Australian Government

Australian Institute of Criminology

AIC reports
Statistical Report 19

Identity crime and misuse in Australia: Results of the 2018 online survey

Penny Jorna
Russell G Smith
Katherine Norman

ISSN: 2206-7930 (Online)
ISBN: 978 1 925304 16 9 (Online)

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

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

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

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

Edited and typeset by the Australian Institute of Criminology

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

Identity crime in Australia

Australian Government

Australian Institute of Criminology

12% of respondents reported having their **personal information misused in the last 12 months,** a decrease on the 13% reported in 2017.

Almost 1 in 4 of the Australians surveyed (24.5%) reported having been a victim at some point in their lives. This was a slight decrease on the 25.2% reported in 2017.

Victims of identity crime spend an average of **22 hours** repairing the damage caused.

Refusal of credit was the most common consequence of identity crime in 2018 **(27%),** but occurred less than in 2017 (35%).

There was a significant **8 percentage point** increase in respondents reporting **misuse of credit/debit card information** between 2017 and 2018.

Average out-of-pocket losses were **over $1,000 less** in 2018 than in 2017, and **total losses almost $1m lower** over the 12 months.

Although **personal information** was still most often used to obtain money from a bank **(41%),** there was a significant **5 percentage point** increase in using it to purchase something.

Theft or hacking of a device was the most common way personal information was obtained **(24%),** a significant increase on the 18% in 2017.

In both 2017 and 2018, **10% of respondents did not report** misuse of their personal information in any way.

Contents

Figures

Tables

Acknowledgements

This study was undertaken as part of the Department of Home Affairs' National Identification of Identity Crime and Misuse project, pursuant to the National Identity Security Strategy. The survey was developed with input and advice from the Department of Home Affairs. 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. The time and willingness of those who completed the survey are gratefully acknowledged.

Acronyms

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
AIC	Australian Institute of Criminology
OAIC	Office of the Australian Information Commissioner
PIN	personal identification number
SD	standard deviation
TFN	tax file number

Abstract

This report presents the findings of the latest survey of identity crime and misuse undertaken by the Australian Institute of Criminology (AIC) as part of the Australian Government's National Identity Security Strategy. Identity crime is one of the most prevalent forms of criminal activity in Australia and can have severe and lasting consequences for victims. In 2018, nearly 10,000 people from across Australia were surveyed about their experience of victimisation, over their lifetime and during the preceding 12 months. The survey results for 2018 are compared with those of the 2017 identity crime survey.

The 2018 survey found 25 percent of respondents had experienced misuse of their personal information at some time during their life, with 12 percent experiencing it in the previous 12 months. Similar numbers of respondents reported out-of-pocket losses in 2018 (945) and 2017 (950). The total out-of-pocket losses experienced were substantially lower in 2018 ($2m) than in 2017 ($2.9m). The results from the 2018 survey help policymakers to raise awareness of identity crime and reduce its impact throughout Australia.

Executive summary

Background

Identity crime is one of the most prevalent crime types in Australia. This is arguably because identity crime perpetrators have exploited changes in personal identification requirements, consumer payment habits and advances in technologies. Identity crime has been defined by the United Nations Economic and Social Council (2007: 18) as ‘crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes’.

In April 2007, the Council of Australian Governments agreed to a National Identity Security Strategy to protect Australians’ identities in a more regulated and efficient way. This arose from emerging evidence at the time that large numbers of Australians experienced criminal misuse of their personal information each year (Cuganesan & Lacey 2003; Office of the Australian Information Commissioner (OAIC) 2007). The strategy sought to enhance identification and verification processes throughout Australia and to develop other measures to combat identity crime, including the creation of a national Document Verification Service to verify the authenticity of identity credentials, and the development of reliable, consistent and nationally interoperable biometric security measures by all jurisdictions (Attorney-General’s Department 2012).

The strategy also recognised the need to quantify the nature and extent of identity crime and the misuse of personal information, particularly the victimisation experiences of Australians. It recommended the creation of a longitudinal measurement framework for identity crime and misuse that could be used to measure the effectiveness of policy and practice throughout Australia. As part of the measurement framework, the Australian Institute of Criminology (AIC) has conducted a series of large-scale surveys to determine respondents’ experiences of victimisation over their lifetime and during the preceding 12 months, and their perceptions of the risk of identity crime occurring in the ensuing 12 months. This report presents the results of the latest survey in the series. This survey was undertaken in December 2018 and January 2019.

