Australian Government
Australian Institute of Criminology

Identity crime and misuse in Australia: Results of the 2013 online survey

Russell G Smith
Alice Hutchings

AIC Reports
Research and Public Policy Series 128

Identity crime and misuse in Australia: Results of the 2013 online survey

Russell G Smith
Alice Hutchings

AIC Reports
Research and
Public Policy Series
128

This report was funded by the Commonwealth Attorney-General's Department (AGD), as part of broader work under the *National Identity Security Strategy* to develop a national identity crime measurement framework.

aic.gov.au

ISSN 1836-2060 (Print)1836-2079 (Online)
ISBN 978 1 922009 66 1 (Print) 978 1 922009 67 8 (Online)

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

Identity crime and misuse of personal information affect all sectors in Australia and cost individuals, business and government many millions of dollars annually. In the public sector, the misuse of personal information has been recognised in income tax evasion, customs duty and GST fraud, superannuation fraud, obtaining welfare and health care benefit fraud achieved through the use of false names, immigration fraud and taking English language tests (a key requirement for visas) for someone else. In the private sector, the problem areas have been identified as opening bank accounts in false names to obtain finance, ATM fraud, online and mobile banking and payment card fraud, funds transfer fraud, and securities and investment fraud. In addition to these and other financial crime risks, misuse of identity can also arise in connection with violent crime, such as where individuals have sought to avoid detection and prosecution for murder, robbery and acts of terrorism by pretending to be someone else.

In May 2013, in order to explore the nature and scope of identity crime and misuse in Australia, the Australian Institute of Criminology was commissioned by the Attorney-General's Department to undertake a national survey. This project is one of a series of initiatives that are 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.

Subsequently, the Australian Institute of Criminology used an online research panel to generate a sample of 5,000 Australians aged 15 years and over to measure personal experiences of identity crime. The survey covered 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.

This report presents the results of the survey. The findings confirm prior research that has found that identity crime affects a relatively high proportion of Australians who report substantial financial and other impacts. Raising awareness of the risks that individuals face, and gathering sound statistical data on the problem, is an effective way to address the problem. In order to monitor changes from year to year in the nature and extent of identity crime, it is proposed that this survey will be replicated on a regular basis.

Dr Adam Tomison
Director

Acknowledgements

The present research was commissioned and funded by the Australian 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 present 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.

At the Australian Institute of Criminology, Dr Rick Brown, Jason Payne and Georgina Fuller provided advice and assistance with data analysis, particularly in relation to data weighting. Penny Jorna also assisted with data analysis.

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

Contents

Tables

Figures

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
AGD	Australian Government Attorney-General's Department
AIC	Australian Institute of Criminology
APWG	Anti-Phishing Working Group
COAG	Council of Australian Governments
HIN	Shareholder Identification Number
NCVS	United States National Crime Victimization Survey
NISS	National Identity Security Strategy
OAIC	Office of the Australian Information Commissioner
PIN	personal identification number
TFN	tax file number

Executive summary

Prior research by the Australian Bureau of Statistics (ABS) (2012) has shown that over 700,000 Australians, or approximately four percent of the population aged 15 years and over, fell victim to identity fraud in 2010–11. Criminal misuse of identity not only impedes consumer activity and confidence in the financial system, but costs business and government substantial sums in responding to and preventing these crimes.

The advent of the internet and online commerce has substantially expanded the opportunities that exist for the commission of identity crime and the Australian Government has responded by developing a *National Identity Security Strategy,* which was endorsed by the Council of Australian Governments (COAG) in 2007. In May 2013, the Australian Institute of Criminology (AIC) was commissioned by the Australian Government Attorney-General's Department (AGD) to undertake a large-scale survey to determine the extent and impact of identity crime and misuse in Australia. This report presents the results of the survey—respondents' experiences of victimisation for the 12 months prior to the survey and their perceptions of the risk of identity crime in the following 12 months. The survey was administered in September 2013.

Definitions

Rather than ask respondents about their experience of *identity crime*, a concept that can be problematic in terms of precise definition, this survey asked about the misuse of various types of *personal information*. This was defined as including misuse of an individual's name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, 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 September 2013, 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 of the ABS (2013). 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 be 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. The results of five respondents were

removed from the sample as they did not normally reside in Australia and therefore were not eligible to participate, leaving a final sample of 4,995 for analysis.

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 (68.8%) of respondents believed that misuse of personal information was *very serious* and a further 27.8 percent believed it was *somewhat serious*.

When asked if they thought the risk of someone misusing their personal information would change over the next 12 months, 19.8 percent believed it would increase greatly and 45.4 percent believed it would increase somewhat. Only one percent believed that the risk would decrease somewhat or greatly.

Both of these levels of perception concerning seriousness and likelihood of change were higher than similar findings reported by Di Marzio Research (2012) and the Office of the Australian Information Commissioner (OAIC) (2013), although the questions asked and sampling frames employed in these two earlier surveys were different from those of the present study.

Experience of misuse of personal information

The present survey found that 20.8 percent of the 4,995 respondents reported misuse of their personal information at some time during their life, with 9.4 percent reporting misuse of their personal information in the previous 12 months.

The number of separate occasions upon which participants believed that their personal information had been misused ranged from one to 20 occasions. Just over half of the participants (53.7%) believed that their personal information had been misused on a single occasion only.

This level of victimisation is somewhat lower than the lifetime prevalence rate of 27 percent of respondents to the National Fraud Authority's (2013) survey of identity fraud in the United Kingdom, but higher than the 8.8 percent of respondents in the United Kingdom who reported experiencing identity fraud in the year 2012. It is also higher than the United States *National Crime Victimization Survey* (NCVS) lifetime prevalence rate of 14 percent and the 12 month prevalence rate of 6.7 percent (Harrell & Langton 2013). The present survey's lifetime prevalence rate of 20.8 percent is also much higher than the 13 percent lifetime rate of identity fraud reported by respondents to the OAICs (2013) survey. 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 last 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 occurred. Almost half (n=210, 45.7%) were not left out-of-pocket. The remaining 250 participants experienced losses that, when weighted, ranged from $1 to $310,000 (mean=$4,101, median $247, SD=$34,062). It was found that over three-quarters (75%) of participants experienced losses of up to $1,000, with some reporting the much higher amounts. Total losses amounted to $1,025,250.

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, had recovered between $2 and $310,000. When the data were weighted, the mean amount reimbursed or recovered was $2,381 and the median amount reimbursed or recovered was $300 (SD=$23,478, n=255). It was found that most participants received reimbursement or recovery of small amounts with

few receiving much higher amounts. The total reimbursed or recovered during the last 12 months was $607,164. The remaining 205 participants (44.6%) did not receive any reimbursement or recover any losses.

In addition to suffering out-of-pocket expenses, some participants experienced other consequences, the most frequent of which were having been refused credit (14.1%), experiencing mental or emotional stress requiring counselling or other treatment (10.7%) and having been wrongly accused of a crime (5.5%).

Participants reported having spent between zero and 500 hours dealing with the consequences of having had their personal information misused over the previous 12 months (mean=18.1 hours, SD=49.5 hours), with 95 percent of respondents spending 60 hours or less. In addition, 56.1 percent of respondents indicated that they had incurred costs dealing with the consequences of having had their personal information misused over the previous 12 months ranging from $1 to $60,000. Half (50.4%) of those who had spent money spent $40 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 3.4 percent (n=168) of respondents indicated that they were aware of victim certificates and had applied for one. It is possible that this question was misunderstood and participants may instead have believed that they were being asked about other actions they could have taken, such as having fraudulent information removed from their credit information file. To date, statutory victim certificates have rarely been applied for and certainly not to the extent reported in this survey (Personal communication, Attorney-General's Department, September 2013).

Reporting the misuse of personal information

Of those who experienced misuse of their personal information, 8.9 percent did not report it in any way, 53.5 percent told a friend or family member, 7.8 percent told a government agency or a business organisation and 29.8 percent told a friend or family member, as well as a government agency or business organisation.

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 the response provided by Medicare Australia (91.7% responded either *satisfied* or *very satisfied*), an internet service provider (91.3%) and a bank, credit union, credit/debit card company or e-commerce provider (89.1%).

In terms of the reasons for not reporting, 39.5 percent of respondents did not report the misuse of their personal information because they did not believe anything could be done about it, 23.6 percent were too embarrassed to report it, 23.1 percent did not know how or where to report the matter and 12 percent did not believe it was a crime.

Behavioural changes arising from the misuse of personal information

Participants were asked how their behaviour had changed as a direct result of having had their personal information misused. The top five behavioural changes were changing passwords (48.5%), being more careful when using or sharing personal information (48.1%), changing banking details (42.5%), reviewing financial statements more carefully (39.6%) and not trusting people as much (39.0%). A minority (5.9%) of participants who experienced misuse of their personal information in the previous 12 months indicated that this did not result in any behavioural changes.

These types of behavioural changes are similar to those identified by the ABS (2008) *Personal Fraud Survey 2007,* 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 the last 12 months. 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 (52.3%), name (40.2%) and bank account information (31.1%).

Participants were asked how they believed that their personal information had been obtained for the most serious occasion of identity crime in the previous 12 months. The top five ways were from theft or hacking of a computer or other computerised device (20.0%), from an online banking transaction (19.5%), by email (18.3%), from information placed on a website other than social media, such as online shopping (15.7%), and from an ATM or EFTPOS transaction (11.0%).

Participants were asked how they believed that their personal information had been misused on the most serious occasion in the previous 12 months. The top three reasons were to obtain money from a bank account (excluding superannuation; 35.4%), to purchase something (32.5%) and to apply for a loan or obtain credit (8.1%).

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 airfares and travel, and electronic devices, such as computer equipment and mobile phones.

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 were receiving a notification from a bank or financial institution and/or credit card company (43.4%), noticing suspicious transactions in a bank statement or account (33.3%) and receiving a bill from a business or company for which they were not responsible (13.5%).

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). No financial loss was experienced by 200 participants (43.5%). The remaining 260 participants experienced losses ranging from $1 to $310,000. When these data were weighted, for those who suffered a loss, the mean financial loss was $4,816, the median loss was $200.00 (SD=$30,541.36). It was found that over three-quarters (75%) of participants experienced losses of up to $800, with few reporting the much higher amounts. The total lost in the most serious occasion was $1,252,177.

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 $310,000. When weighted, the mean amount recovered was $2,209.41, the median recovered was $227.00 (SD=23,944.16, n=246). It was found that most participants received reimbursement or recovery of small amounts with few receiving much higher amounts. The total recovered was $543,514.00. The remaining 214 participants (46.5%) did not receive any reimbursement or recover any losses for the most serious occasion in the past 12 months.

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

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

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

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 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 being more likely to perceive it as being *very serious*. Similarly, a significant relationship was 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.

Two significant relationships were found between place of normal residence and the place from which personal information had been obtained in respect of respondents who had experienced misuse of their personal information in the previous 12 months. First, it was found that respondents located outside a capital city were significantly more likely than those who were located in a capital city to have had their personal information lost or stolen from a business or other organisation (ie a data breach). Second, it was found that respondents located outside a capital city were significantly more likely than those who were located 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 that they reported. No significant relationship was found between the amount of financial loss and age, gender, location, income and Indigenous status.

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.

The number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent, were both found to have a significant medium, positive correlation with amount of financial loss, indicating that the higher the financial loss, the more time and money was spent dealing with the consequences.

Conclusion

The results of this survey confirm prior research that misuse of personal information remains a significant form of criminal activity in Australia in 2013. Those individuals who participated in the survey indicated high levels of victimisation, including both financial losses for which they were out-of-pocket and were not compensated by banks and other organisations, and a range of non-financial losses that involved loss of personal time, as well as mental and emotional consequences for which treatment was required, on occasions. 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.

The results of the survey could be used effectively by those charged with devising fraud prevention initiatives in a number of ways. For example, it would be possible to provide targeted information to those most likely to be victimised outlining how they could better protect themselves against identity crime and misuse. Hopefully, such initiatives may result in future surveys of this kind finding reduced levels of victimisation and lower financial and other consequences for Australians in the years ahead.

Introduction

In the 21st century, one of the most pressing international crime problems that confronts developed societies is the creation and use of misleading and deceptive identities (Smith 2011). Identity crime is a complex concept used to refer to a range of methodologies used to commit specific forms of deception and fraud. The creation, theft and misuse of identification evidence lies at the heart of the concept, but the crimes involved invariably entail fraud or obtaining a financial advantage by deception—rather than legislation that proscribes the misuse of personal information itself (Smith 2014, 2011).

