




Australian Government
Australian Institute of Criminology



Identity crime and misuse in Australia: Results of the 2014 online survey

Russell G Smith
Rick Brown
Shandon Harris-Hogan

AIC Reports
Research and
Public Policy Series **130**

Identity crime and misuse in Australia: Results of the 2014 online survey

Russell G Smith
Rick Brown
Shandon Harris-Hogan

AIC Reports
Research and
Public Policy Series

130

aic.gov.au



© Australian Institute of Criminology 2015

ISSN 1836-2060 (Print) 1836-2079 (Online)
ISBN 978 1 922009 79 1 (Print) 978 1 922009 80 7 (Online)

Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the *Copyright Act 1968* (Cth), no part of this publication may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Inquiries should be addressed to the publisher.

Published by the Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Tel: (02) 6260 9200 Fax: (02) 6260 9299
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, Research and Public Policy series:
Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: Research and Public Policy Series publications are peer reviewed

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

Foreword

Misuse of personal information lies at the heart of identity crime and continues to affect all sectors of the Australian community. The most recent estimate of its national economic impact is \$2.4b for 2014, of which \$2b related to direct and indirect costs, with the remaining \$350m expended in prevention and response costs by government, business and individuals (Emami & Smith 2015).

To understand the trends associated with identity crime and misuse in Australia, the Australian Institute of Criminology (AIC) was, in 2014, commissioned by the Commonwealth Attorney-General's Department to undertake a national survey of the problem for the second time. The study is one of a series of initiatives being implemented as part of the National Identity Security Strategy, Australia's national response to enhancing identity security, which seeks to prevent identity crime and misuse, contribute to national security and facilitate the benefits of the digital economy.

Respondents were asked a series of questions relating to the number of contacts, responses and victimisation incidents experienced, as well as

financial loss and other impacts, reporting and response activities, and victims' perceptions of changing levels of risk. Detailed demographic information was also collected that enabled profiles of victims to be created.

It was found that almost 9 percent of the 5,000 people surveyed experienced criminal misuse of their personal information in the previous 12 months, with almost 5 percent of those surveyed reporting actual out-of-pocket losses. Although these victimisation and loss rates are down slightly on those obtained in 2013, the scale of the problem remains of concern.

Raising awareness of the risks that individuals face, and gathering sound statistical data on the problem, is an effective way in which to address the problem of misuse of personal information. This second report shows how victimisation has changed and assists in identifying how resources could best be allocated to address the problem in the most cost-effective manner.

Dr Adam Tomison
Director and Chief Executive

Acknowledgements

The study was commissioned and funded by the Commonwealth Government Attorney-General's Department and forms part of the National Identification of Identity Crime and Misuse project that is being conducted pursuant to the National Identity Security Strategy. The survey was developed with input and advice from the members of the National Identity Crime and Misuse Framework Working Group, led by the Attorney-General's Department. Their considerable expertise relevant to the study is gratefully acknowledged.

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.

Contents

iii	Foreword	8	Characteristics of the sample
iv	Acknowledgements	12	Perceptions of misuse of personal information
viii	Acronyms and terminology	14	Experience of misuse of personal information
ix	Executive summary	17	Losses, costs and consequences resulting from the misuse of personal information
ix	Background	23	Reporting the misuse of personal information
ix	Definitions	26	Behavioural changes arising from the misuse of personal information
ix	Sample description	28	The most serious occasion of misuse of personal information in the previous 12 months
x	Perceptions of misuse of personal information	35	Characteristics of those who experienced misuse of personal information in the previous 12 months
x	Experience of misuse of personal information	40	Discussion
xi	Losses, costs and consequences resulting from the misuse of personal information	40	Perceptions of misuse of personal information
xi	Reporting the misuse of personal information	40	Experience of misuse of personal information
xii	Behavioural changes arising from the misuse of personal information	41	Losses, costs and consequences resulting from the misuse of personal information
xii	The most serious occasion of misuse of personal information in the previous 12 months	42	Reporting the misuse of personal information
xiii	Characteristics of those who experienced misuse of personal information in the previous 12 months	43	Behavioural changes resulting from the misuse of personal information
xiv	Conclusions	44	The most serious occasion of misuse of personal information in the previous 12 months
1	Introduction	45	Characteristics of those who experienced misuse of personal information in the previous 12 months
2	Prior research into identity crime and misuse	47	Conclusions
5	Method		
5	Research design		
5	Survey questions		
6	Sampling		
6	Weighting of data		
6	Analysis		
8	Results		

- 49 References
- 51 Appendix 1: Identity crime and misuse survey 2014

Figures

- 3 Figure 1 Percentage of respondents reporting identity crime-related victimisation over the preceding 12 months, by survey and year
- 4 Figure 2 Percentage of respondents reporting identity crime-related victimisation over their lifetime, by survey and year
- 11 Figure 3 Number of hours spent the previous week using a computer or computerised device
- 12 Figure 4 Number of hours spent the previous week using a computer or computerised device for work-related activities
- 17 Figure 5 Number of separate occasions participants believed their personal information had been misused
- 19 Figure 6 Distribution of financial losses experienced in the preceding 12 months
- 20 Figure 7 Distribution of funds reimbursed or recovered in the preceding 12 months
- 21 Figure 8 Average financial loss by age and gender
- 25 Figure 9 Respondents who were satisfied or very satisfied with the response, by agency
- 29 Figure 10 Number of types of personal information misused in the most serious occasion in the past 12 months
- 34 Figure 11 Distribution of financial losses experienced on the most serious occasion in the preceding 12 months
- 35 Figure 12 Distribution of funds reimbursed or recovered in the most serious occasion in the preceding 12 months

Tables

- 8 Table 1 Respondents by place of normal residence
- 9 Table 2 Respondents by gender
- 9 Table 3 Respondents by age
- 10 Table 4 Respondents by language most often spoken at home
- 10 Table 5 Respondents who identified as Aboriginal or Torres Strait Islander
- 11 Table 6 Respondents by individual gross income 2012–13
- 13 Table 7 Respondents' perceptions about the seriousness of misuse of personal information
- 13 Table 8 Respondents' perceptions about the risk of misuse of their personal information in the next 12 months
- 14 Table 9 Respondents' awareness of victim certificates
- 15 Table 10 Respondents who experienced misuse of their personal information at any time in the past by place of normal residence
- 16 Table 11 Respondents who experienced misuse of their personal information in the past 12 months by place of normal residence (unweighted data)
- 18 Table 12 Summary statistics for financial losses over 12 months
- 22 Table 13 Consequences experienced as the result of personal information being misused in the previous 12 months (n=266)
- 24 Table 14 Government agencies and business organisations reported to and satisfaction with the response
- 26 Table 15 Reasons for not reporting misuse of personal information
- 27 Table 16 Behavioural changes resulting from the misuse of personal information
- 28 Table 17 Types of personal information respondents believed were misused in the most serious occasion in the previous 12 months

- 30 Table 18 How personal information was obtained on the most serious occasion in the previous 12 months
- 31 Table 19 How personal information was misused on the most serious occasion in the previous 12 months
- 32 Table 20 How misuse of personal information was detected on the most serious occasion in the past 12 months
- 33 Table 21 Summary statistics for financial losses on the most serious occasion
- 36 Table 22 Contingency table for misuse of personal information in the previous 12 months and Indigenous status
- 36 Table 23 Contingency table for misuse of personal information in the previous 12 months and individual gross income
- 37 Table 24 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
- 38 Table 25 Contingency table for place of normal residence of participants who experienced misuse of personal information in the previous 12 months and information lost or stolen from theft of mail

Acronyms and terminology

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	holder 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
TFN	tax file number
UK	United Kingdom
US	United States

Executive summary

Background

In April 2007, the Council of Australian Governments (COAG) agreed to a *National Identity Security Strategy* to better protect the identities of Australians. 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 by all jurisdictions (AGD 2012).

The strategy also recognised the need to quantify the nature and extent of identity misuse, particularly the victimisation experiences of Australians, and 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 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 survey undertaken by the AIC, in May 2014. It updates information obtained in an earlier survey, undertaken in 2013, and provides an indication of how the current identity crime and misuse environment has changed in Australia between the two surveys. Future surveys will continue to track changes in victimisation rates and the economic impact of identity crime and misuse.

Definitions

The 2014 survey adopted the same definitions as the 2013 survey and asked respondents about the misuse of various types of *personal information*. This included 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), holder identification number (HIN), computer and/or other online usernames and passwords, student number, as well as other types of personal information.

Misuse of personal information was defined as *obtaining or using personal information without permission, to pretend to be the person in question or to carry out a business in that person's name without their permission, or other types of activities and transactions*. The use of personal information for direct marketing, even if this was done without permission, was excluded.

Sample description

In May 2014, a questionnaire comprising 23 main questions (see *Appendix 1*) was administered online to a research panel of Australians drawn from all states and territories. The sampling frame and survey hosting were undertaken by i-Link Research Solutions, a commercial provider that provided raw de-identified data for the AIC to analyse.

Data were weighted to reflect the distribution of the Australian population based on census data from the Australian Bureau of Statistics (ABS 2014). Age and gender were used as qualifying variables, so

that the results of respondents were nationally representative. The results have not, however, been weighted to indicate national estimates of prevalence and financial loss that would have been experienced had the entire Australian population aged 15 years-and-over been surveyed, as the sampling frame was insufficiently robust to permit such estimations to be undertaken.

Sampling was completed once quotas had been satisfied and a sample of 5,000 participants obtained. Of the 5,000 respondents in 2014, 446 reported misuse of their personal information in the preceding 12 months. Of these, 15.7 percent had completed the AIC's survey in September 2013. In terms of reported victimisation in the preceding 12 months, therefore, an overlap of four months was present—between May 2013 and September 2013—when those who completed both surveys could have reported the same victimisation events. It was not known, however, precisely how many victims in 2014 were the same individuals as in 2013.

Perceptions of misuse of personal information

Participants were asked, in terms of harm to the Australian economy, how serious they thought misuse of personal information was. A high proportion (68.1%) of respondents believed that misuse of personal information was *very serious* and a further 28.2 percent believed it was *somewhat serious*. These responses were very similar to the perceptions recorded in 2013.

When asked if they thought the risk of someone misusing their personal information would change over the next 12 months, 22 percent believed it would increase greatly and 45 percent believed it would increase somewhat. Only 0.8 percent believed that the risk would decrease somewhat or greatly. Again, these responses were very similar to perceptions of change recorded in 2013. Interestingly, these perceptions do not reflect the actual reported changes in victimisation, which were minimal between 2013 and 2014.

The perceived level of concern disclosed in the current survey is, however, higher than that reported in prior research by Di Marzio Research (2012), the Office of the Australian Information Commissioner (OAIC 2013) and Veda (2014, 2015), although these prior surveys were not directly comparable in terms of samples and questions asked.

Experience of misuse of personal information

The present survey found that 20.4 percent of the 5,000 respondents reported misuse of their personal information at some time during their life, with 8.9 percent reporting misuse of their personal information in the previous 12 months.

The number of separate occasions in which respondents believed that their personal information had been misused ranged from one to 200 occasions. Just more than half of the participants (53.3%) believed that their personal information had been misused on a single occasion only—almost the same as in 2013 (53.7%).

The level of lifetime victimisation (20.4%) is very similar to that reported in the AIC's 2013 survey, but lower than the lifetime prevalence rate reported in the UK National Fraud Authority's (NFA 2013) survey of identity fraud (27%). It is, however, higher than the 13 percent reported in the OAIC's (2013) survey, the 14 percent in the US *National Crime Victimization Survey* (NCVS) (Harrell & Langton 2013) and the 17 percent reported by respondents to Veda's survey (2015).

In terms of reported victimisation in the preceding 12 months, the present survey's 8.9 percent rate is less than the 9.4 percent reported in the AIC's 2013 survey, and almost the same as the UK NFA's (2013) rate of 8.8 percent. It is, however, higher than Di Marzio Research's (2012) 7 percent, Veda's (2015) 5 percent, and the ABS's (2012) 4 percent. Again, these variations are most likely due to the different sampling frames used, data collection techniques employed and the focus of questions asked of respondents.

Losses, costs and consequences resulting from the misuse of personal information

Participants who had experienced misuse of their personal information within 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. Almost half (n=206, 46.2%) were not left out-of-pocket, which was much the same as in 2013 (45.7%). The remaining 240 participants experienced losses that, when weighted, ranged from \$1 to \$200,000 (mean=\$3,572, median=\$300, SD=\$19,554). The mean and standard deviation were higher than in 2013, and the median loss of \$300 was also higher than the \$247 recorded in 2013.

It was also found that three-quarters (75%) of participants experienced losses of up to \$1,000, with few reporting the much higher amounts. Total losses amounted to \$858,599, which was 16.3 percent less than the \$1,025,250 recorded in 2013.

Participants who had been reimbursed by banks or other organisations, or recovered their losses in other ways after the misuse of their personal information in the previous 12 months, recovered between \$1 and \$2m. When the data were weighted, the mean amount reimbursed or recovered was \$15,317 and the median amount reimbursed or recovered was \$350 (SD=\$167,916, n=250). These statistics were much higher than in 2013 owing to the much higher maximum recovered, of \$2m, in one case. It was found that most participants received reimbursement or recovered small amounts, with few receiving much higher amounts. The total reimbursed or recovered during the past 12 months was \$3.8m—considerably higher than the \$607,164 recovered in 2013. The remaining 206 participants (46.2%) did not receive any reimbursement or recover any losses. Amounts recovered in the 12 months preceding the 2014 survey did not necessarily relate to the losses experienced during the same period,

making it impossible to state a percentage of losses recovered during the 12 months in question.

In addition to suffering out-of-pocket expenses, some participants experienced other consequences, the most frequent of which were being refused credit (14.9%), experiencing mental or emotional stress requiring counselling or other treatment (11.9%) and being wrongly accused of a crime (5.2%). These findings were consistent with those reported in 2013. In addition, some victims were denied access to their credit cards, bank accounts and utility accounts, and one victim said that police 'came to arrest me'.

Participants reported having spent between zero and 500 hours dealing with the consequences of having their personal information misused over the previous 12 months (mean=15.3 hours, SD=42.2 hours), with more than half (55.7%) spending three hours or less; this was much the same as in 2013. In addition, almost half (49.1%) of respondents 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 \$100,000. Half (50.2%) of those who had spent money spent \$35 or less.

Participants were also asked if they were aware that a person who has had their personal information misused could apply to a court to obtain a victim certificate to prove what had occurred and if they had done so in the past. It was found that only 171 (3.4%) respondents indicated that they were aware of victim certificates and had applied for one, while 14.9 percent of respondents were aware of the availability of certificates in 2014. These findings are almost identical to those in 2013, indicating a need to raise awareness of victim certificates.

Reporting the misuse of personal information

Of those who experienced misuse of their personal information, 10.1 percent did not report it in any way, 48.5 percent told a friend or family member, 10.6 percent told a government agency or a business organisation and 31 percent told both a friend or

family member and a government agency or business organisation. There was a small (1.2%) increase between 2013 and 2014 in those who failed to make any reports, while overall there was an increase in reporting to government and business. This could be due to increased publicity of the need to report by groups such as the Australasian Consumer Fraud Taskforce (ACFT).

Respondents were 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 satisfactory or very satisfactory outcome. Participants were most satisfied with responses provided by financial institutions (77.5% were either *satisfied* or *very satisfied*), followed by utility companies (74.3% were either *satisfied* or *very satisfied*). Levels of satisfaction with reports to Medicare Australia declined between 2013 and 2014: in 2013, 91.7% were either *satisfied* or *very satisfied*, while in 2014 this had fallen to 63.3%. The lowest levels of satisfaction were in relation to reports to consumer protection agencies.

