consistent with those reported in 2014. In addition, some respondents provided further information indicating that they had experienced reputational damage as a result of the misuse of their personal information (3.4%).

Dealing with victimisation

Respondents reported having spent between zero and 700 hours dealing with the consequences of having their personal information misused over the previous 12 months (mean=18.3 hours, SD=60.2 hours), with more than half (53.5%) spending up to three hours dealing with the consequences. These findings were similar to those in 2014, although in 2016 respondents spent more time dealing with the consequences than those in 2014, with a maximum of 500 hours spent in 2014. Half of the respondents (49.8%) indicated that they had incurred costs dealing with the consequences of having their personal information misused over the previous 12 months, ranging from $1 to $150,000; almost half (48.1%) of those spent $32 or less. These findings were consistent with those in 2014.

Respondents were also asked if they were aware that a person who has had their personal information misused can apply to a court to obtain a victim certificate. They were also asked if they had applied for such a certificate in the past. Only 499 respondents (5%) indicated that they were both aware of victim certificates and had applied for one. Another 14.5 percent were aware of the certificates but had never applied for one. These findings indicate that slightly more people overall were aware of victim certificates in 2016 than in 2014 (14.9% aware of the availability of the certificates). However, there remains a need to raise awareness of victim certificates, although these are not available in all jurisdictions in Australia at present.

Reporting misuse of personal information

Of those who experienced misuse of their personal information:

- 14.3 percent (n=121) did not report the incident in any way—an increase of 41.6% since 2014 when 10.1% did not report;
- 50.8 percent told a friend or family member;
- 8.3 percent told a government agency or business organisation; and
- 26.7 percent told both a friend or family member and a government agency or business organisation.

Between 2014 and 2016, there was a small increase (2.3 percentage points) in the number of people who only told a friend or family member, and a decrease in the number of people who told a government agency or business.

Respondents were asked to specify which government agency or business organisation they had reported to and how satisfied they were with the outcome. Overall, respondents were mostly satisfied or very satisfied with reports made to agencies or organisations. Respondents were most satisfied with responses provided by internet service providers (85.7% were either satisfied or very satisfied), followed by financial institutions (84.5% were either satisfied or very satisfied). These findings contrast with the 2014 findings, which indicated that respondents were most satisfied with responses provided by their financial institutions (77.5% were either satisfied or very satisfied), followed by utility companies (74.3% were either satisfied or very satisfied; compared with 52.4% in 2016). The lowest levels of satisfaction in 2016 related to reports made to credit reporting agencies or media organisations, while in 2014 the lowest levels of satisfaction related to reports made to consumer protection agencies. Relatively few respondents (n=23) reported to the Australian Cybercrime Online Reporting Network (ACORN), although levels of satisfaction with this mode of reporting were generally good.

When asked about their reasons for not reporting misuse of personal information, 33.9 percent of respondents stated that did not make any report because they did not believe anything could be done about it, and 28.1 percent did not know how or where to report the matter. These findings were consistent with the primary reasons provided in the AIC survey in 2014, although there was a moderate decrease in the number of those who did not report because they did not know how or where to report the matter (35.2% in 2014). In 2016, 23.3 percent of respondents did not report the misuse of their personal information because they were embarrassed; a large increase on the 14 percent who gave that reason in 2014.

Behavioural changes arising from misuse of personal information

Respondents were asked to indicate if and how their behaviour had changed as a direct result of having had their personal information misused. Almost all (91.0%) respondents who had experienced misuse of their personal information in the previous 12 months indicated that they had changed their behaviour in some way—almost identical to the result in 2014 (91.6%).

The changes in behaviour were diverse, with some respondents even changing their place of residence (n=49, 5.8%; up from n=13, 2.9% in 2014).

The top five behavioural changes made in 2016 were:

- changing passwords (48.1%);
- changing bank account details (36.2%);
- being more careful when sharing personal information (34.5%);
- reviewing financial statements more carefully (32.7%); and
- not trusting people as much (24.2%).

These top five behavioural changes were the same in 2014 and in 2013, although their order within the top five differed slightly. These types of behavioural changes were similar to those identified by the ABS *Personal Fraud Survey 2014–15* (ABS 2016), where the top behavioural change following both card fraud (37%) and identity theft (34%) was 'becoming more careful or aware' (ABS 2016).

Willingness to use biometrics

The 2016 survey asked respondents whether they had used biometric and other security measures to keep their personal information secure, and if they would be willing to use such measures in the future to protect their personal information. The most commonly used security measure employed by respondents was a password (90.8%) and the least-used security measure used by respondents was iris recognition technology (1.9%). The security measure most respondents would be willing to use in the future was fingerprint recognition (62.9%).

Characteristics of those who experienced misuse of personal information in the previous 12 months

The demographic and behavioural characteristics of those who experienced misuse of personal information in the previous 12 months were explored in more detail using statistical analysis.

Significant relationships

The 2016 survey findings revealed the following statistically significant relationships between variables:

- experience of misuse of personal information in the previous 12 months and Indigenous status—those who identified as Indigenous were more likely to have experienced misuse of their personal information;
- age and misuse of personal information in the previous 12 months—respondents aged 25 to 34 were most likely to have experienced misuse of their personal information;
- individual gross income and misuse of personal information in the previous 12 months—those in the lowest income category (household income of $18,200 and under) and those who declined to specify their total income were less likely to have experienced misuse of their personal information, and those earning over $80,001 were more likely to have experienced misuse;

- perceptions of the seriousness and risk of misuse of personal information and experience of misuse of personal information in the previous 12 months—those who had experienced misuse of personal information in the previous 12 months were more likely than expected to believe that misuse of personal information was a very serious harm to the Australian economy and that the risk of misuse would increase in the future;
- age and the place from which personal information was obtained—those aged 25 to 34 were more likely than other age groups to have had their personal information obtained through a face-to-face meeting and more likely to have had their personal information obtained via telephone or text message; those aged 55 years and over were significantly less likely to have had their personal information obtained via text message; respondents aged 65 years and over were less likely to have had their personal information obtained by email, whereas respondents aged 25 to 34 were more likely than other age groups to have had their personal information obtained that way; and, as was expected, respondents aged 34 years and under were more likely to have had their personal information obtained from information placed on social media than other age groups;
- place of normal residence and the place from which personal information had been obtained—those located in a capital city were significantly more likely than those who were not in a capital city to have had their personal information obtained by telephone or text message, and were significantly less likely to know how their information had been obtained compared to those who lived outside of a capital city; and
- financial loss and the number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent—the higher the financial loss, the more time and money were spent dealing with the consequences.

Conclusion

The results of this third survey undertaken by the AIC to quantify the extent and nature of identity crime in Australia confirm that criminal misuse of personal information continues to occur in Australia. Findings from the 2013, 2014 and 2016 surveys indicate that around 20 percent of respondents have had their personal information misused over their lifetime, with between eight and nine percent of respondents experiencing misuse in the 12 months prior to completing the survey.

Identity crime is one of the most prevalent forms of criminal activity in Australia and remains a persistent concern for many Australians. The results from the 2016 survey should assist those charged with designing awareness programs and prevention initiatives by providing an indication of those who may be more likely to be victims of identity crime, and by providing advice on seeking help and reporting misuse of personal information. It is hoped that such initiatives will lead to lower levels of victimisation and a reduction in the financial and other impacts experienced as a consequence of identity crime and misuse in the future.

Introduction

Identity crime has become one of the most prevalent crimes affecting the Australian public, businesses and governments (ACC 2015; AGD 2016). Historically, identity has been thought of in terms of psychological, social and physical characteristics of individuals (Wang & Huang 2011); however, with the rise of online transactions and the importance of user-authentication systems in economic commerce, identity is now a legal concept as well as a commodity (UN 2011). With these changes in technology, banking, commerce and business, identity crime has come to be recognised as a global concern (Smith 2011; UN 2007). The United Nations Economic and Social Council (2007:18) defined identity crime as a 'crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes'. Identity crime is a key facilitator of other crimes including dishonesty offences, money laundering, human trafficking and terrorism-related crimes (Smith 2011).

Background to the survey

In April 2007, the Council of Australian Governments (COAG) agreed to the National Identity Security Strategy as Australia's national response to enhancing identity security. The aims were to prevent identity crime and misuse, to contribute to national security and to facilitate the benefits of the digital economy, including through the creation of a national Document Verification Service to verify the authenticity of identity credentials used as evidence of identity (AGD 2012).

A review of the National Identity Security Strategy in 2012 recognised the need to quantify the nature and extent of identity misuse, particularly Australians' experiences of victimisation (AGD 2012). As a result, the review recommended the creation of an identity crime and misuse longitudinal measurement framework that could be used to measure the effectiveness of policy and practice throughout Australia. 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, and their views concerning the risk of identity crime in the ensuing 12 months.

Specifically, respondents were asked to report:

- their experience of identity crime;
- how their personal information had been obtained and misused;
- any financial loss and/or other impact they experienced;
- their reporting and response activities and their levels of satisfaction with any responses;
- whether their behaviour had changed in any way as a result of what happened;
- whether they believe that the risk of this type of crime would change over the next 12 months;
- how serious they think identity crime is;
- whether they knew about, or had applied for, an identity crime victim certificate; and
- information about their age, gender, residence, income, language spoken at home, Indigenous background and computer usage (personal and work-related).

The AIC has conducted two previous surveys to provide data for the Attorney-General's Department's *Identity Crime and Misuse in Australia report series* (AGD 2015, 2016). The surveys were conducted in 2013 (Smith & Hutchings 2014) and in 2014 (Smith, Brown & Harris-Hogan 2015) and provide an indication of the prevalence and costs of identity crime and misuse of personal information across Australia. The present survey updates information obtained in the previous surveys and provides an indication of how the identity crime and misuse environment has changed between 2014 and 2016.

Prior research into identity crime and misuse

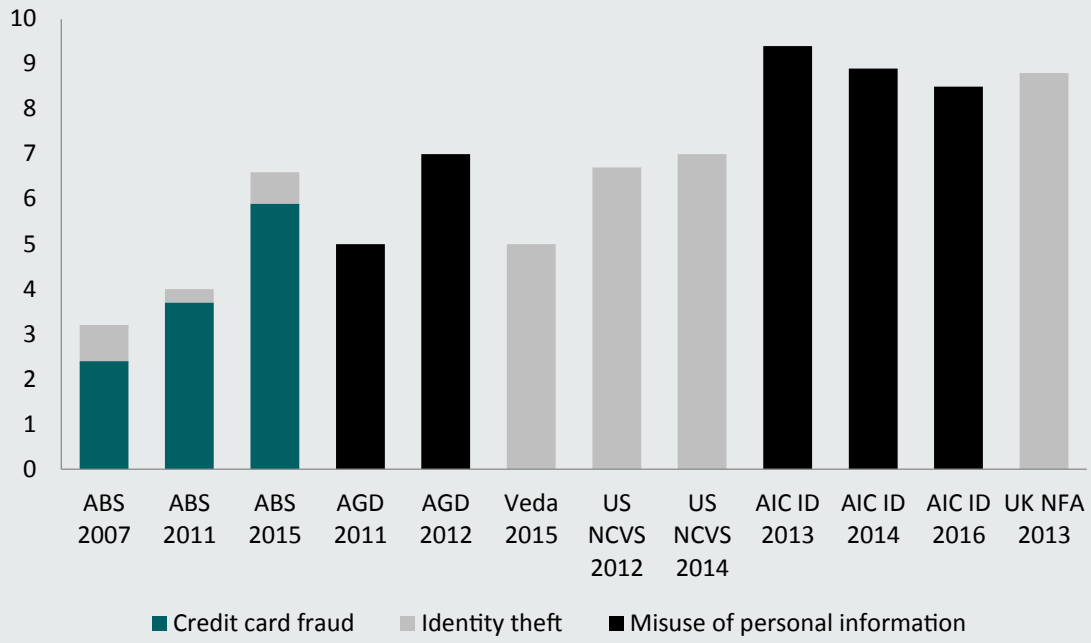
The principal sources of data on the prevalence of identity crime are official administrative data collected by law enforcement and regulatory agencies, as well as surveys of individuals and businesses. These data have been presented annually in the Attorney-General's Department's *Identity Crime and Misuse in Australia reports* (AGD 2015, 2016). Additional comparative research is presented below.

Prevalence

Identity crime is arguably one of the most prevalent criminal activities in Australia, affecting individuals, businesses and government benefits and services. It is estimated that identity crime affects hundreds of thousands of Australians each year (AGD 2016). While there are a number of recent prevalence estimates available, both in Australia and internationally, it is difficult to make direct comparisons owing to differences in definitions and data collection practices.

An indication of the general range of victimisation rates reported by survey respondents in response to questions about identity misuse that occurred during the 12 months preceding survey administration is shown in Figure 2.

Figure 2: Percentage of respondents reporting identity-crime-related victimisation over the preceding 12 months, by survey and year



Note: The AGD surveys asked respondents about their victimisation in the previous six months, whereas the reference period in the other surveys was 12 months prior to survey completion

Sources: ABS 2007 survey (ABS 2008); ABS 2010–11 survey (ABS 2012); ABS 2014–15 survey (ABS 2016) AGD 2011 survey (Di Marzio Research 2011); AGD 2012 survey (Di Marzio Research 2012); Veda (2015a); US NCVS for 2012 (Harrell & Langton 2013); US NCVS for 2014 (Harrell 2015) AIC 2013 survey (Smith & Hutchings 2014); AIC 2014 survey (Smith, Brown & Harris-Hogan 2015); AIC 2016 (Smith & Jorna 2017) (weighted data used for AIC surveys); UK NFA (2013)

As part of its *Multi-Purpose Household Survey,* the Australian Bureau of Statistics (ABS) has asked Australian households to report their experiences of personal fraud, including consumer scams, plastic card fraud and identity theft. The latest survey undertaken by the ABS (2016a) found in the 12 months prior to the survey conducted in 2014–15, an estimated 126,300 Australians (0.7% of the population aged 15 years and over), experienced identity theft. Identity theft was defined by the ABS (2016) as having occurred when:

> a person had their credit, debit, or EFTPOS card, or other personal details or documents, such as driver's licence, tax file number or passport, used by another person for unauthorised gain…People who became aware of an occurrence of identity fraud against them were considered to have experienced identity fraud (ABS 2016a: np).

The 2014–15 ABS identity theft data are not directly comparable with data from the 2010–11 ABS survey due to changes in the wording of questions regarding the experience of identity theft.

Organisations specialising in providing security for monitoring and reviewing credit checks for people who are concerned about or have experienced misuse of their personal information also conduct surveys to review the prevalence of identity theft in Australia. Veda, a data analytics company, sponsored a survey in 2015 of 1,024 Australians aged 18 years and over. That survey found that 17 percent of Australians had experienced a theft of their personal information at some stage in their life, and that 82 percent of Australians were concerned about having their personal information stolen (Veda 2015b).

In the United States, the Bureau of Justice Statistics conducted an *Identity Theft Supplement* to its *National Crime Victimization Survey* (NCVS), which collects data on crime reported and not reported to the police against persons aged 16 years and over from a nationally representative sample of households. The 2014 *Identity Theft Supplement* collected individual data on the prevalence of and victim response to a number of aspects of identity crime including attempted or successful misuse of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes. Respondents were asked whether they had experienced any of these types of misuse, either during the 12 months prior to the interviews (conducted between January and June 2014) or at any point during their lives. Overall, 15 percent of those aged 16 years or older (an estimated 36.5 million people) experienced one or more incidents of identity theft during their lives (Harrell 2015).

In the United Kingdom, the National Fraud Authority (prior to its closure in March 2014) commissioned a survey with a nationally representative sample of 4,213 adults aged 18 years and over to understand the prevalence and cost of identity fraud against individuals. The survey found that 8.8 percent (4.3 million) of UK adults had been a victim of identity fraud within the 12 months prior to the survey and 27 percent of respondents had been a victim of identity fraud at some point in their lives (NFA 2013).

In October 2015, the *Crime Survey for England and Wales* (CSEW) began including questions about fraud and computer misuse in the main headline estimates from the survey. The CSEW is a face-to-face victimisation survey which asks people household residents in England and Wales about their experiences of a selected range of offences in the 12 months prior to the interview (ONS 2016). The CSEW found an estimated 640,000 UK residents aged 16 years and over were victims of 'unauthorised access to personal information' (including hacking) in the period between October 2015 and March 2016.

Although the definitions used in these victimisation surveys differ, it is clear that a considerable proportion of the population experience identity crime and misuse each year, with the rates exceeding all of the principal crime types recorded by the ABS (2016e; AGD 2016).

Cost of identity crime

Estimates of the overall economic cost of identity crime in Australia have varied. One early estimate was $1.1b (with an estimation error of $130m) for 2001–02 (Cuganesan & Lacey 2003), while the most recent estimate for 2014–15 was $2.6b, which included prevention and response costs by government and business organisations (AGD 2016). The direct and indirect costs of identity crime alone amounted to $2.2b of this amount (AGD 2016). For the 2013–14 financial year, the then Australian Crime Commission (ACC; now the Australian Criminal Intelligence Commission) estimated that the cost of serious and organised criminal activity involving identity crimes amounted to $1.2b, including direct costs—that is, financial losses—and indirect costs such as reputational, emotional and psychological impacts (ACC 2015).

Much identity crime involves misuse of credit or debit card details. A growing proportion of this crime occurs online without the cards actually being present. Between 1 July 2014 and 30 June 2015, the Australian Payments Clearing Association (APCA, now AusPayNet) reported 1.9 million fraudulent transactions involving Australian-issued cards, valued at $406m. This represented 0.0272 percent of all Australian-issued card transactions in that financial year (APCA 2015). In its 2014–15 national survey, the ABS (2016a) did not estimate the monetary loss experienced by victims of identity theft; however, it did estimate that Australians lost $2.1b to 'card fraud' in 2014–15. This was double the amount lost to card fraud in 2010–11. After reimbursement and recoveries were taken into account, the out-of-pocket losses in 2014–15 were estimated at $84.8m, a reduction of 59.4 percent from the out-of-pocket losses estimated in 2010–11 (ABS 2016a).

The UK National Fraud Authority's (2013) nationally representative survey found that identity fraud was estimated to cost adult victims in the United Kingdom £3.3b during 2012; it was also estimated that those who experienced a financial loss lost an average of £1,203 each. In the United States, the NCVS *Identity Theft Supplement 2014* found that 65 percent of identity theft victims reported combined direct and indirect financial loss; total losses in 2014 were US$15.4b, down from total victim losses in 2012 of US$24.7b. Overall, the average amount lost was US$1,343, with a median loss of US$300. Fourteen percent of victims of identity theft experienced out-of-pocket losses of US$1 or more in 2014 (Harrell 2015).

Misuse of personal information

Personal information is a commodity that can be bought, sold and traded between different parties. Accordingly, there is a market for those who access, sell and seek to purchase personal information. The *2015 Internet Security Threat Report* released by Symantec (2016) outlined the cost of personal information available on the internet in 2014. Credit card details could be bought for prices ranging from US$0.50 cents to US$20 and could be used for fraudulent purchases. Scans of real passports were available to purchase for between US$1 and US$2 per copy and could be used for identity theft.

The personal information at risk of appropriation and misuse by criminals falls into two categories: life history information and financial information. Each of these categories may also be separated into traditional identity theft details and cyber-enabled details (Roberts, Indermaur & Spiranovic 2013). Traditional identity theft details include name, date of birth, licence number and contact details. Cyber-based identity information includes computer usernames, passwords, email addresses and URLs for web pages (Roberts, Indermaur & Spiranovic 2013; Smith & Hutchings 2014).

How personal information is obtained

Victims of misuse of personal information and identity crime do not always know how their information was obtained (Harrell 2015; Smith & Hutchings 2014). In the United States, most identity theft victims were unaware as to how their personal information was obtained, with only 32 percent of victims aware of how the information was acquired. These findings are slightly higher than those obtained in the ABS *Personal Fraud Survey* (ABS 2016a), which found that in 2014–15, 26 percent of victims were unaware of how their personal information was stolen. Understanding how personal information is obtained by criminals is important for the development of education and prevention strategies; to prevent others from falling victim to the same schemes and to assist victims to identify ways to protect their personal information.

Personal information can be obtained from a variety of sources. These include accidental data leakage from government or business networks; the deliberate harvesting of data through the use of computer hacking and the gathering of documents that contain personal information; and social engineering ('phishing') in which deceptive websites are used to persuade or trick individuals into disclosing their personal information, for subsequent use in criminal activities (Smith 2011). Smith and Hutchings (2014) found that the most successful way to dishonestly obtain personal information is through fraudulent invitations, also known as phishing.