Methodology

Consistent with previous years' surveys, the 2018 survey asked respondents about the misuse of various types of personal information. This included (but was not limited to) misuse of an individual's name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, passwords, personal identification numbers (PINs), tax file numbers, shareholder identification numbers, computer or other online usernames and passwords, and student numbers. Respondents were also given the opportunity to provide details of other types of personal information that may have been misused.

Misuse of personal information was defined as:

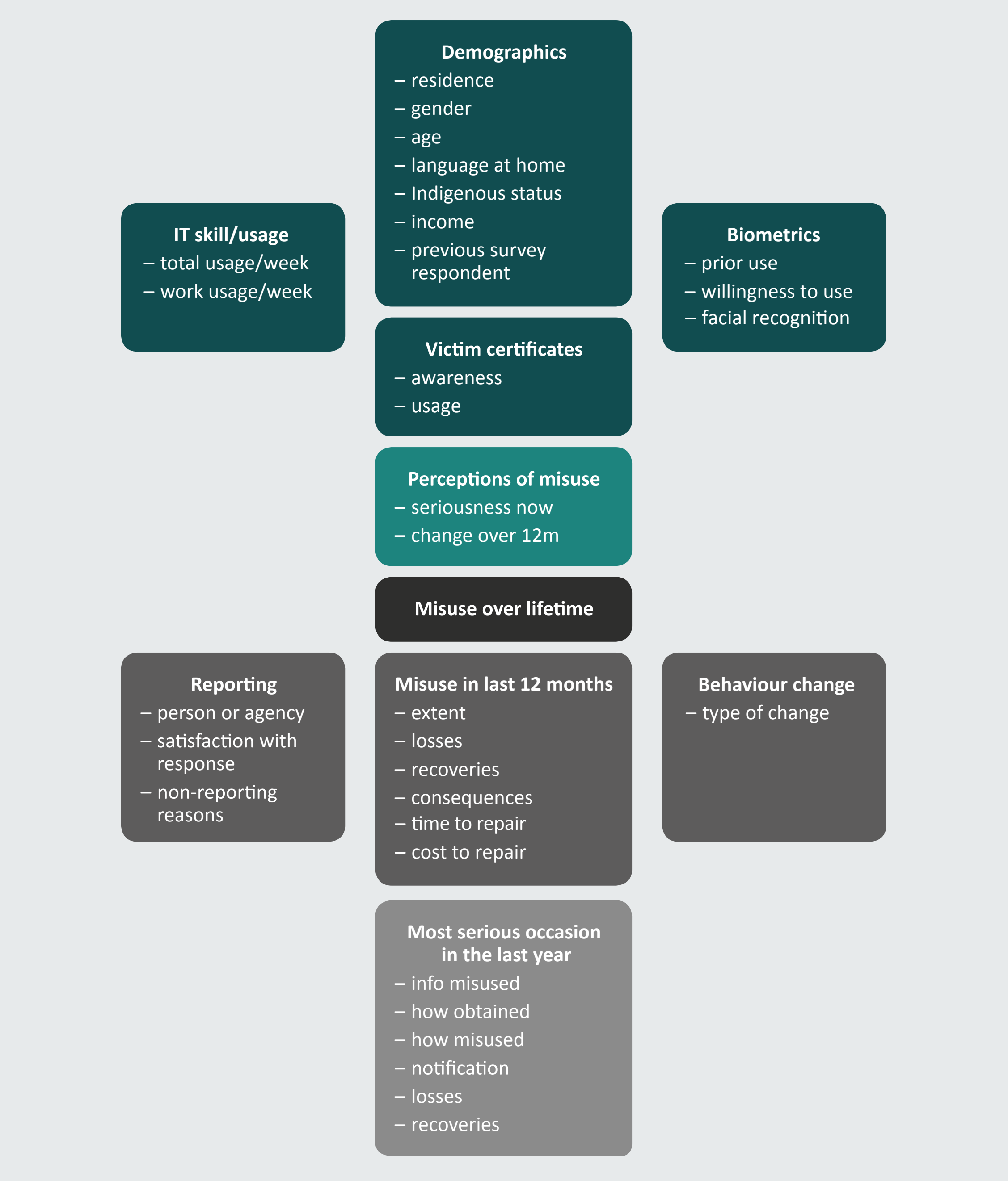
> obtaining or using your personal information without your permission, to pretend to be you, or to carry out a business in your name without your permission, or other types of activities and transactions. This does not include use of your personal information for direct marketing, even if this was done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

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

Between late December 2018 and early January 2019, a questionnaire comprising 40 main questions (see *Appendix A*) was administered online to a research panel of Australians drawn from all states and territories. The sampling frame of more than 300,000 individuals and survey hosting were provided by i-Link Research Solutions, a market research company, which then provided raw de-identified data for the AIC to analyse.