Identity crime and misuse of personal information arise in a wide variety of contexts. In the public sector, misuse of personal information has been recognised in income tax evasion, customs duty and Goods and Services Tax fraud, superannuation fraud, obtaining welfare and healthcare benefits achieved through the use of false names, immigration fraud and taking English language tests for someone else. In the private sector, the principal risk areas have been identified as being opening bank accounts in false names and obtaining finance; ATM, online and mobile banking and payment card fraud; funds transfer fraud; and securities and investment fraud. In addition, there are various criminal activities that are reliant on misuse of personal information including money laundering; motor vehicle re-birthing; art and antiquity fraud; obtaining security guard, motor vehicle, boat and shooters' licences in false names or with the use of fabricated evidence of identity; and even avoiding driving demerit points and local government fees. In the realm of violent crime, individuals have historically sought to avoid detection and prosecution for murder, sexual assault and robbery by pretending to be someone else.

In May 2013, the AIC was commissioned by the AGD to undertake a national survey to determine the extent and impact of identity crime and misuse in Australia. Research of this nature is one in a series of initiatives that are being implemented or developed as part of the *National Identity Security Strategy* (NISS; AGD 2012a). COAG endorsed the NISS in 2007 as Australia's national response to enhancing identity security with the purpose of preventing identity crime and misuse, contributing to national security and facilitating the benefits of the digital economy (AGD 2012a, 2012b).

In 2012, COAG reviewed the NISS and identified five guiding principles to shape identity security in Australia in the future. These principles were that:

- protecting the identity information of Australians is a shared responsibility;
- the community's confidence in business and public trust in government is supported by identity security;

- [in order] to deter crime and foster national security, identity security must be based on a risk management approach;
- commonly accepted identity credentials must be supported by strong security measures; and
- identity security needs to be a core feature of standard business processes and systems (AGD 2012a: 3).

These principles were used to develop an overarching framework of responses that have predominantly focused on the enhancement of existing methods, or implementation of improved, automated forms of, both identity document production and authentication. Complementary activity sought to improve community awareness and understanding of identity crime and misuse, including the development of education and awareness materials on the risks of identity crime and misuse, and the preventative approaches that can be taken to minimise that risk.

Four key objectives were chosen as the policy platform to define the 2012 NISS. These objectives were to:

- prevent and deter identity crime and misuse;
- detect and measure identity crime and misuse;
- support Australians recovering from identity theft or loss; and
- enable trusted online business and interactions through stronger identity security (AGD 2012a: 15).

In early 2013, the AIC undertook research to identify a small suite of indicators that could be used to measure the extent of identity crime and misuse (Bricknell & Smith 2013) and the present survey is one of a number of research activities that aims to populate some of the indicators with quantitative data. The aim was to undertake a small-scale online survey to measure the:

- personal experience of identity crime—number of contacts, responses and victimisation incidents;
- manner of contact and response;
- type of identity crime;
- financial loss and other impact;
- reporting and response activities;
- perceptions of risk over the next 12 months;
- perceptions of criminality of identity crime; and
- demographic information—age, gender, residence, urban/regional, income, marital status, education, employment, place of birth, English language usage, Indigenous status, household size, housing.

This report presents the results of the survey undertaken in 2013. It is proposed that the survey will be replicated regularly so that time-series data can be compiled to measure changes in the information gathered from year to year.

Prior research into identity crime and misuse

The use of stolen, fabricated or manipulated identities to commit or enable crime is not a new phenomenon but one in which the potential for falsification and misuse of identity information has been enhanced with the expansion of new technologies (Smith 2011). The scale and impact of these crimes are variable but issues of definition, low reporting rates and inconsistent data recording practices among agencies that detect or deal with these incidents introduces uncertainty around the true prevalence and cost of the problem (Bricknell & Smith 2013).

A number of attempts have been made in Australia in the past to quantify the level of identity crime. The most rigorous, albeit somewhat dated, estimate of the cost of identity crime identified a financial impact of $1.1b (with an estimation error of $130m) for 2001–02 (Cuganesan & Lacey 2003). Thirty-eight percent of that cost was attributable to actual losses incurred ($420m).

Prevalence estimates are more current but only include individual victimisation rates and are based on a narrow set of offences. The ABS' 2010–11 *Personal Fraud Survey* (ABS 2012) estimated that four percent of the Australian population aged 15 years and over (n=702,100) had experienced identity fraud in the 12 months prior to the survey. For the purposes of that survey, identity fraud was defined as 'the theft of personal details without a person's consent…[that] are then used to engage in fraudulent activities…' (ABS 2012: np). The majority of identity fraud victims experienced credit card fraud (n=662,300, or 3.7% of the Australian population); the rest described themselves as

victims of identity theft (n=44,700, or 0.3% of the Australian population).

In 2013, a study commissioned by the OAIC (2013) was undertaken in which respondents were asked (among other things) whether they or someone they know had ever been the victim of identity fraud or theft. Despite the generality of the question, 13 percent of Australians aged 18 years or over claimed they had been a victim themselves and 21 percent knew someone who had been a victim (OAIC 2013). Overall, a third of respondents (33%) had either been a victim or knew someone who had been a victim of identity fraud or theft.

In the United Kingdom, the prevalence of identity crime has been documented and found to be higher than the data reported by the OAIC (2013). In December 2012, the National Fraud Authority (2013) commissioned a survey with a nationally representative sample of 4,213 adults aged 18 years and over in the United Kingdom to understand the prevalence and cost of identity fraud against individuals. The survey found that identity fraud was estimated to cost adult victims in the United Kingdom £3.3b during 2012 and that 8.8 percent (4.3 million) of UK adults had been a victim, with those who actually lost money (2.7 million) losing an average of £1,203 each. Overall, 27 percent of respondents had been a victim at some point in their lives and 19 percent of those a victim before 2012.

In the United States in 2012, a survey concerning identity theft was administered as a supplement to the Bureau of Justice Statistic's NCVS, which collects data on crime reported and not reported to the police against persons aged 12 years and over from a nationally representative sample of households. The Identity Theft Supplement questions collected individual data on the prevalence of, and victim response to, the attempted or successful misuse of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes. Respondents were asked whether they experienced any of these types of misuse during the 12 months prior to the interviews, which were conducted from July 2011 to June 2012. Most of the Supplement questions asked respondents aged 16 years and over about the most recent incident that they had experienced (apart from total financial losses) that related to all incidents experienced during the previous 12 months (Harrell & Langton 2013).

Overall, it was found that 6.7 percent of persons aged 16 and over had been victims of identity theft in the 12 months preceding the interview. In terms of lifetime prevalence, 14 percent of persons aged 16 and over (or 34.2 million persons) experienced one or more incidents of identity theft at some time during their lives. In 2012, 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 total, identity theft victims reported US$24.7b in direct and indirect losses attributed to all incidents of identity theft experienced in 2012. At the time of the interview, 14 percent of victims had experienced personal out-of-pocket financial losses of US$1 or more. Of these 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 (Harrell & Langton 2013).

These NCVS survey results show higher prevalence rates for the preceding 12 months than the ABS (2012) and OAIC (2013) Australian results, but lower than the UK (NFA 2013) findings. In terms of lifetime prevalence, the NCVS survey reported a lower prevalence (14%) than that of the United Kingdom (27%), but similar to Australia (13%; OAIC 2013).

The type of personal information at risk of misuse by identity criminals falls into two categories—life history information and financial information. Examples of the former include details of a person's name, sex, age, address and a variety of numbers used as identifiers when dealing with government agencies and businesses. Examples of the latter include bank account information such as account names, numbers, commencement and expiry dates, and secure numbers and passwords used to conduct secure electronic transactions. In addition, biometric data such as that obtained from fingerprint or facial scanning is a form of personal information that can be misused for the commission of identity crime (Smith 2011).

Personal identification information can be obtained from a variety of sources including accidental data leakage from government or business networks, deliberate harvesting of data through the use of computer hacking, by gathering documents that contain personal information or by social engineering in which individuals are persuaded or tricked into disclosing personal information for subsequent use in criminal activities. Cases of accidental or negligent data leakage that provide a rich source of personal information for potential misuse by criminals continue to be disclosed.

In an attempt to document these sources of illicit personal information each year, Verizon (2013), in collaboration 19 international data providers including the Australian Federal Police, the Dutch National High Tech Crime Unit, the Irish Reporting and Information Security Service, the Police Central e-Crime Unit, the United States Secret Service and others, publishes a report in which the nature and extent of the external forensic investigations that it conducts are quantified. The report found that 621 data breach incidents were recorded in 2012, involving over 44 million compromised records. The highest percentage (92%) of incidents arose from parties external to organisations. More than half (55%) of breaches were tied to organised criminal activity, including identity theft (Verizon 2013).

Arguably, the most successful means of dishonestly obtaining personal information online is through the range of activities known as phishing (APWG 2013). Phishing involves the use of technological means coupled with social engineering designed to trick unsuspecting users of the internet into disclosing personal information in response to an unsolicited request, usually received by email. Once this information has been obtained, criminals may sell it to another person or use it to commit identity fraud.

The growth in the number of phishing attacks has been exponential until recently, where it appears to be declining slightly. The actual number of phishing sites is, however, still substantial. The Anti-Phishing Working Group (APWG), which is an industry association formed in 2003 to eliminate identity theft and fraud that results from phishing and email spoofing, found in its survey of sites during the period April to June 2013, that unique phishing attack reports submitted to APWG reached a high of 20,086 in April, slightly less than the 20,908 in April 2011. The number of unique phishing websites detected by APWG during May 2013 was 44,511, some 26 percent higher than in May 2011 (n=35,213). The United States has remained the country that hosts the most phishing websites (APWG 2013, 2011).

Criminal misuse of identity lies at the heart of most consumer scams, with offenders pretending to be other people or businesses in order to trick the victim into participating in the scam, while at the same time making their own identity hard for police to discover. A good example of this concerns the various advance fee frauds perpetrated globally by a group of West Africans and others since the 1980s. Various offenders began working from Nigeria targeting victims across the globe. Confederates and other fraudsters in other African countries, the United States, Britain, Canada, Hong Kong and Japan then began using the same techniques. The scale of these frauds increased considerably and created a global problem for law enforcement. Email has proved to be an effective way of disseminating advance fee letters, as the true identity of the sender is easy to disguise and original supporting documentation unable to be checked for authenticity (Smith 2014).

Each year since 2007, the AIC has collected information on consumer scams by conducting an online survey of Australians who have received scam invitations during the preceding 12 months. In 2012, a high proportion of respondents reported receiving a scam invitation (95%), with almost a quarter responding in some way. Eight percent reported losing money—approximately $8,000 per person or $846,170 in total. The most prevalent scam type involved fraudulent lotteries, although computer support scams were also prevalent. In terms of delivery methods, email was the most common scam delivery method, with 72 percent of respondents reporting having received a scam this way (Jorna & Hutchings 2013).

Of those survey respondents who identified their gender (98%), 16.5 percent of females and 12.4 percent of males reported victimisation in 2012, while respondents in the age categories '35 to 44 years' and 'over 65 years' reported the highest percentage of victimisation (16.5% of total respondents within those age categories). In 2012, respondents in the income

category $20,000 to less than $40,000 reported the highest percentage of victimisation (20% of total respondents within that income category; Jorna & Hutchings 2013).

In 2012, the Australian Competition and Consumer Commission (ACCC) received 83,803 scam-related contacts, with consumers and businesses suffering just over $93.4m in financial losses. Online shopping scam reports increased by 65 percent since 2011 to over 8,000 contacts and more than $4m in reported losses (ACCC 2013).

In the United States, consumer complaints have been collected annually since 1997 on the Consumer Sentinel Network, which now has over 8 million reports. In the calendar year 2012, 2,061,495 unverified consumer complaints were recorded and classified into 30 categories, with 18 percent relating to identity theft (369,132 complaints). Complaints of identity theft increased 32 percent between 2011 and 2012, and over 128 percent since 2002. Government documents/benefits fraud (46%) was the most common form of reported identity theft, followed by credit card fraud (13%), phone or utilities fraud (10%) and bank fraud (6%). Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (2%). Forty-two percent of identity theft complainants reported whether they contacted law enforcement. Of those victims, 68 percent notified a police department. Fifty-four percent of these indicated that a report was taken (FTC 2013).

In 2011 and 2012, AGD commissioned pilot research to quantify the extent of identity crime and misuse in Australia (Di Marzio Research 2012, 2011). Online surveys were conducted in May 2011 and June 2012 by a marketing and strategic research consultancy firm with samples of 1,200 respondents across Australia, weighted according to census population statistics for age, gender and area. Respondents came from an online research panel provided by My Opinions Australia as part of an annual *Online Omnibus Survey*. In 2011, five percent of respondents indicated that they had had their identity information stolen or misused 'in the last six months or so' and this increased to seven percent in 2012. In 2011, 12 percent reported that someone they knew had been victimised, which increased to 17 percent in 2012. More males than females reported victimisation in both 2011 and 2012 and the most prevalent age category for personal victimisation was 45 to 54 years in 2011 and 25 to 34 years in 2012. In 2011, the highest proportion of personal victims came from Western Australia, while in 2012 the highest proportion of personal victims came from Queensland. The most frequently reported manner of commission in both 2011 and 2012 was through 'loss of credit cards or debit cards' or 'via the Internet through virus or bad software'. The most prevalent way in which personal information was used in both 2011 and 2012 was 'to purchase goods or services' or 'to obtain finance, credit or a loan'. Most respondents in both years believed that victimisation of this nature would increase over the next year.