A data breach has been defined as the unauthorised access to personal information held by a business, organisation or government agency when that personal information is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference (OAIC 2013). The breach may be accidental, for example, when information is sent to the wrong person, or it may be deliberate, for example, through the use of social engineering or unauthorised access to computer networks. In collaboration with 67 contributing organisations—including the Australian Federal Police, the United States Secret Service, and the United Kingdom Computer Emergency Response Team—Verizon publishes a report which quantifies the nature and extent of the external forensic investigations that it conducts (Verizon 2016). The report includes details about the number of data breaches, phishing attacks and other cyber-related attacks against organisations, and provides security advice about how to reduce these attacks.

The 2016 report included details and analysis of 2,260 confirmed data breaches resulting from 64,199 incidents across 82 countries. More than 80 percent of breaches arose as a result of actions by parties external to the organisations, and 89 percent of breaches involved financial gain or espionage (Verizon 2016).

Purpose of this report

To explore the extent of the problem of identity crime and misuse of personal information in Australia the AGD has previously (2013 and 2014) commissioned the AIC to conduct annual surveys of a large sample of Australians drawn from a national online panel. Although the ABS conducts rigorous, nationally representative research through personal fraud questions in its *National Crime Victimisation Survey*, which forms part of the *Multipurpose Household Survey*, these surveys are not conducted frequently. The AIC's research, while smaller in scale, provides timely, detailed information on the nature of identity crime experienced by a large sample of Australians who have agreed to participate in online market research surveys.

This report details the number, percentage and demographic characteristics of respondents who reported having their personal information misused in the 12 months prior to May 2016. This report focuses on the most serious occasion of misuse of personal information in the last 12 months and describes victim characteristics and changes in victim behaviour as a result of their personal information being misused. The report details:

- how crimes were detected;
- the financial and other impacts of the misuse of personal information;
- the time and money spent dealing with the consequences of the misuse;
- reporting of the misuse to private and public organisations;
- victims' subsequent satisfaction with reporting; and
- respondents' perceptions of the risk of identity crime in the ensuing 12 months.

Where appropriate, comparisons are made with the findings from the 2013 and 2014 surveys. However, since the sample size in 2016 was 10,000, compared with sample sizes of 5,000 in both 2013 and 2014, these are percentage comparisons only.

Methodology

Research design and definitions

This study employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information within the sample at one point in time within the population of Australian residents aged between 15 and 96 years. This methodology replicated that used in two previous studies conducted by the AIC in 2013 and 2014 (see Smith & Hutchings 2013; Smith, Brown & Harris-Hogan 2015). The operational definition of *identity crime and misuse of personal information* was 'the use of personal information without permission'. This included obtaining or using personal information without permission, pretending to be someone else or to carry out a business in someone else's name without their permission, and other types of activities or transactions. This definition excluded the use of personal information for direct marketing, even if this were done without permission. *Personal information* was defined as including: name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg a fingerprint), signature, bank account information, credit or debit card information, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student identification number and other types of personal information.

Survey questions

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

- perceptions of the seriousness of misuse of personal information and of how risks will change over the next 12 months;
- experience of misuse of personal information at any time in the past and over the preceding 12 months;
- methods of victimisation on the most serious occasion in the preceding 12 months;
- actual financial losses, funds recovered, time spent resolving identity crime victimisation, and other consequences of victimisation;
- awareness of the availability of court victimisation certificates;

- reporting of misuse of personal information, and satisfaction with responses from organisations;
- behavioural changes arising from misuse of personal information;
- use of biometric technologies in the past, and willingness to use biometric technologies in the future, to reduce risk of identity crime victimisation; and
- demographic and other characteristics of respondents including age, gender, place of normal residence, income, language spoken at home, Indigenous background and computer usage.

These questions largely replicated those of the previous surveys in 2013 (Smith & Hutchings 2014) and 2014 (Smith, Brown & Harris-Hogan 2015) to allow for direct comparisons over time. The questions were originally developed in consultation with the AGD.

The questions spanned a number of reference periods. These included respondents' current circumstances (eg place of normal residence, age and income), their lifetime experiences of identity crime and misuse, and the identity crime and misuse they had experienced in the previous 12 months. The survey was available for completion over two weeks in May 2016.

The survey had 24 questions in total and took approximately 15 minutes to complete. No identifying information was requested from respondents. A copy of the online questionnaire is attached at Appendix 1.

Sampling

The survey was administered online by an external provider, i-Link Research Solutions, to members of its research panel comprising over 300,000 members in Australia. The non-probability sample consisted of 10,000 Australian residents aged between 15 and 96—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. The sampling frame and survey hosting were provided by i-Link Research Solutions with de-identified data supplied to the AIC for analysis and reporting.

In 2013, 4,995 useable responses were analysed (Smith & Hutchings 2014); followed by 5,000 responses in 2014 (Smith, Brown & Harris-Hogan 2015), and 9,956 in the present survey in 2016. In both 2013 and 2014, sample quotas were established to ensure that respondents reflected the distribution of the Australian population in terms of age (15 and over) and gender. These samples were also weighted to reflect state and territory place of residence.

A larger sample was used in 2016 to allow more extensive analysis of the results. Quotas were not employed, but the final results were weighted to reflect the distribution of the Australian population in terms of age and gender (either male or female only) based on census data from the Australian Bureau of Statistics (ABS 2016b,d). Sampling was completed once the target sample size of 10,000 respondents had been obtained. As quotas were not employed, the data were compared against Australian Bureau of Statistics national data collected from a probability sample of the Australian population.

Table 1 presents comparative statistics between the unweighted number of survey respondents in the AIC panel survey (prior to responses that were removed for analysis) by respondents' normal place of residence, and the estimated resident population based on ABS data as at 2015 (ABS 2016b,d). As can be seen in Table 1, the percentage of AIC panel survey respondents in each place of residence is similar to the ABS percentage of the Australian population residing in each location.

Table 1: Respondents by place of normal residence compared with ABS national data (unweighted data, total respondents)

	n	%	ABS N	ABS %
Sydney	1,883	18.8	4,920,970	20.7
Other New South Wales	1,048	10.5	2,696,714	11.3
Melbourne	2,045	20.5	4,529,496	19.0
Other Victoria	707	7.1	1,407,985	5.9
Brisbane	1,079	10.8	2,308,720	9.7
Other Queensland	997	10.0	2,470,134	10.4
Perth	653	6.5	2,039,193	8.6
Other Western Australia	158	1.6	551,066	2.3
Adelaide	709	7.1	1,316,779	5.5
Other South Australia	221	2.2	381,881	1.6
Canberra (whole of Australian Capital Territory)	160	1.6	390,706	1.6
Hobart	111	1.1	220,953	0.9
Other Tasmania	186	1.9	295,633	1.2
Darwin	26	0.3	142,258	0.6
Other Northern Territory	17	0.2	102,049	0.4
Total	10,000	100.0	23,777,777	100.0

Source: ABS 2016d.

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

- instant member reward points—can be accumulated to redeem gifts such as Caltex/Coles vouchers;
- chances to win a $50,000 prize, drawn quarterly;
- the donation of rewards to an affiliated charity; and
- monthly community member competitions/prizes and draws.

Weighting of data

Data were weighted by age and gender to represent the distribution of the population in Australia. Because the natural spread of respondents in terms of geographical location was similar to that found in nationally representative probability surveys (ABS 2016b,d), weighting by location was not undertaken. The latest available data estimating age and gender for the population of Australia—at 30 June 2015 (ABS 2016b)—were used to develop the weighting matrix for the sample data. The process of weighting involved the application of a formula to the data provided by each respondent (for respondents who specified a gender and age category) to make each response proportionate in relation to the broader population of Australians (see Appendix 2 for the weighting matrix employed). It was necessary to weight these data, despite the use of a non-probability sample, as older and female respondents were over-represented in the sample of respondents.

The demographic data collected by the ABS (2016b) at 30 June 2015 did not provide population data for people who listed their gender as indeterminate/intersex or unspecified. For the purposes of being able to weight data appropriately, those responses were not included in the weightings (n=19). There was also a small number of respondents who did not provide their age category, who were also excluded from the weighted data (n=25). Excluding these two types of responses left a sample size of 9,956 for analysis. The actual weighting for each age and gender group is presented in Table 4 and Appendix 2. All results refer to weighted data, unless otherwise specified.

However, the results have not been weighted to indicate national estimates of the prevalence and financial loss that would have been experienced had the entire Australian population aged 15 years and over been surveyed, as the sampling framework was insufficiently robust to permit such estimations to be undertaken.

In the following pages, results presented all relate to weighted data unless otherwise indicated.

Analysis

The analysis presented in the report is largely descriptive and reports the characteristics of the sample and victim experiences relating to the misuse of personal information. Where applicable, further analyses were undertaken to examine the relationship between identity crime and characteristics of the sample. Appropriate tests for statistical significance are presented where bivariate analyses have been undertaken. In some cases, outliers that did not fit within the range of possible responses were excluded from the analysis.

Where appropriate, comparisons with the 2013 and 2014 surveys have been made. It should be noted that the differences between the surveys have not been tested for statistical significance. It is possible that some of the differences will fall within the margins of sampling error for the surveys, meaning the observed differences may be a function of the survey methodology rather than reflecting true differences in the population. For example, the 2013 and 2014 surveys were weighted by location, whereas the 2016 survey was weighted by age and by gender but not by location.

In addition, the samples obtained in 2013, 2014 and 2016 are not entirely independent. Of the final 9,956 respondents included in the 2016 sample for analysis, eight respondents had completed the surveys in 2013 and 2014 and had reported misuse of their personal information in the preceding 12 months in each survey they completed. All respondents were included in the 2016 sample, as two years had transpired since completing the 2014 survey. However, it should be noted that some of the respondents who had their personal information misused in 2013 may have also completed the survey in 2014.

Ethical considerations

A number of ethical issues were taken into consideration when developing the research design. These included the need for research respondents to remain anonymous, the ability to reach large numbers of respondents, the requirement to provide informed consent, the ability for respondents to withdraw from the research, and any potential for the research questions to cause psychological discomfort, particularly as they related to victimisation experiences. These concerns were addressed through the provision of counselling and support services for respondents and through procedures to maintain confidentiality of responses.

In relation to the anonymity of the research respondents, no information that could be used to identify the respondents was collected. The results are presented in an aggregate form, and since responses are anonymous, they cannot be matched to specific individuals.

In order to ensure that respondents understood the nature of the research and provided informed consent, a plain language statement was provided at the beginning of the survey. This stated that by completing the survey, respondents were consenting to participate in the research. As outlined in the plain language statement, respondents had the option to withdraw from the survey at any stage, and they could also contact the external provider and request that the responses they had already provided be withdrawn from the dataset.

While the risk of psychological distress associated with the research was minimal, it was acknowledged that there was the possibility that a participant may have felt discomfort when answering questions about victimisation. Given the voluntary nature of the survey and the provision of information in the plain language statement which explained the nature of the research, it can be assumed that respondents were aware of the potential sensitivity of the survey contact. Also provided in the plain language statement were telephone and website details for Lifeline crisis support and contact details for IDCARE, a service supported by the Australian Government to assist victims of identity crime.

The project therefore presented an overall low risk to respondents, and the research was approved by the AIC's Human Research Ethics Committee (PO247A).

Limitations of the study

Limitations of the research design arose from the sampling procedure, as those who participated in the online panel may not have been representative of the Australian population. For example, people who subscribed to an online panel may have had a higher exposure to online fraud than people in the general population. Also, the survey was only available to those who had computer access and who subscribed to the online research panel. Surveys conducted using online panel samples are non-probability samples, with participation limited to people who are members of the panel and have a computer. Accordingly, not everyone in the target population had the opportunity to be included in the sample (SRC 2016). Given these limitations, the results presented cannot be generalised to the wider Australian population.

It can also be difficult to measure fraud incidents within a given time frame; it is not always easy to determine when fraud has occurred, due to the time lapses between when the fraudulent conduct occurs, is identified by victims, and then reported (if reported at all). The reference period for the 2016 AIC online survey was the previous 12 months. Respondents were asked whether they had been subject to and responded to identity misuse during this time. It is possible that some respondents may have inadvertently included incidents that occurred before this period.

Despite these limitations, the results of the present survey provide valuable information to inform not only policymakers but also the public about the current extent and nature of identity crime and the misuse of personal information in Australia.

Findings: Characteristics of the sample

This section presents the findings of the AIC's identity crime survey conducted in 2016 and, where applicable, draws comparisons with the earlier 2013 and 2014 identity crime surveys. The results are presented as follows:

- characteristics of the sample, including demographic information and extent of computer usage;
- respondents' perceptions of the seriousness and risk of identity crime;
- respondents' experience of victimisation as a result of identity crime over their lifetime;
- respondents' experience of identity crime in the previous 12 months, including the most serious occasion of misuse of personal information;
- financial impacts of misuse of identity crime, and other consequences;
- how respondents dealt with victimisation;
- reporting of identity crime; and
- any behavioural changes that arose out of victimisation.

At the end of each subsection, the survey findings are compared with prior Australian and international research on the same research questions.

As previously indicated, results presented all relate to weighted data unless otherwise indicated.

Demographic information

Tables 2 and 3 show the unweighted distribution of respondents by age and gender, and Table 4 presents these distributions using weighted data. The differences between the unweighted and weighted numbers reflect the larger numbers of older respondents participating in the survey. For example, there were only four male respondents aged 15 to 17 years. Even when the age category was combined to include 15 to 24 years, male respondents in that category represented only 1.2 percent of the sample; males in that age category represent 8.4 percent of the Australian population as a whole.

Table 2: Respondents by age (unweighted data)		
	n	%
17 years and under	14	0.1
18–24 years	446	4.5
25–34 years	1,296	13.0
35–44 years	1,506	15.1
45–54 years	1,821	18.3
55–64 years	2,350	23.6
65 years and over	2,542	25.5
I'd rather not say	25	0.3
Total	10,000	100.0

Source: Identity Crime Survey 2016 [AIC data file]

Table 3: Respondents by gender (unweighted data)		
	n	%
Male	4,157	41.6
Female	5,813	58.1
Indeterminate/Intersex/Unspecified	12	0.1
I'd rather not say	18	0.2
Total	10,000	100.0

Source: Identity Crime Survey 2016 [AIC data file]

Owing to the small number of respondents aged 17 years and under (n=12), and because only those aged 15 years and over were eligible to participate in the survey, two age groups—17 years and under and 18 to 24 years—were treated together for analysis. The data were weighted to reflect the distribution of the population across age and gender, based on ABS data on the estimated resident population for 2015 (2016b,d). Table 4 shows the multipliers used to weight the data, the unweighted responses received from respondents, and the subsequent responses weighted by age and gender (see Appendix 2 for further details on weighting). All subsequent analyses are based on weighted data unless otherwise stated.

Table 4: Respondents by age and gender (unweighted and weighted data)				
	Unweighted	Multiplier	Weighted	
	n		n	%
24 years and under				
Male	122	6.881	839	8.4
Female	334	2.382	796	8.0
25–34 years				
Male	385	2.352	905	9.1
Female	906	0.991	898	9.0
35–44 years				
Male	560	1.493	836	8.4
Female	942	0.901	849	8.5
45–54 years				
Male	669	1.198	801	8.0
Female	1,149	0.713	820	8.2
55–64 years				
Male	1,035	0.670	693	7.0
Female	1,314	0.830	713	7.2
65 years and over				
Male	1,376	0.610	839	8.4
Female	1,164	0.830	967	9.7
Total	9,956		9,956	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Previous AIC identity crime surveys also weighted data by location to reflect the geographical spread of the resident Australian population (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015). The 2016 identity crime survey, however, had a much larger sample size (10,000 versus 5,000). This meant that over-sampling of smaller regional areas was not required: a sample of 10,000 was large enough to reflect the distribution of the Australian population based on ABS demographic data. Table 5 shows the number of survey respondents (weighted data) by their normal place of residence.

Table 5: Respondents by normal place of residence		
	n	%
Sydney	2,062	20.7
Other New South Wales	925	9.3
Melbourne	2,188	22.0
Other Victoria	623	6.3
Brisbane	1,042	10.5
Other Queensland	875	8.8
Perth	661	6.6
Other Western Australia	143	1.4
Adelaide	718	7.2
Other South Australia	206	2.1
Canberra (whole of Australian Capital Territory)	171	1.7
Hobart	122	1.2
Other Tasmania	171	1.7
Darwin	31	0.3
Other Northern Territory	18	0.2
Total	9,956	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Respondents were asked what language was most often spoken at home. These responses were recoded using the ABS (2011) *Australian Standard Classification of Languages,* although in this instance, English was disaggregated from other 'Northern European' languages. Table 6 shows the weighted results for language most often spoken at home. This indicates that only about seven percent of respondents spoke a language other than English at home, which is lower than national estimates from the ABS census indicating that 23 percent of Australians speak a language other than English (ABS 2011).

Table 6: Respondents by language most often spoken at home		
	n	%
English	9,213	92.5
Southern Asian	217	2.2
Eastern Asian	160	1.6
Southeast Asian	150	1.5
Eastern European	46	0.5
Southern European	66	0.7
Northern European	39	0.4
Southwest and Central Asian	38	0.4
Other languages	27	0.3
Australian Indigenous	0	0
Total	9,956	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Respondents were also asked if they identified as Aboriginal or Torres Strait Islander. Responses provided in Table 7 show that slightly less than two percent (1.8%) of those surveyed identified as either Aboriginal or Torres Strait Islander. The ABS estimate at 30 June 2011 of the Aboriginal and/or Torres Strait Islander population was three percent of the Australian population (ABS 2013); that figure included children aged under 15 years, whereas in the current survey only respondents aged 15 years and older were invited to participate. The panel used for the current survey had a slightly lower representation of Indigenous people than Australia as a whole.

Table 7: Respondents who identified as Aboriginal or Torres Strait Islander

	n	%
Aboriginal	131	1.3
Torres Strait Islander	30	0.3
Both Aboriginal and Torres Strait Islander	19	0.2
No	9,671	97.1
I'd rather not say	106	1.1
Total	9,956	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Respondents were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2014–15 (Table 8). The largest class of respondents (28.9 percent) had an income between $37,001 and $80,000. Twelve percent of respondents preferred not to divulge their income details.

Table 8: Respondents by individual gross income 2014–15

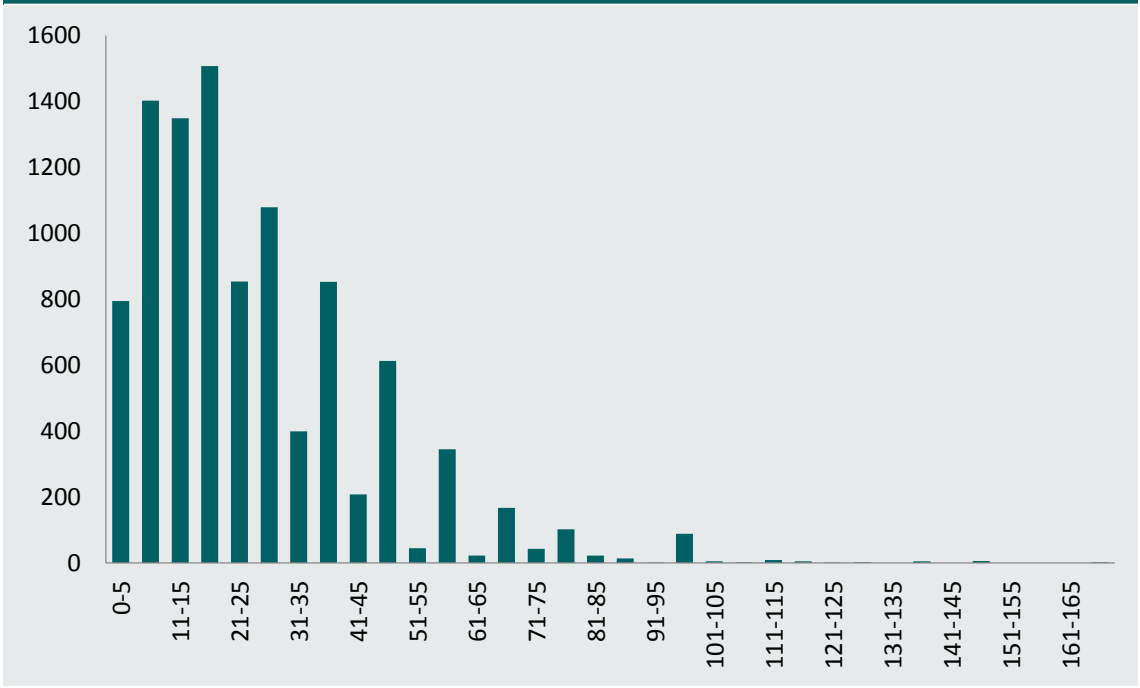
	n	%
$0–$18,200	1,811	18.2
$18,201–$37,000	2,114	21.2
$37,001–$80,000	2,876	28.9
$80,001–$180,000	1,666	16.7
$180,001 and over	254	2.6
I'd rather not say	1,236	12.4
Total	9,956	100.0

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [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. Responses (after weighting) ranged from zero to 167 hours (mean=26.9, SD=19.8, n=9,944). Responses over 168 hours (the maximum number of hours in a week) were excluded from this section of analysis (n=11). As evident in Figure 3, results for 2016—which were similar to the 2014 results—showed that the majority (82.8%) of respondents spent 40 hours or less on a computerised device per week. By contrast, the ABS found individuals spent an average of 10 hours in a typical week on the internet for personal use, with younger people spending an average of 18 hours online (ABS 2016c). In the present survey, some respondents recorded spending more than 40 hours on a computerised device each week, with 88 respondents spending between 96 and 100 hours each week. One explanation for the differences between the two sets of survey results may be the wording of the questions. The ABS survey asked specifically about hours spent accessing the internet, while the AIC questions were broader and asked about the number of hours spent using a computer or computerised device, which included smartphones, tablets and other devices activated throughout the day.