In terms of the reasons for not reporting, 32.5 percent of respondents did not report the misuse of their personal information because they did not believe anything could be done about it and 35.2 percent did not know how or where to report the matter. This latter reason showed a large increase from the 23.1 percent recorded in 2013. In 2014, a further 18 percent did not believe it was a crime and 14 percent were too embarrassed to report it.

Behavioural changes arising from the misuse of personal information

Participants were asked to indicate if, and how, their behaviour had changed as a direct result of having their personal information misused. Almost all (91.6%) indicated that they had changed their behaviour in some way—a similar result to the previous 12 months (94.1% in 2013). Some respondents even indicated that they had changed their place of residence (n=13 in 2014).

The top-five behavioural changes made in 2014 were changing passwords (56.1%), reviewing financial statements more carefully (39.6%), being more careful when using or sharing personal information (38.6%), changing banking details (34%), and not trusting people as much (32.1%). The top-five behavioural changes were the same as in 2013, although the proportion who said they changed passwords increased by 7.6 percentage points over the 12 months. These types of behavioural changes were similar to those identified by the ABS *Personal Fraud Survey 2007* (ABS 2008), which asked comparable questions of a nationally representative sample of Australians (these questions were not included in the ABS 2010–11 survey; ABS 2012).

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

Participants 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 that time. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the participant.

The top-three types of personal information that had been misused were credit and debit card information (51.8%), name (36.7%) and bank account information (24.6%). These were the same top-three categories identified in 2013. Almost half of the respondents (44%) indicated that only one type of personal information had been misused.

Participants were asked how they believed their personal information had been obtained for the most serious occasion of identity crime in the previous 12 months. Of the 339 respondents who responded to this question, 23 percent did not know how their information had been obtained. Others reported the top-five ways as being from theft or hacking of a computer or other computerised device (20.2%), from an online banking transaction (15.1%), from

information placed on a website other than social media (such as online shopping) (13.5%), by email (12.9%), and from information lost or stolen from a business or other organisation (i.e. a data breach) (10%). The top-four sources were the same as in 2013, but information obtained from an ATM or EFTPOS transaction declined by almost 5 percentage points between 2013 and 2014.

Participants 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 were to purchase something (35.8%), to obtain money from a bank account (excluding superannuation) (24.8%), and to file a fraudulent tax return (5.6%). Although the top-two categories of misuse were the same as in 2013, the misuse of information to apply for a loan or to obtain credit declined by 3.1 percentage points between 2013 and 2014.

Participants who indicated that their personal information had been misused to purchase something were asked to specify what was purchased. The most commonly purchased items were consumer electrical goods (n=21), airfares and travel (n=16), fashion items (n=15) and for gambling (n=7), the last two of which were more prevalent in 2014 than in 2013.

Participants were asked how they became 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 (38.9%), noticing suspicious transactions in a bank statement or account (33.3%) and receiving notification from the police (8.4%). Between 2013 and 2014, there was a 6.1 percentage point reduction in individuals becoming aware of misuse after receiving from an organisation a bill for which they were not responsible.

Participants 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 they were able to recover from banks and any costs associated with repairing what occurred). Almost half of the participants (n=222, 49.8%) did not report any out-of-pocket losses. The remaining 224 participants experienced losses ranging from \$1 to \$200,000.

When these data were weighted, for those who suffered a loss, the mean financial loss was \$3,687, and the median loss was \$200 (SD=\$20,181). Three-quarters (75%) of participants experienced losses of up to \$750, with few reporting much higher amounts. The total out-of-pocket losses in the most serious occasion reported in 2014 were \$824,800. This was 34.1 percent less than the total in 2013 (\$1.25m).

Participants who had been reimbursed by banks or other organisations, or recovered their losses in other ways, for the most serious occasion recovered between \$1 and \$60,000. When weighted, the mean amount recovered was \$1,318; the median recovered was \$350 (SD=4,505, n=244). It was found that most participants received reimbursement or recovered only small amounts, with few receiving much higher amounts. The total recovered was \$321,653, which was 40.8 percent less than the \$543,514 recovered in 2013. The remaining 202 participants (45.3%) did not receive any reimbursement or recover anything relating to the most serious occasion of misuse in the previous 12 months.

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 findings of the survey for 2014 found 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 experience misuse of their personal information);
- individual gross income and misuse of personal information in the previous 12 months (those in

the lowest income category, \$18,200 and under, were less likely to experience misuse, and those earning \$37,001 and above were more likely to experience misuse);

- perceptions of the seriousness 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 perceive that risks would increase in future);
- 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 from the theft of their mail);
- age category and the amount of financial loss, with the average financial loss generally increasing with age; 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).

No significant relationships

Variables that were found in 2014 not to have a significant relationship with misuse of personal information in the previous 12 months included place of normal residence, age group, gender, the number of hours spent on a computer or computerised device and language spoken at home.

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 or individual gross income. Further analysis of the relationship between age, gender and amount of financial loss showed that gender was not statistically significant when controlling for age.

Conclusions

The results of this survey confirm prior research that misuse of personal information remained a continuing problem in Australia in 2014, with one in five survey respondents reporting misuse at some time in their lives. Of the one in 11 respondents who experienced misuse of their personal information in the past 12 months, more than half had experienced financial losses for which they were not compensated. In addition, they experienced a range of non-financial losses including loss of personal time, as well as mental and emotional consequences, sometimes requiring treatment. Victims also indicated changes in their personal and online behaviour as a result of their experiences, thus detracting from the positive benefits of online consumer activity. Some categories of victims, including Indigenous Australians and those with higher income levels, experienced significantly higher rates of victimisation, in the same way as reported in the 2013 survey.

The present survey results should assist those charged with devising relevant prevention initiatives by assisting them in determining where to direct targeted information to those most likely to be victimised and indicating the best ways in which those at risk of victimisation can protect themselves against identity crime and misuse. Over time, such initiatives may result in reduced levels of victimisation and lower financial and other consequences for Australians in the years ahead.



Introduction

In April 2007, the Council of Australian Governments (COAG) agreed to a *National Identity Security Strategy* to better protect the identities of Australians. This arose out of evidence emerging 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 by all jurisdictions (AGD 2012).

The strategy also recognised the need to quantify the nature and extent of identity misuse, particularly the victimisation experiences of Australians, and 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 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 other impact they experienced;
- their reporting and response activities;
- whether their behaviour changed in any way as a result of what happened;
- whether they believed that this type of crime would change over the next 12 months;
- how serious they thought identity crime is;
- whether they knew about, or have applied for, an identity crime victim certificate; and
- information about their age, gender, residence, income, language spoken at home, Indigenous background and computer usage.

The surveys will be replicated on an annual basis so that time-series data can be compiled to measure changes in the information gathered from year to year. This report presents the results of the latest survey, undertaken by the Australian Institute of Criminology (AIC) in May 2014. It updates information obtained in an earlier survey, undertaken by the AIC in 2013, and provides an indication of how the current identity crime and misuse environment has changed between the two surveys.

Prior research into identity crime and misuse

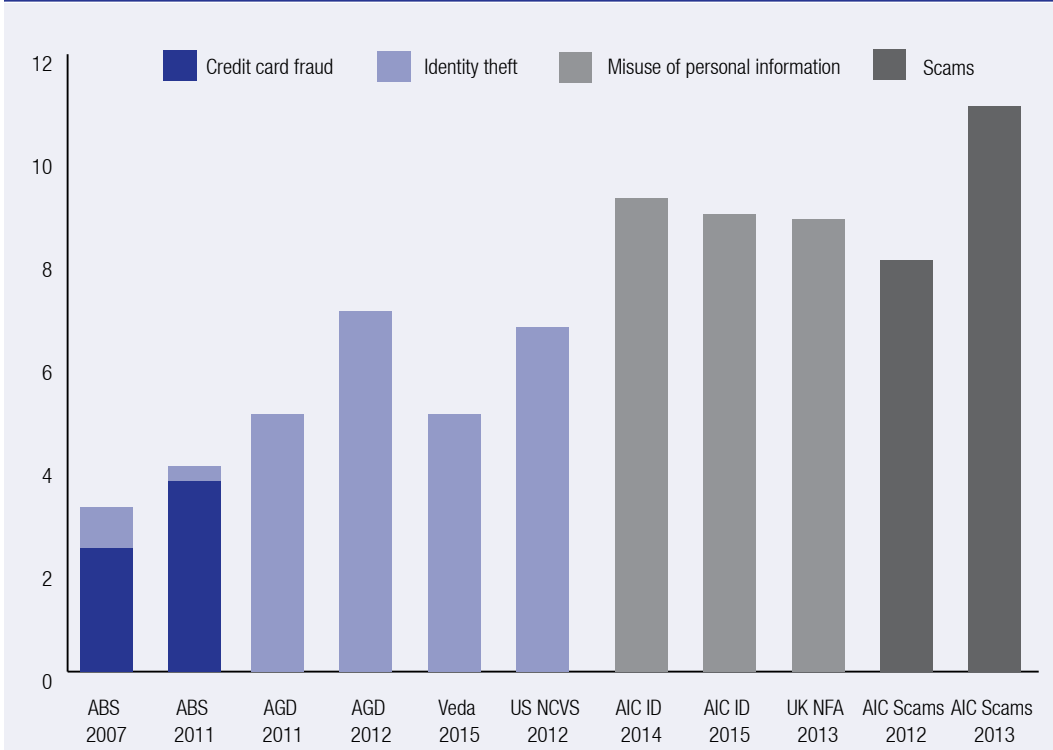
The use of stolen, fabricated or manipulated identities to commit or to enable crime has been on the policy agenda of governments and businesses in developed countries for more than two decades (Smith 2011), and interest in the nature and extent of the problem has increased with the creation of new opportunities for misuse that have followed new technological developments (Smith 2014). Sources of information on identity crime are official administrative data collected by law enforcement and regulatory agencies, as well as surveys of individuals and businesses to measure victimisation rates. Part of the problem associated with quantifying the extent and impact of identity crime is the fact that relevant information is present in a diverse range of sources, a number of which do not specifically address ‘identity crime’ as such, but which deal with other aspects such as privacy infringement, data breaches, fraud and theft.

In Australia, the Commonwealth Attorney-General’s Department (AGD) has recently collected all relevant administrative data from Commonwealth, state and territory agencies and made this available for analysis and review in an annual monitoring report prepared by the AIC (Emami & Smith 2015) and a pilot report prepared by the AGD (2014). Crime victimisation surveys have also been undertaken by a number of organisations including the Australian Bureau of Statistics (ABS), consumer protection agencies and industry consultancy firms. Results of prior victimisation surveys have been reviewed by Smith & Hutchings (2014) and Emami & Smith (2015). The scale and impact of these crimes are variable, with issues of definition, low reporting rates and inconsistent data recording practices among agencies that detect or deal with these incidents creating lack of clarity around the true prevalence and cost of the problem.

Nonetheless, it is possible to identify the general scale of the problem by examining the most recent survey evidence that has been compiled in Australia and in other countries. Of course, any comparisons need to take into account the specific details of how information was gathered including the reference periods used (the period that survey respondents were asked to consider when reporting their victimisation experiences), the precise questions asked, particularly relating to the type of conduct involved (misuse of personal information, credit card fraud, identity theft, consumer scams), and, importantly, the samples of respondents used, be they nationally representative groups, such as those used in ABS surveys, or smaller samples derived from self-selected groups of individuals who agree to participate in online research.

An indication of the 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 1. Lifetime victimisation rates from a range of surveys are shown in Figure 2. The differences relate principally to the type of conduct being examined as well as the period over which victimisation occurred. In relation to victimisation that occurred during the preceding 12 months, rates reported in surveys after 2011 vary between 4 and 9 percent for misuse of personal information and identity theft. Higher rates exist for consumer scams of all types, some of which might not involve misuse of personal information. The AIC’s consumer scam surveys have also involved self-selected online participants with generally smaller sample sizes than most of the other surveys. In relation to lifetime victimisation, rates have varied between 13 and 27 percent for misuse of personal information and identity theft.

Figure 1 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

Sources: ABS 2007 survey (ABS 2008); ABS 2010–11 survey (ABS 2012); AGD 2011 survey (Di Marzio Research 2011); AGD 2012 survey (Di Marzio Research 2012); Veda (2015); US NCVS for 2012 (Harrell & Langton 2013); AIC 2014 survey (Smith & Hutchings 2014); AIC 2015 survey (Smith, Brown & Harris-Hogan 2015); UK NFA (2013); AIC 2012 Scams survey (Jorna & Hutchings 2013); AIC 2013 Scams survey (Jorna 2015).

In relation to the economic cost of identity crime, estimates for Australia as a whole have varied from \$1.1b (with an estimation error of \$130m) for the period 2001–02, 38 percent of which was attributable to actual losses incurred by victims (\$420m) (Cuganesan & Lacey 2003), to the latest estimate of \$2.4b for the entire economic impact of identity crime and misuse in 2013–14, including prevention and response costs by government and business organisations. The direct and indirect costs of identity crime alone amounted to \$2b of this (Emami & Smith 2015).

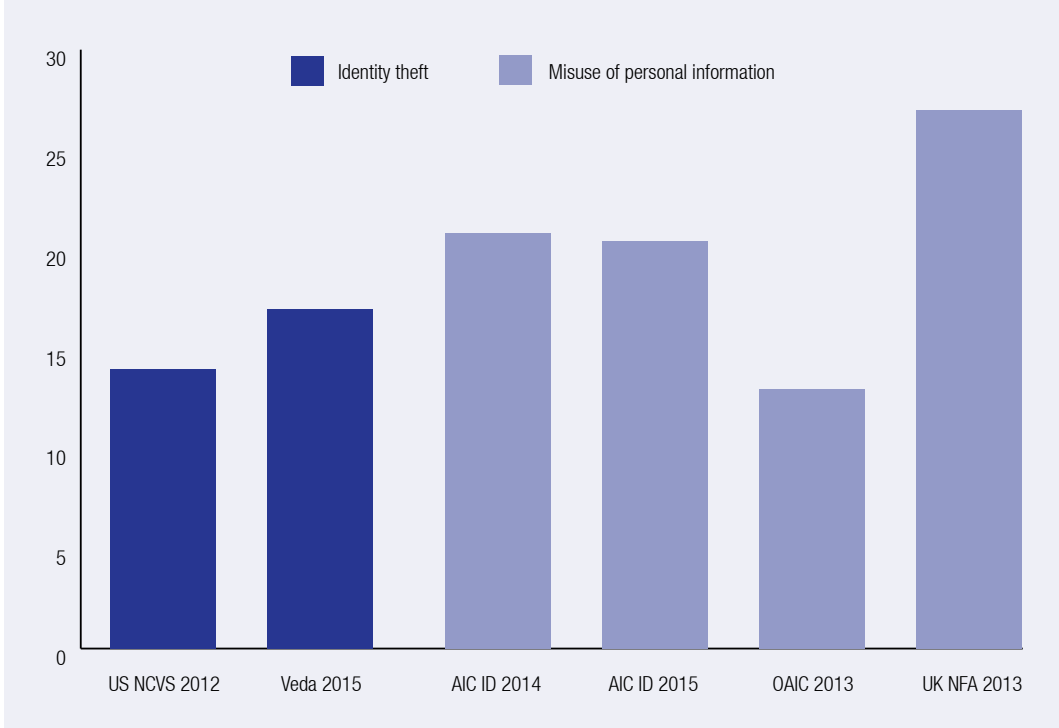
Other Australian sources have identified losses associated with consumer scams reported by victims of \$846,170 in total for 2012 (Jorna & Hutchings 2013), \$1,110,106 (with outliers removed) for 2013

(Jorna 2015), and \$89.1m in financial losses from 91,927 scam-related contacts received by the Australian Competition and Consumer Commission (ACCC) from consumers and small businesses in 2013 (ACCC 2014).