Sampling was completed once a quota of 10,000 respondents had been reached. A requirement of the sample was that respondents had not participated in any of the prior surveys conducted in 2013, 2014, 2016 or 2017. No other quotas were employed as the sample was sufficiently large to ensure good representation from urban and regional areas across Australia. Data were weighted by age and gender to reflect the spread of the population in Australia. The total usable sample was 9,911 respondents.

Figure 1: Survey data collection plan



Demographics
- residence
- gender
- age
- language at home
- Indigenous status
- income
- previous survey respondent

IT skill/usage
- total usage/week
- work usage/week

Biometrics
- prior use
- willingness to use
- facial recognition

Victim certificates
- awareness
- usage

Perceptions of misuse
- seriousness now
- change over 12m

Misuse over lifetime

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

Misuse in last 12 months
- extent
- losses
- recoveries
- consequences
- time to repair
- cost to repair

Behaviour change
- type of change

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

Source: Goldsmid, Gannoni & Smith 2018

Prevalence of identity crime

One-quarter of respondents (25%) reported having experienced misuse of their personal information at some point in their lifetime, the same proportion as in 2017. Almost 12 percent (*n*=1,136) of respondents reported having had their personal information misused in the last 12 months. This was less than the 13 percent reporting recent misuse in 2017, although the difference was not statistically significant. Both lifetime misuse and recent misuse, however, were significantly higher than in 2016.

Men between 25 and 34 years of age were the group most likely to report personal information misuse in the last 12 months. When all age groups were considered, men were more likely than women to report personal information misuse in the last 12 months. When both men and women were considered together, the 25–34 age group was the most likely to report personal information misuse. Just under half (46%) of recent victims had their personal information misused just once in the last 12 months.

On the most serious occasion of misuse in the last 12 months, names were the type of personal information most commonly misused (47%), followed by debit and credit card information (44%). Over half of respondents (55%) had only one or two types of personal information misused. In both 2017 and 2018, personal information was most commonly misused to obtain money from a bank (41% excluding superannuation monies).

Out-of-pocket losses and reimbursements

A slightly higher proportion of respondents experienced out-of-pocket losses from the misuse of personal information in the previous 12 months in 2018 (83%, *n*=945 out of 1,136) than in 2017 (73%, *n*=950 out of 1,307 respondents), although the amounts of money lost were substantially higher in 2017 ($2.9m) compared with 2018 ($2m). Men aged 55–64 years reported the highest mean financial losses in 2018, losing on average $10,590 per person. The total amounts recovered fell substantially from $3.4m in 2017, to $631,800 in 2018. On the most serious occasion of misuse of personal information, respondents in 2017 reported greater losses ($2.4m) than respondents in 2018 ($1.8m). The average amount lost in 2018 ($1,974) was less than the average out-of-pocket loss experienced in 2017 ($2,711). Similarly, the total amount recovered on the most serious occasion in 2018 ($569,342) was much lower than the $1.5m recovered in 2017.

Impact on victims

There was a statistically significant increase in the proportion of recent victims who reported no adverse consequences—from 34 percent in 2017 to 47 percent in 2018. The most common consequence of misuse of personal information was the refusal of credit (27% of recent victims), although this consequence declined by nearly eight percentage points compared with 2017.

Of the 1,136 respondents who had experienced recent victimisation, 51 percent (*n*=582) incurred additional costs associated with the misuse of their personal information. Sixty percent of these respondents (*n*=349) spent $100 or less resolving the problem.

In addition, respondents reported spending 35 hours on average dealing with the consequences of their personal information being misused. Excluding six respondents who each reported spending over 2,000 hours, the mean number of hours victims spent dealing with consequences was 22—similar to the findings in 2017.

Almost all respondents (92%) reported changing their behaviour in some way as a direct result of their personal information having been misused. The most frequently reported behavioural change was changing passwords (45%), which significantly increased from 2017, when 38% of respondents reported changing passwords. This may reflect the increase in the proportion of victims experiencing their personal information being misused through hacking or theft of a computerised device and through online shopping or other websites.