In 2012, AGD determined that more detailed and comprehensive research should be undertaken with a larger sample size that would better reflect the Australian population. With the resources available, the AIC was able to obtain responses from 5,000 participants drawn from an online panel. More rigorous, nationally representative research is being undertaken by the ABS. The ABS will be including a module on personal fraud in its *National Crime Victimisation Survey* for 2014–15 as part of the ABS' *Multipurpose Household Survey*. The survey will collect data about people's experiences of crime victimisation for a select range of personal and household crimes including personal fraud, although the scope of questions relevant to identity crime and misuse will be more restricted than in the current AIC survey.

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. 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 to pretend 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, personal identification number, tax file number, shareholder identification number, computer and/or other online usernames and passwords, student number and other types of personal information.

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 respect of 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 were developed in consultation with the AGD and the survey was distributed to a number of stakeholders for input and suggestions prior to being deployed. Some of the questions were based

on those contained in other similar surveys that have been conducted in Australia and overseas, in order to enable comparison.

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 a two week period in September 2013.

The survey, which included 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 was undertaken by i-Link Research Solutions, with the de-identified data being 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 (2013) census data. 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 provided by the external provider. Examples of the incentives provided by the provider included:

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

Analysis

Descriptive statistics were used to report the characteristics of the sample and experiences relating to the misuse of personal information. Further analyses were undertaken to examine the relationship between identity crime and misuse and the characteristics of the sample.

As the survey was designed to capture information relating to respondents residing in Australia, respondents who indicated they resided elsewhere were excluded from the sample. In some cases, outliers that did not fit within the range of possible responses were excluded from the analysis. In other cases, where participants provided responses in the free text 'other' response option that fit within the categories that were provided, their response was recoded as appropriate.

Weighting of data

Data were weighted by location to represent the spread of the population in Australia. ABS (2013) data that estimated the June 2012 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 located in Sydney made up 11.01 percent of the sample; however, this location contains 20.55 percent of the Australian population (ABS 2013). 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 be surveyed, as the sampling frame was insufficiently robust to permit such estimations to be undertaken.

Ethical considerations

A number of ethical issues were taken into consideration when developing the research design. These included the need for anonymity of research participants, the requirement to provide informed consent, the ability of participants to withdraw from the research and the potential for the research questions to cause psychological discomfort, particularly as they related to victimisation experiences. Once these concerns were addressed, the project presented a low risk to participants and the research was approved by the AIC's Human Research Ethics Committee.

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

In order to ensure that participants provided informed consent, a plain language statement was provided with the survey. This stated that by completing the survey, participants were consenting to participate in the research. As outlined in the plain language statement, at any stage of the survey participants had the option to opt out of completing the survey and by contacting the external provider, could have the responses they had already provided withdrawn from the dataset.

It was acknowledged that, while the risk of psychological distress associated with the research was minimal, there was the possibility that a participant may have felt discomfort answering questions about victimisation. As the participant chose to complete the survey and there was information explaining what the survey is about, it can be assumed that they were aware of the potential sensitivity of the survey content. Telephone and website details for Lifeline crisis support were also provided in the plain language statement.

Limitations of the research design

Limitations of the research design arose from the sampling procedure, as those who participated in the online panel may not have been representative of the Australian population. For example, those who subscribed to an online panel may have had a higher exposure to online fraud than people in the general population. The survey was also only available to those who had computer access.

It can be difficult to measure victimisation and misuse within a given timeframe as it is not always easy to determine when the offence took place due to the time lapse between when personal information is obtained and when it was misused, when it was identified by the victim, and when, if at all, it was reported.

Survey designs such as this also have problems with reliability (such as whether the same survey delivered to the same subjects would elicit the same responses) and validity (whether the survey is measuring what it was intended to measure).

The circumstances and complexity of identity crime may also make constructing a meaningful survey instrument difficult. Problems of telescoping information (ie including events outside the survey reference period), exaggerating facts or reporting selectively—all common problems with surveys and personal interviewing—can affect the accuracy of information gathered using conventional techniques. There may also be problems of veracity, as individuals may be reluctant to report victimisation where they believe that they personally contributed to the problem, such as by voluntarily providing their personal information.

Alongside the challenges of obtaining good-quality data, there are also problems that stem from the volume of 'hidden' or 'undetected' victimisation. Hidden victimisation may occur due to the level of deception that is involved in an incident, which results in it being undetected, or the full extent realised. The result is that calculations of incidence, financial loss and other impacts can, at best, only be estimates.

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

Results

Characteristics of the sample

In total, 5,000 respondents completed the survey instrument; however, the responses of five individuals were removed as those individuals did not normally reside in Australia and therefore were not eligible to participate. The data were weighted to reflect the distribution of the population across jurisdiction based on ABS (2013) census data. Table 1 shows the breakdown of respondents by place of normal residence. Both the unweighted and weighted numbers are provided to show where the population was over or under-sampled. The differences between the unweighted and weighted numbers reflect the under-sampling of larger jurisdictions and the over-sampling of smaller jurisdictions. For example, respondents whose place of normal residence was Sydney comprised 11.0 percent of the sample; however, this jurisdiction contains 20.6 percent of the Australian population.

Table 1 Respondents by place of normal residence

Location	Multiplier	Unweighted		Weighted	
		n	%	n	%
Sydney	1.867	550	11.0	1,026	20.6
Other New South Wales	1.931	300	6.0	579	11.6
Melbourne	1.440	649	13.0	934	18.7
Other Victoria	1.521	200	4.0	304	6.1
Brisbane	1.150	419	8.4	482	9.6
Other Queensland	1.161	450	9.0	522	10.5
Perth	0.643	649	13.0	418	8.4
Other Western Australia	0.589	200	4.0	118	2.4
Adelaide	0.432	650	13.0	281	5.6
Other South Australia	0.417	200	4.0	83	1.7
Canberra	0.271	304	6.1	82	1.7

Table 1 Respondents by place of normal residence (cont.)					
Location	Multiplier	Unweighted		Weighted	
		n	%	n	%
Hobart	0.239	200	4.0	48	1.0
Other Tasmania	0.382	170	3.4	65	1.3
Darwin	0.724	40	0.8	29	0.6
Other Northern Territory	1.626	14	0.3	23	0.5
Total		4,995	100.0	4,995	100.0

Note: Percentages may not total 100 and weighted figures may not total 4,995 due to rounding

Source: Identity Crime Survey 2013 [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. It is noted that in relation to gender, one participant (0.02%) selected the 'other' category, however, when the data were weighted this represented just 0.01% of the sample.

Table 2 Respondents by gender		
Gender	n	%
Male	2,335	46.8
Female	2,660	53.3
Other	0	0.0
Total	4,995	100.0

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 2013 [AIC data file]

Table 3 Respondents by age		
Age group	n	%
17 years and under	265	5.3
18–24 years	465	9.3
25–34 years	876	17.5
35–44 years	1,024	20.5
45–54 years	936	18.7
55–64 years	733	14.7
65 years and over	697	14.0
Total	4,995	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Weighted figures may not total 4,995 due to rounding

Source: Identity Crime Survey 2013 [AIC data file]

Respondents were asked what language was most often spoken at home. These responses were recoded using the ABS' (2011) *Australian Standard Classification of Languages*, although English has been differentiated from other 'Northern European' languages. Table 4 shows the respondents' weighted distributions by language most often spoken at home.

Table 4 Respondents by language most often spoken at home

Language classification	n	%
English	4,695	94.0
Southern Asian	85	1.7
Eastern Asian	80	1.6
Southeast Asian	40	0.8
Eastern European	31	0.6
Southern European	24	0.5
Northern European	15	0.3
Southwest and Central Asian	12	0.3
Other languages	10	0.2
Australian Indigenous	2	0.0
Total	4,995	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Weighted figures may not total 4,995 due to rounding

Source: Identity Crime Survey 2013 [AIC data file]

Participants were asked if they identified as Aboriginal or Torres Strait Islander. Weighted responses are provided in Table 5.

Table 5 Respondents who identified as Aboriginal or Torres Strait Islander

Aboriginal and Torres Strait Islander status	n	%
Aboriginal	78	1.6
Torres Strait Islander	6	0.1
Both Aboriginal and Torres Strait Islander	5	0.1
No	4,851	97.1
Rather not say	54	1.1
Total	4,995	100.0

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Weighted figures may not total 4,995 due to rounding

Source: Identity Crime Survey 2013 [AIC data file]

Participants were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2012–13. Weighted responses are provided in Table 6.

Table 6 Respondents by individual gross income 2012–13

Income category	n	%
$0–$18,200	1,168	23.4
$18,201–$37,000	1,056	21.1
$37,001–$80,000	1,438	28.8
$80,001–$180,000	624	12.5
$180,001 and over	64	1.3
I'd rather not say	645	12.9
Total	4,995	100.0

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

Source: Identity Crime Survey 2013 [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. Eight responses were omitted as they exceeded the number of hours in a week. Weighted responses ranged from none to 168 (mean=25.8, SD=18.0, n=4,987). As shown in Figure 1, 75 percent of respondents spent 35 hours or less on a computerised device per week, with some respondents spending much longer hours.

Figure 1 Number of hours spent the previous week using a computer or computerised device (unweighted data)

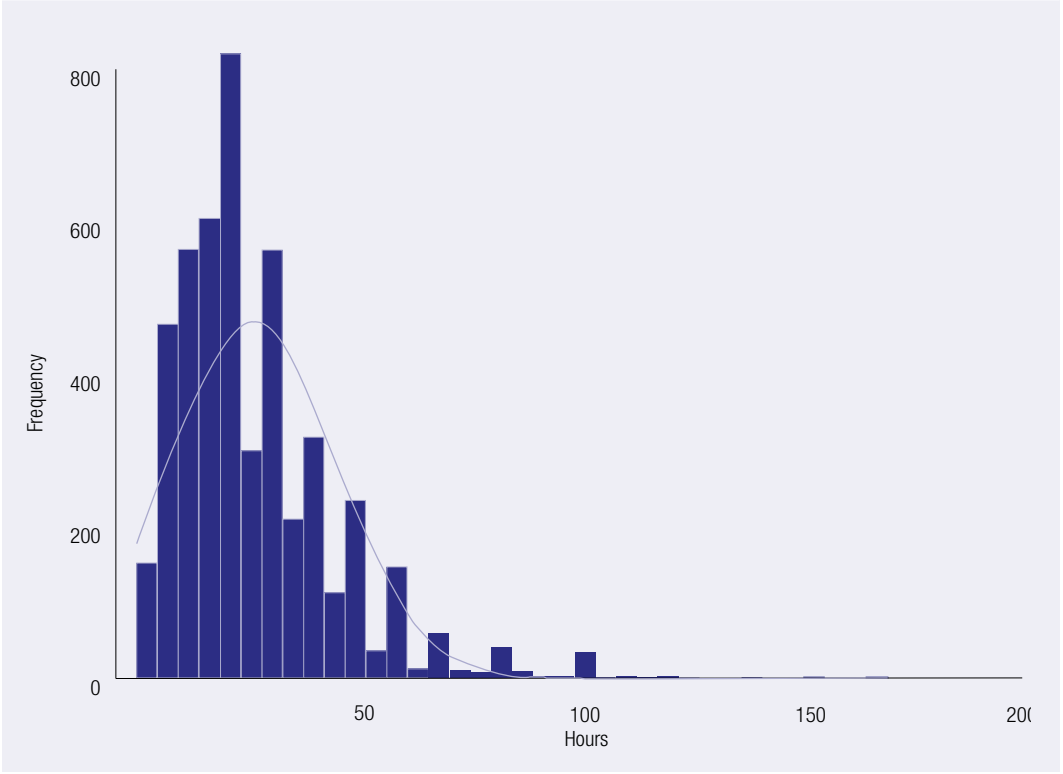
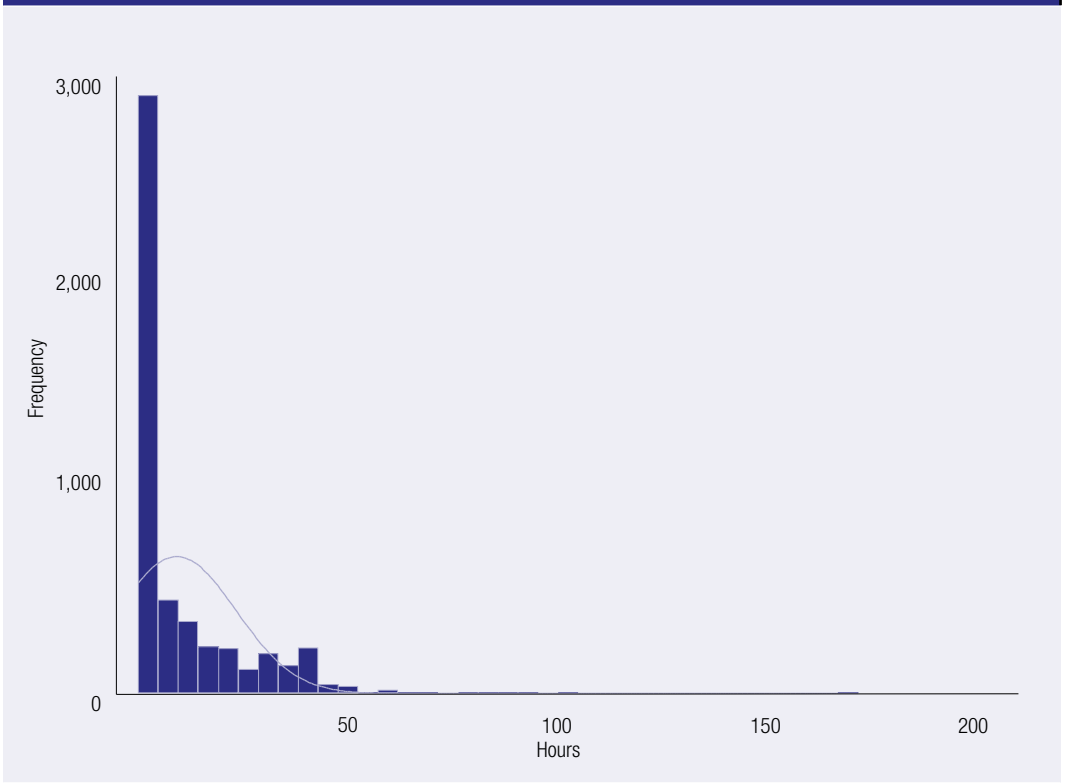