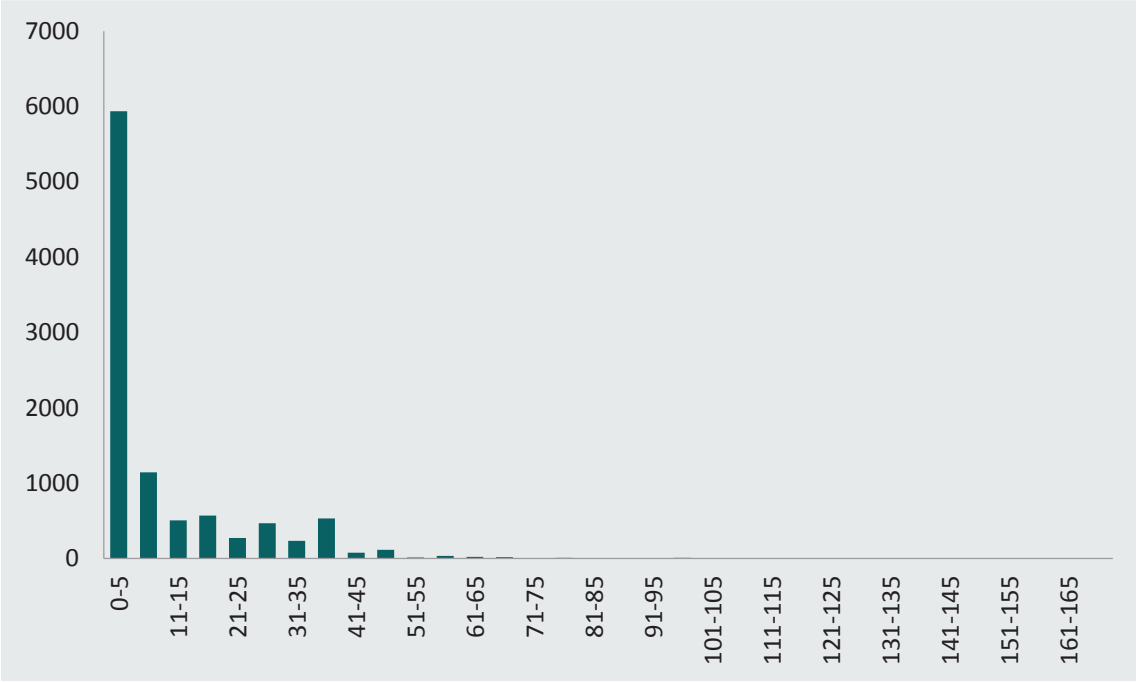
Figure 3: Frequency distribution of number of hours spent the previous week using a computer or computerised device (n)



Source: Identity Crime Survey 2016 [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 167 (mean=10.0, SD=14.8, n=9,955). As shown in Figure 3, the distribution was also positively skewed; that is, the distribution of the data was heavily clustered to the lower time groups, with the majority (76.2%) of respondents spending 15 hours or less on a computerised device per week for work purposes. This compares with the majority in 2014 (75.9%) who spent 12 hours or less on a computerised device per week for work purposes.

Figure 4: Frequency distribution of number hours spent the previous week using a computer or computerised device for work-related activities (n)



Source: Identity Crime Survey 2016 [AIC data file]

A Wilcoxon Mann-Whitney (rank sum) test was used to test for differences in the number of hours spent on a computer or computerised device between those who had experienced misuse of their personal information in the previous 12 months and those who had not. This non-parametric test was used because the dependent variable—the number of hours spent on a computer or computerised device—was not normally distributed and was a continuous variable, ranging from 1 to 168. The test compared the median number of hours for the two groups (those who had experienced misuse in the previous 12 months and those who had not) and found that respondents who had experienced misuse of their personal information spent significantly longer on a computer or computerised device than those who had not ($z=-3.53$, $p<0.01$, $n=9,945$).

As the Mann-Whitney U test could not be replicated with the weighted data, the variable (number of hours spent on a computer or computerised device) was transformed to a normal distribution using logarithmic transformation (natural log) so that the parametric alternative, an independent t-test, could be undertaken. Using the unweighted data, the t-test found that those who experienced misuse of their personal information spent significantly more hours on computerised devices ($M=3.05$, $SD=0.81$) than those respondents who did not experience misuse of their personal information in the previous 12 months ($M=2.97$, $SD=0.81$; $t(9,936)=-2.81$, $p<0.05$). However, when the transformed data were weighted, the difference was no longer significant ($p=0.178$).

Perceptions of misuse of personal information

Seriousness at present

The survey asked respondents how they perceived the risk of misuse of personal information, how serious they thought such conduct would be, and what changes were likely to occur in the years ahead. While some respondents may have had access to independent evidence relating to these matters, the responses reflect the personal views of respondents at the time of the survey and cannot be said to be indicative of objective factual information.

First, respondents were asked how serious they thought misuse of personal information was in terms of harm to the Australian economy. As shown in the weighted responses provided in Table 9, most respondents (95.7%) believed the misuse of personal information was a very serious or somewhat serious issue. This finding was similar to the results obtained in both 2013 and 2014.

Table 9: Respondents' perceptions of seriousness of misuse of personal information

	2013	2014		2016
	%	%	%	n
Very serious	68.8	68.1	63.7	6,340
Somewhat serious	27.8	28.2	32.0	3,188
Not very serious	2.9	3.1	3.6	360
Not at all serious	0.5	0.7	0.7	68
Total	100.0	100.0	100.0	9,956

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding

Risks in the next 12 months

Respondents were also asked if they thought the risk of someone misusing their personal information would change over the next 12 months. Over 60 percent (61.7%) of those surveyed thought the risk of their personal information being misused would increase greatly or somewhat over the next year. This was slightly less than in 2014 (67%). Weighted responses are provided in Table 10.

Table 10: Respondents' perceptions of risk of misuse of their personal information in the next 12 months				
	2013	2014		2016
	%	%	%	n
Risk will increase greatly	19.8	22.0	16.4	1,634
Risk will increase somewhat	45.4	45.0	45.3	4,511
Risk will not change	33.8	32.1	36.6	3,641
Risk will decrease somewhat	0.5	0.5	1.2	115
Risk will decrease greatly	0.5	0.3	0.6	55
Total	100.0	100.0	100.0	9,956

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Respondents were asked if they were aware that a person who has had their personal information misused can apply to a court for a victim certificate to prove that the misuse occurred. They were also asked if they had ever applied for a victim certificate in the past. A victim certificate is designed to assist victims to manage personal and business problems that may have been caused by identity crime.

Table 11: Respondents' awareness of victim certificates				
	2013	2014		2016
	%	%	%	n
I am aware of such certificates, and have applied for one in the past	3.4	3.4	5.0	499
I am aware of such certificates, but have not applied for any	11.2	11.5	14.5	1,446
I am unaware of such certificates	85.5	85.0	80.5	8,011
Total	100.0	100.0	100.0	9,956

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 11, the number of respondents who indicated they were aware of such certificates has increased from less than 15 percent in 2013 and 2014 to over 19 percent in the 2016 survey. In line with that finding, the percentage of respondents who were unaware of such certificates decreased from 85 percent in previous years to 80 percent in 2016.

A significant relationship was also found between perceptions of the seriousness of misuse of personal information in the next 12 months and experience of misuse of personal information in the previous 12 months ($\chi^2(3, n=9,956)=27.39$, $p<0.05$) as shown in Table 12.

Those who experienced misuse of personal information in the preceding 12 months were more likely to view that misuse as very serious than those who had not had their personal information misused in the previous 12 months.

Table 12: Contingency table for misuse of personal information in the previous 12 months and perceptions of the seriousness of the misuse (expected frequencies shown in parentheses) (n)

	Misuse of personal information in previous 12 months		Total
	Yes	No	
Very serious	596 (540)*	5,744 (5,800)	6,340
Somewhat serious	238 (271)	2,949 (2,916)*	3,187
No very serious	14 (31)*	346 (329)	360
Not at all serious	0 (6)*	69 (63)	69
Total	848	9,108	9,956

*chi-square test statistically significant at $p<0.05$, based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

A significant relationship was also found between perceptions of the risk of misuse of personal information in the next 12 months and experience of misuse of personal information in the previous 12 months ($\chi^2(4,n=9,956)=228.44$, $p<0.001$). As shown in Table 13, those who had experienced misuse of personal information in the previous 12 months were more likely to perceive that risks would increase in future.

Table 13: 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 (expected frequencies shown in parentheses) (n)

	Misuse of personal information in previous 12 months		Total
	Yes	No	
Risk will increase greatly	262 (139)*	1,372 (1,495)	1,634
Risk will increase somewhat	433 (384)*	4,078 (4,127)	4,511
Risk will not change	141 (310)	3,500 (3,331)*	3,641
Risk will decrease somewhat	10 (10)	105 (105)	115
Risk will decrease greatly	2 (5)	53 (50)	55
Total	848	9,108	9,956

*chi-square test statistically significant at $p<0.001$, based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Prior research compared

A very high proportion of respondents indicated that misuse of personal information was, in their view, very serious or somewhat serious in terms of harm to the Australian economy (96.7%). This finding is consistent with findings in 2013 (96.6%) and 2014 (96.3%) and shows the level of ongoing concern about misuse of personal information held by members of the Australian public who have responded to the AIC's identity crime surveys.

In 2016, almost two-thirds of respondents (61.7%) considered that the risk of someone misusing their personal information would increase over the next 12 months. This represents a slight reduction on the figures from 2013 (65%) and 2014 (67%).

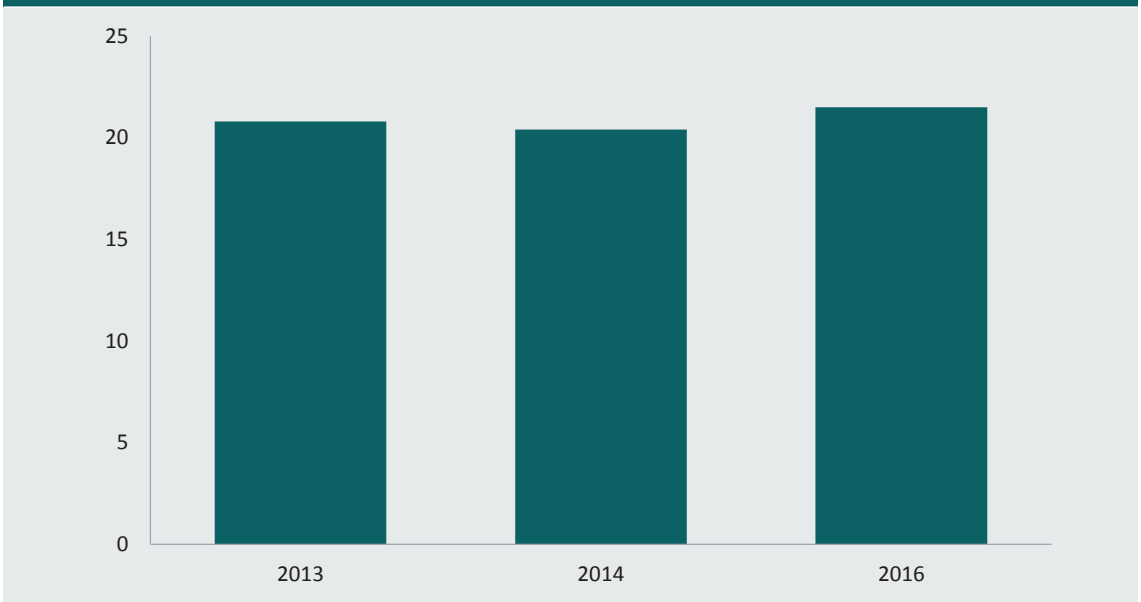
Respondents rated the seriousness of harm due to identity crime and misuse of personal information as very serious. This contrasts with findings in similar Australian and overseas surveys, although the findings are not directly comparable due to the use of different sampling frameworks and questions. For example, Veda conducted a survey of 1,511 Australians which found that 82 percent of respondents reported being concerned about having their personal information stolen (Veda 2015b), while OAIC (2013) found that 25 percent of respondents were very concerned about identity crime and misuse of personal information. These findings differ from the present study in which 64 percent of respondents considered that misuse of personal information involved a very serious harm to the Australian community.

Victimisation rates

Victimisation over lifetime

Respondents were asked if their personal information had been misused at any time in the past, or at any time in the previous 12 months. Of the 9,956 respondents, 2,144 (21.5%) had experienced misuse at some time in their lives. This finding is only a slight, non-statistically significant (comparison of proportions test, N-1 χ^2 p=0.1201, 2014 versus 2016, % difference) increase on the 20 percent reported in both 2013 and 2014 (Figure 5). It is to be expected that misuse of identity will increase over time as increased availability and use of the internet creates increasing opportunities for misuse. The small increase in lifetime victimisation is, therefore, lower than might be expected.

Figure 5: Percentage of respondents experiencing identity misuse in their lifetime, 2013, 2014 and 2016



Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Surveys 2013, 2014 and 2016 [AIC data file], https://www.medcalc.org/calc/comparison_of_proportions.php

Table 14 presents the percentage of respondents who reported experiencing identity misuse at some time in their lives, by age.

Table 14: Respondents who experienced misuse of their personal information at any time in the past, by age		
	n	%
24 years and under (1,635)	332	20.3
25–34 years (1,803)	453	25.1
35–44 years (1,685)	368	21.8
45–54 years (1,621)	345	20.5
55–64 years (1,406)	277	19.7
65 years and over (1,806)	369	20.4
Total (9,956)	2,144	21.5

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Victimisation in the prior 12 months

Respondents were also asked about misuse of their personal information in the previous 12 months. For the total sample (n=9,956), 8.5 percent (n=848) of respondents had experienced such misuse in the past 12 months (Table 15). This represents a slight decrease on 2014 results, which indicated 8.9 percent (n=446) of respondents had experienced misuse during the previous year. When data were weighted to reflect national age and gender distributions, 848 respondents (8.5%) reported experiencing identity misuse in the past 12 months.

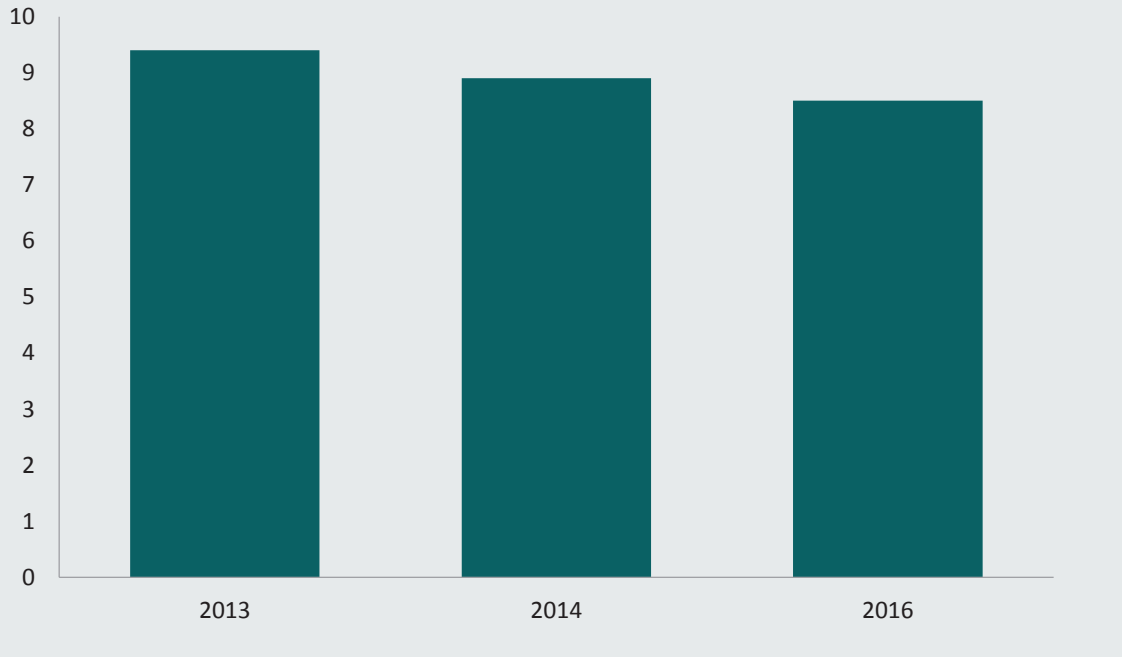
Table 15: Respondents who experienced misuse of their personal information in the past 12 months, by place of normal residence (unweighted data)				
	2013	2014		2016
	%	%	%	n
Sydney (2,062)	10.0	10.3	8.8	183
Other New South Wales (924)	10.4	6.6	9.4	87
Melbourne (2,188)	10.4	11.7	8.3	181
Other Victoria (623)	6.6	7.6	8.8	55
Brisbane (1,042)	6.8	6.6	7.3	76
Other Queensland (875)	9.9	6.9	8.1	71
Perth (661)	9.6	7.9	10.6	70
Other Western Australia (144)	9.3	9.3	15.3	22
Adelaide (719)	9.6	8.2	6.8	49
Other South Australia (206)	7.2	9.8	5.8	12
Canberra and Australian Capital Territory (171)	8.5	9.6	9.9	17
Hobart (122)	8.3	6.4	3.3	4
Other Tasmania (170)	7.7	9.4	10.0	17
Darwin (31)	10.3	20.7	16.1	5
Other Northern Territory (18)	13.0	8.7	0.0	0
National (9,956)	9.4	8.9	8.5	848

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Similar findings were recorded in 2016 for most capital cities. However, even with a larger sample size, there were no respondents whose normal place of residence was in the Northern Territory (outside of Darwin) who had experienced misuse of their personal information within their lifetime. Respondents residing in Canberra, Darwin, Western Australia (outside of Perth), Brisbane and Victoria (outside of Melbourne) all reported higher levels of victimisation in the preceding 12 months than had been reported in those locations in 2013. Respondents residing in other locations reported lower levels of such misuse in the preceding 12 months than levels reported in 2013 and 2014.

Between 2013 and 2016, the percentage of respondents who experienced misuse of identity in the past 12 months has been decreasing steadily, although the decrease is not statistically significant (p=0.0669, 2013 compared with 2016). In the 2013 survey, 9.4 percent of respondents experienced such misuse; in 2016, this had fallen to 8.5 percent of respondents (Figure 6).