Reporting misuse of personal information

Almost 10 percent (of respondents who had experienced misuse of their personal information in the last 12 months did not report the misuse at all. Sixty percent told only a family member or friend, 12 percent reported it to an organisation or a government agency. A further 19 percent told family and friends as well as an organisation or government agency.

Of the respondents who did report to an organisation or government agency, those who reported to IDCARE (a specialised support group for identity crime) or to their bank, credit union, credit/debit card company or e-commerce provider were the most satisfied with the response.

The most common reason respondents gave for not reporting misuse of personal information was that their bank, credit union or credit card company had already resolved the matter (34%), followed by respondents not thinking it was important enough to report (31%, a six percentage point increase from 2017).

Risk and prevention of personal information misuse

Almost one in five (19%) respondents reported believing the risk of their personal information being misused would increase greatly in the next 12 months. A further 44 percent of respondents reported believing the risk of their personal information being misused would ‘increase somewhat’.

Respondents who had experienced misuse of personal information in the last 12 months often believed that their level of risk would increase ‘greatly’ in the next 12 months. Almost all respondents (96%) believed misuse of personal information was ‘very serious’ or ‘somewhat serious’.

The survey also asked respondents about their willingness to use biometrics to protect personal information and to engage with government and business. Passwords, signatures and fingerprint recognition were the security measures most frequently used by respondents in the past. Passwords (95%) and fingerprint recognition (85%) were the most common security measures respondents were willing to use to protect personal information from misuse in the future. Respondents were most willing to use facial recognition for government activities, such as identifying terrorist suspects (89%), identifying criminal suspects (89%) and applying for and using identity documents (eg passport, driver licence; 84%).

Conclusions

The 2018 identity crime survey found the prevalence of misuse of personal information in a large Australian sample had remained stable, with 12 percent of respondents reporting they had experienced misuse in the 12 months prior to participating in the survey, compared with 13 percent of respondents in 2017. Names remained the most commonly misused type of personal information, although the misuse of debit/credit card information increased by eight percentage points from 2017. The proportion of respondents experiencing misuse of an online account name also rose in 2018, to 44 percent. These findings align with the most common reported purposes for which information had been misused, namely to obtain money from a bank (41%) or to purchase something (21%).

In 2018, several serious data breaches were reported, affecting millions of people around the world. These breaches may explain the increase in the proportion of respondents who reported that their personal information had been obtained via hacking or theft of a computerised device (24% in 2018 vs 18% in 2017). An ongoing concern is the proportion of victims who did not know how their personal information had been obtained. This rose slightly to 16 percent of victims in 2018, compared with 15 percent of victims in 2017. Only by understanding where identity crime risks lie, and knowing how information has been obtained, will individuals reduce their vulnerability to identity crime.

The number of respondents in 2018 who reported out-of-pocket losses (945) was similar to the number in 2017 (950), although total losses experienced in 2018 ($1,968,509) were substantially lower than those of 2017 ($2,944,786).

Almost all respondents reported that misuse of personal information was somewhat or very serious in terms of harm to the Australian community, with victims more likely than non-victims to describe it as being very serious. Non-financial impacts were reported by 53 percent of respondents who had experienced misuse of personal information in the last 12 months, suggesting that the consequences of identity crime are far greater than the financial losses.

In sum, the 2018 identity crime survey found that misuse of personal information remains a prevalent crime affecting the Australian public. An increasing number of respondents attributed their victimisation to hacking or theft of a computerised device. In addition, respondents increasingly reported that online user account names had been misused in order to obtain personal information. The data suggest that the primary purpose of misusing personal information was most often to obtain money from victims' bank accounts or to purchase goods.

In terms of reporting victimisation, the survey found victims were most satisfied if they had reported their experiences to an organisation or government agency that could help them deal with the consequences of identity misuse, or teach them to reduce their risk of further victimisation. Satisfaction levels were also higher among victims who felt their concerns had been listened to.

Introduction

Identity crime is one of the most prevalent crime types in Australia (Jorna & Smith 2018). It has adapted and changed over time, from its beginnings in falsified voter registrations and ballot paper fraud to the data breaches, phishing attacks and the many and varied online scams of today (Australian Competition and Consumer Commission (ACCC) 2019). Identity crime involves exploiting vulnerabilities in personal identification credentials, consumer payment systems and technological advances in computing and communications, generally for financial gain. It was defined by the United Nations Economic and Social Council (2007: 18) as 'crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes.' It is, accordingly, an enabler of other types of crime, particularly organised economic crime.