Figure 2 Number of hours spent the previous week using a computer or computerised device for work-related activities (unweighted data)



Source: Identity Crime Survey 2013 [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. Three responses were omitted as they exceeded the number of hours in a week. The remaining weighted responses ranged from none to 168 (mean=9.0, SD=13.4, n=4,992). As shown in Figure 2, the distribution was also positively skewed, with 75 percent 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. Nonetheless, the responses to these questions provide baseline indications of the perceptions of respondents and should the survey be replicated in the future, will indicate changes in perceptions of risk, seriousness and trends.

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 believed the misuse of personal information was *very serious* or *somewhat serious*.

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

Seriousness	n	%
Very serious	3,434	68.8
Somewhat serious	1,390	27.8
Not very serious	147	2.9
Not at all serious	24	0.5
Total	4,995	100.0

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

Source: Identity Crime Survey 2013 [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. 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

Risk of misuse of personal information	n	%
Risk will increase greatly	989	19.8
Risk will increase somewhat	2,270	45.4
Risk will not change	1,690	33.8
Risk will decrease somewhat	23	0.5
Risk will decrease greatly	23	0.5
Total	4,995	100.0

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

Source: Identity Crime Survey 2013 [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 if they had done so in the past. Weighted responses are provided in Table 9.

Table 9 Respondents' awareness of victim certificates

Awareness of victim certificates	n	%
I am aware of such certificates, and have applied for one in the past	168	3.4
I am aware of such certificates, but have not applied for any	557	11.2
I am unaware of such certificates	4,270	85.5
Total	4,995	100.0

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 2013 [AIC data file]

It is noted that the number of respondents (n=168) who reported being aware of victim certificates and had applied for them in the past is low. This percentage (3.4%) does not parallel the number of victim certificates applied for through the court system. It is possible that the question has been misunderstood and participants may have instead believed they were being asked about other actions they could have taken, such as having fraudulent information removed from their credit information file.

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 4,995 respondents, 1,032 (20.7%) had experienced identity misuse at some time. Some of the locations with a smaller population that were oversampled to obtain a larger sample size experienced lower levels of misuse (eg Darwin and Tasmania) and some of the locations with a larger population that were under-sampled experienced higher levels of misuse (eg Sydney and Melbourne). When the data were weighted to correct for this over and under-sampling, the level of lifetime misuse of personal information increased to 20.8 percent (n=1,040) of respondents. While the weighted data allow examination of the prevalence of misuse of personal information based on the surveyed respondents, the unweighted responses demonstrate the prevalence of misuse of personal information by place of normal residence, particularly where the population is relatively small. The unweighted data by place of normal residence are presented in Table 10.

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

Location	n	%
Sydney (n=550)	122	22.2
Other New South Wales (n=300)	60	20.0
Melbourne (n=649)	145	22.3
Other Victoria (n=200)	40	20.0
Brisbane (n=419)	70	16.7
Other Queensland (n=450)	92	20.4
Perth (n=649)	134	20.7
Other Western Australia (n=200)	47	23.5
Adelaide (n=650)	138	21.2
Other South Australia (n=200)	42	21.0
Canberra (n=304)	63	20.7
Hobart (n=200)	37	18.5
Other Tasmania (n=170)	32	18.8
Darwin (n=40)	7	17.5
Other Northern Terrirory (n=14)	3	21.4
Nationally (n=4,995)	1,032	20.7

Source: Identity Crime Survey 2013 [AIC data file]

Participants were also asked about misuse of their personal information in the previous 12 months. For the total sample (n=4,995), 9.2 percent (n=460) of respondents experienced identity misuse in the past 12 months. When these data were weighted to reflect national population distributions, 9.4 percent (n=471) of respondents experienced identity misuse in the previous 12 months. Again, while the weighted data allow examination of the prevalence of misuse of personal information using nationally representative data, the unweighted responses demonstrate the prevalence of misuse of personal information by place of normal residence, particularly for those with smaller populations. The unweighted data by place of normal residence are presented in Table 11.

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

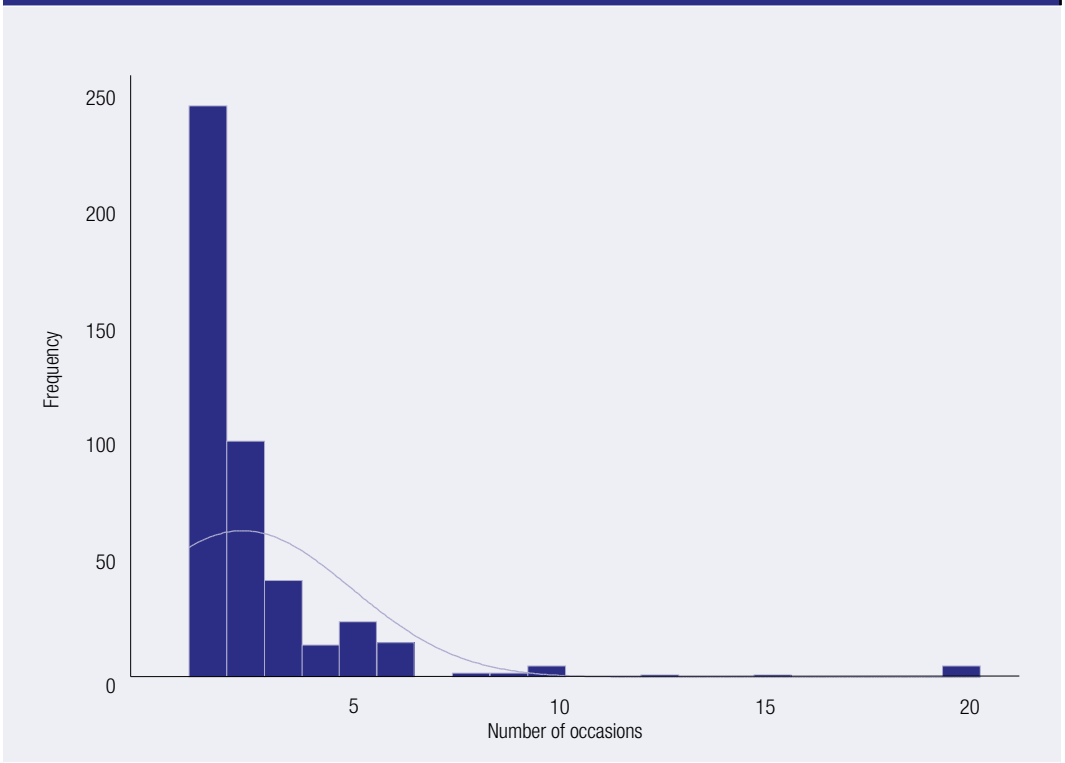
Location	n	%
Sydney (n=550)	55	10.0
Other New South Wales (n=300)	31	10.3
Melbourne (n=649)	67	10.3
Other Victoria (n=200)	13	6.5
Brisbane (n=419)	29	6.9
Other Queensland (n=450)	45	10.0
Perth (n=649)	62	9.6
Other Western Australia (n=200)	19	9.5
Adelaide (n=650)	62	9.5
Other South Australia (n=200)	15	7.5
Canberra (n=304)	26	8.6
Hobart (n=200)	18	9.0
Other Tasmania (n=170)	12	7.1
Darwin (n=40)	4	10.0
Other Northern Territory (n=14)	2	14.3
Nationally (n=4,995)	460	9.2

Source: Identity Crime Survey 2013 [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 Sydney, other New South Wales, Melbourne, other Queensland, Perth, other Western Australia, Adelaide, Darwin and the other Northern Territory. Interestingly, while the first two have the largest populations in Australia, the latter two are included in the locations with the smallest populations, particularly when considering the geographic distances they encompass. Respondents in other Victoria, Brisbane, Hobart and other areas of Tasmania experienced the lowest rates of misuse of personal information over their lifetimes as well as in the previous 12 months.

The 460 respondents who experienced misuse of their personal information within the last 12 months were asked further questions relating to their experience. When the data were weighted, the number of separate occasions that participants believed that their personal information had been misused ranged from one to 20 (mean=2.2, SD=2.4, n=460). As shown in Figure 3, half of the participants (53.7%) believed that their personal information had been misused on a single occasion.

Figure 3 Number of separate occasions participants believed their personal information had been misused (unweighted data)



Source: Identity Crime Survey 2013 [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 last 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 set out in Table 12.

Table 12 Summary statistics for financial losses over the last 12 months

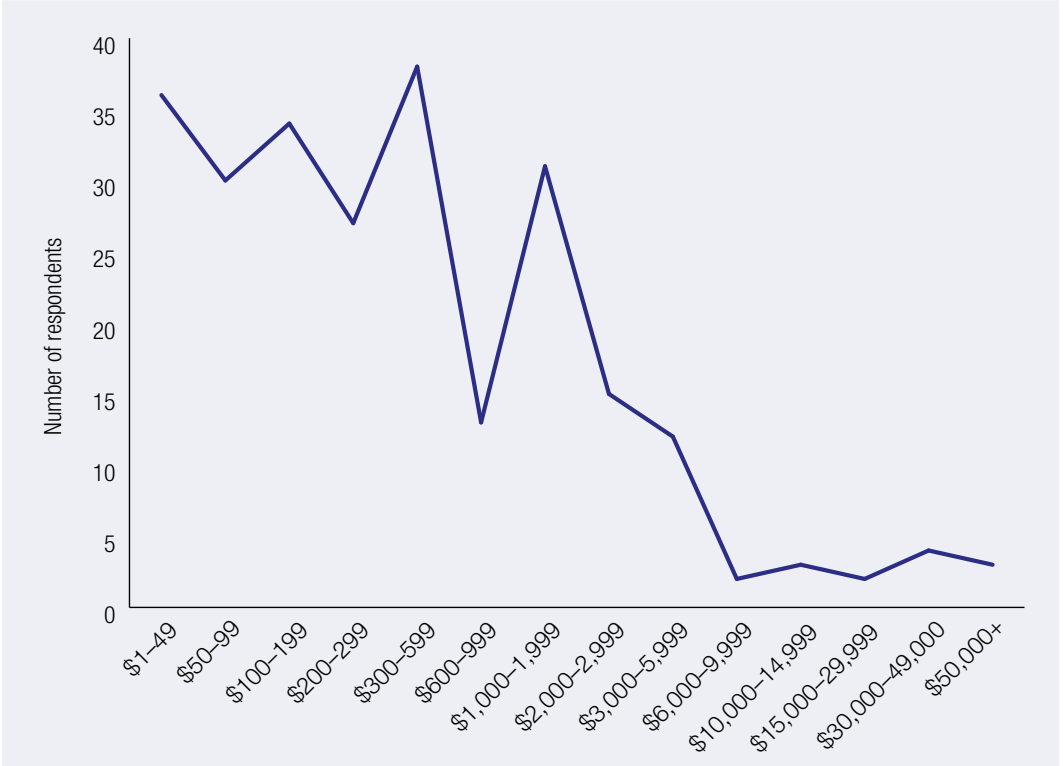
Statistic	Out-of-pocket losses ($)	Recovered ($)
Number of respondents	250	255
Minimum	1	2
Maximum	310,000	310,000
Mean	4,101	2,381
Median	247	300
Standard deviation	34,062	23,478
25% quartile	80	98
75% quartile	1,000	1,000
Total	1,025,250	607,164

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

Source: Identity Crime Survey 2013 [AIC data file]

Almost half (n=210, 45.7%) of the survey participants had not suffered a financial loss. The remaining 250 participants experienced losses that when weighted ranged from $1 to $310,000, with a median loss of $247. The distribution was positively skewed, with the majority of participants experiencing smaller losses. Total losses amounted to $1,025,250. The distribution of out-of-pocket losses suffered by respondents is shown in Figure 4.