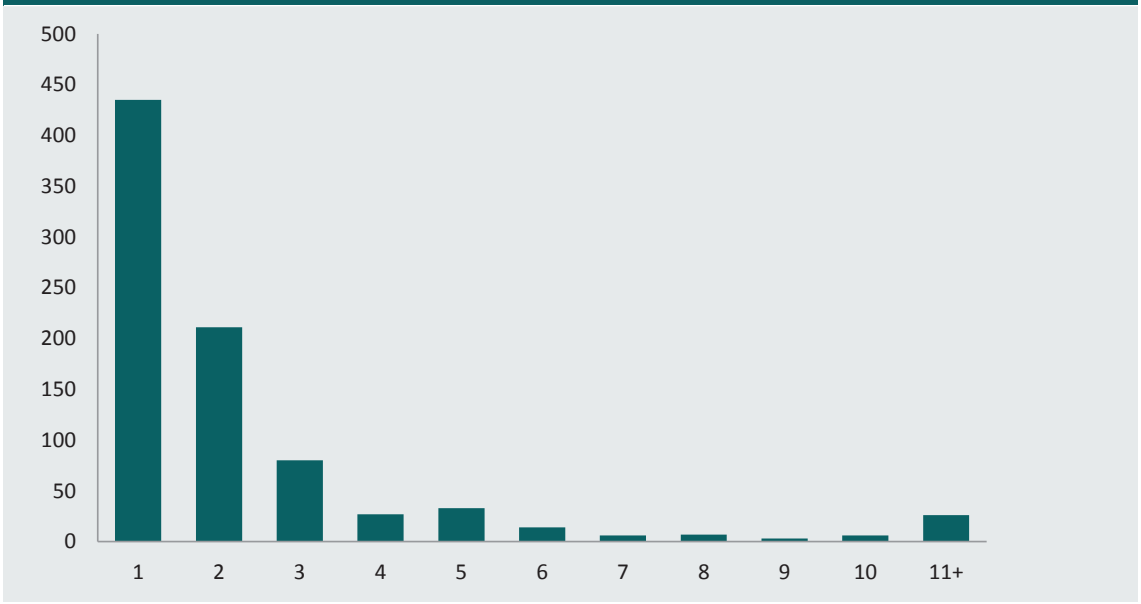
Figure 6: Percentage of respondents experiencing identity misuse in past 12 months, 2013, 2014 and 2016 (weighted data)



Source: Identity Crime Survey 2013, 2014 and 2016 [AIC data file]; https://www.medcalc.org/calc/comparison_of_proportions.php

Respondents who had experienced misuse of their personal information within the past 12 months were asked further questions about their experience. In 2016, the number of separate occasions on which respondents believed that their personal information had been misused ranged from one to 255 (mean=3.2, SD=10.2, n=848, weighted data). As shown in Figure 7, more than half of respondents (51.4%) believed that their personal information had been misused on only a single occasion, which represents a slight decrease on the findings for 2014 (53.3%).

Figure 7: Frequency distribution of number of separate occasions on which respondents believed their personal information had been misused (n)



Source: Identity Crime Survey 2016 [AIC data file]

Prior research compared

Victimisation over lifetime

Research conducted by Veda in 2015 found 25 percent of Australians aged 18 years and over were victims of identity theft at some stage in their life (2015b); this was an increase of seven percent from Veda's 2014 survey. The present research found that 21.5 percent (n=2,144) of respondents reported misuse of personal information at some time during their life. This finding is slightly higher than the findings from previous AIC surveys, where 20.8 percent (2013) and 20.4 percent (2014) of respondents reported experiencing misuse of personal information at some point during their life.

Victimisation in the prior 12 months

The percentage of respondents who reported misuse of their personal information in the previous 12 months in 2016 (8.5%) had declined since the 2013 (9.4%) and 2014 (8.9%) surveys. Although this decline is welcome, it is relatively small. The 2016 result indicates that recent experience of misuse is still a concern. The most recent ABS *Personal Fraud Survey*—conducted in 2014–15—found that 8.5 percent of the Australian population (N=1.6 million) aged 15 years and over experienced personal fraud in the 12 months prior to the survey and that, of these, 123,300 (0.7% of all Australians) experienced identity theft (ABS 2016). In the United States, the Bureau of Justice Statistics found approximately seven percent of persons aged 16 or older were victims of identity theft in 2014, which was similar to findings in 2012 (Harrell 2015). In the United Kingdom, the National Fraud Authority's nationally representative survey of 4,213 adults aged 18 years and over found that 8.8 percent (equivalent to 4.3 million residents) of those surveyed had been a victim of identity fraud within the 12 months prior to the survey (NFA 2013). Even higher rates of identity crime were found by UK fraud protection service Cifas. In an analysis of 276,993 frauds reported to Cifas in 2014, 41.1 percent (n=113,839) involved identity fraud (Cifas 2015).

The most serious occasion of misuse of personal information in the previous 12 months

Respondents who experienced misuse of their personal information within the previous 12 months were asked further questions about the most serious occasion on which misuse had occurred during this time. This was defined as the occasion that resulted in the largest financial or other harm to the participant. The aim was to seek respondents' own best recollections or assessments of the facts and circumstances in question; however, it should be emphasised that some respondents might not have had access to enough information to answer these questions with certainty.

Type of information misused

Weighted responses for the types of personal information that were misused are provided in Table 16. Respondents could indicate more than one type of personal information that had been misused.

Table 16: Types of personal information respondents believed were misused, most serious occasion in the previous 12 months

	2013	2014		2016
	%	%	%	n
Credit/debit card information	52.3	51.8	49.8	422
Name	40.2	36.7	34.6	293
Bank account information	31.1	24.6	27.0	229
Address	24.6	24.7	22.8	193
Date of birth	22.0	21.4	22.1	188
Password	18.8	21.2	19.6	166
Online account username	18.0	14.6	13.3	113
Gender	18.9	13.7	14.3	122
Computer username	14.7	11.4	10.6	90

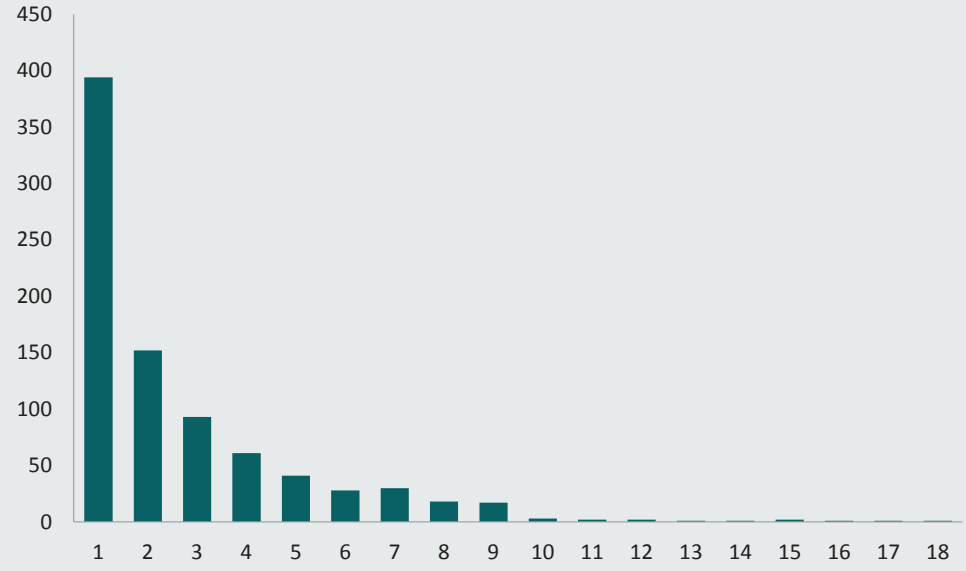
Table 16: Types of personal information respondents believed were misused, most serious occasion in the previous 12 months (continued)

	2013	2014		2016
	%	%	%	n
Place of birth	9.5	9.1	9.2	78
Driver's licence information	10.2	7.3	8.9	75
Signature	8.1	6.4	6.8	58
Personal identification number (PIN)	8.0	5.6	7.0	59
Passport information	4.9	3.8	4.1	35
Medicare information	5.3	3.5	6.0	51
Tax file number (TFN)	6.7	3.2	4.0	34
Student number	2.8	1.0	0.4	3
Biometric information (eg fingerprint)	2.2	0.2	0.6	5
Shareholder information number (HIN)	2.2	0.2	1.3	11
Other	6.8	9.8	7.4	63

Source: Identity Crime Survey 2016 [AIC data file]

Respondents indicated that between one and 18 different types of personal information had been misused on the most serious occasion in the past 12 months (weighted mean=2.7, SD=2.5, n=848). As shown in Figure 8, the distribution of this data is positively skewed, with over half (50.7%) of respondents indicating that only one type of information had been misused and three quarters of respondents noting that three or fewer types were misused.

Figure 8: Frequency distribution of number of types of personal information misused, most serious occasion in the past 12 months



Source: Identity Crime Survey 2016 [AIC data file]

Sources of information

Respondents were asked how they believed their personal information had been obtained on the most serious occasion of misuse in the previous 12 months (Table 17). Respondents could indicate more than one way in which they believed their personal information had been obtained.

For those respondents who had indicated how their personal information had been obtained (n=632), the majority (n=364, 57.6%) indicated that only one method had been used (weighted mean=1.8, SD=1.3, range 1–11).

Table 17: How personal information was obtained on the most serious occasion in the previous 12 months

	2014		2016
	%	%	n
From theft or hacking of a computer or other computerised device (eg smartphone)	20.2	20.0	169
From an online banking transaction	15.1	15.8	134
By email	12.9	18.4	156
From information placed on a website other than social media (eg online shopping)	13.5	14.3	121
From an ATM or EFTPOS transaction	6.4	6.9	58
By telephone (excluding text messages)	8.4	11.7	99
Theft of mail	7.2	3.3	28
From information lost or stolen from a business or other business or organisation (ie data breach)	10.0	9.2	78
In a face-to-face meeting (eg a job interview or a doorknock appeal)	5.3	9.6	82
From information placed on social media (eg Facebook, Linked-in)	5.6	9.2	78
Text message (SMS)	4.1	8.5	72
Theft of an identity or other personal document	1.3	2.1	18
Theft of a copy of an identity or other personal document	0.6	1.2	10
Other	7.4	6.1	52
Don't know	23.0	21.8	185

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

How information was misused

Respondents were asked how they believed their personal information had been misused on the most serious occasion in the previous 12 months (Table 18). Respondents could indicate more than one way in which they believed their personal information had been misused.

Table 18: How personal information was misused on the most serious occasion in the previous 12 months

	2014 (n=446)	2016 (n=848)	
	%	%	n
To obtain money from a bank account (excluding superannuation)	24.8	31.1	264
To purchase something	35.8	29.7	252
To apply for a loan or obtain credit	5.0	6.1	52
To file a fraudulent tax return	5.6	8.6	73
To obtain money from an investment (eg shares)	1.7	7.5	63
To apply for a job	2.7	3.9	33
To open a mobile account	3.3	4.7	40
To apply for government benefits	2.8	3.3	28
To provide false information to police	4.6	3.1	26
To obtain superannuation monies	2.7	5.1	43
To open an online account (eg Facebook, eBay)	4.1	4.9	42
To rent a property	1.8	1.8	16
Other	12.1	9.4	80
Don't know	17.0	13.6	111

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Respondents who indicated that their personal information had been misused to purchase something were asked to specify what was purchased. Forty-eight respondents indicated they did not know what had been purchased. Among the remaining respondents, who knew what was purchased, a wide range of purchases was identified, the most frequent of which were airfares and travel (n=33), electrical goods (n=22), overseas purchases (n=21), online games (n=11), groceries and liquor (n=11), and hotels and accommodation (n=8).

For those respondents who advised their personal information had been misused (n=848; includes those who did not know how their information had been misused), the weighted number of different ways in which it had been misused ranged from one to 10 (mean=1.3, SD=0.9). More than eight in 10 respondents (n=669, 81.5%) indicated that their personal information had been misused in only one way (compared with 84.9% in 2014).

Detection methods

Respondents were asked how they became aware of the misuse of their personal information on the most serious occasion in the previous 12 months (Table 19). Respondents could indicate more than one way in which they had discovered that their personal information had been misused.

Table 19: How misuse of personal information was detected on the most serious occasion in the past 12 months

	2014 (n=446)	2016 (n=848)	
	%	%	n
Received a notification from a bank or financial institution and/or credit card company	38.9	42.9	364
Noticed suspicious transactions in bank statements or accounts	33.3	30.6	259
Received a notification from police	8.4	11.9	101
Received a bill from a business or company for which they were not responsible	7.4	5.8	50
Received a notification from another company	7.2	6.4	54
Was unsuccessful in applying for credit	4.9	8.4	71
Was contacted by debt collectors	4.1	3.0	25
Received a notification from a government agency or authority other than the police	0.6	1.1	10
Other	18.2	14.9	126

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

In 2016, most respondents (n=674, 80.9%) had detected the most serious misuse of personal information over the past 12 months using just one method, which was an increase on the results for 2014 (79.2%). When the data were weighted, the mean number of methods used to detect the most serious misuse of personal information was 1.3 (SD=0.6, range 1–5).

Prior research compared

The top three types of personal information that were misused were credit or debit card information (49.8%), name (34.6%) and bank account information (27.0%). The same top three categories were identified in 2014 and 2013, suggesting that these types of personal information continue to be at greater risk than other types of personal information. Similarly, in the United States, the NCVS found that 86 percent of the most recent incidents of identity crime involved the unauthorised use of an existing account—such as a credit card or bank account—and that, among identity theft victims, the most commonly misused types of information were existing bank accounts (38% compared with 37% in 2012) or credit card accounts (42% compared with 40% in 2012; Harrell 2015). These findings are not surprising, given the large number of transactions in Australia involving debit and credit cards, with 1.9 million of these being fraudulent (ACPA 2015).

Respondents were asked how they believed their personal information had been obtained on the most serious occasion in the previous 12 months. The top five methods were: through the theft or hacking of a computer or other computerised device (20.0%); by email (18.4%, 5.5 percentage points more than the 12.9% in 2014); through an online banking transaction (15.8%); from information placed on a website other than social media (14.3%); and by telephone, excluding text messages (11.7%). These findings differed slightly from the 2014 identity crime findings, where information lost or stolen from a business or other organisation (ie data breach) was one of the top five ways that information had been obtained. The 2016 survey was the first time respondents reported that they believed one of the main ways their information had been obtained was by telephone. A high percentage (21.8%) of respondents did not know how their information had been obtained on the most serious occasion of misuse of their personal information. This finding is similar to research from the NCVS in the United States, where only 32 percent of identity theft victims knew how their personal information had been obtained (Harrell 2015).

Respondents were asked how they believed their personal information had been misused on the most serious occasion in the previous 12 months. The top three reasons provided were: to obtain money from a bank account, excluding superannuation (31.1%, up from 24.8% in 2014); to purchase something (29.7%, down from 35.8% in 2014); and to file a fraudulent tax return (8.6%, up slightly from 5.6% in 2014). In the 2014 survey, while the top three categories were the same, using the information to purchase something was the primary reason respondents believed their information had been misused. Over the course of the 2016, 2014 and 2013 AIC surveys—and the earlier survey by Di Marzio Research (2012)—people's belief that their personal information was used to obtain finance, credit or a loan decreased from 31 percent of respondents in 2012 to 8.1 percent in 2013, and to just 6.1 percent in the current study.

Respondents were asked how they became aware of the misuse of their personal information on the most serious occasion in the previous 12 months. Most respondents became aware of the misuse after being notified by a bank, financial institution and/or credit card company (42.9%, up from 38.9% in 2014), with 30.6% becoming aware of the misuse after noticing suspicious transactions in a bank statement or account (down from 33.3% in 2014). These two methods of detecting identity misuse were the same in the 2013 and 2014 identity crime surveys conducted by the AIC.

These findings were also similar to research carried out in the United States by the NCVS which found 45 percent of respondents discovered the incident of identity theft via a financial institution contacting them. This increased to 48 percent if the respondent was a victim who experienced unauthorised use of an existing account, and decreased to 15 percent if their personal information was misused to open a new account. Victims of identity theft where the information was used to open new accounts were most likely to discover the incident when a non-financial institution contacted them (21%), or when they had problems with loans, government benefits, or taxes (16%; Harrell 2015). These findings were slightly higher than the present study, where only 8.4 percent of respondents detected the identity crime when they were unsuccessful in applying for credit, although this was an increase from 2014 findings where only 4.9 percent of respondents detected the misuse that way.

Financial and other impacts

Out-of-pocket losses

Respondents who had experienced misuse of their personal information during the previous 12 months were asked how much they were left out of pocket as a result, excluding any money that they were able to recover from banks and any costs associated with repairing what had occurred. Summary statistics are shown in Table 20.

Table 20: Summary statistics for financial losses over 12 months

	2014	2016	2014	2016
	Out-of-pocket losses ($)	Out-of-pocket losses ($)	Recovered ($)	Recovered ($)
Number of respondents	240	488	250	550
Minimum	1	1	1	1
Maximum	200,000	500,000	2,000,000	4,500,000
Mean	3,572	3,696	15,317	14,026
Median	300	300	350	400
Standard deviation	19,554	28,680	167,916	215,586
25% quartile	28	100	120	100
75% quartile	1,000	1,000	998	1,022
Total	858,599	1,802,893	3,831,440	7,725,761

Source: Identity Crime Survey 2016 [AIC data file]

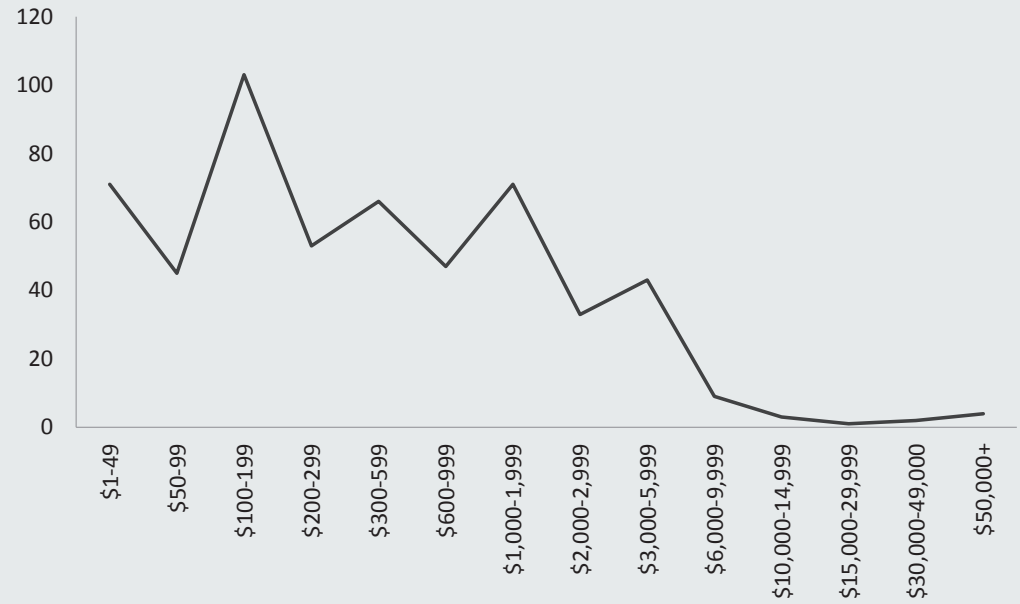
In 2016, 488 respondents indicated that they had suffered a financial loss ranging between $1 and $500,000. The median loss was $300, and total losses amounted to $1,802,893. In 2014, the median loss was also $300, but total losses were lower ($858,599) owing to the smaller sample size. As in previous years, the distribution of losses in 2016 was positively skewed, with the majority of respondents experiencing losses of less than $600. The distribution of the out-of-pocket losses suffered by respondents for 2014 and 2016 is shown in Figure 9, as a percentage of the number of respondents for each category of dollar losses.

Figure 9: Frequency distribution of financial losses in 2014 and 2016 (%)

Source: Identity Crime Survey 2016 [AIC data file]

Respondents who had experienced misuse of their personal information in the previous 12 months but had been reimbursed by banks or other organisations, or recovered their losses in other ways, recovered between $1 and $4.5m. When the data were weighted, the mean amount reimbursed or recovered was $14,026, and the median amount reimbursed or recovered was $400. The total amount reimbursed or recovered was $7,725,761—double the amount in 2014 ($3,831,440). This difference in the amounts reimbursed or recovered in 2014 and 2016 is substantially due to two large amounts which were recovered of $4.5m and $2,345,678. Given that the third-highest amount was $480,000, these large amounts were unusual. Figure 10 presents the distribution of reimbursed or recovered amounts for 2016. As noted above, amounts recovered in any given year do not necessarily correspond with amounts lost during that same year as some losses may not be recovered until sometime in the future. It is therefore not possible to say what percentage of losses has been recovered in any given year.