In the United Kingdom, the NFA (2013) estimated that identity fraud cost adult victims £3.3b during 2012, with an average loss of £1,203 per victim.

In the United States, the Bureau of Justice Statistics Identity Theft survey covering the 12 months prior to interviews conducted from July 2011 to June 2012 found direct and indirect losses of US\$24.7b, with a mean loss of US\$1,769 and a median loss of US\$300 (Harrell & Langton 2013).

Figure 2 Percentage of respondents reporting identity crime-related victimisation over their lifetime, by survey and year



Sources: US NCVS for 2012 (Harrell & Langton 2013); Veda (2015); AIC ID survey for 2014 (Smith & Hutchings 2014); AIC ID 2015 survey (Smith, Brown & Harris-Hogan (2015); OAIC (2013); NFA (2013).

Explanations for these different estimates in the cost of identity crime relate to the extent and representativeness of those included in the research samples, the definitions of identity crime and misuse employed, and the scope of the costs included—be they direct losses, indirect costs or more general economic impacts that include prevention and response costs. It is clear, however, that many individuals and organisations suffer substantial losses as a result of their victimisation and that there are considerable economic and intangible harms suffered by the communities affected each year.

To explore the extent of the problem in Australia over time, the AGD has commissioned the AIC to

conduct annual surveys of a large sample of Australians drawn from a national online panel. More rigorous, representative research is being undertaken by the ABS through the personal fraud questions in its *National Crime Victimisation Survey* that forms part of the *Multipurpose Household Survey*. Although ABS data will provide the best evidence of national prevalence trends for personal fraud, the smaller-scale research conducted by the AIC reported in this and other publications continues to provide timely, detailed information on the nature of identity crime experienced by a large sample of Australians who have agreed to participate in the online market research surveys that have been undertaken.



Method

Research design

This research employed a quantitative, cross-sectional survey design, examining identity crime and misuse within the sample at one point in time. This methodology replicated a similar study that was completed in 2013. The operational definition of *identity crime and misuse* 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, or other types of activities or transactions. This definition excluded the use of personal information for direct marketing, even if this was done without permission. For this research, personal information was defined as: 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, passport, PIN, TFN, HIN, computer and/or other online usernames and passwords, student number and other types of personal information.

A range of ethical issues was raised with this research design, as well as a number of limitations to the methodology. These are similar to those identified in the previous year's survey. For further

details regarding these issues, see Smith and Hutchings (2014).

Survey questions

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

- perceptions of the seriousness of misuse of personal information and 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 in the most serious occasion in the preceding 12 months;
- actual financial losses, funds recovered and other consequences of victimisation;
- awareness of the availability of court victimisation certificates;
- reporting misuse of personal information;
- behavioural changes arising from misuse of personal information; and
- demographic and other characteristics of the sample 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 study in 2013 (Smith & Hutchings 2014) to allow for direct comparisons between the two years.

The questions spanned a number of reference periods. These included participants' current circumstances (eg place of normal residence, age and income), their lifetime experiences of identity crime and misuse, as well as identity crime and misuse they had experienced in the previous 12 months. The survey was delivered over two weeks in May 2014.

The survey, which had 23 questions in total, took approximately 10 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 to an online survey panel by i-Link Research Solutions, an external provider. The sample consisted of 5,000 Australians aged 15 years and over who had internet access and who had registered with the online survey panel provider. The sampling frame and survey hosting were undertaken by i-Link Research Solutions, with the de-identified data provided to the AIC for analysis and reporting.

Potential respondents were randomly selected and invited to participate in the survey using quotas—namely, location, age and gender. Respondents were stratified across location, so that there was an oversampling in smaller states and territories, and under-sampling of the larger states compared with their representation in the Australian population aged 15 years and over. Age and gender were used as qualifying variables, so that the respondents were nationally representative according to ABS (2014) census data at 31 December 2013. Sampling was completed once the quotas had been met and a sample size of 5,000 participants had been obtained.

Participants received an incentive in exchange for completing the survey. Participants were able to select the type of reward they wished to receive from the range of incentives offered by the external

provider. Examples of the incentives offered by the provider included:

- instant member reward points (accumulated to redeem gifts—such as Caltex/Coles vouchers);
- chance to win \$50,000 prize draw quarterly;
- donate rewards to an affiliated charity; and
- monthly community member competitions/prizes and draws.

Weighting of data

Data were weighted by location to represent the spread of the population in Australia. ABS (2014) data estimating the 31 December 2013 resident population by greater capital city and by state and territory were used to develop the weighting matrix for the sample data. The process of weighting involved the application of a formula to data provided by each respondent to make each response proportionate in relation to the broader population from which the sample was derived. For example, respondents in Sydney made up 11 percent of the sample; however, this location contains 20.5 percent of the Australian population (ABS 2014). The actual weighting for each location is shown in Table 1. All results refer to weighted data, unless otherwise specifically noted.

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

Analysis

The analysis presented in this report is largely descriptive in nature, although appropriate tests for statistical significance are presented where bivariate analyses have been undertaken. The commentary with the analysis provides comparisons with the previous survey completed in 2013. It should be noted that the differences between the two surveys

have not been tested for statistical significance and it is possible that some of the differences will fall within the margins of sampling error for the two surveys, meaning the observed differences may be a function of the survey methodology, rather than true differences in the population.

In addition, the samples obtained in 2013 and 2014 are not entirely independent. Of the 5,000 respondents in 2014, 446 reported misuse of their

personal information in the preceding 12 months. Of these, 15.7 percent had completed the AIC's survey in September 2013. In terms of reported victimisation in the preceding 12 months, therefore, an overlap of four months was present, between May 2013 and September 2013, when those who completed both surveys could have reported the same victimisation events. It was not known, however, precisely how many victims in 2014 were the same individuals as in 2013.

Results

Characteristics of the sample

In total, 5,000 respondents completed the survey instrument. The data were weighted to reflect the distribution of the population across jurisdictions based on ABS (2014) census data. Table 1 shows the breakdown of respondents by place of normal residence.

Table 1 Respondents by place of normal residence

Location	Multiplier	Unweighted		Weighted	
		n	%	n	%
Sydney	1.859	551	11.0	1,026	20.5
Other New South Wales	1.909	300	6.0	574	11.5
Melbourne	1.767	530	10.6	938	18.8
Other Victoria	0.999	301	6.0	301	6.0
Brisbane	1.151	421	8.4	485	9.7
Other Queensland	1.160	451	9.0	524	10.5
Perth	0.656	650	13.0	427	8.5
Other Western Australia	0.586	200	4.0	118	2.4
Adelaide	0.429	650	13.0	280	5.6
Other South Australia	0.410	200	4.0	82	1.6
Canberra	0.258	320	6.4	83	1.7
Hobart	0.235	200	4.0	47	0.9
Other Tasmania	0.376	170	3.4	64	1.3

Table 1 Respondents by place of normal residence cont.

Location	Multiplier	Unweighted		Weighted	
		n	%	n	%
Darwin	0.706	41	0.8	29	0.6
Other NT	1.516	15	0.3	23	0.5
Total		5,000	100	5,000	100.0

Note: Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Only respondents aged 15 years and over were eligible to participate in the survey. Tables 2 and 3 show the respondents' weighted distributions by gender and age group respectively.

Table 2 Respondents by gender

Gender	n	%
Male	2,115	42.3
Female	2,878	57.6
Other	7	0.1
Total	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Table 3 Respondents by age

Age group	n	%
17 years and under	184	3.7
18–24 years	303	6.1
25–34 years	826	16.5
35–44 years	977	19.5
45–54 years	1,083	21.7
55–64 years	877	17.5
65 years and over	750	15.0
Total	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding Source: Identity Crime Survey 2014 [AIC data file]

Respondents were asked what language was most often spoken at home. These responses were recoded using the ABS's (2011) *Australian Standard Classification of Languages*, although in this instance English has been disaggregated from 'Northern European' languages. Table 4 shows the respondents' weighted distributions by language most often spoken at home. This indicates that only about five percent of those surveyed most often spoke a language other than English at home.

Table 4 Respondents by language most often spoken at home

Year	2014	2014
Language classification	n	%
English	4,724	94.5
Southern Asian	51	1.0
Eastern Asian	69	1.4
Southeast Asian	47	0.9
Eastern European	26	0.5
Southern European	30	0.6
Northern European	12	0.2
Southwest and Central Asian	10	0.2
Other languages	30	0.6
Australian Indigenous	0	0.0
Total	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Participants were also asked if they identified as Aboriginal or Torres Strait Islander. Weighted responses are provided in Table 5 and show that two percent of those surveyed identified as either Aboriginal or Torres Strait Islander.

Table 5 Respondents who identified as Aboriginal or Torres Strait Islander

Year	2014	2014
Aboriginal and Torres Strait Islander status	n	%
Aboriginal	85	1.7
Torres Strait Islander	8	0.2
Both Aboriginal and Torres Strait Islander	4	0.1
No	4,851	97.0
Rather not say	53	1.0
Total	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding Source: Identity Crime Survey 2014 [AIC data file]

Participants were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2013–14. Weighted responses are provided in Table 6.

Table 6 Respondents by individual gross income 2013–14

Year	2014	2014
Income category	n	%
\$0–\$18,200	1,001	20.0
\$18,201–\$37,000	1,166	23.3
\$37,001–\$80,000	1,373	27.5
\$80,001–\$180,000	715	14.3
\$180,001 and over	70	1.4
I'd rather not say	675	13.5
Total	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Respondents were asked how many hours in the previous week they had spent using a computer or computerised device, including desktops, laptops, smartphones and tablets. Responses (after weighting) ranged from zero to 168 (mean=25.7, SD=18.5, n=4,991). As Figure 3 demonstrates, similar to 2013, in 2014, the majority (77.8%) of respondents spent 35 hours or less on a computerised device per week. Some respondents, however, recorded spending much longer hours.

Figure 3 Number of hours spent the previous week using a computer or computerised device

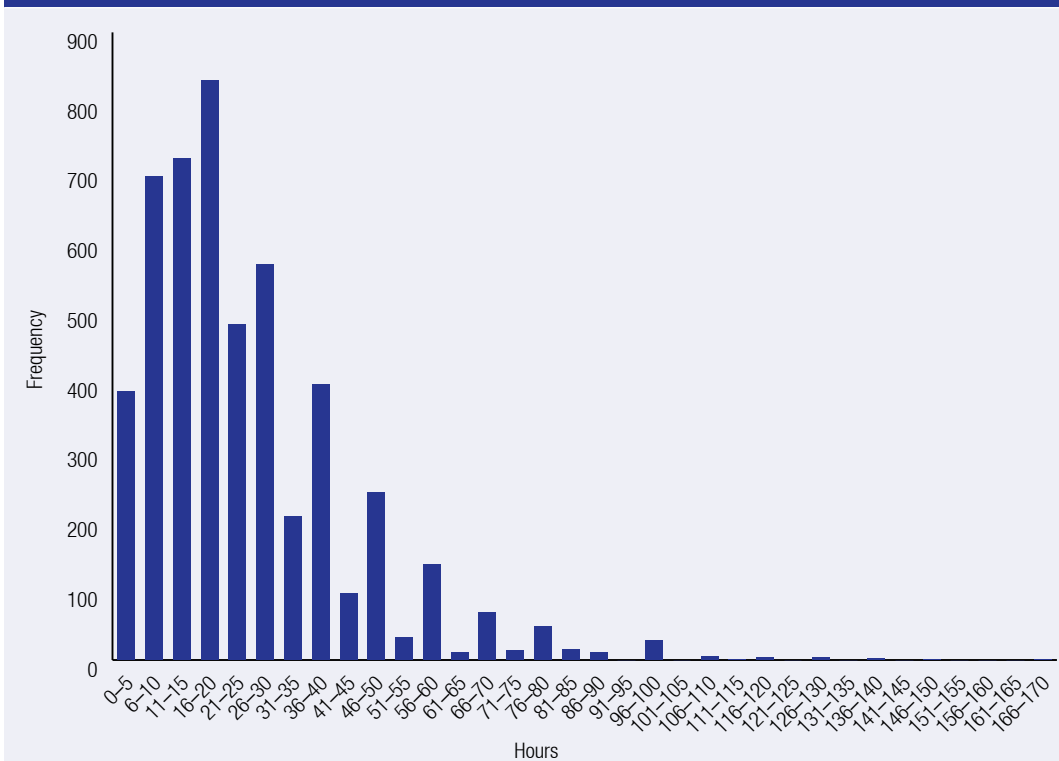
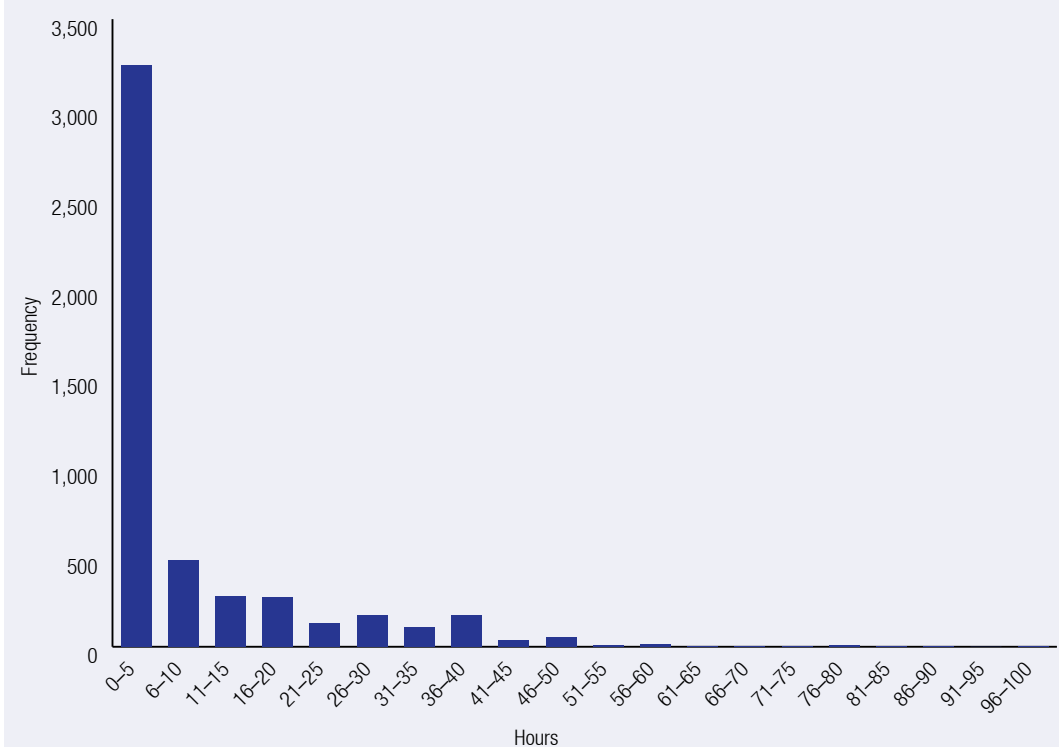


Figure 4 Number of hours spent the previous week using a computer or computerised device for work-related activities



Source: Identity Crime Survey 2014 [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 100 hours (mean=8.4, SD=13.3, n=5,000). As shown in Figure 4, the distribution was also positively skewed, with the majority (75.9%) of respondents spending 12 hours or less on a computerised device per week for work purposes.