Figure 4 Distribution of financial losses experienced in the preceding 12 months (n)

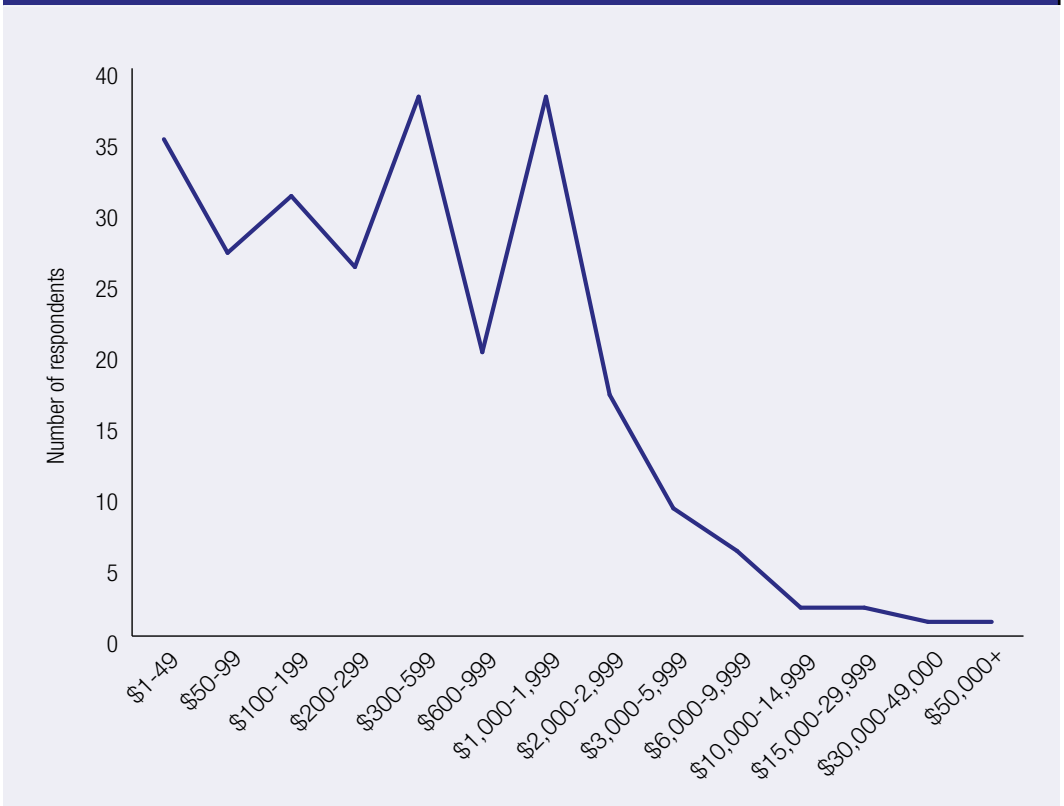


Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2013 [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, had recovered between $2 and $310,000. When the data were weighted, the mean amount reimbursed or recovered was $2,381 and the median amount reimbursed or recovered was $300. The total reimbursed or recovered during the last 12 months was $607,164. The remaining 205 participants (44.6%) did not receive any reimbursement or recover any losses.

Figure 5 Distribution of funds reimbursed or recovered in the preceding 12 months (n)

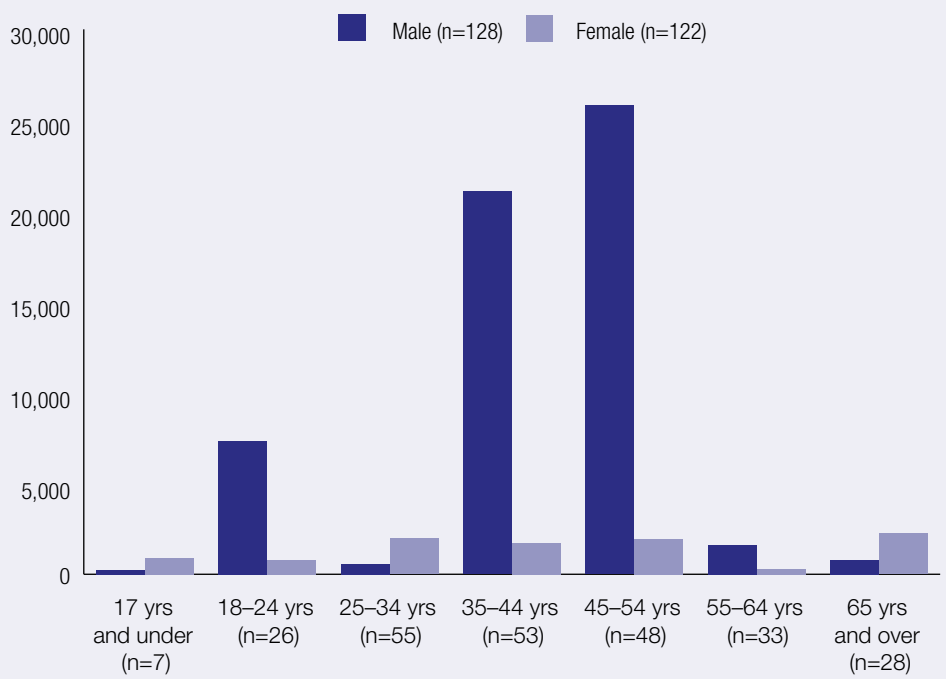


Note: Data were weighted to reflect the distribution of the population across jurisdictions

Source: Identity Crime Survey 2013 [AIC data file]

Figure 6 shows, for those who reported a financial loss (n=250), the average loss by age and gender. It is noted that the one participant who selected 'other' in relation to gender did not report a financial loss. 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 4). Therefore, further analyses are reported later in this chapter to determine the statistical significance of the relationship between amount of financial loss, age and gender.

Figure 6 Average financial loss by age and gender ($)



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

Source: Identity Crime Survey 2013 [AIC data file]

Participants were asked what other negative consequences they had experienced as a result of their personal information having been 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. When the data were weighted, almost half (48.2%, n=222) of the participants did not experience any other negative consequence following misuse of their personal information. Weighted responses for the other consequences that were experienced are provided in Table 13.

Table 13 Consequences experienced as the result of personal information being misused in the previous 12 months (n=460)

Consequences	n	%
I was refused credit	65	14.1
I experienced mental or emotional distress requiring counselling or other treatment	49	10.7
I was wrongly accused of a crime	25	5.5
I experienced physical health problems requiring medical treatment by a doctor	25	5.4
I had to commence legal action to clear debts and/or to clear my name	23	5.0
I experienced financial difficulties resulting in the repossession of a house or land, motor vehicle or other items	22	4.8
I experienced other reputational damage	20	4.4
I was refused government benefits	17	3.8
I was refused other services	10	2.2
Other	83	18.0

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

Source: Identity Crime Survey 2013 [AIC data file]

Participants who had been refused other services were asked to specify the type of service they had been refused as the result of their personal information being misused. These included access to existing credit cards (n=3), bank accounts (n=4), online games (n=1), eBay (n=1), electricity (n=1) and insurance products including health, car and house (n=2). Responses provided by participants in relation to other reputational damage that had been experienced as the result of misuse of personal information included 'criminal charges due to misuse of personal information', 'I was refused housing', 'my credit rating made companies hesitate before allowing me to [buy] products even with a debit card', 'my image was damaged', 'our email account was compromised causing many people on our address list become distressed about their addresses being subject to compromise', 'bullying', 'classed as a fool', 'cost me my job', 'defamation' and 'employer accused me of sharing my passwords with criminals'.

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:

> Police have not found the other person. I was not charged as my identity was used in a different state in Australia.

> Huge sense of mistrust!! Very stressful emotional time!!

> My mobile phone was in police custody under investigation. It was a stressful time for me and left me feeling paranoid and anxious because someone had used my mobile number to threaten someone else's life.

> Mental and emotional stress—no counselling…I am very unhappy!!!

Participants were asked how many hours they had spent dealing with the consequences of having their

personal information misused over the previous 12 months. 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 (mean=18.1, SD=49.5). This distribution was positively skewed, with 95 percent of the respondents spending 60 hours or less and half (50.0%) of the population spending three hours or less. The weighted total number of hours spent dealing with the consequences of personal information misuse was 8,518.9.

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 202 (43.9%) of participants. 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 $60,000 (mean=576.23, SD=3,615.32). It was found that half (50.4%) of the respondents who had spent any money spent $40 or less.

Reporting the misuse of information

Of those who experienced misuse of their personal information, 41 (8.9%) did not report it in any way. A further 246 respondents (53.5%) told a friend or family member, 36 (7.8%) told a government agency or a business organisation and 137 (29.8%) told a friend or family member as well as a government agency or business organisation. 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 173 participants reported a weighted average of 2.1 agencies or organisations about the misuse of their personal information in the previous 12 months (range=1–10, SD=1.6).

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

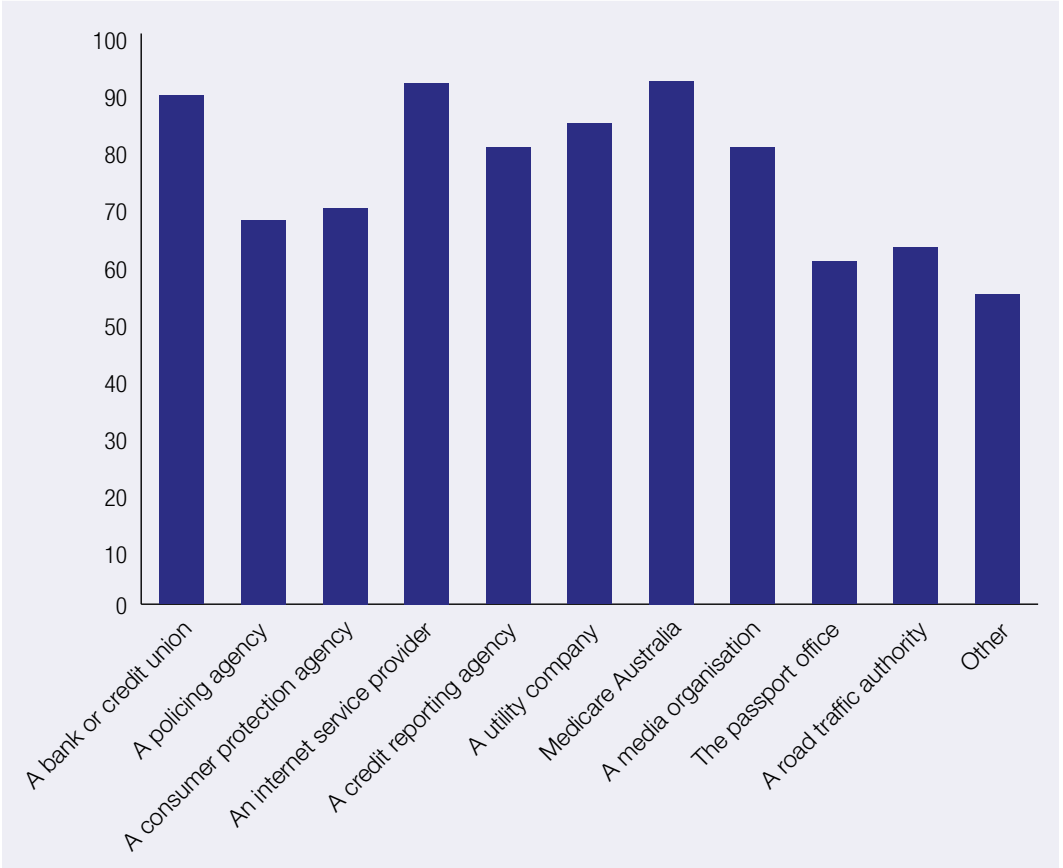
Agency/organisation reported to		Level of satisfaction			
		Very satisfied	Satisfied	Unsatisfied	Very unsatisfied
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal) (n=129)	n	80	35	10	4
	%	62.6	27.2	7.8	2.7
A policing agency (n=49)	n	14	19	10	8
	%	28.3	38.7	20.4	12.6
A consumer protection agency (eg SCAMwatch, Consumer Affairs, Office of Fair Trading) (n=36)	n	11	14	5	5
	%	30.2	39.0	13.0	17.8
An internet service provider (n=23)	n	11	10	2	1
	%	47.0	41.5	8.4	3.1
A credit reporting agency (eg Veda or Dun and Bradstreet) (n=20)	n	9	7	2	2
	%	44.1	34.5	10.4	11.1
A utility company (eg gas, electricity, telephone, water etc) (n=19)	n	7	9	3	1
	%	34.7	45.2	17.1	3.0
Medicare Australia (n=12)	n	4	7	-	2
	%	31.1	54.3	-	14.7
A media organisation (n=10)	n	2	6	2	-
	%	21.3	56.7	17.9	-
The Passport Office (n=10)	n	4	2	4	-
	%	42.3	18.9	38.8	-
A road traffic authority (n=8)	n	2	3	-	3
	%	22.0	36.6	-	41.4
Other (n=35)	n	9	10	10	6
	%	26.3	28.6	27.7	17.4

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 2013 [AIC data file]

Figure 7 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 Medicare Australia (91.7% responded either *satisfied* or *very satisfied*), an internet service provider (91.3%) and a bank, credit union, credit/debit card company or e-commerce provider (89.1%).