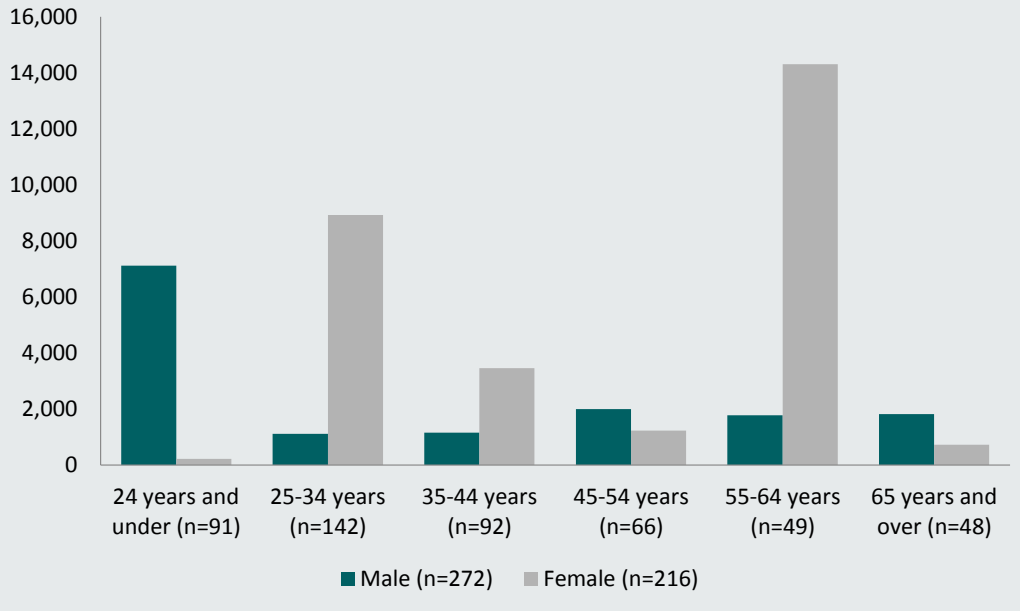
Figure 10: Frequency distribution of funds reimbursed or recovered in the preceding 12 months (n)



Source: Identity Crime Survey 2016 [AIC data file]

Figure 11 shows the mean loss by age and gender for those who reported a financial loss in 2016 (n=488). As the numbers within each category are relatively low, the average financial loss reported may be affected by outliers in the form of the high values that were reported by a few respondents (see Figure 6). Later in the report, further analyses examine the relationship between age, gender and other demographics and financial loss.

Figure 11: Mean financial loss by age and gender ($)



Source: Identity Crime Survey 2016 [AIC data file]

Other consequences of victimisation

Respondents were asked what other negative consequences they had experienced as a result of having their personal information misused over the previous 12 months. No causal connection between misuse of personal information and the specified consequences was suggested, and respondents were asked to make their own judgement about whether the results occurred 'as a result' of the misuse of their personal information or not. Respondents were able to select multiple responses. When the data were weighted, over half of the respondents (n=472, 55.9%) reported not having experienced any negative consequences following the misuse of their personal information. Weighted responses for the other consequences that were experienced are provided in Table 21.

Table 21: Consequences experienced as the result of personal information being misused in the previous 12 months

	2014 (n=446)	2016 (n=848)	
	%	%	n
I was refused credit	14.9	16.2	137
I experienced mental or emotional distress requiring counselling or other treatment	11.9	9.8	83
I was wrongly accused of a crime	5.2	6.6	56
I experienced physical health problems requiring medical treatment by a doctor	6.7	3.0	25
I had to commence legal action to clear debts and/or to clear my name	5.5	4.3	37
I experienced financial difficulties resulting in the repossession of a house, land, motor vehicle or other items	4.8	5.2	44
I experienced other reputational damage	2.6	3.4	29
I was refused government benefits	5.2	5.3	45
I was refused other services	2.7	1.4	12
I experienced other consequences not mentioned above	NA	8.6	73
I did not experience any consequences as a result of the misuse of my personal information	NA	55.9	472

Note: NA indicates not categories in 2014 survey
Source: Identity Crime Survey 2016 [AIC data file]

Respondents who had been refused other services as a result of their personal information being misused were asked to specify the type of service they had been refused. These included the ability to withdraw funds from ATM accounts (n=4), accessing email accounts (n=3), being able to renew a passport (n=1) and purchasing flights and accommodation (n=1). Responses provided in relation to other reputational damage that had been experienced as a result of misuse of personal information included:

- 'called a liar';
- 'job loss';
- 'rumours spread';

- 'work reputation tarnished'; and
- 'my reputation was dragged through the mud'.

In relation to other consequences they had experienced, responses included:

- 'my bank account was frozen temporarily';
- 'billed for telephone calls by provider';
- 'quit job';
- 'I couldn't do my shopping that day';
- 'I had to cancel my Visa card while overseas'; and
- 'I had to replace my credit card during that time, I had payments that were meant to be made but couldn't until I had received it'.

Most serious occasion of misuse of personal information

Out-of-pocket losses

Respondents were asked how much they were left out-of-pocket due to the misuse of personal information for the most serious occasion in the past 12 months (excluding any money that they were able to recover from banks and any costs associated with repairing what occurred). Summary statistics are shown in Table 22.

Table 22: Summary statistics for financial losses on the most serious occasion

	2014	2016	2014	2016
	Out-of-pocket losses ($)	Out-of-pocket losses ($)	Recovered ($)	Recovered ($)
Number of respondents	224	460	244	525
Minimum	1	1	1	1
Maximum	200,000	654,646	60,000	480,000
Mean	3,687	12,466	1,318	3,067
Median	200	199	350	340
Standard deviation	20,181	82,856	4,505	25,552
25% quartile	50	77	100	100
75% quartile	750	1483	1,000	1,200
Total	824,800	5,726,706	321,653	1,610,730

Source: Identity Crime Survey 2016 [AIC data file]

In 2016, 388 respondents (45.8%) experienced no financial loss (compared with 49.8% in 2014). The remaining 460 respondents experienced losses ranging from $1 to $654,646. When data were weighted, the median financial loss was $199. As shown in Figure 12, the distribution of losses was positively skewed, with more than three-quarters (77%) of respondents experiencing losses of $1,000 or less. In 2016, total financial losses due to the most serious occasion of misuse of personal information amounted to $1,610,730.

Figure 12: Frequency distribution of financial losses experienced on the most serious occasion in the preceding 12 months (n)

Source: Identity Crime Survey 2016 [AIC data file]

Funds recovered

With respect to the most serious occasion of misuse of personal information, amounts recovered by the 525 respondents—who had been reimbursed by banks and other organisations or recovered their losses in other ways—ranged between $1 and $480,000. When weighted, the median amount recovered was $340. Most respondents received reimbursement or recovery of small amounts, with large amounts received by only a few (see Figure 13). The total amount recovered was $1,610,730. The remaining 323 respondents did not receive any reimbursement or recover anything from the most serious occasion of misuse in the previous 12 months.

Figure 13: Frequency distribution of funds reimbursed or recovered on the most serious occasion in the preceding 12 months (n)

Source: Identity Crime Survey 2016 [AIC data file]

Prior research compared

Respondents who had experienced misuse of their personal information in the 12 months prior to the survey were asked how much they were left out-of-pocket as a result of all experiences of misuse of personal information within that 12-month period. Out-of-pocket-losses were defined as money paid out, excluding any money that respondents had been able to recover from banks and other organisations and any costs associated with repairing what had occurred.

In 2016, 460 respondents experienced out-of-pocket losses ranging from $1 to $500,000 with a median loss of $300. Total losses amounted to $1,802,893. In 2014, median losses were the same at $300, with losses ranging from $1 to $200,000. The distribution of losses was positively skewed with the majority of respondents experiencing losses in the lower range. This is consistent with the findings of previous AIC identity crime surveys.

In addition to the out-of-pocket losses, banks and other organisations reimbursed respondents for other financial losses they had suffered, resulting in an additional loss to those banks and other organisations. In 2016, the mean amount reimbursed or recovered was $14,026 and the median amount reimbursed or recovered was $400 (SD=$215,586, n=550). In 2016, the single largest amount recovered was $4.5m, while in 2014 the largest recovery was $4.0m.

Finally, some respondents experienced other consequences. The most commonly experienced of these were: being refused credit (16.2%, up from 14.9% in 2014); experiencing mental or emotional stress requiring counselling or other treatment (9.8%, down from 11.9% in 2014); and being wrongly accused of a crime (6.6%, up from 5.2% in 2014). In 2016, some victims were concerned about reputational damage, and damage to their character experienced as a consequence. One respondent said: 'I was called a liar.' Though there are some small variations, the findings largely reflect those of the previous two AIC surveys.

These findings of financial and other impacts reflect other Australian data on this issue. The ABS found that one in 10 people (9%) who experienced card fraud indicated they had lost money even after having received reimbursement (ABS 2016a). Two-thirds of Australians (66%, n=730,500) who experienced card fraud sought reimbursement. Of these, 89.7 percent received reimbursement of lost monies and 10.3 percent sought but did not receive any reimbursement (ABS 2016). In 2014–15, losses attributable to card fraud in Australia totalled over $2.1b, with total out-of-pocket losses amounting to $84.8m (ABS 2016a) after reimbursements from financial institutions.

In Australia, commercial schemes govern the operation of debit and credit payment systems, including international credit and debit card schemes (Visa, MasterCard, Amex, Diners etc.) and the domestic debit card scheme, EFTPOS. Each scheme administers rules and standards for participation. According to the Australian Payments Clearing Association, frauds perpetrated in Australia (using credit, debit and charge cards) and overseas (on Australian-issued cards) amounted to $383.6m (APCA 2015). While not all of this amount would fall within the definition of out-of-pocket losses arising from misuse of personal information (within the terms of the present research), there was an increase in 2105 in losses associated with card-not-present fraud—from $256.5m in 2013–14 to $322.7m in 2014–15—and the vast bulk of this kind of fraud involves misuse of personal information (APCA 2015).

The UK National Fraud Authority (NFA 2013) estimated that identity fraud cost UK adults £3.3b during 2012 (equivalent at that time to A$5.95b). Those who actually lost money (2.7 million individuals) lost an average of £1,203 each (equivalent at that time to A$2,169). Financial Fraud Action UK, which coordinates fraud protection in the financial services sector, found the cost of card-not-present fraud rose in the UK from £331.5m in 2014 to £398.2m in 2015 (Financial Fraud Action UK 2016).

In the United States, identity theft victims reported a total of US$15.4b in direct and indirect losses attributed to all incidents of identity theft experienced in 2014—a decrease of 33.9 percent when compared to total losses experienced in 2012 (US$24.7b). In 2014, the US *National Crime Victimization Survey* (NCVS) found that 65 percent (17.6 million) of victims reported a direct and indirect financial loss as a result of the most recent incident of identity crime. The average amount lost as a result of identity crime was US$1,343 with a median loss of US$300—similar to the 2012 NCVS findings (Harrell 2015). The NCVS also found 14 percent of identity theft victims experienced out-of-pocket losses of $1 or more. This is similar to findings in the current AIC research. Out-of-pocket losses were skewed toward smaller losses, with half of the US respondents suffering losses of less than US$100 (Harrell 2015).

The US survey found that around 36 percent of identity theft victims reported moderate or severe emotional distress as a result of the most recent incident of identity theft, although the level of emotional distress varied by type of identity theft. Twenty-one percent of victims of personal information fraud reported experiencing severe emotional distress, compared to just five percent of victims of credit card identity theft. Thirty-six percent of respondents who had experienced multiple types of identity theft described the experience as severely distressing (Harrell 2015). Comparing these results with the findings of the 2016 AIC survey, the median losses are similar to those documented in the United States study; however, the percentage of respondents experiencing higher levels of emotional distress was higher in the US than it was in Australia.

The most recent estimate of the total economic impact of identity crime in Australia for 2014–15—undertaken by the Attorney-General's Department as part of the National Identity Security Strategy— was approximately $2.6b (AGD 2016). This figure was higher than the 2013–14 estimate of $2.4b (AGD 2015). The 2016 estimate comprises:

- the costs of preventing and responding to identity crime (approximately $388m);
- the cost of identity crime as a percentage of Commonwealth fraud ($89m);
- the cost of identity crime against individuals ($660m);
- the cost of identity crime as a percentage of serious fraud ($148.5m); and
- the cost of identity crime as a percentage of police-recorded fraud (approximately $1.3b).

The losses identified by victims in the present survey form just one element of this total impact.

Dealing with victimisation

Time burden

In addition, the 848 respondents who had experienced misuse of their personal information in the previous 12 months were asked how many hours they had spent dealing with the consequences. For example, this included the time taken to have their credit rating fixed, to have new cards issued or to have bank accounts changed. In 2016, the weighted number of hours ranged from zero to 700 (compared with a maximum of 500 hours in 2014), with a mean of 18.3 hours and a standard deviation of 60.2 hours (compared with a mean of 15.3 hours and a standard deviation of 42.4 hours in 2014). More than half (53.3%) spent three hours or less dealing with the consequences of misuse of personal information (compared with 55.7% in 2014).

Respondents were also asked how much money they had spent dealing with the consequences of having their personal information misused during the previous 12 months. This included, for example, the cost of getting legal advice, lost income, telephone charges, postage or fees. A nil cost was experienced by 426 (50.2%) of respondents in 2016 (compared with 50.9% of respondents in 2014). For the remainder of respondents who had experienced misuse of personal information in the previous 12 months, the weighted estimated financial cost of dealing with the consequences ranged from $1 to $150,000 (mean=$350.23, SD=$4,548.86) compared with a range of $1 to $100,000 in 2014 (mean=$1,358.77, SD=$9,104.01). In 2016, almost half (48.1%) of respondents spent $32 or less dealing with the consequences of having their personal information misused over the previous 12 months (compared with 50.2% of respondents who spent $35 or less in 2014).

Reporting misuse of personal information

Of the 848 respondents who had experienced misuse of their personal information in the previous 12 months, 121 (14.3%) did not report the misuse in any way in 2016 (compared with 10.1% in 2014). A further 431 respondents (50.8%) told a friend or family member (compared with 48.5% in 2014), while 70 (8.3%) told a government agency or a business organisation (compared with 10.6% in 2014). Finally, 226 (26.7%) told a friend or family member as well as a government agency or business organisation (compared with 31% in 2014).

Respondents were also asked to specify which government agency or business organisation they had reported to and how satisfied they were with the outcome. As shown in the weighted

responses provided in Table 23, the majority of reports resulted in a very satisfactory or satisfactory outcome. In 2016, 296 respondents reported to either a government agency or business organisation or a friend or family as well as to a government agency or business organisation. These 296 individuals reported the misuse of their personal information to a weighted average of 1.6 agencies or organisations in the previous 12 months (range=1–10, SD=1.2), which compares with an average of 1.9 agencies in 2014.

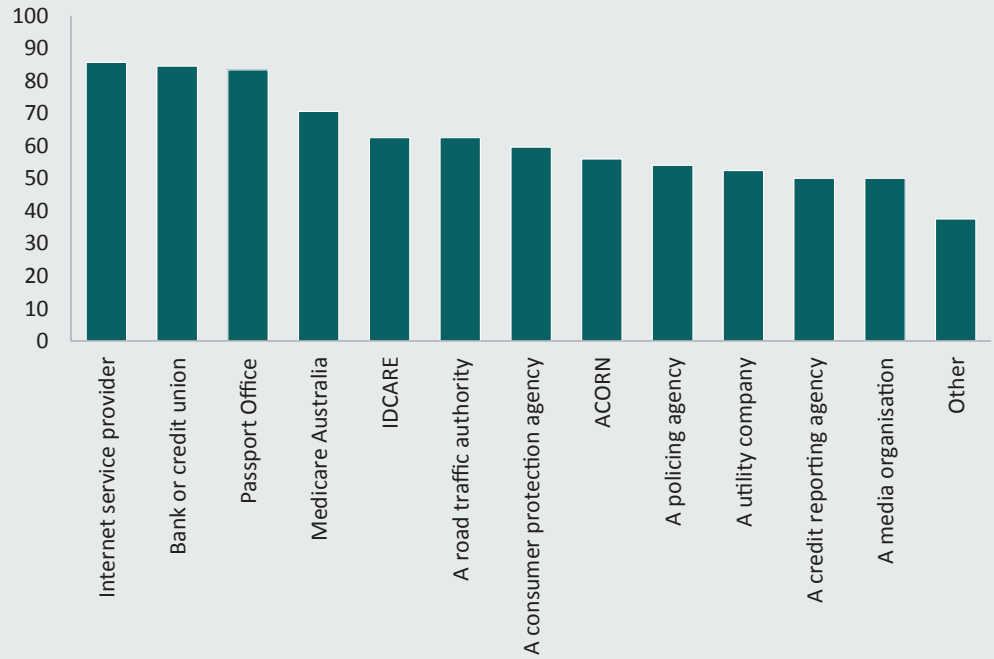
Table 23: Government agencies and business organisations reported to and satisfaction with the responses, 2016

		Level of satisfaction			
		Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
A bank or credit union, a credit/debit card company (eg Visa, MasterCard) or an e-commerce provider (eg PayPal) (n=206)	n	113	61	18	14
	%	54.9	29.6	8.7	6.8
A policing agency (n=58)	n	15	17	12	14
	%	25.2	28.8	21.0	25.0
A consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading (n=33)	n	7	13	10	3
	%	20.4	39.2	32.1	8.4
An internet service provider (n=28)	n	7	17	2	2
	%	25.0	60.7	7.1	7.1
A credit reporting agency (eg Veda, Dun & Bradstreet) (n=8)	n	2	2	3	1
	%	25.0	25.0	37.5	12.5
A utility company (eg gas, electricity, telephone, water) (n=21)	n	6	5	7	3
	%	28.6	23.8	33.3	14.3
Medicare Australia (n=17)	n	0	12	1	4
	%	0	70.6	5.9	23.5
A media organisation (n=6)	n	3	0	2	1
	%	50.0	0	33.3	16.7
Passport Office (n=12)	n	5	5	1	1
	%	41.7	41.7	8.3	8.3
A road traffic authority (n=16)	n	0	10	3	3
	%	0	62.5	18.8	18.8
Australian Cybercrime Online Reporting Network (ACORN) (n=23)	n	2	11	7	3
	%	8.7	47.8	30.1	13.0
IDCARE (n=8)	n	2	3	1	2
	%	25.0	37.5	12.5	25.0
Other (n=40)	n	12	3	14	11
	%	30.0	7.5	35.0	27.5

Source: Identity Crime Survey 2016 [AIC data file]

Figure 14 shows the percentage of respondents who were satisfied or very satisfied with the response from each agency. As shown, respondents were most satisfied with the response provided by their internet service provider (85.7%), a bank or credit union (84.5%) and the Passport Office (83.4%). Although relatively few respondents (n=23) reported to the Australian Cybercrime Online Reporting Network (ACORN), levels of satisfaction were generally good.

Figure 14: Respondents who were satisfied or very satisfied with the response, by agency (%)



Source: Identity Crime Survey 2016 [AIC data file]

Respondents who indicated that they had not reported the misuse of their personal information were asked why they had not done so. Weighted responses are provided in Table 24. Respondents could select more than one reason for not reporting.

Table 24: Reasons for not reporting misuse of personal information (n=121)

	2014	2016	
	%	%	n
I did not believe the police or any other authority would be able to do anything	32.5	33.9	41
I was too embarrassed to report it	14.0	23.3	27
I did not know how or where to report the matter	35.2	28.1	34
I did not believe it was a crime	18.0	19.0	23
Other	12.8	10.7	13

Note: Respondents could select more than one reason for not reporting the misuse of their personal information
Source: Identity Crime Survey 2016 [AIC data file]

Examples of other reasons for not reporting misuse of personal information included:

- 'I was notified';
- 'The bank contacted me'; and
- 'Everything got sorted out'.

Prior research compared

Prior research in Australia and overseas has found reporting of misuse of identity and personal information to be relatively low. In 2016, of those who experienced misuse of their personal information, 121 (14.3%) respondents did not report in any way. This is an increase compared to the percentage of respondents who did not report misuse in the earlier AIC surveys—10.1 percent in 2014; 8.9 percent in 2013. In 2016, 431 respondents (50.8%) reported the misuse of their personal information to a friend or family member—an increase from 48.5 percent in 2014—however, all other reporting rates declined between 2014 and 2016: 8.3 percent of respondents told a government agency or a business organisation (compared with 10.6% in 2014) and 26.7 percent told a friend or family member as well as a government agency or business organisation (compared with 31% in 2014).

These 2016 AIC results on reporting of misuse of information are lower than the rates of reporting recorded in the ABS *Personal Fraud Survey* (2016a), which examined reporting rates for scams, card fraud and identity theft. In the ABS survey, of all those who experienced identity theft in the five years prior to the survey, 51 percent (n=172,300) reported the most recent incident to an authority, where an authority included a business, the police and the issuer of the document (2016a). As may have been expected, even higher rates of reporting were associated with card fraud: 57 percent of individuals who had experienced an incident of card fraud (621,700 individuals) reported the incident. Of those respondents who reported the incident, 77.5 percent reported to a bank or financial institution, 13.8 percent reported to a credit card company, and 14.1 percent reported to police (ABS 2016a).