Identity crime is rarely an end in itself, but it is an important element in a wide range of other criminal activities. These include credit card fraud; superannuation and other financial frauds against individuals; welfare, tax and other frauds against government agencies; money laundering and financing of terrorism; unauthorised access to sensitive information or facilities for unlawful purposes; and the concealment of other activities such as drug trafficking or the production and distribution of child exploitation material. Misuse of identity has also been connected with the commission of terrorist acts.

The economic impact of identity crime and misuse in Australia was most recently estimated to be $2.65b in 2015–16 (Smith & Jorna 2018b). A substantial proportion of those costs, worth an estimated $272m, relate to government actions to combat identity crime and to implement strategies such as the use of biometrics to strengthen identity security (Smith & Jorna 2018b). The present study sought to assess the nature and extent of identity crime among a large sample of the Australian community in 2018 and, where applicable, to compare the survey findings with those from previous years to discern any patterns or changes in methods, prevalence and losses.

Types of identity crime

Personal information has a wide range of uses for the criminally inclined, and criminals obtain it in a wide range of ways. One of the most efficient means of obtaining personal information is to use the data exposed by hacking networks or through data breaches. A data breach is a confirmed disclosure of data to an unauthorised party (Verizon 2019). In February 2018, in response to a series of data breaches reported in the media, the Office of the Australian Information Commissioner (OAIC) introduced the Notifiable Data Breaches scheme. This scheme obliges agencies covered by the Privacy Act 1988 to notify the OAIC and affected individuals of any data breach likely to result in serious harm (OAIC 2019). In just one year, 812 data breaches were reported, with the numbers increasing each quarter. Four large data breaches reported to the OAIC in 2018 involved information belonging to over 100,000 individuals (OAIC 2019). Since the commencement of the Notifiable Data Breaches scheme, the causes of data breaches have changed from 'human error' to 'malicious or criminal attacks'—the latter accounting for 64 percent of data breaches in the last quarter of 2018 (OAIC 2019).

Verizon has monitored data breaches since 2007 through voluntary reporting by organisations across the world (Verizon 2019). The 2019 *Data breach investigations report* showed that 43 percent of breaches involved small business victims, and the most common method involved hacking (52%), followed by social media attacks (33%) and malware (28%; Verizon 2019). In 2019, 71 percent of breaches were financially motivated, with 69 percent of attacks perpetrated by outsiders. Nation-state or state-sponsored actors were involved in 23 percent of attacks. The top category of threat action in 2019 was phishing, followed by use of stolen credentials. The next group involved the installation and subsequent use of backdoor or 'command and control' malware, which enables actors to manipulate systems and alter or remove data. Ransomware was also prevalent (Verizon 2019).

Recent reports by the Anti-Phishing Working Group have found changes in the way phishing attacks are delivered. Currently, attacks are often conducted using social media to disseminate phishing URLs (Anti-Phishing Working Group 2019). Phishing attacks also rely on malware to record sensitive data that can subsequently be used to defraud individuals or to facilitate fraud against businesses, government agencies and other organisations. Spear-phishing, which targets users with specific characteristics and vulnerabilities, is also prevalent—and was used in the recent attacks on the Australian National University (ANU 2019).

Background to the survey

In 2007, the Council of Australian Governments endorsed the National Identity Security Strategy as Australia's national response to identity crime. A review of the strategy in 2012 recognised the need to quantify the nature and extent of identity misuse, particularly the victimisation experiences of Australians. As a result, it recommended the creation of an identity crime and misuse longitudinal measurement framework that could be used to measure the effectiveness of policy and practice throughout Australia. As part of the measurement framework, large-scale surveys have been conducted to determine respondents' experiences of victimisation over their lifetime and during the preceding 12 months, and their views concerning the risk of identity crime in the ensuing 12 months.

This survey is the fifth undertaken by the Australian Institute of Criminology (AIC). Previous surveys were conducted in 2013 (Smith & Hutchings 2014), 2014 (Smith, Brown & Harris-Hogan 2015), 2016 (Smith & Jorna 2018a) and 2017 (Goldsmid, Gannoni & Smith 2018).