Perceptions of misuse of personal information

The survey sought the views of participants on a number of matters concerning how they perceived

the risk of misuse of personal information, how serious they perceived such conduct to be and what changes were likely to occur in the years ahead. Although some participants may have had access to independent verifiable evidence relating to these matters, others would not. The responses, therefore, reflected the personal views of participants at the time of the survey and cannot be said to be indicative of objective factual information.

Participants were asked initially, in terms of harm to the Australian economy, how serious they thought misuse of personal information was. As shown in the weighted responses provided in Table 7, most respondents (96.3%) believed the misuse of personal information was a *very serious* or *somewhat serious* issue. These results were similar to those from the 2013 survey (96.6%).

Table 7 Respondents' perceptions about the seriousness of misuse of personal information

Year	2013	2014	2014
Seriousness	%	n	%
Very serious	68.8	3,403	68.1
Somewhat serious	27.8	1,409	28.2
Not very serious	2.9	154	3.1
Not at all serious	0.5	34	0.7
Total	100.0	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Participants were also asked if they thought the risk of someone misusing their personal information would change over the next 12 months. Two-thirds of those surveyed (67%) thought the risk of their personal information being misused would *increase greatly* or *somewhat* over the next year. This was slightly higher than in 2013 (65.2%). Weighted responses are provided in Table 8.

Table 8 Respondents' perceptions about the risk of misuse of their personal information in the next 12 months

Year	2013	2014	2014
Risk of misuse of personal information	%	n	%
Risk will increase greatly	19.8	1,099	22.0
Risk will increase somewhat	45.4	2,252	45.0
Risk will not change	33.8	1,607	32.1
Risk will decrease somewhat	0.5	25	0.5
Risk will decrease greatly	0.5	17	0.3
Total	100.0	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Participants were asked if they were aware that a person who has had their personal information misused could apply to a court to obtain a victim certificate to prove what occurred and were asked if they had done so in the past. Weighted responses are provided in Table 9.

Table 9 Respondents' awareness of victim certificates

Year	2013	2014	2014
Awareness of victim certificates	%	n	%
I am aware of such certificates, and have applied for one in the past	3.4	171	3.4
I am aware of such certificates, but have not applied for any	11.2	576	11.5
I am unaware of such certificates	85.5	4,253	85.0
Total	100.0	5,000	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 and weighted figures may not total 5,000 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

It should be noted that the number of respondents (n=171) who reported being aware of victim certificates and had applied for them in the past is low. This percentage (which is identical to the 2013 result) does not parallel the number of victim certificates applied for through the court system.

Experience of misuse of personal information

Participants were asked if their personal information had been misused at any time in the past, as well as any time in the previous 12 months. Of the 5,000 respondents, 1,008 (20.2%) experienced identity misuse at some time in their lives. This finding is almost identical to the 2013 results, which saw 1,032 (20.7%) experiencing identity misuse at some time in their lives. The unweighted data by place of normal residence are presented in Table 10. When data were weighted to restore national representativeness, 1,019 (20.4%) reported experiencing identity misuse at some time in their lives.

Table 10 Respondents who experienced misuse of their personal information at any time in the past by place of normal residence (unweighted data)

Year	2013	2014	2014
Location	%	n	%
Sydney (n=551)	22.2	132	24.0
Other New South Wales (n=300)	20.0	48	16.0
Melbourne (n=530)	22.3	126	23.8
Other Victoria (n=301)	20.0	56	18.6
Brisbane (n=421)	16.7	73	17.3
Other Queensland (n=451)	20.4	73	16.2
Perth (n=650)	20.7	118	18.2
Other Western Australia (n=200)	23.5	45	22.5
Adelaide (n=650)	21.2	127	19.5
Other South Australia (n=200)	21.0	43	21.5
Canberra (n=320)	20.7	78	24.4
Hobart (n=200)	18.5	41	20.5
Other Tasmania (n=170)	18.8	30	17.7
Darwin (n=41)	17.5	16	39.0
Other Northern Territory (n=15)	21.4	3	20.0
National (n=5,000)	20.7	1,008	20.2

Source: Identity Crime Survey 2014 [AIC data file]

Participants were also asked about misuse of their personal information in the previous 12 months. For the total sample (n=5,000), 8.7 percent (n=434) of respondents experienced identity misuse in the past 12 months. This represents a slight decline on 2013 results, which indicated that 9.2 percent (n=460) of respondents experienced identity misuse during that period. The unweighted data by place of normal residence are presented in Table 11. When data were weighted to restore national representativeness, 446 (8.9%) reported experiencing identity misuse in the past 12 months.

Table 11 Respondents who experienced misuse of their personal information in the past 12 months by place of normal residence (unweighted data)

Year	2013	2014	2014
Location	%	n	%
Sydney (n=551)	10.0	57	10.3
Other New South Wales (n=300)	10.3	20	6.7
Melbourne (n=530)	10.3	62	11.7
Other Victoria (n=301)	6.5	23	7.6
Brisbane (n=421)	6.9	28	6.7
Other Queensland (n=451)	10.0	31	6.9
Perth (n=650)	9.6	51	7.9
Other Western Australia (n=200)	9.5	19	9.5
Adelaide (n=650)	9.5	53	8.2
Other South Australia (n=200)	7.5	19	9.5
Canberra (n=320)	8.6	32	10.0
Hobart (n=200)	9.0	14	7.0
Other Tasmania (n=170)	7.1	15	8.8
Darwin (n=41)	10.0	9	22.0
Other Northern Territory (n=15)	14.3	1	6.7
National (n=5,000)	9.2	434	8.7

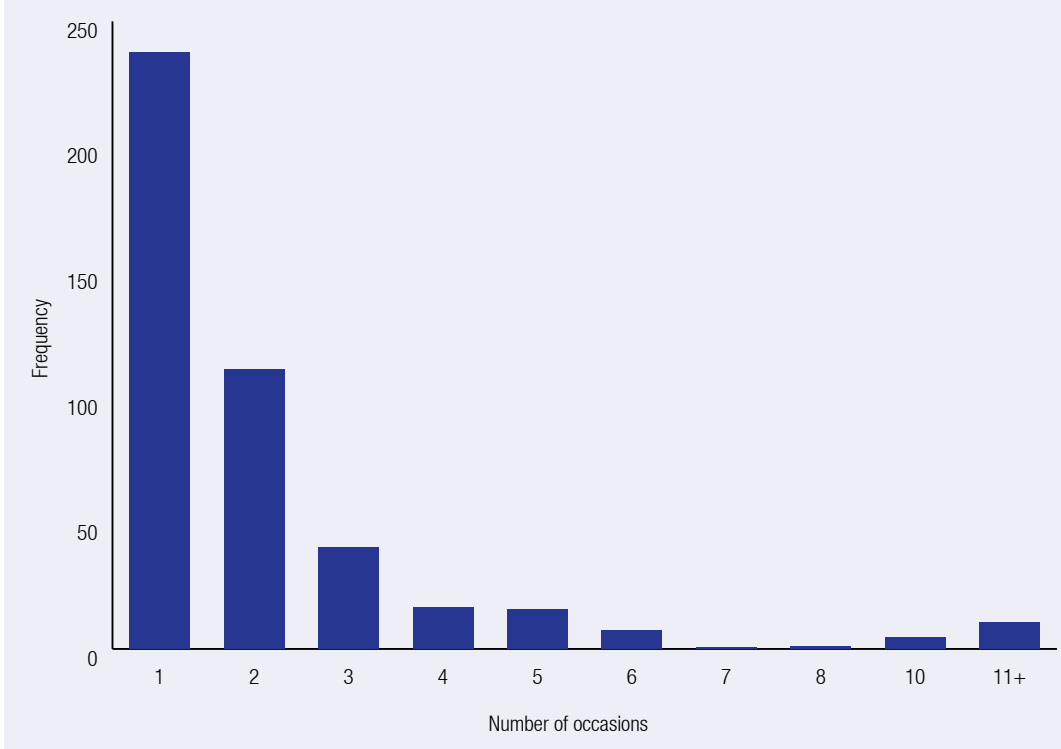
Source: Identity Crime Survey 2014 [AIC data file]

Locations with respondents who experienced higher than the national rates of misuse of personal information over their lifetime as well as the previous 12 months included Australia's largest population centres, Melbourne and Sydney. Other areas with above-average lifetime and 12-month prevalence estimates include Canberra, regional Western Australia and regional South Australia.

The 434 respondents who experienced misuse of their personal information within the past 12 months

were asked further questions relating to their experience. In 2014, the number of separate occasions on which participants believed that their personal information had been misused ranged from one to 200 (mean=2.9, SD=11.2, n=434). As shown in Figure 5, more than half of participants (53.3%) believed that their personal information had been misused on only a single occasion, which is similar to the findings for 2013 (53.7%).

Figure 5 Number of separate occasions participants believed their personal information had been misused



Source: Identity Crime Survey 2014 [AIC data file]

Losses, costs and consequences resulting from the misuse of personal information

Participants who had experienced misuse of their personal information within the past 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 occurred. Summary statistics are shown in Table 12.

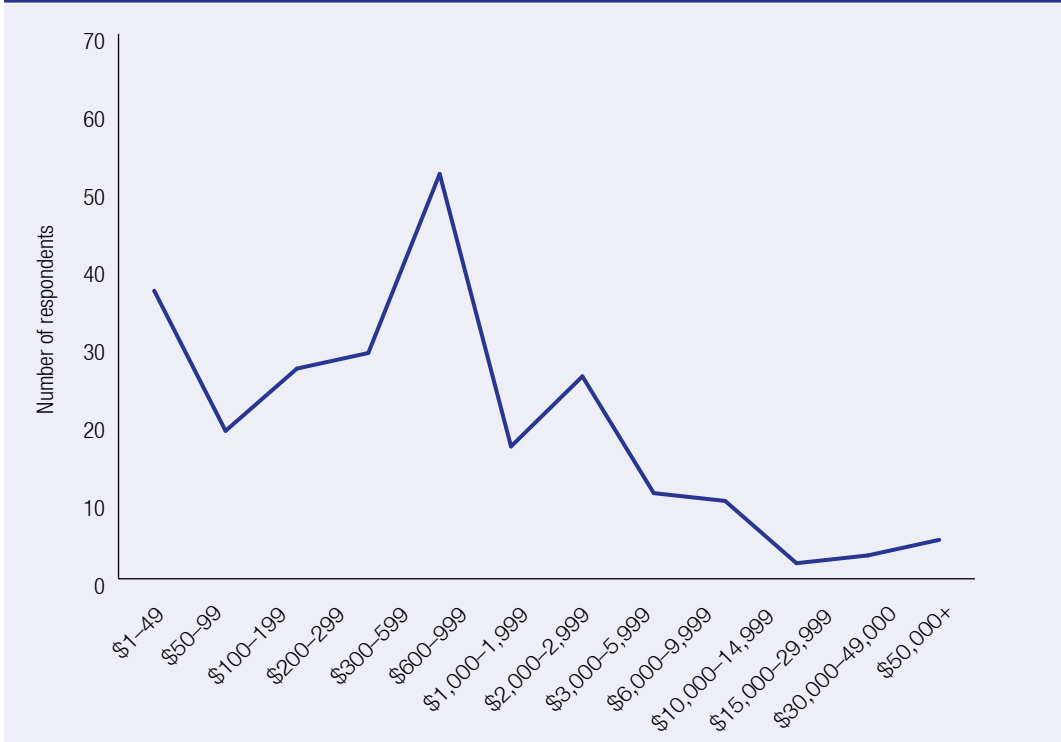
Table 12 Summary statistics for financial losses over 12 months				
Year	2013	2014	2013	2014
Statistic	Out-of-pocket losses (\$)	Out-of-pocket losses (\$)	Recovered (\$)	Recovered (\$)
Number of respondents	250	240	255	250
Minimum	1	1	2	1
Maximum	310,000	200,000	310,000	2,000,000
Mean	4,101	3,572	2,381	15,317
Median	247	300	300	350
Standard deviation	34,062	19,554	23,478	167,916
25% quartile	80	28	98	120
75% quartile	1,000	1,000	1,000	998
Total	1,025,250	858,599	607,164	3,831,440

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

In 2014, 240 participants indicated suffering a financial loss ranging between \$1 and \$200,000. The median loss was \$300 and total losses amounted to \$858,599. This compares with 2013, when 250 respondents experienced a median loss of \$247. As with 2013, in 2014, the distribution of losses is positively skewed, with the majority of participants experiencing smaller losses. The distribution of out-of-pocket losses suffered by respondents is shown in Figure 6.

Figure 6 Distribution of financial losses experienced in the preceding 12 months (n)

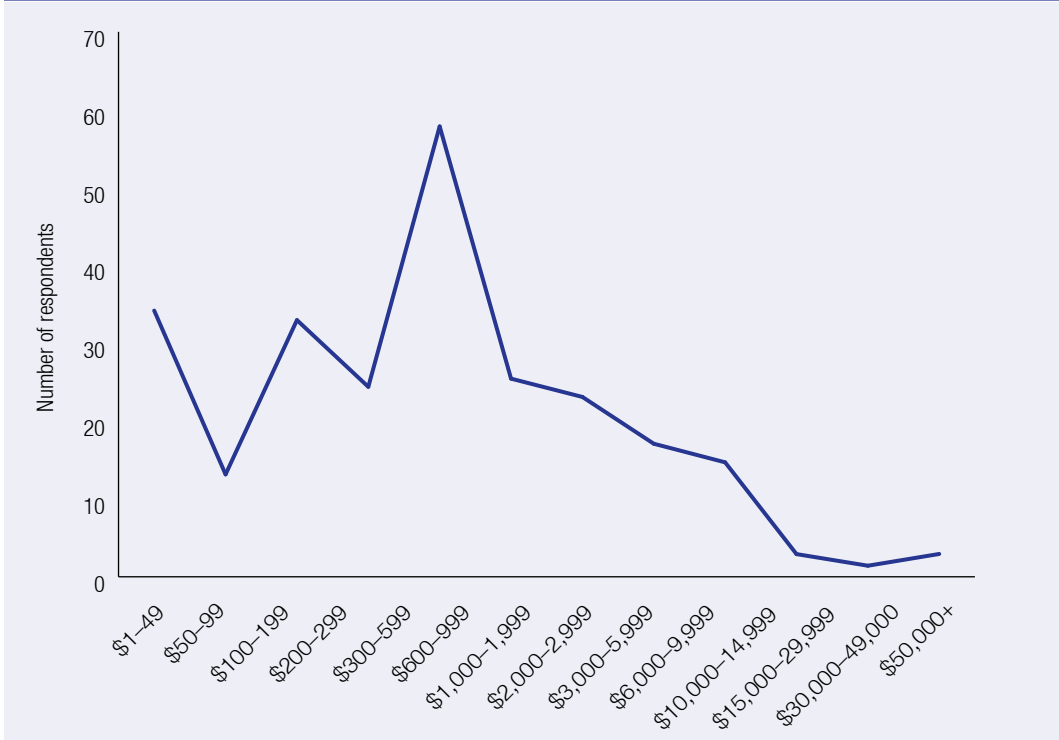


Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

Participants who had been reimbursed by banks or other organisations, or recovered their losses in other ways, as the result of the misuse of their personal information in the previous 12 months, recovered between \$1 and \$2,000,000. When the data were weighted, the mean amount reimbursed or recovered was \$15,317, and the median amount reimbursed or recovered was \$350. While the total recovered losses in 2014 (\$3,831,440) were significantly higher than in 2013 (\$607,164) this was skewed by a single reported recovery totalling \$2m dollars, which was somewhat of an outlier, given that the next highest figure reimbursed was \$60,000.