Figure 7 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 2013 [AIC data file]

The 41 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. It is noted that participants could select more than one reason for not reporting.

Table 15 Reasons for not reporting misuse of personal information

Reason for not reporting	n	%
I did not believe the police or any other authority would be able to do anything	16.19	39.5
I was too embarrassed to report it	9.68	23.6
I did not know how or where to report the matter	9.47	23.1
I did not believe it was a crime	4.91	12.0
Other	9.05	22.1

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

Source: Identity Crime Survey 2013 [AIC data file]

Reasons for not reporting under *other* included 'no need', 'my head office handled the problem', 'sorted privately' and 'usual data theft'.

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, a minority (5.9%, n=27) of participants who experienced misuse of their personal information in the previous 12 months indicated that this did not result in some behaviour change.

Table 16 Behavioural changes resulting from the misuse of personal information (n=460)

Behavioural change	n	%
Changed password(s)	223	48.5
More careful when using or sharing personal information	221	48.1
Changed banking details	195	42.5
Review financial statements more carefully	182	39.6
Don't trust people as much	179	39.0
Use better security for computer or other computerised devices	174	37.9
Shred personal documents before disposing of them	127	27.6
Changed email address(es)	73	15.8
Changed social media account(s)	63	13.6
Lock mailbox	56	12.3
Redirect mail when away or move residence	44	9.7
Changed telephone number(s)	43	9.4
Applied for a credit report	40	8.8
Use a registered post box	36	7.8
Changed place of residence	33	7.1
Signed up for a commercial identity theft alert/protection service	27	5.8
Other	18	4.0
Behaviour has not changed	27	5.9

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

Source: Identity Crime Survey 2013 [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 (n=460) 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 certainly. Future surveys could include additional questions that assess the level of certainly in terms of evidence on which participants based their answers to these questions.

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 on the most serious occasion in the previous 12 months (n=460)

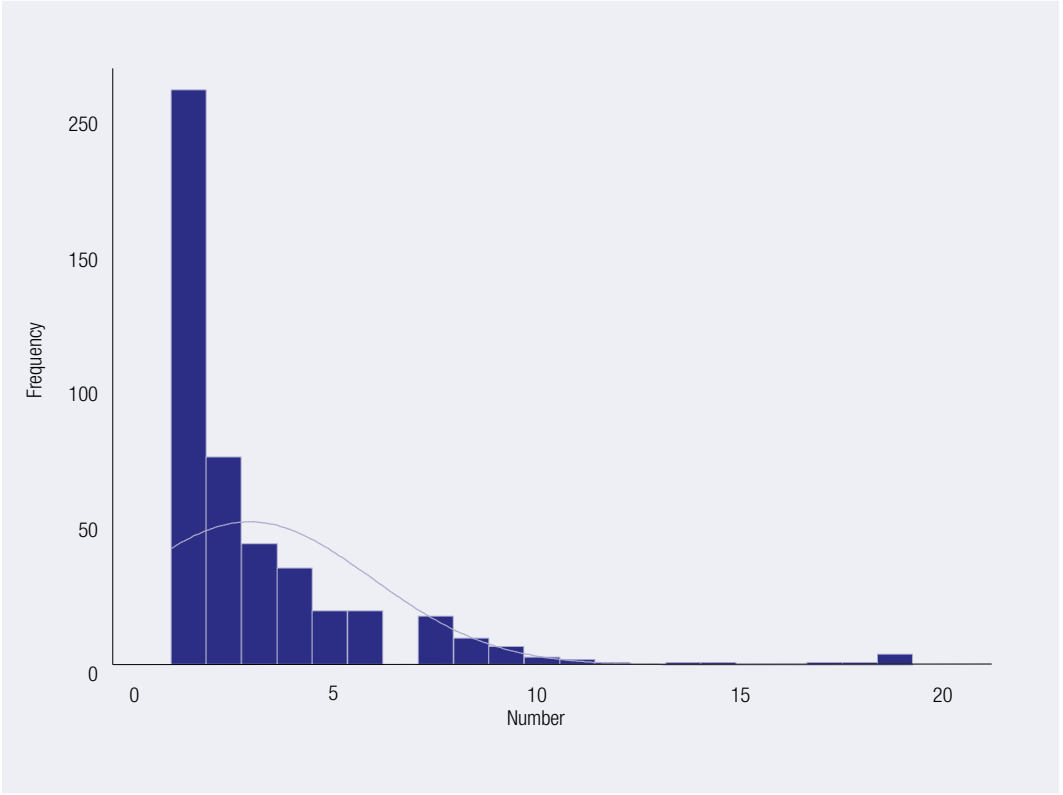
Type of personal information	n	%
Credit/debit card information	241	52.3
Name	185	40.2
Bank account information	143	31.1
Address	113	24.6
Date of birth	101	22.0
Gender	87	18.9
Password	87	18.8
Online account username	83	18.0
Computer username	67	14.7
Driver's licence information	47	10.2
Place of birth	44	9.5
Signature	37	8.1
PIN	37	8.0
TFN	31	6.7
Medicare information	24	5.3
Passport information	23	4.9
Student number	13	2.8
Biometric information (eg fingerprint)	10	2.2
HIN	10	2.2
Other	31	6.8

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

Source: Identity Crime Survey 2013 [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=3.1, SD=3.3, n=460). As shown in Figure 8, this distribution is positively skewed, with almost half (46.3%, n=213) of participants indicating that only one type of information had been misused and over three-quarters (80.7%, n=371) indicating that four or fewer types of personal information had been misused.

Figure 8 Number of types of personal information misused in the most serious occasion in the past 12 months (unweighted data)



Source: Identity Crime Survey 2013 [AIC data file]

Participants were asked how they believed their personal information had been obtained on the most serious occasion 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=360), the majority (n=229, 63.6%) indicated that only one method had been used (weighted mean=1.4, SD=1.6, range 1–11).

Table 18 How personal information was obtained on the most serious occasion in the previous 12 months (n=460)

Way of obtaining personal information	n	%
From theft or hacking of a computer or other computerised device (eg smartphone)	92	20.0
From an online banking transaction	90	19.5
By email	84	18.3
From information placed on a website (other than social media, eg online shopping)	72	15.7
From an ATM or EFTPOS transaction	51	11.0
By telephone (excluding SMS)	48	10.5
Theft of mail	44	9.6
From information lost or stolen from a business or other organisation (ie a data breach)	44	9.6
In a face-to-face meeting (eg a job interview or a doorknock appeal)	35	7.5
From information placed on social media (eg Facebook, Linked-in etc)	32	6.9
By text message (SMS)	29	6.4
Theft of an identity or other personal document	9	2.0
Theft of a copy of an identity or other personal document	4	0.8
Other	26	5.7
Don't know	90	19.7

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

Source: Identity Crime Survey 2013 [AIC data file]

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=460)

Misuse	n	%
To obtain money from a bank account (excluding superannuation)	163	35.4
To purchase something	150	32.5
To apply for a loan or obtain credit	37	8.1
To file a fraudulent tax return	33	7.2
To obtain money from an investment (eg shares)	30	6.5
To apply for a job	30	6.4
To open a mobile phone account	29	6.4
To apply for government benefits	19	4.1
To provide false information to police	24	5.3
To obtain superannuation monies	23	5.1
To open an online account, such as Facebook, eBay	14	3.2
To rent a property	11	2.3
Other	41	8.9
Don't know	68	14.7

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

Source: Identity Crime Survey 2013 [AIC data file]

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 airfares and travel (n=23), and electronics, such as computer equipment and mobile phones (n=21). Other purchases included clothing and accessories (such as shoes and watches) (n=11), expenditure on gaming sites (n=6), restaurants and food (n=5), vehicles (including cars and motorbikes) (n=4), hotels (n=4), and cosmetics (n=4). Drugs (n=2) and, in one case, a gun were also purportedly purchased by misusing participants' personal information.

For those participants who knew how their personal information had been misused (n=386), the weighted number of different ways it had been misused ranged from one to ten (mean=1.5, SD=1.4). Over three-quarters (n=305, 79.0%) indicated just one way in which their personal information had been misused.

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=460)

Detection method	n	%
Received a notification from a bank or financial institution and/or credit card company	199	43.3
Noticed suspicious transactions in bank statements or accounts	153	33.3
Received a bill from a business or company for which they were not responsible	62	13.5
Was unsuccessful in applying for credit	42	9.1
Received a notification from the police	36	7.9
Received a notification from another company	24	5.2
Was contacted by debt collectors	24	5.1
Received a notification from a government agency or authority other than the police	17	3.6
Other	73	15.8

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

Source: Identity Crime Survey 2013 [AIC data file]

Most participants (n=366, 79.6%) had detected the most serious misuse of personal information over the past 12 months using just one method. When the data were weighted, the average number of methods used to detect the most serious misuse of personal information was 1.4 (SD=0.9, range=1–6).

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

Statistic	Out-of-pocket losses ($)	Recovered ($)
Number of respondents	260	246
Minimum	1	1
Maximum	310,000	310,000
Mean	4,816	2,209
Median	200	227
Standard deviation	30,541	23,944
25% quartile	50	87
75% quartile	800	920
Total	1,252,177	543,514

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

Source: Identity Crime Survey 2013 [AIC data file]

No financial loss was experienced by 200 participants (43.5%). The remaining 260 participants experienced losses ranging from $1 to $310,000. When the data were weighted, the median financial loss was $200. The distribution was positively skewed as shown in Figure 9, with over three-quarters (75.4%) of participants experiencing losses of up to $800. The total lost on the most serious occasion was $1,252,177.

Figure 9 Distribution of financial losses experienced in respect of 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 2013 [AIC data file]

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 $310,000. When weighted, the median amount recovered was $227. It was found that most participants received reimbursement or recovery of small amounts, with few receiving much higher amounts (see Figure 10).The total amount recovered was $543,514. The remaining 214 participants (46.5%) did not receive any reimbursement or recover any losses in respect of the most serious occasion in the past 12 months.

Figure 10 Distribution of funds reimbursed or recovered in respect of 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 2013 [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, which test the assumption that the frequencies observed within each cell are obtained by chance, were used for categorical variables. Table 22 shows the results of the chi-square tests for those variables that were found not to have a significant relationship with misuse of personal information in the previous 12 months.

Table 22 Variables that did not have a significant relationship with misuse of personal information in the previous 12 months (n=4,995)

Variable	df	χ^2	Significance
Place of normal residence	14	10.16	.654
Place of normal residence dichotomised (capital city/outside capital city)	1	0.07	.828
Age group	6	7.36	.495
Language spoken at home dichotomised (English/language other than English)	1	0.80	.451

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

Source: Identity Crime Survey 2013 [AIC data file]

In relation to gender, Fisher's exact test, which is a more conservative statistical measure, was used as an alternative to chi-square, as the assumption that there be no more than 20 percent of the expected frequencies with a value less than five was violated. No significant relationship was found between experiencing misuse of personal information in the previous 12 months and gender (df=2, p=.095).

As shown in Table 23, 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=4,995)=37.78, p<.001). These results indicate that those who identified as Indigenous were more likely to experience misuse of their personal information.