Purpose of this report

This report details the number, percentage and demographic characteristics of respondents who reported that their personal information had been misused in the 12 months prior to December 2018/January 2019. It also examines respondents' views on the use of biometric technologies to reduce the risk of misuse of personal information. Specific findings relating to the most serious occasion of misuse of personal information in the last 12 months are also canvassed, along with characteristics of victims and how they changed their behaviour as a result of their personal information being misused. The report presents data on how crimes were detected, the types of personal information misused and how respondents believed their personal information was obtained. The report also contains information about respondents' views on the seriousness of identity crime, whether they thought the risk of identity crime would change over the next 12 months and, for victims, whether their behaviour had changed as a result of experiencing misuse of their personal information.

Methodology

Research design and definitions

This study employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information among a sample of Australian residents aged 15 to 96 years. This methodology replicated four previous studies conducted by the AIC in 2013, 2014, 2016 and 2017 (see Smith & Hutchings 2013; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018a and Goldsmid, Gannoni & Smith 2018, respectively).

The definition of identity crime and misuse of personal information used in the survey was:

> 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.

Personal information was defined as including:

> name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, Personal Identification Number (PIN), Tax File Number (TFN), Shareholder Identification Number (HIN), computer and/ or other online usernames and passwords, student identification number and various other types of personal information.

Survey questions

A questionnaire was administered online that contained a mixture of closed-response and open-ended questions on the following topics:

- demographic and other characteristics of respondents including age, gender, usual place of residence, income, language spoken at home, Aboriginal and Torres Strait Islander status and computer usage;
- experience of misuse of personal information at any time in the past and over the preceding 12 months;
- method of victimisation on the most serious occasion in the preceding 12 months;
- actual financial losses, funds recovered and other consequences of victimisation;

- whether and how respondents reported misuse of personal information and their satisfaction with the responses;
- behavioural changes arising from the misuse of personal information;
- awareness of the availability of court-issued Victims' Certificates;
- perceptions of the seriousness of misuse of personal information;
- perceptions of the risk of identity crime over the next 12 months; and
- use of security measures, including biometric technologies, in the past and willingness to use them in the future to reduce the risk of identity crime victimisation.

These questions largely replicated those of the previous surveys so that direct comparisons could be made with earlier findings. The questions were developed by the AIC in consultation with the Department of Home Affairs.

The questions spanned a number of reference periods. Demographic questions (eg usual place of residence, age and income) related to respondents' circumstances at the time of responding. Other questions asked about lifetime experience of identity crime and misuse, as well as identity crime and misuse in the 12 months prior to completing the survey. The survey was available for completion from mid-December 2018 to early January 2019 (hereafter referred to as the 2018 survey).

The survey, which had 40 questions in total, took approximately 10 to 15 minutes to complete. At the end of the questionnaire respondents were asked if they would be willing to participate in a follow-up interview. For those who agreed, a contact telephone number was requested. No other identifying information was requested from respondents and all analyses were conducted using de-identified data. The questionnaire is presented in *Appendix A.*

Sample characteristics

Data were weighted by age and gender to reflect the spread of the population in Australia. Australian Bureau of Statistics (ABS) data (ABS 2018) were used to develop the weighting matrix for the sample (see *Appendix B*). The Australian demographic statistics, which were based on the 2016 Census, did not allow people to list their gender as 'indeterminate/intersex or unspecified'. Accordingly, responses from 55 respondents who selected this response were excluded from analysis as weighting could not be undertaken. A small number of respondents who did not specify their age were excluded from the analysis (*n*=56). Some respondents provided neither their age nor gender, so the total number of respondents excluded was 89. This resulted in a usable sample of 9,911 respondents.

Further information on how sampling and weighting were undertaken as well as methods of data analysis, ethical considerations and limitations of the methodology are presented in *Appendix B.*

Place of residence

The distribution of survey respondents and ABS Australian demographic statistics by usual place of residence were closely aligned (see Table 1). Tasmania was slightly over-represented in the survey data (2.4% vs 2.1%), as was Queensland (21.4% vs 20.1%), while the Northern Territory (0.6% vs 1.0%) and Western Australia (9.6% vs 10.3%) were slightly under-represented compared with Census data. This variation in distributions is relatively minor, however, with most the sample being within a few percentage points of the Australian population distribution for most locations.