Figure 7 Distribution of funds reimbursed or recovered in the preceding 12 months (n)

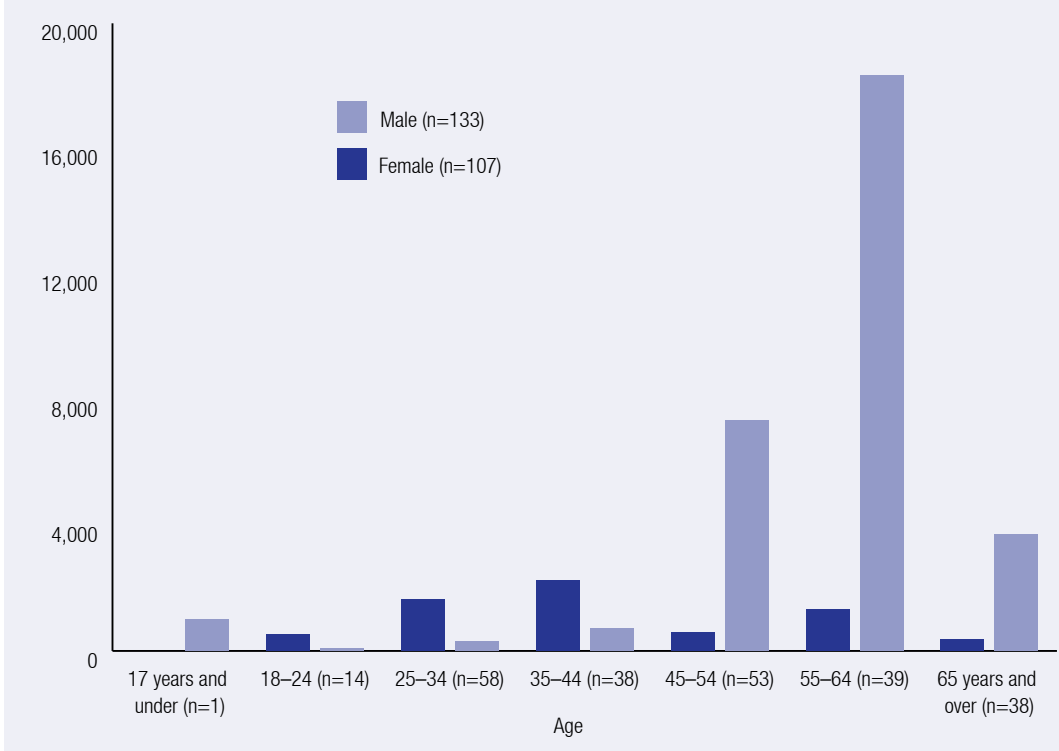


Note: Data were weighted to reflect the distribution of the population across jurisdictions
 Source: Identity Crime Survey 2014 [AIC data file]

Figure 8 shows the average loss by age and gender for those who reported a financial loss in 2014 (n=240). As the number within each category was relatively small, the averages reported here are sensitive to statistical outliers or high values in excess of \$6,000 that were reported by few respondents (see Figure 6). Therefore, further analyses are reported below to determine the statistical significance of the relationship between the amount of financial loss, age and gender.

Participants were asked what other negative consequences they had experienced as a result of having their personal information misused over the previous 12 months. Any causal connection between misuse of personal information and the specified consequences was not suggested, and participants were asked to make their own judgment about whether the results occurred ‘as a result’ of the misuse or not. Participants were able to select multiple responses. Weighted responses for the other consequences that were experienced are provided in Table 13.

Figure 8 Average financial loss by age and gender (\$)



Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

Table 13 Consequences experienced as the result of personal information being misused in the previous 12 months (n=446)

Year	2013 (n=460)	2014	2014
Consequences	%	n	%
I was refused credit	14.1	67	14.9
I experienced mental or emotional distress requiring counselling or other treatment	10.7	53	11.9
I was wrongly accused of a crime	5.5	23	5.2
I experienced physical health problems requiring medical treatment by a doctor	5.4	30	6.7
I had to commence legal action to clear debts and/or to clear my name	5.0	25	5.5
I experienced financial difficulties resulting in the repossession of a house or land, motor vehicle or other items	4.8	22	4.8
I experienced other reputational damage	4.4	11	2.6
I was refused government benefits	3.8	23	5.2
I was refused other services	2.2	12	2.7

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

Participants who had been refused other services were asked to specify the type of service they had been refused as a result of their personal information being misused. These included access to existing credit cards (n=3), bank accounts (n=2) and utility services (n=2). Responses provided by participants in relation to other reputational damage that had been experienced as a result of misuse of personal information included:

- 'I also had two regular payments dishonoured because of lack of funds in my account, which had been hacked';
- 'Someone claiming to be me was submitting my CV in order to get work';
- 'My credit company called my work and gave the impression I owed money';
- 'My licence details were used in another country'; and
- 'People on my mailing list felt my emails could not be trusted'.

Participants were also able to outline other consequences they had experienced. In many cases, participants provided context to the answers they had already given in the categories provided. For example, responses included:

- 'I experienced financial difficulties resulting in not being able to afford food';
- 'I got a dishonour fee from my bank';
- 'I had to cancel an ATM card';
- 'They came to arrest me';
- 'I was put into debt for a while as I couldn't pay some bills and got behind';
- 'I had to change all my passwords and credit card details'; and
- 'My bank account was frozen for three days'.

In addition, the 446 participants who experienced the misuse of personal information in the previous 12 months were asked how many hours they had spent dealing with the consequences. This included, for example, the time taken to have their credit rating fixed, having new cards issued or accounts changed. The weighted number of hours ranged from none to 500 (the same as in 2013), with a mean of 15.3 hours and a standard deviation of 42.4 hours (compared with a mean of 18.1 hours and a standard deviation of 49.5 hours in 2013). More than half (55.7%) spent three hours or less dealing with

the consequences of personal information misuse (compared with 50% in 2013).

Participants were also asked how much money they had spent dealing with the consequences of having their personal information misused over the previous 12 months. This included, for example, the cost of getting legal advice, lost income, telephone charges or postage and fees. A nil cost was experienced by 227 (50.9%) participants in 2014 (compared with 43.9% of participants in 2013). For the remainder of participants who experienced misuse in the previous 12 months, the weighted estimated financial cost to deal with the consequences ranged from \$1 to \$100,000 (mean=\$1,358.77, SD=\$9,104.01) compared with a range of \$1 to \$60,000 in 2013 (mean=\$576.23, SD=\$3,615.32). In 2014, half (50.2%) of participants spent \$35 or less dealing with the consequences of having their personal information misused over the previous 12 months (compared with 50.4% of participants spending \$40 or less in 2013).

Reporting the misuse of personal information

Of 446 participants who experienced misuse of their personal information in the previous 12 months, 45 (10.1%) did not report in any way in 2014 (compared with 8.9% in 2013). A further 216 participants (48.5%) told a friend or family member (compared with 53.5% in 2013), while 47 (10.6%) told a government agency or a business organisation (compared with 7.8% in the previous year). Finally, 138 (31%) told a friend or family member as well as a government agency or business organisation (compared with 29.8% in the previous year).

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 14, the majority of reports resulted in a *very satisfactory* or *satisfactory* outcome. It is noted that the 179 participants who responded to this question (six provided no response) reported to a weighted average of 1.9 agencies or organisations about the misuse of their personal information in the previous 12 months (range=1–6, SD=1.2), compared with an average of 2.1 agencies/organisations in 2013.

Table 14 Government agencies and business organisations reported to and satisfaction with the response

Agency/organisation reported to	Level of satisfaction				
		Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal) (n=125)	n	63	34	15	13
	%	50.6	26.9	11.8	10.6
A policing agency (n=51)	n	14	14	17	6
	%	27.2	26.9	33.3	12.5
A consumer protection agency (eg SCAMwatch, Consumer Affairs, Office of Fair Trading) (n=20)	n	2	10	3	5
	%	10.1	49.3	14.9	25.6
An internet service provider (n=24)	n	6	10	5	3
	%	24.7	42.3	21.2	11.7
A credit reporting agency (eg Veda or Dun & Bradstreet) (n=11)	n	6	2	3	–
	%	50.8	19.3	29.9	–
A utility company (eg gas, electricity, telephone, water) (n=14)	n	3	7	2	2
	%	21.3	53	12.9	12.9
Medicare Australia (n=8)	n	–	5	3	–
	%	–	63.3	36.7	–
A media organisation (n=9)	n	–	5	2	2
	%	–	57.4	22.1	20.5
The Passport Office (n=3) ^a	n	–	–	–	–
	%	–	–	–	–
A road traffic authority (n=4) ^a	n	–	–	–	–
	%	–	–	–	–
Other (n=19)	n	8	2	5	4
	%	41.9	10.3	25.9	21.7

– not applicable

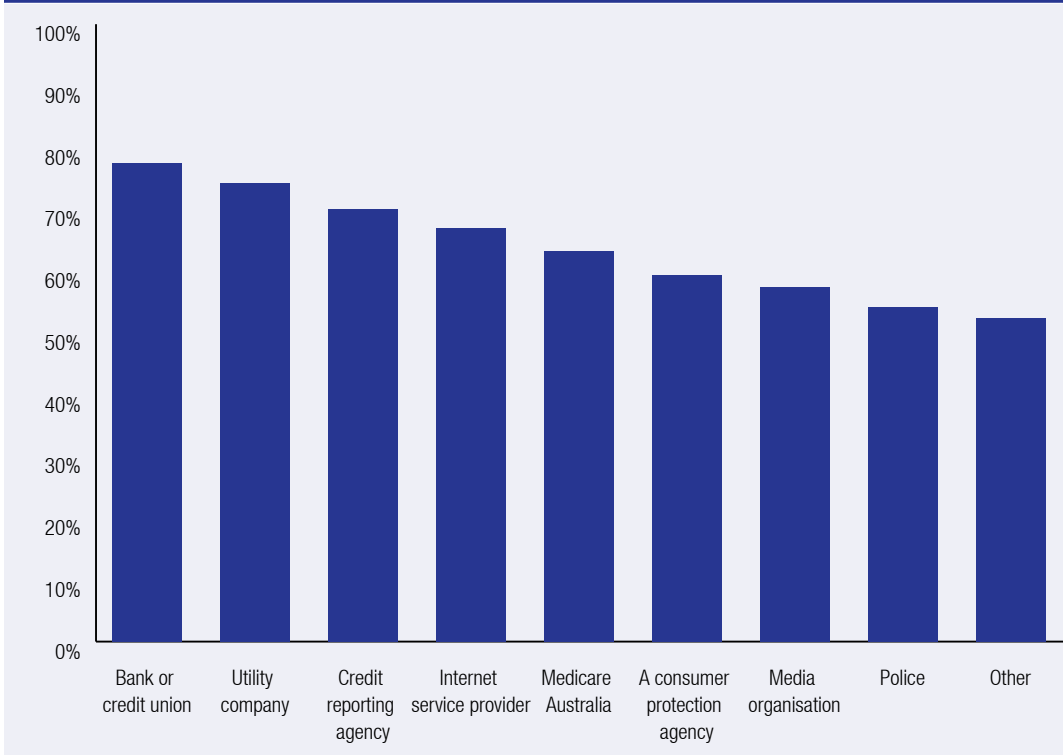
a Agencies/organisations with fewer than five responses were excluded from the analysis

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100 due to rounding

Source: Identity Crime Survey 2014 [AIC data file]

Figure 9 shows the percentage of respondents who were satisfied or very satisfied with the response by each agency. As shown, participants were most satisfied with the response provided by a bank or credit union, credit/debit card company or e-commerce provider (77.5% responded either satisfied or very satisfied), a utility company (74.3%) and by a credit reporting agency (70.1%).

Figure 9 Respondents who were satisfied or very satisfied with the response, by agency (%)



Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

The participants who indicated that they had not reported the misuse of their personal information were asked why they had not. Weighted responses are provided in Table 15. Participants could select more than one reason for not reporting.

Reasons for not reporting under other included 'the bank did all the work', 'it wasn't that big of a deal', 'it was not worth the time for such a small amount' and 'it was taken care of by authorities in USA at no loss to us'.

Table 15 Reasons for not reporting misuse of personal information (n=45)

Year	2013	2014	2014
Reason for not reporting	%	n	%
I did not believe the police or any other authority would be able to do anything	39.5	15	32.5
I was too embarrassed to report it	23.6	6	14.0
I did not know how or where to report the matter	23.1	16	35.2
I did not believe it was a crime	12.0	8	18.0
Other	22.1	6	12.8

Note: Data were weighted to reflect the distribution of the population across jurisdictions.

Source: Identity Crime Survey 2014 [AIC data file]

Behavioural changes arising from the misuse of personal information

Participants were asked how their behaviour had changed as a direct result of having their personal information misused. Weighted responses are provided in Table 16. It is noted that participants could select more than one way in which their behaviour had changed. When the data were weighted, almost all (91.6%, n=408) participants who 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 previous 12 months.

Table 16 Behavioural changes resulting from the misuse of personal information (n=446)

Year	2013	2014	2014
Behavioural change	%	n	%
Changed password(s)	48.5	250	56.1
More careful when using or sharing personal information	48.1	172	38.6
Changed banking details	42.5	151	34.0
Review financial statements more carefully	39.6	177	39.6
Don't trust people as much	39.0	143	32.1
Use better security for computer or other computerised devices	37.9	136	30.4
Shred personal documents before disposing of them	27.6	122	27.5
Changed email address(es)	15.8	53	11.8
Changed social media account(s)	13.6	50	11.1
Lock mailbox	12.3	46	10.3
Redirect mail when away or move residence	9.7	30	6.7
Changed telephone number(s)	9.4	35	7.8
Applied for a credit report	8.8	28	6.4
Use a registered post box	7.8	35	7.8
Changed place of residence	7.1	13	2.9
Signed up for a commercial identity theft alert/protection service	5.8	20	4.6
Other	4.0	22	4.9
Behaviour has not changed	5.9	37	8.4

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

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

Participants 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. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the participant. The aim was to seek participants' own best recollections or assessments of the facts and circumstances in question, although it should be emphasised that some participants might not have had access to evidence sufficient to answer these questions with certainty. Future surveys could include additional questions that assess the level of certainty in terms of evidence on which participants based their answers to these questions.

Type of information

Weighted responses for the types of personal information that had been misused are provided in Table 17. It is noted that participants could select more than one type of personal information that had been misused.

Table 17 Types of personal information respondents believed were misused in the most serious occasion in the previous 12 months (n=446)

Year	2013	2014	2014
Type of personal information	%	n	n
Credit/debit card information	52.3	231	51.8
Name	40.2	163	36.7
Bank account information	31.1	110	24.6
Address	24.6	110	24.7
Date of birth	22.0	95	21.4
Gender	18.9	61	13.7
Password	18.8	94	21.2
Online account username	18.0	65	14.6
Computer username	14.7	51	11.4
Driver's licence information	10.2	33	7.3
Place of birth	9.5	41	9.1
Signature	8.1	29	6.4
Personal identification number (PIN)	8.0	25	5.6
Tax file number (TFN)	6.7	14	3.2
Medicare information	5.3	16	3.5
Passport information	4.9	17	3.8
Student number	2.8	4	1.0

Table 17 Types of personal information respondents believed were misused in the most serious occasion in the previous 12 months (n=446) cont.