Table 23 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	25 (8)	65 (82)	90
Did not identify as Indigenous	441 (457)	4,410 (4,394)	4,851
Preferred not to say	4 (5)	50 (49)	54
Total	471	4,524	4,995

p<.001

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

Source: Identity Crime Survey 2013 [AIC data file]

A significant relationship was also found between individual gross income category and experience of misuse of personal information in the previous 12 months (χ^2(5, 4,995)=32.25, p<.001; see Table 24). These results 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. Interestingly, those who preferred not to indicate their income were also less likely to experience misuse of their personal information. This may be because they were reluctant to divulge their information and therefore undertake fewer behaviours that may result in personal information being stolen.

Table 24 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	80 (110)	1,088 (1,058)	1,168
$18,201–$37,000	99 (99)	957 (956)	1,056
$37,001–$80,000	156 (135)	1,281 (1,302)	1,438
$80,001–$180,000	83 (59)	541 (566)	624
$180,001 and over	9 (6)	55 (58)	64
I'd rather not say	42 (61)	603 (584)	645
Total	471	4,524	4,995

p<.001

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

Source: Identity Crime Survey 2013 [AIC data file]

As shown in Table 25, a significant relationship was found between *perceptions* of the seriousness of misuse of personal information and experiencing misuse of personal information in the previous 12 months ($\chi^2(3, 4,995)=20.74$, $p<.01$), with those who had experienced misuse more likely to perceive it as being *very serious*.

Table 25 Contingency table for misuse of personal information in the previous 12 months and perceptions of the seriousness of misuse of personal information (expected frequencies are shown in parentheses)

Seriousness	Misuse of personal information in previous 12 months		Total
	Yes	No	
Very serious	363 (323)	3,071 (3,111)	3,434
Somewhat serious	102 (131)	1,288 (1,259)	1,390
Not very serious	5 (14)	142 (133)	147
Not at all serious	0 (2)	24 (22)	24
Total	471	4,524	4,995

$p<.01$

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

Source: Identity Crime Survey 2013 [AIC data file]

A significant relationship was also found between perceptions about the risk of misuse of personal information in the next 12 months and experiencing misuse of personal information in the previous 12 months ($\chi^2(4, 4,995)=123.81$, $p<.001$), as shown in Table 26.

Table 26 Contingency table for misuse of personal information in the previous 12 months and perceptions about the risk of misuse of personal information in the next 12 months (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	169 (93)	819 (895)	989
Risk will increase somewhat	213 (214)	2,057 (2,056)	2,270
Risk will not change	81 (159)	1,609 (1,531)	1,690
Risk will decrease somewhat	7 (2)	16 (21)	23
Risk will decrease greatly	0 (2)	22 (21)	23
Total	471	4,524	4,995

$p<.001$

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

Source: Identity Crime Survey 2013 [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 owing to the fact that the dependent variable, 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 ($z=2.12$, $p<.05$, n=4,987).

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=3.07, SD=0.75) than those who had not (M=3.00, SD=0.77; $t(4,984)=1.96$, $p<.05$). However, when the data were weighted, the difference was no longer significant ($p=.069$).

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 compared with those who may have lived further apart. Table 27 shows the results of the chi-square tests for those methods by which personal information had been obtained that were found not to have a significant relationship with participants' place of normal residence.

Table 27 Methods by which personal information had been obtained that did not have a significant relationship with participants' place of normal residence (dichotomised) (n=460)

Variable	df	χ^2	Significance
In a face-to-face meeting (eg a job interview or a doorknock appeal)	1	3.13	.156
By telephone (excluding SMS)	1	1.53	.328
By text message (SMS)	1	0.40	.596
By email	1	0.01	.919
From theft or hacking of a computer or other computerised device (eg smartphone)	1	0.03	.885
Theft of an identity or other personal document	1	0.90	.335
Theft of a copy of an identity or other personal document	1	0.00	.942
Theft of mail	1	0.78	.474
From an online banking transaction	1	0.02	.896
From information placed on social media (eg Facebook, Linked-in etc)	1	1.15	.391
From an ATM or EFTPOS transaction	1	0.40	.598
Other	1	0.00	.992

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

Source: Identity Crime Survey 2013 [AIC data file]

Table 28 shows the relationship between place of normal residence and data breaches for respondents who had experienced misuse of their personal information in the previous 12 months. It was found that respondents located outside a capital city were significantly more likely than those who were not located outside a capital city to have had their personal information obtained from information lost or stolen from a business or other organisation (ie a data breach; $\chi^2(1, 460)=5.34$, $p<.05$).

Table 28 Contingency table for place of normal residence for participants who experienced misuse of personal information in the previous 12 months and information lost or stolen from a business or other organisation (expected frequencies are shown in parentheses)

Location	Information lost or stolen from a business or other organisation		Total
	Selected	Not selected	
Capital city	22 (29)	284 (277)	306
Outside capital city	22 (15)	132 (139)	154
Total	44	416	460

$p<.05$

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

Source: Identity Crime Survey 2013 [AIC data file]

Those who resided outside a capital city were significantly more likely to have had their personal information stolen from information used on a website (other than social media eg online shopping) ($\chi^2(1, n=460)=9.00$, $p<.05$; see Table 29).

Table 29 Contingency table for place of normal residence of participants who experienced misuse of personal information in the previous 12 months and information obtained from a website other than social media (expected frequencies are shown in parentheses)

Location	Information obtained from a website other than social media		Total
	Selected	Not selected	
Capital city	37 (48)	269 (258)	306
Outside capital city	35 (24)	118 (130)	154
Total	72	388	460

$p<.05$

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

Source: Identity Crime Survey 2013 [AIC data file]

As shown in Table 30, a significant relationship was found between the place of normal residence for those participants who experienced misuse of their personal information in the previous 12 months and not knowing how their personal information had been obtained ($\chi^2(1, n=460)=5.50$, $p<.05$). This table indicates that those who live in capital cities were significantly more likely than those who did not, to know how their personal information had been obtained.

Table 30 Contingency table for place of normal residence of participants who experienced misuse of personal information in the previous 12 months and did not know how their personal information was obtained (expected frequencies are shown in parentheses)

Location	Don't know how personal information was obtained		Total
	Selected	Not selected	
Capital city	51 (60)	256 (246)	306
Outside capital city	40 (30)	114 (123)	154
Total	90	370	460

$p<.05$

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

Source: Identity Crime Survey 2013 [AIC data file]

Further analyses were undertaken to test the relationship between the characteristics of respondents who reported a financial loss (n=250) and the amount that 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 respondent who indicated 'other' did not report a financial loss; $t(249)=0.39$, $p=.534$), location (dichotomised; $t(249)=2.32$, $p=.129$) and Indigenous status (dichotomised; $t(249)=0.87$, $p=.353$). A significant relationship was found in relation to language spoken at home, with those who spoke English reporting having lost significantly more than those who spoke a language other than English ($t(249)=4.94$, $p<.05$).

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 ($F(5, 245)=1.51$, $p=.189$). Similarly, respondents' age categories were not significantly related to amount of financial loss ($F(6, 244)=2.04$, $p=.062$).

As Figure 4 showed some potentially interesting results, the relationship between age, gender and amount of financial loss was explored further. However, with the transformed data, there were no statistically significant differences between men and women at all age points ($F(7, 243)=1.74$, $p=.101$). A series of interaction tests were examined to determine whether any specific age and gender combinations were significant, however, these tests indicated no significant findings.

The number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent, were normalised using logarithmic transformation and the relationship with these weighted variables and financial loss were investigated using Pearson product-moment correlation coefficients. Both these variables were found to have a significant medium, positive correlation with amount of financial loss, indicating that the higher the financial loss, the more time ($r=.36$, $n=248$, $p<.001$) and money ($r=.45$, $n=187$, $p<.001$) was 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 form baseline data that may be used to measure changes over time should future, comparable surveys be undertaken on a regular basis. Although differences in sample sizes, survey methodology and questions asked of respondents exist in comparison to prior research of this nature, it is possible to identify some areas of general comparison between the results reported here and comparable research conducted in Australia and overseas.

Perceptions of misuse of personal information

In relation to how respondents perceive 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 (96.6%). Almost two-thirds of the respondents (65.2%) also considered that the risk of someone misusing their personal information would increase over the next 12 months.

Both of these perceptions concerning seriousness and likelihood of change were higher than similar perceptions reported by Di Marzio Research (2012), although the questions asked and sampling frame were not exactly comparable to those of the present study. In 2012, 89 percent of respondents to the Di Marzio Research (2012) survey indicated that identity theft and misuse caused them a lot of concern or some concern, while 61 percent believed that the risk of having their identity information stolen or misused would increase.

The survey conducted by the OAIC (2013) found that in total, over two-thirds of Australians expressed concern about the possibility of becoming the victim of identity theft and fraud in the next year (69%); a significant change compared with 2007 (60%; OAIC 2007). The OAIC (2013) also found a large change in the level of concern—a quarter of people interviewed in 2013 said they were *very concerned* (25%) compared with one in six (17%) in 2007. These findings are considerably lower than those of the present study, where 69 percent of respondents indicated *very serious* levels of concern. Both the OAIC (2013) and Di Marzio Research (2012) surveys has much lower sample sizes than the present study.

Experience of misuse of personal information

The present survey found that 20.8 percent of respondents reported misuse of personal information at some time during their life, with 9.4 percent reporting misuse of their personal information in the previous 12 months. This is somewhat lower than the lifetime prevalence rate of 27 percent of respondents to the National Fraud Authority'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 the year 2012. The present survey's lifetime prevalence rate of 20.8 percent is also much higher than the 13 percent lifetime rate of identity fraud reported by respondents to the OAICs (2013) survey and also higher than the US NCVS lifetime prevalence rate of 14 percent and the 12 month prevalence rate of 6.7 percent (Harrell & Langton 2013).

The present survey's 9.4 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'. These variations are most likely due to the different sampling frames used, data collection techniques employed and 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 also excluding any costs associated with repairing what occurred.

Over half of the respondents (54.3%) reported being left out-of-pocket with losses ranging from between $1 and $310,000 (mean=$4,101, median $247, SD=$34,062). The majority of participants experienced smaller losses. Total losses amounted to $1,025,250. 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 $2,381 and the median amount reimbursed or recovered was $300 (SD=$23,478, n=255). It was found that most participants received reimbursement or recovery of small amounts, with some receiving much higher amounts. The total amount reimbursed or recovered during the last 12 months was $607,164. Finally, just over half of the respondents (56.1%) reported spending money dealing with the consequences of personal information misuse. The financial consequences of misuse of personal information during the 12 month period were, accordingly, total of out-of-pocket losses, amounts reimbursed and the cost of dealing with the consequences of misuse.

In addition to these costs, some participants experienced other consequences, the most frequent of which were being refused credit (14.1%), experiencing mental or emotional stress requiring counselling or other treatment (10.7%) and having been wrongly accused of a crime (5.5%). Participants also reported having spent between zero and 500 hours dealing with the consequences of having had their personal information misused over the previous 12 months, with 95 percent of respondents spending 60 hours or less.

These financial and other impacts are somewhat higher compared with 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 over $1,000. It was also found that just over a 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.

The Australian Payments Clearing Association (2013) reported scheme credit, debit and charge cards fraud perpetrated in Australia and overseas on Australia-issued cards amounted to $244,984,380 in 2012. Not all of this would fall within the definition of misuse of personal information within the terms of the present research.

In the United Kingdom, however, identity fraud was estimated by the National Fraud Authority (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 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).

Reporting the misuse of information

As with prior research in Australia and overseas, reporting of misuse of identity was relatively low among survey respondents. Of those who experienced misuse of their personal information in the present survey, 8.9 percent did not report it in any way, 53.5 percent told a friend or family member, 7.8 percent told a government agency or a business organisation and 29.8 percent told a friend or family member as well as a government agency or business organisation. More than a third of respondents (39.5%) did not report the misuse of their personal information because they did not believe anything could be done about it, 23.6 percent were too embarrassed to report it, 23.1 percent did not know how or where to report the matter and 12 percent did not believe it was a crime.

These results are similar to those found in the AICs Online Consumer Fraud Survey 2012 (Jorna & Hutchings 2013). Respondents to this survey, which covered all types of consumer fraud including identity misuse, reported that family and friends were the most common recipients of scam complaints, with 43 percent of the total sample reporting to this category. Overall in 2012, 69 percent of the total sample reported a scam to at least one person or organisation. The most common reasons provided for not reporting scams were 'unsure of which agency to contact' (40% of the total sample), 'I didn't think anything would be done' (32%) and 'not worth the effort' (29%).

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 the response provided by Medicare Australia (91.7% responded either *satisfied* or *very satisfied*), an internet service provider (91.3%) and a bank, credit union, credit/debit card company or e-commerce provider (89.1%).

In the survey conducted by Di Marzio Research (2012), almost half of the respondents (48%) indicated that private sector organisations were of assistance in recovering stolen identity information, while 32 percent indicated that police were of assistance and eight percent named government agencies.