Respondents in the present survey were also asked to specify which government agency or business organisation they had reported to and how satisfied they were with the outcome. The majority of reports resulted in a very satisfactory or satisfactory outcome. Respondents were most satisfied with responses provided by their internet service provider—85.7 percent were either satisfied or very satisfied—followed by a financial institution—84.5 percent were either satisfied or very satisfied. The lowest levels of satisfaction were with reports made by respondents to credit reporting agencies and to the media.

The 2016 identity crime survey findings with respect to reporting behaviour are very similar to the findings of the NCVS in the United States in 2014 (Harrell 2015). In that survey, only eight percent of identity theft victims reported the incident to police (compared with 7% in the present survey). In the 2016 identity crime survey, respondents who had experienced misuse of personal information and indicated they had not reported the incident were asked why they had not done so. The most common reason for not reporting was a belief that nothing could be done (33.9%); however, over a quarter of respondents (28.1%) indicated they did not know how or where to report the incident. These findings are similar to previous identity crime surveys, with 10.1 percent of respondents in 2014 not reporting their most recent incident of identity crime.

The Australian Cybercrime Online Reporting Network (ACORN) was launched in November 2014 as a government response to low reporting levels. ACORN provides a mechanism for the Australian public to report a variety of cybercrimes including identity crime. Reports to ACORN are then referred to the most appropriate law enforcement agency for consideration and possible investigation (AGD 2015). The 2016 identity crime survey was therefore the first to ask about reporting to ACORN. It found that 23 (2.7%) respondents reported to ACORN, 57 percent of whom were satisfied or very satisfied with ACORN's handling of the matter.

Behavioural changes arising from misuse of personal information

Respondents were asked how their behaviour had changed as a direct result of having their personal information misused (Table 25). It is noted that respondents could select more than one way in which to report behavioural changes. Almost all (91.0%, n=772) respondents who had experienced misuse of their personal information in the previous 12 months indicated that they had changed their behaviour in some way as a direct result of their experience—a similar result to the findings in 2014 (91.6%). Interestingly, while there was a decrease in the numbers of respondents who shredded documents or changed passwords between 2014 and 2016, there has been an increase in the numbers of respondents making applications for credit reports and changing their place of residence.

Table 25: Behavioural changes resulting from the misuse of personal information

	2014	2016 (n=848)	
	%	%	n
Changed passwords	56.1	48.1	408
More careful when using or sharing personal information	38.6	34.5	293
Changed banking details	34.0	36.2	307
Review financial statements more carefully	39.6	32.7	277
Don't trust people as much	32.1	24.2	205
Use better security for computer and other computerised devices	30.4	23.5	199
Shred personal documents before disposing of them	27.5	19.0	161
Changed email address(es)	11.8	14.2	120
Changed social media account(s)	11.1	11.5	97
Lock mailbox	10.3	11.1	94
Redirect mail when away or move residence	6.7	7.3	62
Changed telephone numbers	7.8	7.1	60
Applied for a credit report	6.4	9.0	77
Use a registered post box	7.8	7.3	62

Table 25: Behavioural changes resulting from the misuse of personal information (continued)			
	2014	2016 (n=848)	
	%	%	n
Changed place of residence	2.9	5.8	49
Signed up for a commercial identity theft alert/protection service	4.6	6.5	55
Other	4.9	5.8	49
Behaviour has not changed	8.4	8.9	76

Source: Identity Crime Survey 2016 [AIC data file]

Prior research compared

Respondents were asked to indicate if, and how, their behaviour had changed as a direct result of their personal information being misused. Almost all (91%) indicated that they had changed their behaviour in some way—a result similar to the findings in 2014 (91.6%) and 2013 (94.1%). The top five behavioural changes in 2016 were the same as in 2014, although the rank order had changed. These five behavioural changes were: changing passwords (48.1% in 2016 compared with 56.1% in 2014); changing banking details (36.2% in 2016 compared with 34.0% in 2014); being more careful when using or sharing personal information (34.5% in 2016 compared with 38.6% in 2014); reviewing financial statements more carefully (32.7% in 2016 compared with 39.6% in 2014); and not trusting people as much (24.2% in 2016 compared with 32.1% 2014). In both 2016 and 2014, a small minority (8.9% in 2016 compared with 8.4% in 2014) of respondents who had experienced misuse of their personal information in the previous 12 months indicated that they did not make any behavioural changes as a result of the misuse.

In the 2015 ABS *Personal Fraud Survey,* respondents were asked in what way (if any) they believed that their behaviour had changed after experiencing identity theft: 46 percent (representing an estimated 156,500 people in Australia) advised they had changed their behaviour as a result of the identity theft incident they experienced. The most common behavioural change was becoming more careful or aware (73.7%), followed by changing credit card details (16.3%). A further 9.6 percent of respondents indicated they had become more apprehensive or withdrawn as a result of the misuse of their personal information (ABS 2016a).

In the United States, the 2014 NCVS found that a greater percentage of victims (97%) than non-victims (84%) had engaged in at least one preventive action, and that approximately 13 percent of victims who took preventive action did so in response to an experience of identity theft in the previous 12 months. Overall, the two most common preventive actions in 2014 were checking bank or credit statements (76.4%) and shredding or destroying documents containing personal information (68.6%). A higher percentage of victims than non-victims engaged in both of these preventive actions. As a response to an incident of identity crime in the past year, 26 percent of victims began checking bank or credit statements and 28 percent of victims changed passwords on their financial accounts. The least common behavioural changes as a result of identity crime were purchasing identity theft insurance or credit monitoring services (5.5%); using identity theft security programs on computers (5.2%); and purchasing identity theft protection (3.9%; Harrell 2015).

Victim certificates

Respondents were asked if they were aware that a person who has had their personal information misused can apply to a court to obtain a victim certificate to prove what occurred. They were also asked if they had done this in the past. A victim certificate is designed to assist victims to manage personal and business problems that may have been caused by identity crime.

Table 26: Respondents' awareness of victim certificates

	2013	2014		2016
	%	%	%	n
I am aware of such certificates, and have applied for one in the past	3.4	3.4	5.0	499
I am aware of such certificates, but have not applied for any	11.2	11.5	14.5	1,446
I am unaware of such certificates	85.5	85.0	80.5	8,011
Total	100.0	100.0	100.0	9,956

Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 26, the number of respondents who indicated they were aware of such certificates has increased, from less than 15 percent in 2013 and 2014 to over 19 percent in the present survey. Correspondingly, the percentage of respondents who were unaware of such certificates decreased, from 85 percent in previous years to 80 percent in 2016.

A statistically significant relationship was found between those respondents who had experienced misuse of personal information in the previous 12 months and an awareness of victim certificates (χ^2 (2, n=9,956)=404.15, p<0.001). As shown in Table 27, respondents who had their personal information misused in the previous 12 months were significantly more likely to be aware of victim certificates and/or to have applied for one in the past.

Table 27: Contingency table for respondents who experienced misuse of personal information in the previous 12 months and awareness of victim certificates

	Misuse of personal information in previous 12 months		
	Yes	No	Total
I am aware of such certificates and have applied to a court for one in the past	162 (43)*	337 (456)	499
I am aware of such certificates, but have not applied for any	145 (123)*	1,301 (1,323)	1,446
I am unaware of such certificates	541 (682)	7,470 (7,329)*	8,011
Total	848	9,108	9,956

Statistically significant at $p<0.001$, *Denotes direction of association based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Willingness to use biometric security measures to protect personal information

The 2016 survey asked respondents about their use of biometric and other security measures to keep their personal information secure. Table 28 shows the number and percentage of respondents who have used various biometric and security measures to protect their personal information in the past, and those willing to use such methods in the future. The most common security measure employed by respondents was passwords (90.8%) and the least common was iris recognition technology (1.9%). The security measure which most respondents would be willing to use in the future was fingerprint recognition (62.9%).

Table 28: Use of or willingness to use security measures to protect personal information (n=9,956)

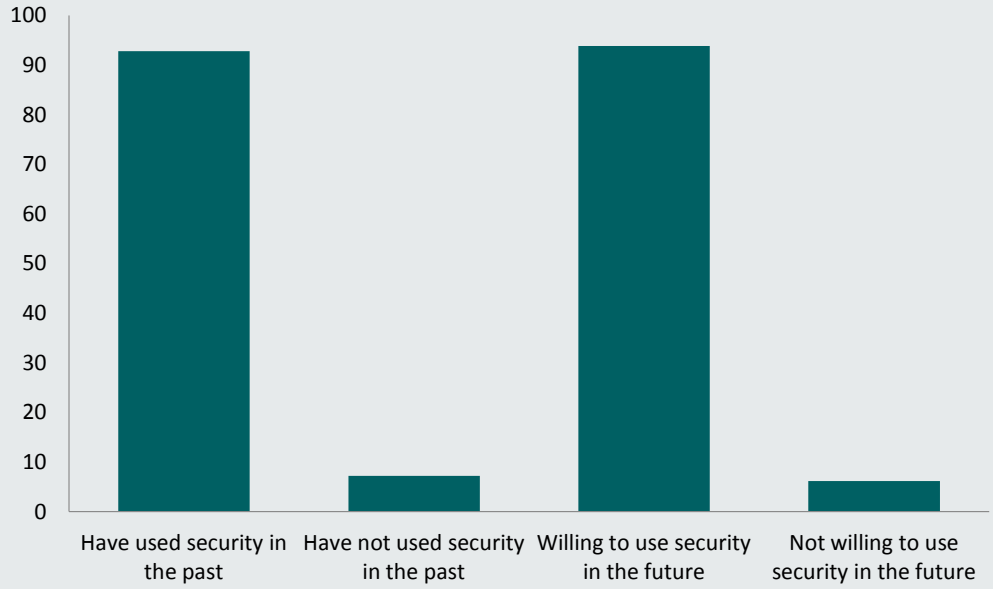
	Used in the past		Willing to use in the future	
	n	%	n	%
Passwords	9,035	90.8	7,748	22.2
Signatures	4,165	41.8	4,340	43.6
Voice recognition	1,147	11.5	3,306	33.2
Fingerprint recognition	2,655	26.7	6,266	62.9
Facial recognition	657	6.6	4,238	42.6
Iris recognition	193	1.9	3,943	39.6

Note: Data were weighted to reflect the distribution of the population by age and gender. Percentages may not total 100 and weighted figures may not total 9,956 due to rounding

Source: Identity Crime Survey 2016 [AIC data file]

Figure 15 shows the large number of respondents who had used security measures in the past to protect their personal information from misuse. Ninety-three percent of respondents had used some form of security measure in the past, and almost 94 percent of respondents advised they would be willing to use a security measure in the future.

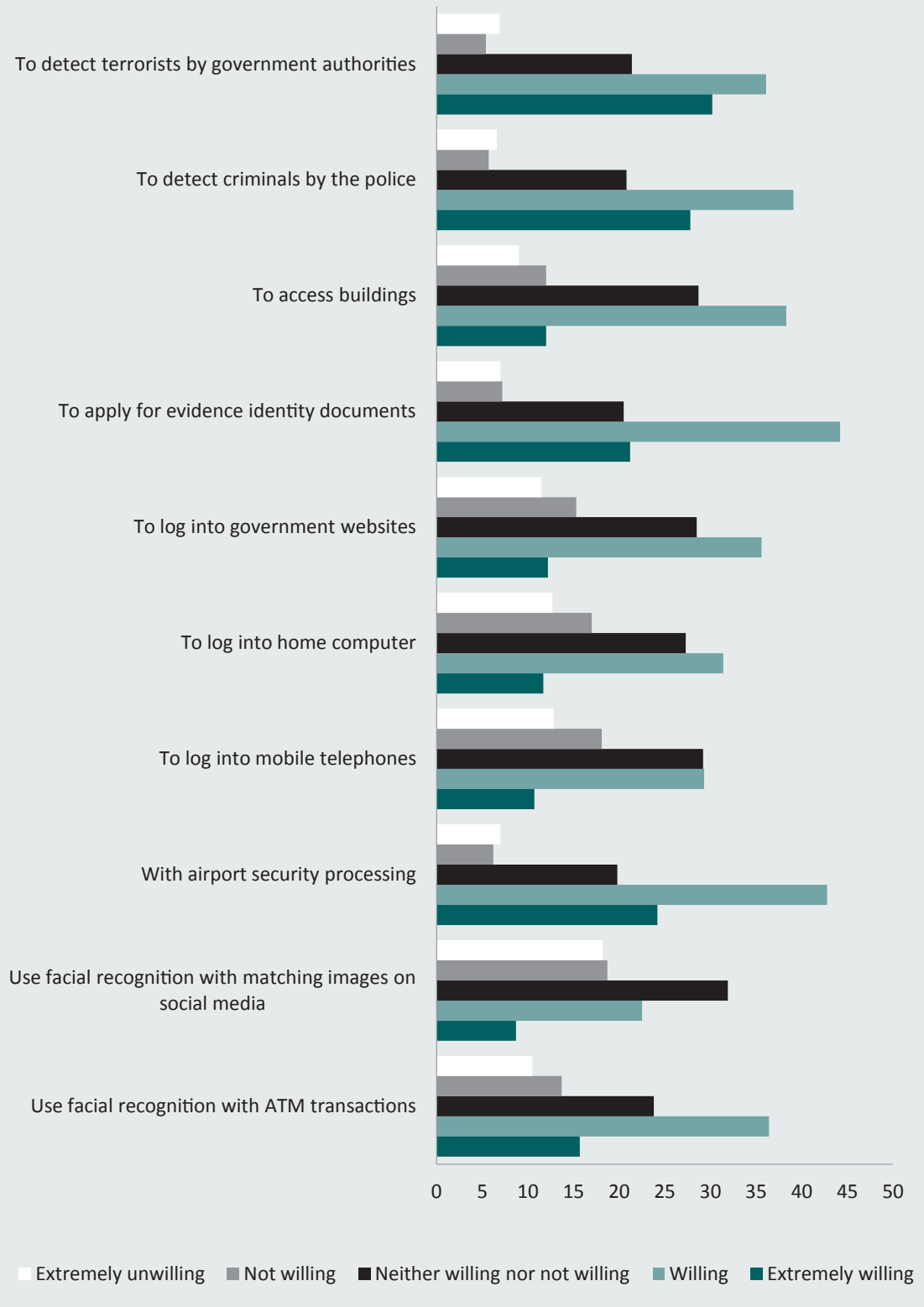
Figure 15: Respondents' use of security technology to protect personal information (%)



Source: Identity Crime Survey 2016 [AIC data file]

Respondents were asked additional questions about their willingness to use a popular security technology, facial recognition, for a number of specified purposes. Figure 16 indicates respondents' willingness to use facial recognition technology in different scenarios, with responses ranging from extremely willing through to extremely unwilling. Respondents were most likely to be extremely willing to use facial recognition technology for the detection of terrorists by government authorities (30.2%). They were least willing to use facial recognition technology for matching images on social media (18.2%). Generally, respondents were more willing to use facial recognition technology for government-authorised purposes rather than for business or private sector activities.

Figure 16: Willingness of respondents to use facial recognition technologies for specific purposes (%)



Note: Percentages may not total 100 and weighted figures may not total 9,956 due to rounding
Source: Identity Crime Survey 2016 [AIC data file]

Statistical significance of relationships between variables

The characteristics of those who experienced misuse of personal information in the previous 12 months were explored in more detail and a number of statistically significant relationships were found (below).

In 2016, however, no significant relationship was found between misuse of personal information in the previous 12 months and the following variables: place of normal residence (not dichotomised), gender, number of hours spent on a computer or computerised device, and language spoken at home. Chi-square tests—which test the assumption that the frequencies observed within each cell are obtained by chance—were used for categorical variables; that is, variables with two or more categories but no agreed way in which to order them. Using weighted data, Table 29 shows the results of chi-square tests for those variables that were found not to have a significant relationship with misuse of personal information in the previous 12 months.

Table 29: Variables that did not have a significant relationship with misuse of personal information in the previous 12 months (n=9,956)

	Degrees of freedom	χ^2	Significance
Place of residence	14	29.24	0.336
Place of residence dichotomised (capital city/outside capital city)	1	0.80	0.488
Gender	1	0.67	0.517
Language spoken at home dichotomised (English/language other than English)	1	3.43	0.225

Source: Identity Crime Survey 2016 [AIC data file]

Victimisation and Indigenous status

As shown in Table 30, a statistically significant relationship was found between experiencing misuse of personal information in the previous 12 months and Indigenous status, where Indigenous was defined as those who identified as Aboriginal, Torres Strait Islander or both Aboriginal and Torres Strait Islander (χ^2 (2, n=9,956)=31.13, p<0.01). These results indicate that those who identified as Indigenous were more likely than others to experience misuse of their personal information.

Table 30: Contingency table for the misuse of personal information in the previous 12 months and Indigenous status (expected frequencies shown in parentheses)

	Misuse of personal information in previous 12 months		
	Yes	No	Total
Identified as Indigenous	35 (15)*	144 (164)	179
Did not identify as Indigenous	799 (824)	8,872 (8,847)	9,671
Preferred not to say	14 (9)	92 (97)	106
Total	848	9,108	9,956

Statistically significant at p<0.01 *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Victimisation and income levels

Further analyses were undertaken to test the relationship between the characteristics of respondents who reported a financial loss and the amount they reported. No significant relationship was found between the amount of financial loss and gender, location, language spoken at home, Indigenous status, age or individual gross income. In 2014, a statistically significant relationship was found between respondents' age categories, gender and the amount of financial loss (although when controlling for age, gender was not statistically significant); however, these findings were not confirmed in 2016—see below.

The results of Table 31 indicate that those earning over $80,001 per annum were more likely to experience misuse of their personal information than those in other income groups, while those who would rather not say what their income was were much less likely than those in any other income group to experience misuse of their personal information (χ^2 (5, n=9,956)=53.33, p<0.001).

Table 31: Contingency table for misuse of personal information in the previous 12 months and individual gross income (expected frequencies shown in parentheses)

	Misuse of personal information in previous 12 months		
	Yes	No	Total
$0–$18,200	113 (154)	1,697 (1,657)	1,811
$18,201–$37,000	189 (180)	1,925 (1,934)	2,114
$37,001–$80,000	39 (22)	216 (232)	254
$80,001–$180,000	266 (245)*	2,610 (2,631)	2,876
$180,001 and over	175 (142)*	1,490 (1,524)	1,666
I'd rather not say	66 (105)*	1,170 (1,131)	1,236
Total	848	9,108	9,956

Statistically significant at $p<0.001$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Victimisation and financial loss

Further analyses were undertaken to test the relationship between the characteristics of respondents who reported a financial loss (n=488; weighted data) and the amount that they reported losing. The reported financial loss distribution was positively skewed—that is, the majority of data fell towards the lower end of the loss scale and the distribution was not normal. This variable was therefore normalised using a natural logarithmic transformation prior to these analyses being undertaken. The data were weighted and t-tests did not reach statistical significance when examining the mean differences between financial loss and gender; $t((426)=0.92$, $p=0.338)$, financial loss and location (dichotomised; $t(426)=0.16$, $p=0.874)$, financial loss and language (dichotomised to English or another language; $t(426)=0.83$, $p=0.629)$ or financial loss and Indigenous status (dichotomised to Indigenous or not Indigenous; $t(419)=-0.13$, $p=0.163)$.

A one-way between groups analysis of variance was conducted to explore the impact of income on the amount of financial loss. No statistically significant difference was found between the amount of financial loss and individual gross income ($F(5,420)=0.83$, $p=0.525$). Similarly, respondents' age categories were not significantly related to amount of financial loss ($F(5,420)=0.93$, $p<0.462$).

As descriptive statistics earlier in this report indicated, on average, women experienced higher out-of-pocket losses as a result of the misuse of their personal information in the previous 12 months than men (women mean= $5,879, men mean= $1,817; unweighted data; see Figure 7 for example). Bivariate analyses also indicated potential age-related differences in respondents' experiences of misuse of their personal information, and so the relationship between age, gender and amount of financial loss was explored further. However, with the transformed data there were no statistically significant differences between men and women at any of the age points ($F(6, 420)=0.60$, $p=0.730$). A series of interaction tests were examined to determine whether any specific age and gender combinations differed significantly; however, these tests also suggested no significant findings.

The number of hours spent dealing with the consequences of misuse of personal information, as well as the amount of money lost, was normalised using natural logarithmic transformation, and the relationship between those (weighted) variables and financial loss was explored using Pearson's correlation coefficients. Both these variables were found to have statistically significant positive correlations between the amount of money lost due to misuse of personal information and subsequent hours spent dealing with those consequences (r=0.16, n=414, $p<0.05$) and the financial losses and amount of money spent trying to rectify the consequences of the misuse of personal information (r=0.33, n=270, $p<0.001$). In other words, the greater the financial loss, the more hours a person spent trying to rectify the situation; and the greater the financial impact, the more money was spent trying to resolve the consequences of misuse of personal information.