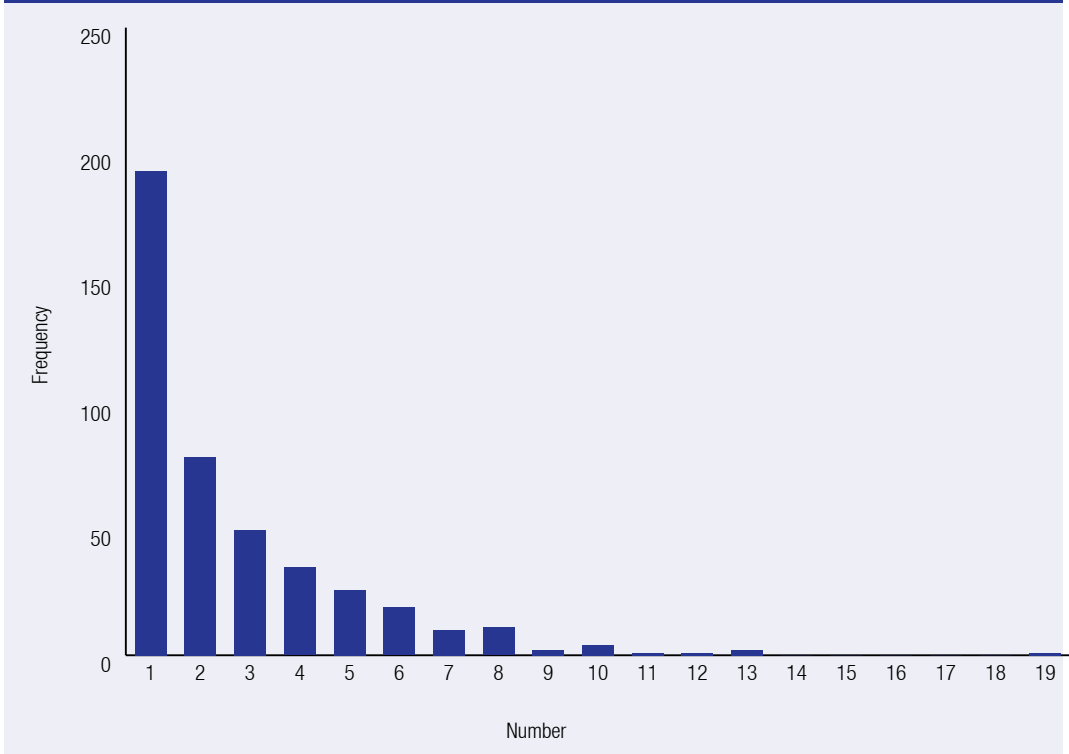
Year	2013	2014	2014
Type of personal information	%	n	n
Biometric information (eg fingerprint)	2.2	1	0.2
Holder identification number (HIN)	2.2	1	0.2
Other	6.8	44	9.8

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Respondents could select multiple types

Source: Identity Crime Survey 2014 [AIC data file]

Participants indicated that between one and 19 different types of personal information had been misused in the most serious occasion in the past 12 months (weighted mean=2.7, SD=3.3, n=434). As shown in Figure 10, this distribution is positively skewed, with almost half (44%) of participants indicating that only one type of information had been misused and eight in 10 participants noting that four or fewer types were misused.

Figure 10 Number of types of personal information misused in the most serious occasion in the past 12 months (unweighted data)



Source: Identity Crime Survey 2014 [AIC data file]

Source of information

Participants were asked how they believed their personal information had been obtained on the most serious occasion of misuse in the previous 12 months. Weighted responses are provided in Table 18. It is noted that participants could select more than one way in which they believed their personal information had been obtained.

For those participants who had indicated how their personal information had been obtained (n=339), the majority (n=231, 68.2%) indicated that only one method had been used (weighted mean=1.5, SD=0.9, range 1–6).

Table 18 How personal information was obtained on the most serious occasion in the previous 12 months (n=446)

Year	2013 (n=460)	2014	2014
Way of obtaining personal information	%	n	%
From theft or hacking of a computer or other computerised device (eg smartphone)	20.0	90	20.2
From an online banking transaction	19.5	67	15.1
By email	18.3	58	12.9
From information placed on a website other than social media (eg online shopping)	15.7	60	13.5
From an ATM or EFTPOS transaction	11.0	29	6.4
By telephone (excluding SMS)	10.5	37	8.4
Theft of mail	9.6	32	7.2
From information lost or stolen from a business or other organisation (i.e. a data breach)	9.6	44	10.0
In a face-to-face meeting (eg a job interview or a doorknock appeal)	7.5	24	5.3
From information placed on social media (eg Facebook, Linked-in)	6.9	25	5.6
By text message (SMS)	6.4	18	4.1
Theft of an identity or other personal document	2.0	6	1.3
Theft of a copy of an identity or other personal document	0.8	3	0.6
Other	5.7	33	7.4
Don't know	19.7	102	23

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Respondents could select multiple types

Source: Identity Crime Survey 2014 [AIC data file]

Misuse of information

Participants were asked how they believed their personal information had been misused on the most serious occasion in the previous 12 months. Weighted responses are provided in Table 19. It is noted that participants could select more than one way in which they believed their personal information had been misused.

Table 19 How personal information was misused on the most serious occasion in the previous 12 months (n=446)

Year	2013 (n=460)	2014	2014
Misuse	%	n	%
To obtain money from a bank account (excluding superannuation)	35.4	111	24.8
To purchase something	32.5	160	35.8
To apply for a loan or obtain credit	8.1	22	5.0
To file a fraudulent tax return	7.2	25	5.6
To obtain money from an investment (eg shares)	6.5	8	1.7
To apply for a job	6.4	12	2.7
To open a mobile phone account	6.4	15	3.3
To apply for government benefits	4.1	13	2.8
To provide false information to police	5.3	21	4.6
To obtain superannuation monies	5.1	12	2.7
To open an online account, such as Facebook, eBay	3.2	18	4.1
To rent a property	2.3	8	1.8
Other	8.9	54	12.1
Don't know	14.7	76	17.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Respondents could select multiple types

Source: Identity Crime Survey 2014 [AIC data file]

Participants who indicated that their personal information had been misused to purchase something were asked to specify what was purchased. A wide range of purchases was identified, among the most frequent of which were consumer electrical goods (n=21), airfares and travel (n=16), fashion (n=15), gambling (n=7), phones (n=6) and hotels (n=6).

For those participants who knew how their personal information had been misused (n=446) the weighted number of different ways in which it had been misused ranged from one to five (mean=1.2, SD=0.6). More than eight in 10 (n=370, 84.9%)

indicated just one way in which their personal information had been misused (compared with 79% in 2013).

Detection methods

Participants were asked how they became aware of the misuse of their personal information on the most serious occasion in the previous 12 months. Weighted responses are provided in Table 20. It is noted that participants could select more than one way in which they had become aware that their personal information had been misused.

Table 20 How misuse of personal information was detected on the most serious occasion in the past 12 months (n=446)

Year	2013 (n=460)	2014	2014
Detection method	%	n	%
Received a notification from a bank or financial institution and/or credit card company	43.3	174	38.9
Noticed suspicious transactions in bank statements or accounts	33.3	148	33.3
Received a bill from a business or company for which they were not responsible	13.5	33	7.4
Was unsuccessful in applying for credit	9.1	22	4.9
Received a notification from police	7.9	38	8.4
Received a notification from another company	5.2	32	7.2
Was contacted by debt collectors	5.1	18	4.1
Received a notification from a government agency or authority other than the police	3.6	3	0.6
Other	15.8	81	18.2

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Respondents could select multiple types

Source: Identity Crime Survey 2014 [AIC data file]

Most participants (n=353, 79.2%) had detected the most serious misuse of personal information over the past 12 months using just one method, which was similar to the results for 2013 (79.6%). When the data were weighted, the mean number of methods used to detect the most serious misuse of personal information was 1.2 (SD=0.6, range=1–6).

Out-of-pocket losses

Participants 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 21.

Table 21 Summary statistics for financial losses on the most serious occasion

Year	2013	2014	2013	2014
Statistic	Out-of-pocket losses (\$)	Out-of-pocket losses (\$)	Recovered (\$)	Recovered (\$)
Number of respondents	260	224	246	244
Minimum	1	1	1	1
Maximum	310,000	200,000	310,000	60,000
Mean	4,816	3,687	2,209	1,318
Median	200	200	227	350
Standard deviation	30,541	20,181	23,944	4,505
25% quartile	50	50	87	100
75% quartile	800	750	920	1,000
Total	1,252,177	824,800	543,514	321,653

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

In 2014, 222 participants (49.8%) experienced no financial loss (compared with 43.5% in 2013). The remaining 224 participants experienced losses ranging from \$1 to \$200,000. When the data were weighted, the median financial loss was \$200. The distribution was positively skewed, as shown in Figure 11, with more than three-quarters (76%) of participants experiencing losses of up to \$750. The total lost on the most serious occasion was \$824,800 (compared with \$1,252,177 in 2013).

Figure 11 Distribution of financial losses experienced on the most serious occasion in the preceding 12 months (n)



Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

Funds recovered

Among the 244 participants who had been reimbursed by banks or other organisations, or recovered their losses in other ways, in respect of the most serious occasion, recovered between \$1 and \$60,000. When weighted, the median amount recovered was \$350. It was found that most participants received reimbursement or recovery of

small amounts, with few receiving higher amounts (see Figure 12). The total amount recovered was \$321,653 (compared with \$543,514 in 2013). The remaining 202 (45.3%) participants did not receive any reimbursement or recover anything from the most serious occasion of misuse in the previous 12 months.

Figure 12 Distribution of funds reimbursed or recovered in the most serious occasion in the preceding 12 months (n)



Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

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

The characteristics of those who experienced misuse of personal information in the previous 12 months were explored in more detail. Chi-square tests (χ^2), which test the assumption that the frequencies observed within each cell are obtained by chance, were used for categorical variables (those with two or more categories but no agreed way in which to order them). Using weighted data, the results of chi-square tests indicated that for a number of variables there was no significant relationship with misuse of personal information in the previous 12 months. These variables were:

- age group;
- gender;
- place of normal residence;
- place of normal residence dichotomised (capital city/outside capital city);
- language spoken at home dichotomised (English/ language other than English); and
- perception of seriousness of misuse of information.

As shown in Table 22, a significant relationship was found between experiencing misuse of personal information in the previous 12 months and Indigenous status (Indigenous was defined as those who identified as Aboriginal, Torres Strait Islander or both Aboriginal and Torres Strait Islander) (χ^2 (2, n=5,000)=11.31, p<0.05). These results indicate that those who identified as Indigenous were more likely than others to experience misuse of their personal information.

Table 22 Contingency table for misuse of personal information in the previous 12 months and Indigenous status (expected frequencies are shown in parentheses)

Indigenous status	Misuse of personal information in previous 12 months		Total
	Yes	No	
Identified as Indigenous	18 (9)	79 (88)	97
Did not identify as Indigenous	422 (433)	4,429 (4,418)	4,851
Preferred not to say	6 (5)	46 (48)	52
Total	446 (446)	4,554 (4,554)	5,000

$p < 0.05$

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

The results of Table 23 indicate that those in the lowest income category (\$18,200 and under) were less likely to experience misuse of their personal information and those earning \$37,001 and above were more likely to experience misuse ($\chi^2(5, n=5,000)=36.24, p < 0.001$).

Table 23 Contingency table for misuse of personal information in the previous 12 months and individual gross income (expected frequencies are shown in parentheses)

Income category	Misuse of personal information in previous 12 months		Total
	Yes	No	
\$0–\$18,200	60 (89)	941 (912)	1,001
\$18,201–\$37,000	108 (104)	1,058 (1,062)	1,166
\$37,001–\$80,000	137 (122)	1,236 (1,250)	1,373
\$80,001–\$180,000	85 (64)	630 (651)	715
\$180,001 and over	14 (6)	56 (64)	70
I'd rather not say	42 (60)	633 (615)	675
Total	446	4,554	5,000

$p < 0.001$

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [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 experiencing misuse of personal information in the previous 12 months ($\chi^2(4, n=5,000)=118.11, p < 0.001$), as shown in Table 24. Those who had experienced misuse of personal information in the previous 12 months were more likely than expected to perceive that risks would increase in future.

Table 24 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 are shown in parentheses)

Risk of misuse of personal information	Misuse of personal information in previous 12 months		Total
	Yes	No	
Risk will increase greatly	167 (98)	932 (1,001)	1,099
Risk will increase somewhat	214 (201)	2,039 (2,052)	2,252
Risk will not change	58 (143)	1,549 (1,464)	1,607
Risk will decrease somewhat	6 (2)	19 (23)	25
Risk will decrease greatly	1 (1)	15 (15)	17
Total	446	4,554	5,000

$p < 0.001$

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

A Mann-Whitney U 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. The test, which 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), found that participants who experienced misuse spent significantly more hours on a computer or computerised device than those who had not ($z = -2.10$, $p < 0.05$, $n = 4,995$).

As the Mann-Whitney U test could not be replicated with the weighted data, the number of hours spent on a computer or computerised device variable was normalised using logarithmic transformation so that the parametric alternative, an independent t-test, could be undertaken. With the unweighted data, the t-test also found that those who experienced misuse spent significantly more hours on a computer or computerised device ($M = 3.06$, $SD = 0.79$) than those who had not ($M = 2.97$, $SD = 0.81$; $t(4) = 2.09$, $p < 0.05$).

When the data were weighted, however, the difference was no longer significant ($p = 0.051$).

For those 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 was then undertaken of the methods that had been used to obtain their personal information. This was to test whether those who lived in closer density were more likely to have their personal information misused by tactics such as mail theft than those who lived further apart. A number of the methods used to obtain personal information were found to be statistically unrelated to participants' place of normal residence. These were:

- in a face-to-face meeting (eg 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;

- theft of a copy of an identity or other personal document;
- from information lost or stolen from a business or other organisation (i.e. a data breach);
- from an online banking transaction;
- from information placed on social media (eg Facebook, Linked-in);
- from information placed on a website (other than social media);
- from an ATM or EFTPOS transaction;
- other; and
- don't know how personal information was obtained.

Table 25 shows the relationship between place of normal residence and theft of mail for respondents who had experienced misuse of their personal information in the previous 12 months. It was found that respondents located in a capital city were significantly more likely than those who were not in a capital city to have their personal information obtained from the theft of their mail ($\chi^2(1, n=446)=6.14, p<0.05$).

Table 25 Contingency table for place of normal residence of participants who experienced misuse of personal information in the previous 12 months and information lost or stolen from theft of mail (expected frequencies are shown in parentheses)

Location	Information lost or stolen from theft of mail		Total
	Selected	Not selected	
Capital city	29 (23)	293 (299)	322
Outside capital city	3 (9)	121 (115)	124
Total	32	414	

Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2014 [AIC data file]

Further analyses were undertaken to test the relationship between the characteristics of respondents who reported a financial loss ($n=224$) and the amount they reported losing. As the reported financial loss distribution was positively skewed, this variable was normalised using logarithmic transformation prior to these analyses being undertaken.

The data were weighted and t-tests found no significant relationship between the amount of financial loss and gender (dichotomised as male/female, as the respondents who indicated 'other' gender did not report a financial loss; $t(215)=1.31$ NS), location (dichotomised; $t(215)=2.71$ NS), language (dichotomised; $t(215)=3.61$ NS) or Indigenous status (dichotomised; $t(215)=2.62$, NS).

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 ($F(5,211)=0.73$, NS). There was, however, a significant relationship between respondents' age

categories and the amount of financial loss ($F(6,210)=12.05$, $p<0.001$), with the average financial loss generally increasing with age.

Further analysis of the relationship between age, gender and amount of financial loss showed that gender was not statistically significant when controlling for age ($t(215)=-1.65$ NS). A series of interaction tests examining specific age and gender combinations found no statistically significant findings.