Table 1: Respondents by usual place of residence

Source	ABS Australian demographic statistics, June 2018	Survey sample data	
Location	**%**	***n***	**%**
Sydney	31.9	1,970	19.9
Other New South Wales		1,130	11.4
Melbourne	26.0	1,957	19.7
Other Victoria		597	6.0
Brisbane	20.1	1,073	10.8
Other Queensland		1,051	10.6
Perth	10.3	759	7.7
Other Western Australia		192	1.9
Adelaide	6.9	592	6.0
Other South Australia		171	1.7
ACT (including Canberra)	1.7	125	1.3
Hobart	2.1	105	1.1
Other Tasmania		126	1.3
Northern Territory (including Darwin)	1.0	63	0.6
Total	**100.0**	**9,911**	**100.0**

Note: ABS data are unweighted and identity crime survey data are weighted

Source: ABS 2018; Identity crime survey 2018 [AIC data file]

Language

Almost all survey respondents (94%) indicated that English was the language most often spoken at home (see Table 2). One hundred and fifty respondents (1.6%) indicated they spoke a language not listed. These responses included a range of Eastern and Western European languages not listed (*n*=29), Nepali (14), Bengali (*n*=12), Urdu (*n*=10), Malaysian (*n*=7) and other Chinese dialects (*n*=6).

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

Language	*n*	%
English	9,290	93.7
Mandarin	76	0.8
Hindi	75	0.8
Cantonese	64	0.6
Vietnamese	32	0.3
German	25	0.3
Arabic	24	0.2
Spanish	23	0.2
French	21	0.2
Telugu	21	0.2
Tamil	19	0.2
Indonesian	19	0.2
Italian	11	0.1
Greek	11	0.1
Farsi	10	0.1
Korean	9	0.1
Russian	9	0.1
Japanese	6	0.1
Swahili	2	<0.1
Other	150	1.5
I'd rather not say	17	0.2
Total	**9,911**	**100.0**

Note: Percentages may not total 100 due to rounding. Data are weighted and may not total 9,911 due to rounding

Source: Identity crime survey 2018 [AIC data file]

Indigenous status

Four percent of survey respondents self-identified as being of Aboriginal or Torres Strait Islander descent or both, which was 1.4 percentage points more than the number so identifying in the 2016 census (see Table 3).

Table 3: Respondents by Indigenous status

Source	ABS Census data 2016	Survey sample data	
Indigenous status	%	*n*	%
Aboriginal	2.5	346	3.5
Torres Strait Islander	0.1	29	0.3
Both Aboriginal and Torres Strait Islander	0.1	39	0.4
All Indigenous	2.8	414	4.2
Non-Indigenous	91.0	9,397	94.8
I'd rather not say	6.2	100	1.0
Total	**100.0**	**9,911**	**100.0**

Note: Survey data are weighed, ABS data are not. ABS Census data were used as the Australian demographic statistics for June 2018 did not contain details about Indigenous status

Source: ABS 2017; Identity crime survey 2018 [AIC data file]

Income

Respondents were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2017–18 (Table 4). Respondents most commonly reported having income of between $37,000 and $80,000 (29%). Almost 10 percent of respondents preferred not to divulge their income.

Table 4: Respondents by individual gross income, 2017–18

Income	*n*	%
$0–$18,200	1,863	18.8
$18,201–$37,000	2,087	21.1
$37,001–$80,000	2,843	28.7
$80,001–$180,000	1,817	18.3
$180,001 and over	323	3.3
I'd rather not say	978	9.9
Total	**9,911**	**100.0**