Victimisation and place of residence

For those respondents who had experienced misuse of their personal information within the previous 12 months, their place of normal residence was dichotomised to compare those who resided in capital cities with those who did not. An analysis of the methods used to obtain their personal information was then undertaken. This was to test whether those who lived in more densely populated areas were more likely to have their personal information misused by tactics such as mail theft than those who lived in more sparsely populated areas. A number of methods used to obtain personal information were found to be statistically unrelated to respondents' place of normal residence, as shown in Table 32.

Table 32: Methods by which personal information had been obtained and which did not have a significant relationship with respondents' place of normal residence (dichotomised) (n=848)

	Degrees of freedom	χ^2	Significance
In a face-to-face meeting (eg a job interview, doorknock appeal)	1	3.49	0.275
By email	1	6.89	0.074
From theft of hacking of a computer or other computerised device (eg smartphone)	1	0.42	0.519
Theft of an identity document or other personal document	1	0.13	0.722
Theft of a copy of an identity document or other personal document	1	1.07	0.301
Theft of mail	1	0.73	0.392
From a business or other organisation	1	0.15	0.702
From an online banking transaction	1	2.48	0.159
From information placed on social media (eg Facebook, LinkedIn)	1	1.86	0.172
From information placed on a website other than social media	1	1.13	0.288
From an ATM transaction	1	0.63	0.427
From an EFTPOS transaction	1	0.66	0.415
From some other way not mentioned above	1	0.95	0.331

Source: Identity Crime Survey 2016 [AIC data file]

Table 33 shows the relationship between place of normal residence and information obtained by telephone for respondents who had experienced misuse of their personal information in the previous 12 months. This test found that respondents located in a capital city were significantly more likely to have their personal information obtained by telephone than those who were not in a capital city ($\chi^2(1, n=848)=9.75$, $p<0.05$).

Table 33: Contingency table for place of normal residence for respondents who experienced misuse of personal information in the previous 12 months and information obtained by telephone (expected frequencies shown in parentheses)

	Information obtained by telephone		
	Selected	Not selected	Total
Capital city	82 (68)*	502 (516)	584
Outside capital city	17 (31)	247 (233)	264
Total	99	749	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Those who resided in a capital city were significantly more likely to have had their personal information obtained by text message than those residing outside of a capital city ($\chi^2(1, n=848)=7.65$, $p<0.05$; see Table 34).

Table 34: Contingency table for place of normal residence for respondents who experienced misuse of personal information in the previous 12 months and information obtained by text message (expected frequencies shown in parentheses)

	Information obtained by text message		
	Selected	Not selected	Total
Capital city	60 (50)*	424 (534)	584
Outside capital city	12 (22)	252 (242)	264
Total	72	776	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 35, a significant relationship was found between place of normal residence for those respondents who experienced misuse of their personal information in the previous 12 months and not knowing how their personal information had been obtained ($\chi^2(1, n=848)=7.27$, $p<0.05$). This test found that those who live in capital cities were significantly more likely to know how their personal information had been obtained than those who live outside capital cities.

Table 35: Contingency table for place of normal residence of respondents who experienced misuse of personal information in the previous 12 months and did not know how their personal information was obtained (expected frequencies shown in parentheses)			
	Don't know how personal information was obtained		
	Selected	Not selected	Total
Capital city	112 (127)	472 (457)*	584
Outside capital city	73 (58)*	191 (206)	264
Total	185	663	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Respondents who had experienced misuse of their personal data in the previous 12 months were asked additional questions concerning any behavioural changes as a result of having their personal information misused. Analysis was then undertaken to determine if changes to behaviour were more likely to be made by respondents with different demographic characteristics, such as place of normal residence, age and gender. There were a number of changes in behaviour that were found to be statistically unrelated to a respondent's place of normal residence, age and gender. Gender was found not to be related to any of the ways respondents changed their behaviours as a result of their personal information being misused. The other changes that were found to be statistically unrelated were:

- changes to social media accounts;
- changed place of residence;
- 'I lock my mailbox';
- changed email address;
- redirect mail when I am away or move residence;
- applied for a copy of my credit report;
- signed up for a commercial identity theft alert/protection service; and
- 'I don't trust people as much'.

Table 36 shows the relationship between place of normal residence and respondents who reported that, as a result of their personal information being misused in the previous 12 months, they were more careful when using and sharing their personal information. Respondents located outside a capital city were significantly more likely than respondents who were in a capital city to have changed their behaviour—as a result of the misuse of their personal information—by becoming more careful when using and sharing their personal information ($\chi^2(1, n=848)=9.47$, $p<0.05$).

Table 36: Contingency table for place of normal residence of respondents who experienced misuse of personal information in the previous 12 months and those who changed their behaviour to be more careful when using and sharing personal information (expected frequencies shown in parentheses)

	Behavioural change—more careful when using personal information		
	Selected	Not selected	Total
Capital city	182 (202)*	402 (382)	584
Outside capital city	111 (91)**	153 (173)	264
Total	293	555	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Those who resided outside of a capital city were significantly more likely than respondents whose place of normal residence was in a capital city to have changed their behaviour by changing their passwords ($\chi^2(1, n=848)14.61$, $p<0.01$, see Table 37).

Table 37: Contingency table for place of normal residence of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by changing passwords (expected frequencies shown in parentheses)

	Behavioural change—changed passwords		
	Selected	Not selected	Total
Capital city	255 (281)	329 (303)	584
Outside capital city	153 (127)*	111 (137)	264
Total	408	440	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

A significant relationship was found between the place of normal residence for those respondents who had experienced misuse of their personal information in the previous 12 months and changing their behaviour to now use a registered post box. As shown in Table 38, respondents living in a capital city were significantly more likely to use a registered post box as a result of the misuse of their personal information than respondents living outside of a capital city ($\chi^2(1, n=848)=7.96$, $p<0.01$).

Table 38: Contingency table for place of normal residence of respondents who experienced misuse of personal information in the previous 12 months and those who changed their behaviour as a result of the misuse by now using a registered post box (expected frequencies shown in parentheses)

	Behavioural change—now use registered post box		
	Selected	Not selected	Total
Capital city	53 (43)*	531 (541)	584
Outside capital city	9 (19)	255 (245)	264
Total	62	786	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 39, respondents who resided outside of a capital city were significantly more likely to now shred their personal documents as a result of having their personal information misused in the previous 12 months than respondents located in capital cities ($\chi^2(1, n=848)=9.17$, $p<0.01$).

Table 39: Contingency table for place of normal residence of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by now shredding documents (expected frequencies shown in parentheses)

	Behavioural change—now shred personal documents		
	Selected	Not selected	Total
Capital city	94 (111)	490 (473)	584
Outside capital city	67 (50)*	197 (214)	264
Total	161	687	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Victimisation and age

A statistically significant relationship between misuse of personal information and age was found. As shown in Table 40, the findings indicate that those aged 25 to 34 were more likely to experience misuse of their personal information than those in other age groups ($\chi^2(5, n=9,956)=28.61$, $p<0.05$).

Table 40: Contingency table for misuse of personal information in the previous 12 months and age (expected frequencies shown in parentheses)

	Misuse of personal information in previous 12 months		
	Yes	No	Total
24 years and under	138 (139)	1,497	1,635
25–34 years	205 (154)*	1,599 (1,649)	1,803
35–44 years	152 (143)	1,533 (1,541)	1,685
45–54 years	120 (138)	1,501 (1,483)	1,621
55–64 years	96 (120)	1,309 (1,286)	1,406
65 years and over	137 (154)	1,669 (1,652)	1,806
Total	848	9,108	9,956

Statistically significant at $p<0.05$, based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

The age groups of those who had experienced misuse of their personal information in the previous 12 months were analysed with the methods used to obtain personal information. This was to test if different methods of gaining personal information were more successful with different age groups—such as theft of mail with older respondents, or having their personal information misused after placing details on social media sites with younger respondents. A number of the methods used to obtain personal information were found to be statistically unrelated to respondents' age, as shown in Table 41.

Table 41: Methods by which personal information had been obtained that did not have a significant relationship with respondents' age (n=848)			
	Degrees of freedom	χ^2	Significance
From theft or hacking of a computer or other computerised device (eg smartphone)	5	9.57	0.302
Theft of an identity or other personal document	5	17.77	0.078
Theft of mail	5	3.72	0.702
From information lost or stolen from a business	5	6.04	0.405
From an online banking transaction	5	14.04	0.063
From an ATM transaction	5	8.80	0.360
From an EFTPOS transaction	5	3.60	0.680
From information placed on a website (other than social media, eg online shopping)	5	8.94	0.318
Other	5	3.09	0.712

Source: Identity Crime Survey 2016 [AIC data file]

Table 42 shows the relationship between age of respondents who had experienced misuse of personal information in the previous 12 months and that information being obtained through a face-to-face meeting (such as a doorknock appeal or job interview). It was found that respondents aged 25 to 34 were more likely to have had their personal information obtained in this way than respondents aged 65 years and over ($\chi^2(5, n=848)=48.62$, $p<0.01$).

Table 42: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and personal information being obtained through a face-to-face meeting (expected frequencies shown in parentheses)			
	Information obtained through face-to-face meeting		
	Selected	Not selected	Total
24 years and under	19 (13)	119 (125)	138
25–34 years	40 (20)*	165 (185)	205
35–44 years	16 (15)	135 (136)	151
45–54 years	5 (12)	115 (108)	120
55–64 years	2 (9)	94 (87)	96
65 years and above	0 (13)	138 (125)*	138
Total	82	766	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Statistically significant associations were also found between respondents' age and their personal information being obtained by telephone (excluding text messages). Table 43 shows that respondents aged 25 to 34 were more likely to have had their personal information obtained by telephone than respondents aged 55 years and over ($\chi^2(5, n=848)=36.83$, $p<0.01$).

Table 43: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and information obtained by telephone (expected frequencies shown in parentheses)			
	Personal information obtained by telephone		
	Selected	Not selected	Total
24 years and under	21 (16)	117 (122)	138
25–34 years	44 (24)*	161 (181)	205
35–44 years	19 (18)	133 (134)	152
45–54 years	9 (14)	111 (106)	120
55–64 years	3 (11)	93 (85)*	96
65 years and above	3 (16)	134 (121)*	137
Total	99	749	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Table 44 shows the relationship between age and information obtained by text message for respondents who had experienced misuse of their personal information in the previous 12 months. It was found that respondents aged 25 to 34 were significantly more likely than those aged 55 years or older to have had their personal information obtained via text message ($\chi^2(5, n=848)=44.28$, $p<0.01$).

Table 44: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and information obtained by text message (expected frequencies shown in parentheses)			
	Personal information obtained by text message		
	Selected	Not selected	Total
24 years and under	9 (12)	129 (126)	138
25–34 years	38 (17)*	167 (188)	205
35–44 years	15 (13)	137 (139)	152
45–54 years	8 (10)	112 (110)	120
55–64 years	2 (8)	94 (88)*	96
65 years and above	0 (12)	137 (125)*	137
Total	72	776	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

A statistically significant relationship was found between age of respondents who experienced misuse of personal information in the previous 12 months and their information being obtained by email. Table 45 indicates that those respondents aged 25 to 34 were more likely to have had their personal information obtained by email than respondents aged 55 years and above ($\chi^2(5, n=848)=25.91$, $p<0.05$).

Table 45: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and personal information obtained by email (expected frequencies shown in parentheses)

	Personal information obtained by email		
	Selected	Not selected	Total
24 years and under	37 (25)	101 (113)	138
25–34 years	48 (38)*	157 (167)	205
35–44 years	34 (28)	118 (124)	152
45–54 years	17 (22)	103 (98)	120
55–64 years	8 (18)	88 (78)*	96
65 years and above	12 (25)	125 (112)*	137
Total	156	692	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 46, a significant relationship was found between age for those respondents who experienced misuse of their personal information in the previous 12 months and having their information obtained from details placed on social media ($\chi^2(5, n=848)=25.87$, $p<0.05$). Respondents aged 34 and under were significantly more likely than those aged 65 and over to have had their personal information obtained through information they had placed on social media sites.

Table 46: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and personal information obtained from social media (expected frequencies shown in parentheses)

	Personal information obtained from social media		
	Selected	Not selected	Total
24 years and under	23 (7)*	115 (125)	138
25–34 years	26 (19)*	178 (186)	205
35–44 years	10 (14)	142 (138)	152
45–54 years	11 (11)	109 (109)	120
55–64 years	5 (9)	91 (87)	96
65 years and above	1 (13)	136 (124)*	137
Total	78	770	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Age and behavioural change

Statistically significant relationships were found between age and the various ways in which respondents who had their personal information misused in the previous 12 months had changed their behaviour. Table 47 suggests that respondents who were aged 45 to 54 were significantly more likely than respondents aged 25 to 34 to change their bank details as a result of having their personal information misused ($\chi^2(5, n=848)=23.58$, $p<0.05$).

Table 47: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by changing banking details (expected frequencies shown in parentheses)

	Behavioural change—changed banking details		
	Selected	Not selected	Total
24 years and under	54 (50)	84 (88)	138
25–34 years	46 (74)	159 (131)*	205
35–44 years	60 (55)	92 (97)	152
45–54 years	54 (43)*	66 (77)	120
55–64 years	36 (35)	60 (61)	96
65 years and over	57 (50)	80 (87)	137
Total	307	541	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Table 48 shows that those aged 25 to 34 were significantly more likely to have changed their telephone number as a result of misuse of their personal information in the previous 12 months than respondents aged 65 and over ($\chi^2(5, n=848)=27.59$, $p<0.001$).

Table 48: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by changing their telephone number (expected frequencies shown in parentheses)

	Behavioural change—changed telephone number		
	Selected	Not selected	Total
24 years and under	0 (10)	138 (128)	138
25–34 years	27 (15)*	178 (190)	205
35–44 years	10 (11)	142 (141)	152
45–54 years	13 (8)	107 (112)	120
55–64 years	6 (7)	90 (89)	96
65 years and over	4 (10)	133 (127)*	137
Total	60	788	848

Statistically significant at $p<0.001$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

A significant relationship was also found between age of respondents and those who began using better security for their computer as a result of their personal information being misused in the previous 12 months. The test findings shown in Table 49 suggest respondents aged 65 and over were significantly more likely to upgrade their computer security systems after having their personal information misused than respondents aged 25 to 34, who were significantly less likely to do so ($\chi^2(5, n=848)=23.41$, $p<0.05$).

Table 49: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by using better security for their computer (expected frequencies shown in parentheses)

	Behavioural change—using better security for computer		
	Selected	Not selected	Total
24 years and under	19 (32)	119 (106)	138
25–34 years	38 (48)	167 (157)*	205
35–44 years	30 (36)	122 (116)	152
45–54 years	39 (28)	81 (82)	120
55–64 years	29 (23)	67 (73)	96
65 years and over	44 (32)*	93 (105)	137
Total	199	649	848

Statistically significant at $p<0.05$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Respondents aged 25 to 34 were more likely to have changed their behaviour as a result of having their personal information misused by now using a registered post box to secure their mail ($\chi^2(5, n=848)=27.21$, $p<0.01$; see Table 50).

Table 50: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by now using a registered post box (expected frequencies shown in parentheses)

	Behavioural change—using a registered post box		
	Selected	Not selected	Total
24 years and under	2 (10)	136 (128)	138
25–34 years	29 (15)*	176 (190)	205
35–44 years	17 (11)*	135 (141)	152
45–54 years	6 (9)	114 (111)	120
55–64 years	3 (7)	93 (89)	96
65 years and over	5 (10)	132 (127)	137
Total	62	786	848

Statistically significant at $p<0.01$, based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

As shown in Table 51, a significant relationship was found between the age of victims and their shredding of personal documents before disposing of them ($\chi^2(5, n=848)=31.80$, $p<0.001$). This table indicates that those who aged 65 and over were significantly more likely than other age groups to now shred their personal documents as a result of their personal information being misused, whereas respondents aged 24 and under were significantly less likely to shred their personal documents as a result of the misuse.

Table 51: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by now shredding personal documents (expected frequencies shown in parentheses)

	Behavioural change—now shredding personal documents		
	Selected	Not selected	Total
24 years and under	7 (26)	131 (112)*	138
25–34 years	36 (39)	169 (166)	205
35–44 years	30 (29)	122 (123)	152
45–54 years	24 (23)	96 (97)	120
55–64 years	20 (18)	76 (78)	96
65 years and over	44 (26)*	93 (111)	137
Total	161	687	848

Statistically significant at $p<0.001$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

A significant relationship was found between the age of victims and their more careful review of financial statements as a result of the misuse ($\chi^2(5, n=848)=36.37$, $p<0.01$). As shown in Table 52, the findings indicate respondents aged 65 and over were significantly more likely than other age groups to review their financial statements more carefully as a result of their personal information being misused. Respondents aged 34 years and under were significantly less likely to do so as a result of their personal information being misused.

Table 52: Contingency table for age of respondents who experienced misuse of personal information in the previous 12 months and behavioural change as a result of the misuse by now reviewing financial statements more carefully (expected frequencies shown in parentheses)

	Behavioural change—reviewing financial statements more carefully		
	Selected	Not selected	Total
24 years and under	24 (45)*	114 (93)	138
25–34 years	53 (67)*	152 (138)	205
35–44 years	51 (50)	101 (102)	152
45–54 years	47 (39)	73 (81)	120
55–64 years	37 (31)	59 (65)	96
65 years and over	66 (45)*	71 (92)	137
Total	278	570	848

Statistically significant at $p<0.01$, *based on analysis of adjusted residuals
Source: Identity Crime Survey 2016 [AIC data file]

Prior research compared

Prior research in Australia and overseas has generally presented only simple descriptive statistics concerning the relationship between demographic characteristics of respondents and victimisation. It was therefore not possible to compare the statistical test results obtained in the present study with a number of previous research surveys. In the present study, it was found that a number of demographic variables had no significant association with the prevalence of misuse of information in the previous 12 months. These included place of normal residence, gender, language spoken at home and the place of normal residence dichotomised (capital city/outside capital city).

However, a statistically significant relationship was found to exist between experiencing misuse of personal information in the previous 12 months and Indigenous status, where Indigenous was defined as those who identified as Aboriginal, Torres Strait Islander or both Aboriginal and Torres Strait Islander. These results indicate that those who identified as Indigenous were more likely than others to experience misuse of their personal information.

Two significant relationships were found between age group and experience of misuse of personal information in the previous 12 months. These results indicated that participants aged 25 to 34 were more likely to experience misuse of their personal information than other age groups, and that participants aged 55 to 64 were less likely to experience misuse of their personal information. There were no other statistically significant relationships found between age and the prevalence of misuse of personal information in the previous 12 months.

A significant relationship was also found between individual gross income and experience of misuse of personal information in the previous 12 months. These results suggest that those earning $80,001 and over were more likely to experience misuse of their personal information than those earning $80,000 and under. Additionally, those who preferred not to disclose their individual gross income level were statistically less likely to experience misuse of their personal information than those who did provide income details.

A survey by Di Marzio Research found statistically significant relationships at the 95 percent confidence level for victimisation (over the preceding six months or so) and gender, age categories and state of residence (Di Marzio Research 2012). Significant relationships were also found for a number of types of victimisation and perceptions of risk, although statistical test results were not reported for all variables.

A survey conducted by the OAIC (2013) found that men (14%) and women (11%) were equally likely to be victimised; victimisation rates were lower for people aged under 25 (2%) and over 65 (9%); and victimisation rates increased with household income—seven percent of those living in households earning less than $25,000 compared with 15 percent of those living in households earning more than $100,000. The OAIC survey also found that people who were least likely to be the victims of identity fraud and theft were those most concerned about the possibility of it happening to them (OAIC 2013). It also found that younger Australians were the least likely to think that they may become a victim of identity theft and fraud in the next 12 months, and that Australians living in Western Australia were most likely to have been a victim of identity theft (18%) or knew someone who was (40%).

The ABS (2016a) *Personal Fraud Survey* was a representative sample, and the data could be extrapolated to population data. Accordingly, no statistical analysis was required to determine differences between victimisation and demographic variables. The ABS (2016a) survey found people aged 25 to 34 were most likely to experience identity theft (1.0% of people in that age group) and people aged 55 and over were least likely to experience identity theft (0.4% of people in that age group). The survey also found that people with a degree, diploma, or other higher qualification were more likely (0.8%) than those without such qualifications (0.5%) to experience identity theft (ABS 2016a).