The number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent, was normalised using logarithmic transformation, and the relationship between these weighted variables and financial loss was investigated using Pearson product moment correlation coefficients. Both these variables were found to have significant positive correlation with the amount of financial loss, indicating that the higher the financial loss, the more time ($r=0.27$, $n=211$, $p<0.01$) and money ($r=0.60$, $n=148$, $p<0.001$) were spent dealing with the consequences.

Discussion



The present study sought to quantify the nature and extent of identity crime and misuse in Australia by obtaining the views of a large sample of Australians aged 15 years and over who resided across all states and territories. These results build on the baseline data collected in the 2013 survey and begin to demonstrate consistent views over time.

Perceptions of misuse of personal information

In relation to how respondents perceived the seriousness of the problem of identity crime and misuse, a large proportion of respondents from the present survey indicated that misuse of personal information was *very serious* or *somewhat serious* in terms of harm to the Australian economy. The figure of 96.3% in 2014 is almost identical to the findings of 2013 (96.6%) and reflects the serious nature of the threat. Two-thirds of the respondents (67%) also considered that the risk of someone misusing their personal information would increase over the next 12 months (consistent from 65.2% in 2013).

Although both of these perceptions concerning the seriousness and likelihood of change were higher than similar perceptions reported by Di Marzio Research (2012) and the OAIC (2013), these prior

surveys were not directly comparable in terms of sample and questions asked. More recently, a survey conducted by Veda of 1,511 Australians found that 82 percent of respondents reported being concerned about having their personal information stolen. Generation Ys were less likely to worry, with 76 percent stating they were concerned about identity theft, compared with 86 percent of generation Xs and 81 percent of baby boomers (Veda 2015). An earlier study by Veda (2014) found that 89 percent of people were concerned about the security of their personal information when using the internet and more than two-thirds (69%) did not trust social media to protect their information (Veda 2014).

Interestingly, these perceptions do not reflect the actual reported risk of victimisation (see below). Although almost two-thirds of respondents to the AIC's 2014 survey thought that the risk of someone misusing their personal information would increase over the next 12 months, between the AIC's surveys in 2013 and 2014 there was almost no change.

Experience of misuse of personal information

The present survey found that 20.4% of respondents reported misuse of personal information at some

time during their life, with 8.9 percent reporting misuse of their personal information in the previous 12 months. This finding closely mirrors 2013, when 20.8 percent of respondents reported misuse of personal information at some time during their life, and 9.4 percent reported misuse of their personal information in the previous 12 months.

These findings are somewhat lower than the lifetime prevalence rate of 27 percent of respondents to the NFA's (2013) survey of identity fraud, but higher than the 8.8 percent of respondents in the United Kingdom who reported experiencing identity fraud in 2012. The present survey's lifetime prevalence rate of 20.4 percent is also much higher than the 13 percent lifetime rate of identity fraud reported by respondents to the OAIC's (2013) survey and the 17 percent reported by respondents to Veda's survey (2015). Rates similar to those in the Veda (2015) study were also present in the US NCVS, with a lifetime prevalence rate of 14 percent and a 12-month prevalence rate of 6.7 percent (Harrell & Langton 2013).

The present survey's 8.9 percent rate of reported victimisation in the preceding 12 months is also much higher than that reported by the ABS (2012), which found that four percent of respondents had experienced identity fraud in the preceding 12 months, and arguably higher than Di Marzio Research's (2012: 7) survey finding that seven percent of respondents experienced identity theft 'in the last 6 months or so'. Veda's (2015) 5 percent victimisation rate for the past 12 months appears similar to that of the ABS's (2012) national survey. These variations are most likely due to the different sampling frames used, the data collection techniques employed and the focus of questions asked of respondents.

Losses, costs and consequences resulting from the misuse of personal information

Participants who 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. Out-of-pocket losses were defined as being money paid out, excluding any money that they were able to recover from banks and any costs associated with repairing what occurred.

In 2014, 240 respondents indicated suffering a financial loss ranging between \$1 and \$200,000. The median loss was \$300 and total losses amounted to \$858,599. The majority of participants experienced smaller losses. This compares to 2013, when 45.7% (n=210) of survey participants did not suffer a financial loss, while 250 participants experienced losses that when weighted ranged from \$1 to \$310,000 (with a median loss of \$247). As with 2013, in 2014, the distribution of losses is positively skewed, with the majority of participants experiencing smaller losses.

In addition to these losses, banks and other organisations reimbursed respondents for losses they had suffered, resulting in an additional loss to those banks and other organisations. When the data were weighted, the mean amount reimbursed or recovered was \$15,317, and the median amount reimbursed or recovered was \$50. While the total recovered losses in 2014 (\$3,831,440) were significantly higher than in 2013 (\$858,599), this was skewed by a single reported recovery totalling \$2m.

Finally, some participants experienced other consequences, the most frequent of which were being refused credit (14.9%, up from 14.1% in 2013), experiencing mental or emotional stress requiring counselling or other treatment (11.9%, up from 10.7% in 2013) and being wrongly accused of a crime (5.2%, down from 5.5% in 2013). In 2014, some victims were denied access to their credit cards, bank accounts and utility accounts, and one victim said that police 'came to arrest me'. Though there are small variations, 2014 results largely reflect those seen in the 2013 survey.

These financial and other impacts are somewhat different from other Australian data. The ABS (2012) found that one in three victims (33.2%) of credit card fraud had lost money, even after receiving reimbursement from banks and other organisations, with 15.2 percent of victims losing \$100 or less, 9.1 percent losing between \$101 and \$500, 4.2 percent losing between \$501 and \$1,000, and 4.8 percent losing more than \$1,000. It was also found that just more than one-quarter (26.9%) of all victims of identity theft in the five years prior to interview had incurred

financial losses as a result of the incident(s), with 24.1 percent losing \$10,000 or less and 2.8 percent losing more than \$10,000.

In 2013–14, the Australian Payments Clearing Association reported a total of 6.1 billion transactions involving a credit or debit card in Australia. Of these transactions, 1,543,197 were fraudulent—worth approximately \$304m (APCA 2014: 7). Not all of this would fall within the definition of out-of-pocket losses arising from misuse of personal information within the terms of the present research.

In the United Kingdom, however, identity fraud was estimated by the NFA (2013) to cost UK adults £3.3b during 2012, with those who actually lost money (2.7 million individuals) losing an average of £1,203 each (the equivalent of A\$2,169).

In the United States, identity theft victims reported a total of US\$24.7b in direct and indirect losses attributed to all incidents of identity theft experienced in 2012. The US *National Crime Victimization Survey* (NCVS) found that 68 percent of identity theft victims reported a combined direct and indirect financial loss associated with the most recent incident, with a mean loss of US\$1,769 and a median loss of US\$300. In addition to any direct financial loss, six percent of all identity theft victims reported indirect losses associated with the most recent incident of identity theft. Victims who suffered an indirect loss of at least US\$1 reported an average indirect loss of US\$4,168, with a median loss of US\$30. With the exception of victims of personal information fraud, identity theft victims who reported indirect financial loss had a median indirect loss of US\$100 or less. At the time of the interview, 14 percent of victims had experienced personal out-of-pocket financial losses of US\$1 or more. Of those victims who suffered an out-of-pocket financial loss, 49 percent had total losses of US\$99 or less, while approximately 18 percent reported out-of-pocket expenses of between US\$100 and US\$249. An additional 16 percent reported out-of-pocket expenses of US\$1,000 or more.

About 36 percent of identity theft victims reported moderate or severe emotional distress as a result of the incident, although the level of emotional distress varied by type of identity theft. Thirty-two percent of victims of personal information fraud reported that they found the incident severely distressing, compared with five percent of credit card fraud

victims. Twenty-two percent of victims of new account fraud reported that the crime was severely distressing. At the time of the interview, 86 percent of identity theft victims had resolved any problems associated with the incident and, of these, the majority spent a day or less clearing up the problems, while about 29 percent spent a month or more (Harrell & Langton 2013). Comparing these results with those obtained in the present Australian survey, it appears that median losses were similar to those in the United States, while the proportion experiencing emotional harm was higher in the United States (although definitions of harm differed).

The most recent estimate of the total economic impact of identity crime in Australia in 2014, undertaken as part of the National Identity Security Strategy's Measurement Framework, was approximately \$2.4b. This comprises: the costs of preventing and responding to identity crime (approximately \$350m); the cost of identity crime as a percentage of Commonwealth fraud (\$28.5m); the cost of identity crime to individuals (\$434.9m); 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 \$1.4b) (Emami & Smith 2015). The losses identified by victims in the present survey form just one element of this total impact.

Reporting the misuse of personal information

As with prior research in Australia and overseas, among survey respondents, reporting of misuse of identity was relatively low.

Of those who experienced misuse of their personal information, 45 (10.1%) did not report in any way. This is a small escalation from the previous year, when only 8.9 percent did not report this misuse. A further 216 respondents (48.5%) told a friend or family member (compared with 53.5% in 2013), while 47 (10.5%) told a government agency or a business organisation (compared with 7.8% in the previous year). Finally, 138 (31%) told a friend or family member as well as a government agency or business organisation—a result almost identical to the previous year.

These results are similar to those found in the AIC's *Online Consumer Fraud Survey 2013 (Jorna 2015)*. Respondents to this survey, which covered all types of consumer fraud including identity misuse, indicated that they most often reported to family and friends (51% of those victimised) followed by reports to the ACCC's SCAMwatch website (41.2%). Overall in 2013, 11 percent failed to report their scam victimisation to anyone, which is similar to the 10.1 percent who failed to report in the AIC's current identity crime survey. Similar to the 2014 identity crime survey results, in 2013, the most common reasons provided for not reporting scams were 'unsure of which agency to contact' (39.7% of the total sample), 'I didn't think anything would be done' (31.4%) and 'not worth the effort' (26.9%) (Jorna 2015).

Respondents to 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. Participants were most satisfied with responses provided by financial institutions (77.5% were either *satisfied* or *very satisfied*), followed by utility companies (74.3% were either *satisfied* or *very satisfied*). The lowest levels of satisfaction were in relation to reports to consumer protection agencies.

The findings in the current 2014 identity crime survey with respect to reporting behaviour are very similar to those reported in the NCVS in the United States in 2012 (Harrell & Langton 2013). Arguably, further efforts are needed to improve reporting rates, particularly to government agencies responsible for handling consumer complaints, by coordinating their activities and publicising avenues for reporting. The results of the current survey found that more than one-third of respondents simply did not know to whom a report should be made.

Behavioural changes resulting from the misuse of personal information

Participants were asked to indicate if, and how, their behaviour had changed as a direct result of having their personal information misused. Almost all

(91.6%) indicated that they had changed their behaviour in some way—a result similar to that found in 2013 (94.1%). Some respondents even indicated that they had changed their place of residence (n=13 in 2014).

The top-five behavioural changes were the same as in 2013. These included changing passwords (56.1%), reviewing financial statements more carefully (39.6%), being more careful when using or sharing personal information (38.6%), changing banking details (34%) and not trusting people as much (32.1%). Once again, a minority (8.4%) of participants who experienced misuse of their personal information in the previous 12 months indicated that this did not result in any behavioural change.

In its *Personal Fraud Survey 2007*, the ABS (2008) asked respondents to indicate how their behaviour had changed as a result of the most recent incident of various types of personal fraud victimisation. In relation to identity theft, 24.5 percent of respondents said that they were more aware or careful; 8.8 percent said they experienced reduced wellbeing; 3.9 percent had changed their internet service provider, email address, payment method, credit card details or internet security; 6.7 percent had stopped engaging, ignored or no longer dealt with that organisation or person; 3.4 percent made changes to contact details or physical or home security; and 3.2 percent indicated other behavioural changes (owing to high relative standard error rates, some of these findings were unreliable). In total, 47 percent of respondents had changed their behaviour in some way following identity theft victimisation (the same percentage who indicated changed behaviour following card fraud).

In the United States, the NCVS found that a greater percentage of victims (96%) than non-victims (84%) had engaged in at least one preventive action, and that about 12 percent of victims who took preventive action did so in response to experiencing identity theft in the past year. Overall, the two most common preventive actions in 2012 were checking bank or credit statements (75%) and shredding or destroying documents containing personal information (67%). A higher percentage of victims than non-victims engaged in both of these preventive actions; however, about 13% of victims began shredding or destroying documents containing personal

information as a result of experiencing identity theft during the previous 12 months and 26% began checking bank or credit statements as a result of the victimisation. Less than 10 percent of victims purchased identity theft protection (4%) or insurance (6%) or used an identity theft security program on the computer (6%) after experiencing identity theft, while about one-quarter of victims checked financial accounts or changed passwords on these accounts as a result of the victimisation (Harrell & Langton 2013).

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

Participants 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. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the participant.

In 2014, the top-three types of personal information that had been misused were credit and debit card information (51.8%), name (36.7%) and bank account information (24.6%). These were the same top-three categories identified in 2013. These results were similar to those reported in Di Marzio Research's (2012) survey, in which the most prevalent way in which identity theft or misuse had occurred was loss of credit card or debit card, which was reported by 35 percent of respondents. Similarly, in the United States, the NCVS found that the majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information, and that among identity theft victims, existing bank (37%) or credit card accounts (40%) were the most common types of misused information (Harrell & Langton 2013). This is not surprising given that in 2013–14, Australians undertook 6.1 billion transactions involving a credit or debit card, with 1.5 million of these being fraudulent (APCA 2014).

Participants were asked how they believed their personal information had been obtained on the most serious occasion in the previous 12 months. The top-five ways were from theft or hacking of a computer or other computerised device (20.2%), from an online banking transaction (15.1%), by email (12.9%—down from 18.3% in 2013), from information placed on a website other than social media (such as online shopping) (13.5%) and from information lost or stolen from a business or other organisation (i.e. a data breach) (10%). Notably, the category of details obtained via an ATM or EFTPOS transaction was down from 11 percent in 2013 to 6.4 percent in 2014. Di Marzio Research's (2012) survey also found a high incidence of identity theft and misuse taking place through internet viruses and scams (31% and 27% respectively). In the United States, the NCVS found that approximately one-third (32%) of identity theft victims knew how the offender had obtained their information, and of the 5.3 million victims who knew how the identity theft occurred, the most common way offenders obtained information (43%) was to steal it during a purchase or other transaction (Harrell & Langton 2013).

Participants were asked how they believed their personal information had been misused on the most serious occasion in the previous 12 months. The two top reasons were the same as reported in 2013—namely, to purchase something (35.8%) and to obtain money from a bank account (excluding superannuation) (24.8%). In 2014, the third most prevalent way in which information had been misused was to file a fraudulent tax return (5.6%), while the misuse of information to apply for a loan or to obtain credit declined by 3.1 percent between 2013 and 2014. Di Marzio's (2012) earlier survey found that 59 percent of respondents believed that their identity information had been used to purchase goods or services and a further 31 percent believed that it had been used to obtain finance, credit or a loan.

Participants who indicated that their personal information had been misused to purchase something were asked to specify what was purchased. The most commonly purchased items included were consumer electrical goods (n=21), airfares and travel (n=16), fashion items (n=15) and

for gambling (n=7), the last two of which were more prevalent in 2014 than in 2013.