In the United States, the NCVS found that in 2012, 88 percent of all victims of identity theft reported the incident to one or more non-law enforcement agencies—either government or a commercial agency. About 86 percent of identity theft victims contacted a credit card company or bank to report misuse or attempted misuse of an account or personal information, while six percent of all identity theft victims contacted a credit monitoring service and a further three percent contacted an agency that issues identity documentation. One percent contacted the Federal Trade Commission and another one percent contacted a government consumer affairs agency or other consumer protection organisation. Nine percent of identity theft victims contacted a credit bureau to report the incident.

About nine percent of identity theft victims reported the incident to police. Victims of personal information fraud were the most likely to report the incident to police (40%), followed new account fraud victims (23%) and victims of multiple types of identity theft (22%). Fewer than 10 percent of victims of existing credit card (4%), existing bank account (9%) and other existing account misuse (6%) reported the incident to police. The 91 percent of identity theft victims who did not report an incident to police offered a variety of reasons for not reporting. Among all victims who did not report the incident to police, the most common reason was that the victim handled it another way (58%). About a third (29%) of non-reporting victims did not contact police because they suffered no monetary loss. One in five non-reporting victims did not think that the police could help and another 15 percent did not know how to report the incident to law enforcement (Harrell & Langton 2013).

Behavioural changes resulting from the misuse of personal information

Participants were asked how their behaviour had changed as a direct result of having their personal information misused. The top five behavioural changes were changing passwords (48.5%), being more careful when using or sharing personal information (48.1%), changing banking details (42.5%), reviewing financial statements more carefully (39.6%) and not trusting people as much (39.0%). A minority (5.9%) of participants who experienced misuse of their personal information in the previous 12 months indicated that this did not result in any behaviour 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 with personal information (67%). A higher percentage of victims than non-victims engaged in both of these preventative actions. However, about 13% of victims began shredding or destroying documents with personal information as a result of

experiencing identity theft during the prior 12 months and 26 percent 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 a 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.

The top three types of personal information that had been misused were credit and debit card information (52.3%), name (40.2%) and bank account information (31.1%). These results were similar to those reported in Di Marzio Research's (2012) survey where the most prevalent way in which identity theft or misuse had occurred was loss of credit card or debit card, 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).

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 (20.0%), from an online banking transaction (19.5%), by email (18.3%), from information placed on a website other than social media, such as online shopping (15.7%) and from an ATM or EFTPOS transaction (11.0%). Di Marzio Research's (2012) survey also found a high incidence of identity theft and misuse taking place through internet viruses or 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 top three reasons were to obtain money from a bank account (excluding superannuation; 35.4%), to purchase something (32.5%) and to apply for a loan or obtain credit (8.1%). Di Marzio Research's (2012) 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 to the present survey 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 airfares and travel, and electronics such as computer equipment and mobile phones.

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 were receiving a notification from a bank or financial institution and/or credit card company (43.4%), noticing suspicious transactions in a bank statement or account (33.3%) and receiving a bill from a business or company for which they were not responsible (13.5%). 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). 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). No financial loss was experienced by 43.5 percent of participants. The remaining participants experienced losses ranging from $1 to $310,000. The mean out-of-pocket loss was $5,179.23 in respect of the most serious occasion in the past 12 months.

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 $310,000. The mean amount recovered was $2,866.09 in respect of the most serious occasion in the past 12 months.

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

The demographics and 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 is not possible to compare the statistical test results obtained in the present study with a number of previous research surveys.

Di Marzio Research's (2012) survey found statistically significant relationships at the 95 percent confidence level in respect of victimisation ('over the last 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 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 ages 18 to 24 years (5%) and 65 years and above (5%). After accounting for credit card ownership, persons ages 16 to 24 were the least likely to experience the misuse of an existing account, while persons age 65 years and above had a similar prevalence rate as persons aged 25 to 34 years. Among those who had a bank account, persons ages 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).

In the present survey, it was found that a number of variables did not have a significant relationship with misuse of personal information in the previous 12 months. They included place of normal residence, age group, gender, language spoken at home and the number of hours spent on a computer or computerised device variable.

A significant relationship was, however, 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 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. These results indicate that those in the lowest income category ($18,200 and under) were less likely to experience misuse of their personal information than were those earning $37,001 and above.

A significant relationship was 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 being more likely to perceive it as being *very serious*. Similarly, a significant relationship was found between perceptions about the risk of misuse of personal information in the next 12 months and experiencing misuse of personal information in the previous 12 months.

Two significant relationships were found between place of normal residence and the place from which personal information had been obtained in respect of respondents who had experienced misuse of their personal information in the previous 12 months. First, it was found that respondents located outside a capital city were significantly more likely than those who were located in a capital city to have had their personal information lost or stolen from a business or other organisation (ie a data breach). Secondly, it was found that respondents located outside a capital city were significantly more likely than those who were located 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 that reported a financial loss and the amount that they reported. No significant relationship was found between the amount of financial loss and age, gender, location, income and Indigenous status.

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.

The number of hours spent dealing with the consequences of identity misuse, as well as the amount of money spent, were both found to have a significant medium, positive correlation with amount of financial loss, indicating that the higher the financial loss, the more time and money was spent dealing with the consequences.

Conclusion

In recent years, continued attention has been given to the problem of identity crime by government policymakers, business security analysts and academic researchers. Evidence of the full nature and extent of victimisation is now becoming evident, although differences in research methods have made comparative analysis across jurisdictions problematic. The present research sought to provide up-to-date data on the experiences of a large sample of Australians drawn from all states and territories, concerning their perceptions of the risks of misuse of personal information and the extent to which they have suffered victimisation of this kind. The results indicate that it appears that identity crime continues to affect many Australians. In the years ahead, further survey research will enable trends in the data to be plotted to determine

how risks of identity crime change and whether crime prevention initiatives have been effective.

It was found in the present survey that a high proportion of respondents believed that misuse of personal information was serious, with almost two-thirds believing that the risk of someone misusing their personal information would increase over the next 12 months. Both of these perceptions concerning seriousness and likelihood of change were higher than similar findings reported by previous Australian research (Di Marzio Research 2012; OAIC 2013). In terms of reported victimisation, the present survey found that 20 percent of respondents reported misuse of their personal information at some time during their lives, with just over nine percent reporting misuse during the previous 12 months. Although these levels of victimisation differ from previous Australian and overseas research, there is arguably a need to publicise the results of the present survey so that perceptions more accurately reflect the actual levels of victimisation experienced in Australia.

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 over $1m. In addition, banks and other organisations reimbursed victims over $600,000 in respect of claims made during the preceding year. 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 having been refused credit (14.1%), experiencing mental or emotional stress requiring counselling or other treatment (10.7%) and having been wrongly accused of a crime (5.5%). The experience of victimisation also resulted in a range of behavioural changes including reduced levels of trust and increased caution in conducting transactions. 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 and re-victimisation in the first place.

As occurs with other types of fraud, the levels of reporting to official agencies, including law enforcement agencies, was low, although respondents were generally satisfied with the outcomes when they reported to some government agencies and financial institutions. Almost one-quarter of respondents said that they did not know how or where to report the matter and 12 percent did not report because they did not believe it was a crime. The implementation of the Australian Online Crime Reporting Network may assist to make reporting more attractive to victims of identity crime, although victims' expectations of the level of assistance available will need to be carefully managed.

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 or to obtain finance.

In terms of the characteristics of victims, it was found that Indigenous Australians were more likely to experience misuse of their personal information than others, while those earning $37,000 and above were more likely to experience misuse. It was also found that respondents located outside a capital city were significantly more likely than those who were located in a capital city to have had their personal information lost or stolen from a business or other organisation and that respondents located outside a capital city were significantly more likely than those who were located in a capital city to have had their personal information obtained from a website other than social media (eg during online shopping). Those who spoke English were found to have lost significantly more than those who spoke a language other than English at home. These findings were all statistically significant.

Further research would be required to understand fully the reasons associated with these relationships. Smith and 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 of online services owing to face-to-face transactions being less available. Other possible

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. 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 prior research that misuse of personal information remains an important form of criminal activity in Australia in 2013. The results could be used effectively by those tasked with devising fraud prevention initiatives in a number of ways. For example, it would be possible to provide targeted information to those most likely to be victimised outlining how they could better protect themselves against identity crime and misuse. Such initiatives may result in future surveys of this kind finding reduced levels of victimisation and fewer financial and other consequences for Australians in the years ahead.

References

All URLs correct at February 2014

Anti-Phishing Working Group (APWG) 2013. *Phishing activity trends report 2nd quarter 2013*. New York: APWG. http://www.antiphishing.org

Anti-Phishing Working Group (APWG) 2011. *Phishing activity trends report 2nd quarter 2011*. New York: APWG. http://www.antiphishing.org

Attorney-General's Department (AGD) 2012a. The National Identity Security Strategy 2012. Unpublished policy paper

Attorney-General's Department (AGD) 2012b. Report to the Council of Australian Governments. A review of the National Identity Security Strategy 2012. Unpublished policy paper

Australian Bureau of Statistics (ABS) 2013. *Australian demographic statistics, Dec 2012*. ABS cat. no. 3101.0. Canberra: ABS. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/3101.0Dec%202012?OpenDocument#Time

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 ed. 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

Australian Competition and Consumer Commission (ACCC) 2013. *Targeting scams: Report of the ACCC on scam activity 2012*. Canberra: ACCC

Australian Payments Clearing Association (APCA) 2013. *Fraud statistics 2012*. Sydney: APCA. http://www.apca.com.au/payment-statistics/fraud-statistics/2012-calendar-year

Bricknell S & Smith RG 2013. Developing a monitoring framework for identity crime and misuse. A report to the Australian Government Attorney-General's Department. Canberra: Australian Institute of Criminology

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

Federal Trade Commission (FTC) 2013. *Consumer sentinel network data book for January 2012 to December 2012*. Washington: FTC. http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2012/sentinel-cy2012.pdf

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

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: National Fraud Authority. 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: Office of the Australian Information Commissioner. 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: Office of the Australian Information Commissioner

Smith RG 2014. Transnational cybercrime and fraud, in Reichel P & Albanese J (eds), *Handbook of transnational crime and justice*, 2nd ed. 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 & 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

Verizon 2013. *Data breach investigations report 2012*. Basking Ridge, NJ: Verizon

Appendix

Appendix: Identity crime and misuse survey 2013

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), share holder 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; 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 Russell.Smith@aic.gov.au who is in charge of the study. You can also obtain further information or make a complaint about the study by contacting Tracy.

Cussen@aic.gov.au or (02) 6260 9208.

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 2012–2013 (ie before tax has been deducted)?

$0–$18,200

$18,201–$37,000

$37,001–$80,000

$80,001–$180,000

$180,001 and over

I'd rather not say

Q7a) Last week, how many hours did you spend using a computer or computerised devices including a desktop, laptop, smartphone and tablet?

Insert number of whole hours only_____

Q7b) Of these hours spent using a computer (including a desktop, laptop, smartphone and tablet), how many hours were spent on work-related activities only?

Insert number of whole hours only_____

_____

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 (eg fingerprint), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, 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 (eg Scamwatch, Consumer Affairs, Office of Fair Trading)					
A Road Traffic Authority					
The Passport Office					
Medicare Australia					
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)					
A credit reporting agency (eg Veda or Dun and Bradstreet)					
Your internet service provider					
A utility company (eg gas, electricity, telephone, water etc.)					
A media organisation					
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(es)

I changed my banking details

I changed my telephone number(s)

I changed my place of residence

I use better security for my computer or other computerised devices

I lock my mailbox

I redirect my mail when I am away or move residence

I use a registered post box

I shred personal documents before disposing of them

I review my financial statements more carefully

I applied for a copy of my credit report

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

I don't trust people as much

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 (eg 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 (eg smartphone)

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

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

Theft of your mail

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

From an online banking transaction

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

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

From an ATM 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 (eg shares)

To apply for a job

To provide false information to police

To rent a property

To purchase something—(please specify what was purchased)

_____

To apply for government benefits

To apply for a loan or obtain credit

To open a mobile phone account

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

Other (please specify)

_____

Don't know

Q22) On this most serious occasion, how did you become aware that your personal information had been misused? (select all that apply)

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

Received a notification from another company (please specify) _____

Received a notification from the police

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

Noticed suspicious transactions in bank statements or accounts

Was unsuccessful in applying for credit

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

Was contacted by debt collectors

Other (please specify) _____

Q23a) On this most serious occasion, how much were you left out-of-pocket as a result of the misuse of your personal information? $_____ (insert your best estimate of the total losses in whole dollars excluding any money that you were able to recover from banks etc. and also excluding any costs associated with repairing what occurred)

Q23b) On this most serious occasion, how much money was reimbursed to you by banks or other organisations, or recovered in other ways, as a result of the misuse of your personal information? $_____

Thank you for your time in answering these questions.

AIC Reports Research and Public Policy Series 128

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

aic.gov.au