In the United States, the NCVS found similar percentages for males (6.9%) and females (7.2%) who had experienced identity theft in 2014. The rates did not change over the different types of identity theft and were similar to the prevalence rates found in the NCVS survey in 2012. After accounting for whether a person owned a credit card and bank account, prevalence rates for the fraudulent opening of a new credit card and new bank account misuse did not vary by gender. However, the misuse of an existing bank account was more prevalent among females (3.9%) than males (3.5%), and was statistically significant at the 95 percent confidence level. More people aged 65 years or older were victims of identity crime in the US in 2014 (2.6 million) than in 2012 (2.1 million). There were no other statistically significant age-related changes between the 2012 and 2014 surveys (Harrell 2015).

Among those who owned credit cards, people aged 18 to 24 (2.5%) were the least likely to experience existing credit card fraud. Among those who had an existing bank account, respondents aged 16 to 17 were the least likely to experience bank account fraud. When accounting for those who had a credit card, whites (6%) experienced higher rates of existing credit card fraud than blacks/African Americans (3%) and Hispanics (3%). The NCVS survey also found that those in the highest income category (annual household income of more than US$75,000) experienced higher rates of existing credit card account misuse among those who had a credit card (8%). Those in that income category also experienced higher rates of victimisation among those who had a bank account (4%) compared with people whose annual household income was $49,999 or less (Harrell 2015).

In the present study, age was found to have a statistically significant relationship with certain behavioural changes made by some participants after their personal information had been misused in the previous 12 months. Victims aged 25 to 34 were significantly more likely to have changed their telephone number than those in other age groups. In contrast, participants aged 65 and over were significantly less likely than those in other age groups to change their telephone number after experiencing such misuse. Participants aged 65 and over were significantly more likely than those in other age groups to use better security for their computer after experiencing misuse of their personal information. Participants between the ages of 25 and 44 were significantly more likely than other age groups to begin using a registered mail box after having their personal information misused.

Conclusions

The 2016 AIC identity crime survey sought to quantify the nature and extent of misuse of personal information—identity crime—in Australia by obtaining the views of a large sample of Australians aged 15 years and over and residing across all states and territories. The study identified the number and demographic details of respondents who indicated they had their personal information misused in the previous 12 months (n=848). The results of the 2016 study are consistent with the findings of both the inaugural identity crime survey conducted in 2013 and the previous survey in 2014.

Perceptions of identity crime

A high proportion (63.7%) of respondents believed that misuse of personal information was a very serious concern in terms of harm to the Australian economy, and a further 32 percent believed it was somewhat serious (95.7% for both categories). When asked if they thought the risk of someone misusing their personal information would change over the next 12 months, 16.4 percent believed it would increase greatly (slightly lower than 22% in 2014) and 45.3 percent believed it would increase somewhat (almost identical to the findings in 2014). Less than one percent (0.6%) believed the risk would decrease greatly and 1.2 percent believed it would decrease somewhat. These responses were similar to the perceptions of changed risk in the 2014 survey. These perceived levels of risk of misuse of personal information do not reflect the actual reported changes in victimisation between 2014 and 2016, which were minimal.

Identity crime and victimisation

Identity crime and the misuse of personal information continue to be of concern to law enforcement, government policymakers, business security analysts, academic researchers, the media, and victim support groups. This research presents the findings of the third in a series of surveys undertaken by the AIC to quantify the extent and document the nature and impact of identity crime and misuse of personal information across a large sample of Australians drawn from all states and territories. The results indicate that identity crime affects many Australians, with substantial financial and other impacts. For each of the three years surveyed, around 20 percent of respondents had experienced misuse of their personal information during their lifetime; between eight and 10 percent of respondents had experienced misuse of their personal information in the 12 months prior to the survey being conducted; and approximately five percent of respondents had experienced out-of-pocket losses.

The rates of victimisation experienced by respondents have remained constant over the three years of survey results, as have the numbers of respondents who believed that the risk of misuse of their personal information would increase over the next 12 months—approximately two-thirds of respondents believed that the risk would increase somewhat or greatly. However, victimisation rates did not change, meaning that there was a disjunction between levels of concern and actual victimisation. This could be due to increased publicity about the problem in the media, where misuse of personal information is regularly reported, including in social media reporting. The work done by government agencies to raise awareness of the problem could also lead to increased levels of concern.

Identity crime: Financial impact and harms

Looking at the harms caused by misuse of personal information, the 2016 survey found that more than half of respondents (57.5%) who had experienced misuse suffered out-of-pocket financial losses—these amounted to more than $1.8m in total. In addition, banks and other organisations reimbursed victims approximately $4m in respect of claims made during the preceding year. It should be noted that total losses vary considerably across survey years, particularly when large losses occur in individual cases. Although these losses relate only to those completing the survey in 2106, the financial impact felt by respondents was high. Comparisons could not be made between financial losses experienced in 2016 and prior years due to the use of a larger sample size in 2016.

Respondents also identified a range of other, non-pecuniary impacts including being refused credit, experiencing mental or emotional stress requiring counselling, and being wrongly accused of a crime (an impact which was felt by double the number of victims in 2016 compared with 2014). Some victims detailed how they experienced other impacts such as not being able to access bank accounts when shopping and other reputational damage. One victim said that their ‘reputation was dragged through the mud’. The experience of victimisation also resulted in more than 90 percent of respondents changing their behaviour in some way, most commonly by changing passwords and bank account details; however, some respondents reported even changing their place of residence as a result of their experience. Such impacts can have lasting consequences for personal wellbeing as well as affecting confidence in others and in the online marketplace. Ideally, victims of such crimes would be provided with training and educational tools to ensure they are not re-victimised.

Finally, it was found that the higher the financial loss, the more time and money were spent dealing with the consequences of the misuse of personal information.

Reporting and responses

There are impediments to reporting crimes of this nature. Initially, victims must realise that they have been the victim of a crime, and they must know where and how they can report such incidents. In this study, over 14 percent of respondents whose personal information had been misused did not report the misuse in any way, not even telling a family member or friend. Thirty-five percent of respondents who reported the incident to a government agency or a business organisation (including those who told both a family member/friend and an organisation), and the majority of this group were generally satisfied with the responses they received. Worryingly, 34 percent of respondents did not report the misuse of their personal information because they did not know how or where to report the matter.

While this finding was similar to the previous survey findings, it had been expected that the number of respondents not reporting identity crimes would decrease after the Australian Cybercrime Online Reporting Network (ACORN) commenced in late 2014. However, the presence of ACORN appears not to have improved reporting rates. These findings indicate an ongoing need to teach Australians that their personal information is a valuable commodity, and that when it is misused there can be financial and other implications. More also needs to be done to encourage victims to report the misuse of their personal information to the relevant authorities.

Incident and victim characteristics

The 2016 survey also explored the circumstances of the most serious occasion on which misuse had occurred during the previous year—that is, in the 12 months prior to the survey collection period. It was found that the type of personal information misused most frequently was credit or debit card information, as was the case in 2014 and 2013. However, the results concerning the manner of obtaining that personal information differed from the two previous surveys. In the 2016 findings, the most common methods for accessing personal information were via theft or hacking of a computer or other computerised device, via email, and through an online transaction. In 2014, the most common methods were theft or hacking of a computer or other computerised device, online banking, social media, and card-based transactions.

A number of statistically significant relationships were identified in the data relating to the characteristics of victims. Those who identified as Indigenous were more likely than others to experience misuse of their personal information, as were those in the higher income categories ($80,001 and over). Those who preferred not to provide their income details and those who earned less than $18,200 were significantly less likely to experience misuse of their personal information. Unlike the findings in 2013 and 2014, the 2016 survey found there was a relationship between age and misuse of personal information, with those aged 25 to 34 significantly more likely than those in other age groups to have had their personal information misused in the previous 12 months. Respondents aged 25 to 34 were significantly more likely to have had their personal information obtained through face-to-face meetings, or by text message or telephone than other age groups. Respondents aged 65 and over were significantly less likely to have had their information obtained through the use of email than those aged 25 to 34.

Those who resided in a capital city were significantly more likely that those who lived outside a capital city to have had their personal information obtained by telephone or text message. Those respondents who lived outside of a capital city were significantly more likely not to know how their personal information was obtained. In 2016, the following victim characteristics were found not to have a significant relationship with an experience of misuse of personal information in the previous 12 months: normal place of residence (not dichotomised to capital city or outside of a capital city), gender, number of hours spent on a computer or computerised device, and language spoken at home.

As suggested in the 2014 identity crime report, further qualitative research—for example, through the use of in-depth interviews—would help in understanding some of the reasons for these associations. For example, the 2016 survey found relationships between age and misuse of personal information. Through in-depth interviews, Cross (2015) has explored the relationship between seniors and their understanding of the value of their personal and identity information. Based on the findings in the present research, it may be useful to conduct similar in-depth research to explore the value placed by younger Australians on their personal information.

This report is the third in a series of AIC identity crime surveys undertaken using large samples of the Australian public. Over the three years (2013, 2014 and 2016), some consistent findings indicate areas where educational campaigns are needed to change behaviours and attitudes. Each survey has recorded a large number of respondents who did not report the misuse of their personal information; while this may be due to a variety of reasons, overwhelmingly, the main reason given by respondents for not doing so has been not knowing where or how to report the incident. While ACORN has only recently commenced operation, its existence has not led to an improvement in reporting behaviour. The ACORN website (www.acorn.gov.au) provides information for the public on what to do if they think that they have been a victim of identity crime—through hacking of their online accounts, phishing emails, or through misuse of information they had placed on social media. Although some incidents of misuse of personal information are not within ACORN's ambit—that is, if they do not involve cybercrime—the most common method reported for obtaining respondents' personal information was the hacking or theft of a computer or computerised device, which falls within the definition of cybercrime and can therefore be reported to ACORN.

Generally, the results of the 2016 identity crime survey confirm the findings of the earlier surveys in 2013 and 2014 that misuse of personal information remains an ongoing concern for many Australians, and an enduring form of criminal activity in Australia.

References

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

AGD 2015. *Identity crime and misuse in Australia 2013–14.* Canberra: AGD

AGD 2012. National Identity Security Strategy 2012. Policy paper. Canberra: AGD

Australian Bureau of Statistics (ABS) 2016a. *Personal fraud 2014–15.* ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats%5Cabs@.nsf/0/1FF970676E24FDFECA2574740015CA71?Opendocument

ABS 2016b. *Australian demographic statistics, Sept 2015.* ABS cat. no. 3101.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

ABS 2016c. *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

ABS 2016d. *Estimated resident population, by greater capital city statistical areas, 1991 to 2015.* Canberra: ABS. http://www.abs.gov.au/websitedbs/D3310114.nsf/Home/2016%20QuickStats

ABS 2016e. *Crime victimisation, Australia, 2014–15.* ABS Cat No.4530.0, Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0

ABS 2013. *Estimates of Aboriginal and Torres Strait Islander Australians, June 2011.* ABS cat. no. 3238.0.55.001 Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3238.0.55.001Main+Features1June%202011?OpenDocument

ABS 2012. Personal fraud 2010–11. ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/3BD3727225A2C89CCA257F9A001B2907?opendocument

ABS 2008. Personal fraud 2007. ABS cat. no. 4528.0 Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/226E9A7C56865433CA2579E40012097D?opendocument

Australian Competition and Consumer Commission (ACCC) 2014. *Targeting scams: Report of the ACCC on scam activity 2013*. Canberra: ACCC

Australian Crime Commission (ACC) 2015. *The costs of serious and organised crime in Australia 2013–14.* Canberra: ACC. https://www.acic.gov.au/publications/intelligence-products/costs-serious-and-organised-crime-australia

Australian Payments Clearing Association (APCA) 2016. *Australian payments fraud: Details and data 2016*. APCA: Sydney. www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf

Cifas 2015. *Fraudscape: UK fraud trends*. London: Cifas. https://www.cifas.org.uk/fraudscape_latest

Cross C 2015. 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. *Security Journal* 1–15 online publication

Cuganesan S & Lacey D 2003. *Identity fraud in Australia: An evaluation of its nature, cost and extent*. Sydney: SIRCA

Di Marzio Research 2012. *Identity theft concerns and experiences.* Melbourne: Di Marzio Research

Di Marzio Research 2011. *Identity theft concerns and experiences*. Melbourne: Di Marzio Research

Financial Fraud Action UK 2016. *Fraud the facts 2015: The definitive overview of payment industry fraud.* London: Financial Action UK. https://www.financialfraudaction.org.uk/publications/

Harrell E 2015. *Victims of identity theft, 2014*. Washington, DC: Bureau of Justice Statistics, United States Department of Justice. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408

Harrell E & Langton L 2013. *Victims of identity theft, 2012*. Washington, DC: Bureau of Justice Statistics, United States Department of Justice. http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821

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

Roberts LD, Indermaur D & Spiranovic C 2013. Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, 20(3): 315–328

Office of the Australian Information Commissioner (OAIC) 2013. *Community attitudes to privacy survey, research report 2013*. Canberra: OAIC. http://www.oaic.gov.au/ privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013#_ Toc368300726

Office for National Statistics (ONS) 2016. *Overview of fraud statistics: year ending Mar 2016*. Crime Statistics for England and Wales. London: ONS. http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

Smith RG 2011. International identity crime, in Smith CJ, Zhang SX & Barberet R (eds), *Routledge handbook of criminology: An international perspective*. New York: Taylor & Francis: 142–152

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 paper no. 130. Canberra: Australian Institute of Criminology (AIC)

Smith RG & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey*. Research and public policy series paper no. 128. Canberra: AIC

Smith RG, Jorna P, Sweeney J & Fuller G 2014. *Counting the costs of crime in Australia: A 2011 estimate*. Research and public policy series paper no. 129. Canberra: AIC

Social Research Centre 2016. *Online panels benchmarking study (technical report)*. Melbourne: The Social Research Centre. https://www.ada.edu.au/ada/01329

Symantec 2016. *Internet security threat report*, April 2016. California: Symantec Corporation World Headquarters. http://www.symantec.com/threatreport/

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 crime*. Vienna: United Nations

United Nations Office on Drugs and Crime 2011. *Handbook on identity-related crime.* Vienna: United Nations. http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

Veda 2015a. *Identity theft in Australia: April 2015*. Sydney: Veda Group. http://www.identitywatch.com.au/security-centre/identity-theft-hits-772000-australian-victims-past-year

Veda 2015b. *Identity theft in Australia: The current problem*. Omnibus survey by The Leading Edge. Sydney: Veda Group

Verizon 2016. *2016 Data breach investigation report*. New York: Verizon Enterprise LLC http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Wang S-Y K & Huang W 2011. The evolutional view of the types of identity thefts and online frauds in the era of the internet. *Internet Journal of Criminology*. www.internetjournalofcriminology.com

Appendix 1: Identity Crime and Misuse Survey 2016

About the Identity Crime Survey

This survey examines your attitudes to, and experience of, identity crime over the last 12 months. Identity crime is an important issue in Australia and your answers will provide information that can be used to prevent crimes of this kind in the future.

Identity crime 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;
- 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, or have applied for, a 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.

The results of the survey will be available from the Australian Institute of Criminology's website later in 2016, 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

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

Male

Female

Indeterminate / Intersex / Unspecified

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

Q4) What language is most often spoken at your home?

Please specify one language _____

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 was your individual gross income from all sources for the year 2014–2015 (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

Q7a) 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_____

Q7b) 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_____

Q8a) 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)

Q8b) In order to prevent misuse of personal information in the future, would you be willing to use any of the following technologies?

Technology	(Q8a) Select if you have ever used this technology in the past, in any way	(Q8b) 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		

Q8c) 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 not willing**	**Very willing**	**Extremely willing**
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.

Q8) 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

Q9) 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

Q10) 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 applied to a court for one in the past

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

No, I am unaware of such certificates

Q11) 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.

Q12a) 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

Q12b) If you answered Yes, on how many separate occasions do you believe that your personal information was misused? _____ (insert number)

Q13a) 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)

Q13b) 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? $_____

14) 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

Q15a) 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 _____

Q15b) 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) _____

Q16a) Over the last 12 months, did you tell anyone about the misuse of your personal information?

No, I told no-one

Yes, I told a friend or family member

Yes, I told a government agency or a business organisation

Q16b) 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)

Q16BB: If you made a report to a government agency or a business organisation, how satisfied are you with the outcome?

Organisation	Select if no report was made to:	Select if a 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. _____	

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).

Q19) 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)

_____

_____

Q20) 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

Other (please specify)_____ or

I don't know how my information was obtained

Q21) On this most serious occasion, in which of the following ways do you believe that your personal information was misused (select all that apply)

Misuse of personal information

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

Q22) 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) _____

Q23a) 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)

Q23b) 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? $_____

Q24) Have you participated in our Identity Crime Surveys in the past? (select one only)

Yes – in 2013

Yes – in 2014

No

Don't know

Thank you for your time in answering these questions.

Appendix 2: Note on weighting of the data

In order to quantify the nature and extent of identity crime and misuse in Australia, the AIC developed a large-scale survey to determine respondents' experiences of victimisation, in the preceding 12 months and over their lifetime, and their perceptions of the risk of identity crime or misuse occurring in the ensuing 12 months. The survey sampling frame of over 300,000 Australians aged 15 to 94 was provided by i-Link Research Solutions, a research company specialising in online research. Quotas were not employed other than receipt of 10,000 completed responses from the panel members. The final results were weighted to reflect the distribution of the Australian population in terms of age and gender (either male or female only) based on demographic statistical data from the Australian Bureau of Statistics (ABS) for gender and age at 30 June 2015, the latest ABS statistics available (ABS 2016b,d).

The number of respondents by age and gender are provided in Table 53. Because ABS demographic data at 30 June 2015 did not include indeterminate/intersex or unspecified as gender categories, respondents in the current survey who responded with this designation were removed from analysis (n=19) as it was not possible to weight the data. There was also a small number of respondents who did not specify their age who were also removed from the analysis (n=25). Accordingly, the final sample size used for weighting and analysis was 9,956.

Table 53: AIC 2016 identity crime survey: Age and gender of respondents (n)

	Age category						
	15–24	25–34	35–44	45–54	55–64	65–94	Total
Male	122	385	560	669	1,035	1,376	4,147
Female	334	906	942	1,149	1,314	1,164	5,809
Total	456	1,291	1,502	1,818	2,349	2,540	9,956

Source: Identity Crime Survey 2016 [AIC data file]

Table 54 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 in the age category 65–94; however, in the AIC survey there are twice as many people in the 65–94 age category as there are in the 24–34 age category. Since older respondents and females were over-represented in the AIC data when compared with the ABS data, it was decided that weighting the AIC data from the non-probability sample was appropriate to achieve a national distribution for age and gender.

Table 54: ABS age and sex data at 30 June 2015 N (n)

	Age category						
	15–24	25–34	35–44	45–54	55–64	65–94	Total
Male	1,604,935	1,730,968	1,598,448	1,531,893	1,324,464	1,604,575	9,395,283
Female	1,520,955	1,716,803	1,622,455	1,567,020	1,362,519	1,848,040	9,637,792
Total	3,125,890	3,447,771	3,220,903	3,098,913	2,686,983	3,452,615	19,033,075

Source: ABS (2016b,d)

The method used to calculate weights involved finding the percentage of the population for each age and gender category using ABS data, performing the same calculations on the AIC data, and then dividing the ABS data percentages by the AIC data percentages for each of the age and sex categories. Table 55 presents the weights applied to the AIC data to generate the altered distribution of age and gender ratios using the AIC survey results. These weights were then applied across the entire sample for each respondent's data.

Table 55: Weight calculations used for AIC 2016 identity crime survey participants to reflect the age/gender distribution of the Australian population

	Age category						
	15–24	25–34	35–44	45–54	55–64	65–94	Total
Male	6.8813484	2.3518209	1.4930915	1.1977833	0.6693846	0.6099827	1.1850912
Female	2.3820223	0.9912158	0.9009438	0.7133956	0.5424043	0.8304898	0.8678649
Total	3.5857894	1.3969733	1.1217179	0.8916439	0.5983535	0.7110340	1.0000000

Source: Identity Crime Survey 2016 [AIC data file]

Although the results used for analysis reflect the Australian population in terms of age and gender, these results cannot be used to estimate national population prevalence and losses. Accordingly, the data presented in this report are indicative only of the experiences of the 9,956 respondents included in the analysis.

Authors

Dr Russell G Smith is Principal Criminologist and Penny Jorna is a Research Analyst at the AIC.

AIC reports

Statistical Report

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

aic.gov.au