Participants were asked how they became aware of the misuse of their personal information on the most serious occasion in the previous 12 months. The clear top ways included receiving notification from a bank or financial institution and/or credit card company (38.9%, down from 43.4% in 2013) and noticing suspicious transactions in a bank statement or account, which produced an identical result to the previous year (33.3%). This was similar to the results of the NCVS in the United States, which found that among victims who experienced the unauthorised use of an existing account, 45 percent discovered the identity theft when a financial institution contacted them about suspicious activity on their account. By comparison, 15 percent of victims who experienced the misuse of personal information to open a new account or for other fraudulent purposes discovered the incident when a financial institution contacted them. Victims of these other types of identity theft were more likely than victims of existing account misuse to discover the incident when another type of company or agency contacted them (21%) or after they received an unpaid bill (13%). Twenty percent of victims of existing account misuse discovered the incident because of fraudulent charges on their account, compared with eight percent of victims of other types of identity theft (Harrell & Langton 2013). In the AIC's identity crime surveys, by way of comparison, between 2013 and 2014, there was a 6.1 percentage point decline in individuals becoming aware of misuse after receiving from an organisation a bill for which they were not responsible.

Participants 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 they were able to recover from banks and any costs associated with repairing what occurred). No out-of-pocket losses were experienced by 222 participants (49.8%), up from 43.5% in 2013. The remaining participants experienced losses ranging from \$1 to \$200,000. The mean out-of-pocket loss was \$3,687 and the median loss was \$200.

Participants who had been reimbursed by banks or other organisations, or recovered their losses in

other ways, for the most serious occasion recovered between \$1 and \$60,000. The mean amount recovered was \$1,318 for the most serious occasion in the past 12 months. The total recovered was \$321,653, which was 40.8 percent less than the \$543,514 recovered in 2013, although these amounts could have related to losses suffered in previous years.

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. Prior research in Australia and overseas has generally presented only simple descriptive statistics without statistically testing the presence and power of relationships between variables. As such, it was not generally possible to compare the statistical test results obtained in the present study with some of the findings from previous studies.

Previous studies

Di Marzio Research's (2012) survey found statistically significant relationships at the 95 percent confidence level for victimisation ('over the past six months or so') and gender, age categories and state of residence. 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.

The 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 (7% of those living in households earning less than \$25,000 versus 15% of those living in households earning more than \$100,000). The OAIC (2013) 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. It was also found that younger Australians were the least likely to think that they may become the 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%).

In the United States, the NCVS found that a similar percentage of males and females (7%) had experienced identity theft in 2012, and that across all types of identity theft, prevalence rates did not vary significantly by sex. After accounting for whether a person owned a credit card and bank account, prevalence rates for existing credit card and existing banking account misuse did not vary by sex. In terms of age, it was found that persons aged 16 to 17 years (less than 1%) were the least likely to experience identity theft, followed by persons aged 18 to 24 years (5%) and 65 years and above (5%). After accounting for credit card ownership, persons aged 16 to 24 were the least likely to experience the misuse of an existing account, while persons aged 65 years and above had a prevalence rate similar to persons aged 25 to 34 years. Among those who had a bank account, persons aged 16 to 17 years and 65 years and above were the least likely to experience bank account fraud. Overall, persons in the highest income category (those with an annual household income of US\$75,000 or more) had a higher prevalence of identity theft than persons in other income brackets. After accounting for credit card ownership, persons in the highest income bracket had the highest rate of existing credit card account misuse. Among persons who had a bank account, there were no significant differences in the prevalence of identity theft across income categories, with the exception of the unknown category (Harrell & Langton 2013).

AIC identity crime survey findings

A statistically significant relationship was found between experiencing misuse of personal information in the previous 12 months and Indigenous status (*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.

A significant relationship was also found between individual gross income category and experience of misuse of personal information in the previous 12 months. Those in the lowest income category (\$18,200 and under) were less likely to experience misuse of their personal information and those earning \$37,001 and above were more likely to experience misuse.

A significant relationship was also found between perceptions of the seriousness of misuse of personal information and experiencing misuse of personal information in the previous 12 months, with those who had experienced misuse of personal information in the previous 12 months being more likely than expected to perceive that risks would increase in future.

Only one significant relationship was found in 2014 between place of normal residence and the place from which personal information had been obtained for respondents who had experienced misuse of their personal information in the previous 12 months. It was found that respondents 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 from the theft of their mail. This differed from the findings in 2013, when it was found that respondents located outside a capital city were significantly more likely than those in a capital city to have had their personal information lost or stolen from a business or other organisation (i.e. a data breach) and also that respondents located outside a capital city were significantly more likely than those in a capital city to have had their personal information obtained from a website other than social media (eg during online shopping).

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, Indigenous status or individual gross income.

There was, however, a significant relationship between respondents' age categories and the amount of financial loss. Further analysis of the

relationship between age, gender and amount of financial loss showed that gender was not statistically significant when controlling for age.

A significant positive relationship was also found between financial loss and the number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent. This meant that the higher the financial loss, the more time and money were spent dealing with the consequences—as one might expect—and this confirms the same finding observed in 2013.

Variables that were found in 2014 not to have a significant relationship with misuse of personal information in the previous 12 months included place of normal residence, age group, gender, the number of hours spent on a computer or computerised device and language spoken at home. In 2013, a significant relationship was found between financial loss and language spoken at home, with those who spoke English having lost significantly more than those who spoke a language other than English at home, but this was not confirmed in the 2014 findings.

Conclusions

Misuse of personal information and identity crime continue to be of concern for government policymakers, business security analysts and academic researchers, as evidence continues to accrue of the extent and impact of the problem globally. The present report adds to this developing body of knowledge by documenting the nature and extent of criminal misuse of personal information among a large sample of Australians surveyed in May 2014. Information was obtained concerning their perceptions of the risks they face of misuse of personal information and the extent to which they have suffered victimisation. The results indicate that identity crime continues to affect many Australians, with substantial financial and other impacts occurring each year.

The risk environment

The 2014 survey found a similarly high level of concern among respondents to that identified in the

2013 survey regarding misuse of personal information. In both 2013 and 2014, more than two-thirds of respondents believed that misuse would increase over the next year. This level of concern is, however, at odds with the actual reported incidence of victimisation, with less than one-quarter of respondents reporting lifetime experience of victimisation and approximately 9 percent reporting misuse in the 12 months prior to the 2014 survey. Although these levels of victimisation differ from previous Australian and overseas research, there is a need to publicise the results of the present survey so that perceptions more accurately reflect the actual levels of victimisation experienced in Australia.

Identity crime impact and harms

In terms of harms caused by misuse of personal information, the survey found that approximately half of those who had experienced misuse suffered out-of-pocket financial losses totalling more than \$850,000, which was 16 percent less than losses reported in 2013. Total losses, however, vary considerably from year to year, particularly when large losses occur in individual cases. Although such losses relate only to the misuse experienced by those who responded to the survey, this level of financial impact is high. In addition, respondents identified a range of other non-pecuniary impacts including being refused credit, experiencing mental or emotional stress requiring counselling or other treatment, and being wrongly accused of a crime. In addition, some victims were denied access to their credit cards, bank accounts and utility accounts, and one victim said that police ‘came to arrest me’. The experience of victimisation also resulted in more than 90 percent of respondents changing their behaviour in some way, including changing passwords, losing trust in people and even changing their place of residence. Such impacts can have important consequences for personal wellbeing as well as confidence in the online marketplace. Ideally, potential victims of crimes of this nature need to be supported in dealing with the consequences of their victimisation and, more importantly, in avoiding victimisation in the first place and re-victimisation.

Responses

As occurs with other types of fraud, for this the levels of reporting to official agencies, including law enforcement agencies, continued to be low, although respondents were generally satisfied with the outcomes when they reported to some government agencies and financial institutions. There was a small (1.2%) increase in those who failed to make any reports between 2013 and 2014, while overall there was an increase in reporting to government and business. Of concern is the 35 percent of respondents who said that they did not know how or where to report the matter, which increased from the 21 percent who gave this reason for non-reporting in 2013. Future survey results could see an improvement in respondents reporting identity crime following the implementation of the Australian Online Crime Reporting Network (ACORN) in late 2014.

Incident and victim characteristics

The present research also explored the circumstances of the most serious occasion on which misuse had occurred during the previous year. It was found that personal information was most often misused in connection with online commercial transactions, particularly card fraud. Online banking, social media and card-based transactions were thought to have been most often the source of misuse, with stolen information most often used for commercial purchases. There were few changes of this kind reported between 2013 and 2014, although personal information obtained from an ATM or EFTPOS transaction declined by almost five percentage points between 2013 and 2014.

In terms of the characteristics of victims, a number of statistically significant relationships were evident in the data. Those who identified as Indigenous were more likely than others to experience misuse of their personal information, while those in the lowest income category (\$18,200 and under) were less likely to experience misuse, and those earning \$37,001 and above were more likely to experience misuse. Those who resided in a capital city were significantly more likely than those who did not to have their personal information obtained from the theft of their mail, while age category and the

amount of financial loss were associated. Finally, it was found that the higher the financial loss, the more time and money were spent dealing with the consequences of misuse. Variables that were found in 2014 not to have a significant relationship with misuse of personal information in the previous 12 months included place of normal residence, age group, gender, the number of hours spent on a computer or computerised device and language spoken at home.

Further research would be required to understand fully the reasons for these relationships. Smith & Jorna (2011) have explored some of the vulnerabilities to fraud of those living in regional and remote communities, including their lower levels of income and financial literacy, as well as their increased reliance on online services owing to face-to-face transactions being less available. Other areas to explore could include the possibility that people living in rural areas might have higher levels of trust when using online transactions than those in cities, while at the same time having less knowledge of the security weaknesses of the technologies they use. Or perhaps it might also be the case that rural, remote and Indigenous respondents were more willing to report the circumstances of their victimisation, perhaps being less concerned about embarrassment when reporting. Some of these findings might also be an artefact of the survey sampling frame and methodology used. As suggested in 2013, qualitative research through the use of in-depth interviewing would help to understand and explain the findings presented in this report in more depth.

The results of this survey confirm the findings of the AIC's survey in 2013 that misuse of personal information remains an enduring form of criminal activity in Australia. Although in many respects the findings in 2014 confirm those obtained in 2013, there are a number of subtle changes that may be indicative of improvement, and also deterioration, in the identity crime risk environment in Australia that warrant further attention.

References

All URLs correct at April 2015

Attorney-General's Department (AGD) 2014. *Identity crime and misuse in Australia—Key findings from the National Identity Crime and Misuse Measurement Framework Pilot*. Canberra: Attorney-General's Department. <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx>

Attorney-General's Department (AGD) 2012. *The National Identity Security Strategy 2012*. Policy paper. Canberra: Attorney-General's Department

Australian Bureau of Statistics (ABS) 2014. *Australian demographic statistics, Dec 2013*. ABS cat. no. 3101.0. Canberra: ABS. <http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/FA627CA7C5708380CA257D5D0015EB95?opendocument>

Australian Bureau of Statistics (ABS) 2012. *Personal fraud 2010–2011*. ABS cat. no. 4528.0. Canberra: ABS. <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4528.0Main+Features12010-2011?OpenDocument>

Australian Bureau of Statistics (ABS) 2011. *Australian standard classification of languages*, 2nd edn. ABS cat. no. 1267.0. Canberra: ABS. <http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/1267.02011?OpenDocument>

Australian Bureau of Statistics (ABS) 2008. *Personal fraud, 2007*. ABS cat. no. 4528.0. Canberra: ABS. [http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/\\$File/45280_2007.pdf](http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf)

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

Australian Payments Clearing Association (APCA) 2014. *Australian payments fraud details and data*. Sydney: APCA. <http://apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2014.pdf>

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

Emami C and Smith RG 2015. *Identity crime and misuse in Australia 2013–14*. Canberra: AIC/AGD.

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>

Jorna P 2015. *Australasian Consumer Fraud Taskforce: Results of the 2013 online consumer fraud survey*. Technical and Background Paper no. 58. Canberra: Australian Institute of Criminology. http://aic.gov.au/media_library/publications/tbp/tbp058/tbp058.pdf

Jorna P & Hutchings A 2013. *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey*. Technical and Background Paper no. 56. Canberra: Australian Institute of Criminology. <http://aic.gov.au/publications/current%20series/tbp/41-60/tbp056.html>

National Fraud Authority (NFA) 2013. *Annual fraud indicator*. London: NFA. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

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 of the Australian Information Commissioner (OAIC) 2007. *Community attitudes to privacy survey: Research report 2007*. Canberra: OAIC

Smith RG 2014. Transnational cybercrime and fraud, in Reichel P & Albanese J (eds), *Handbook of transnational crime and justice*, 2nd edn. New York: Sage Publications: 119–142

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 & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey*. Research and Public Policy Series paper 128. Canberra: Australian Institute of Criminology

Smith RG & Jorna P 2011. Fraud in the 'outback': Capable guardianship in preventing financial crime in regional and remote communities. *Trends & Issues in Crime and Criminal Justice* no. 413. Canberra: Australian Institute of Criminology. <http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi413.html>

Smith RG, Brown R & Harris-Hogan 2015. Identity crime and misuse in Australia: Results of the 2014 online survey. *Research and Public Policy Series paper*. Canberra: Australian Institute of Criminology

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

Veda 2014. *Australia's view of personal information security. The consumer security survey*. Sydney: Veda Group

Appendix 1: Identity crime and misuse survey 2014

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), 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;
- Your experience of, and willingness to use biometric technologies to protect your personal information; and
- Some information about your: age, gender, residence, income, language at home, Indigenous background and computer usage.

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: info@i-linkresearch.com or by calling (02) 9262 7171.

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 early in 2014, at www.aic.gov.au. You can obtain further information from [] who is in charge of the study. You can also obtain further information or make a complaint about the study by contacting [].

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

Other

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 2013–2014 (i.e. 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 _____

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), 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 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? \$_____

Q14) 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, and how satisfied are you with the outcome? (Select all that apply)

Organisation	Select if no report was made to:	Select if a report was made to:			
		Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
The police					
A consumer protection agency (e.g. 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 (e.g. Visa or MasterCard) or an e-commerce provider (e.g. PayPal)					
A credit reporting agency (e.g. Veda or Dun and Bradstreet)					
Your internet service provider					
A utility company (e.g. gas, electricity, telephone, water etc.)					
A media organisation					
Others (please specify)					
1. _____					
2. _____					
3. _____					

Q17a) If you did NOT report the misuse of your personal information to a government agency or a business organisation, please indicate why (select all that apply)

I did not know how or where to report the matter

I was too embarrassed to report it

I did not believe it was a crime

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

Other (please specify) _____

Q18) As a direct result of having had your personal information misused, in what ways has your behaviour changed? (select all that apply)

I am more careful when I use or share personal information

I changed my password(s)

I changed my social media account(s)

I changed my email address(is)

I changed my banking details

I changed my telephone number(s)

I changed my place of residence

I use better security for my computer or other computerised devices

I lock my mailbox

I redirect my mail when I am away or move residence

I use a registered post box

I shred personal documents before disposing of them

I review my financial statements more carefully

I applied for a copy of my credit report

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

I don't trust people as much

Other (please specify) _____

My behaviour has not changed

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

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

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)
- 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 (e.g. 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 (e.g. Facebook, Linked-in etc.)
- From information you placed on a website (other than social media, e.g. online shopping)
- From an ATM or 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 (e.g. 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? \$_____

Q24a) In order to prevent misuse of your personal information in the future, would you be willing to use any of the following technologies?

Q24b) Please also indicate if you have 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)

Technology	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.)	Select if you have ever used this technology in the past, in any way
Passwords		
Signatures		
Voice recognition		
Fingerprint recognition		
Facial recognition		
Iris recognition		

Q-25 Did you participate in the I-Link Identity Crime Survey in 2013?

Yes

No

Don't know

Thank you for your time in answering these questions.

AIC Reports Research and Public Policy Series 130

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

aic.gov.au