Note: Percentages may not total 100 due to the rounding of weighted data

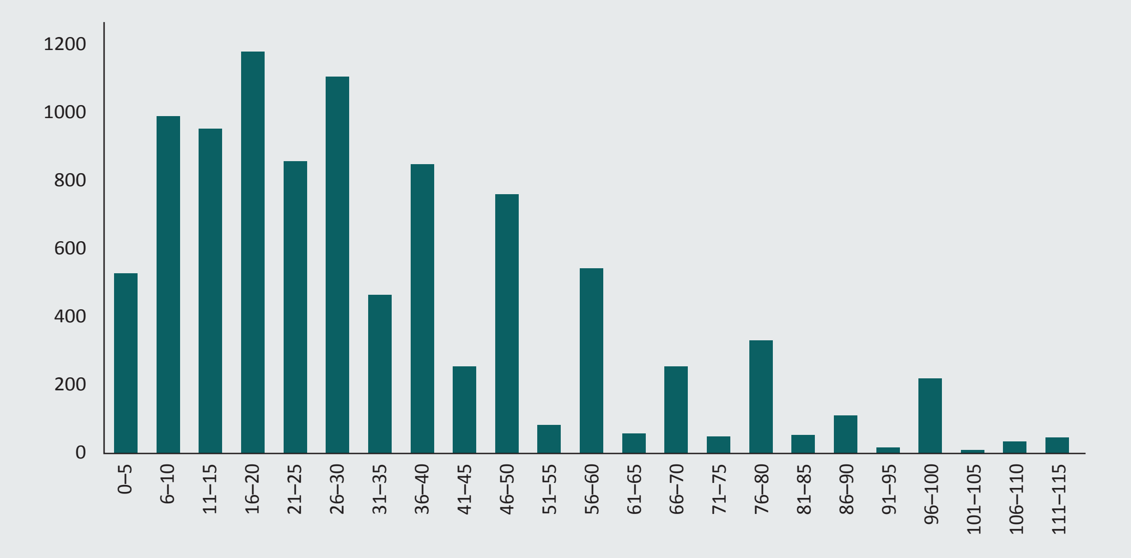
Source: Identity crime survey 2018 [AIC data file]

Computer use

Respondents were asked how many hours in the previous week they had spent using a computer or device (including desktop computers, laptops, smartphones and tablets; see Figure 2). Responses (after weighting) ranged from 0 to 115 hours (mean=34.3, *SD*=24.1, *n*=9,764). One-hundred and forty-seven respondents indicated that they used a computer or device 116 hours or more, which equates to over 16 hours per day. Of these, 22 respondents reported using computers or devices for 168 hours per week (24 hours a day). Such responses could, arguably, have come from respondents who used digital devices such as watches, fit-bits, and other digital monitors while sleeping. These responses were excluded from analyses involving time spent using a computer or device. Those participants were retained in the sample for other analyses.

There was no change in the average number of hours participants spent using a computer or device between 2017 (mean=34.6 hours) and 2018 (mean=34.3 hours).

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

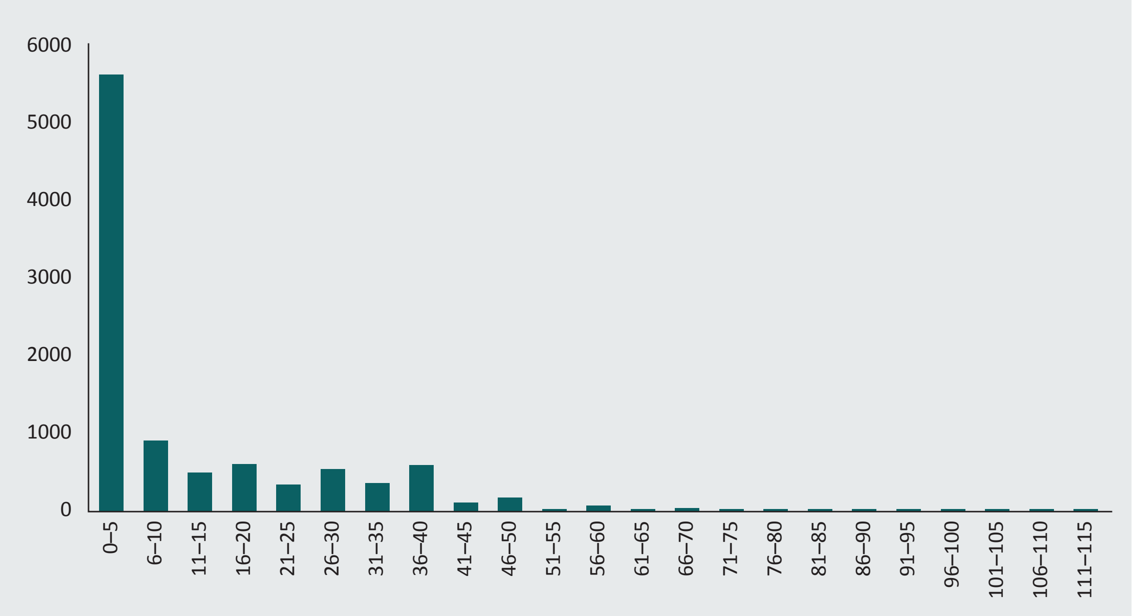


Note: Excludes responses greater than 115 hours. Weighted figures may not total 9,911 due to rounding

Source: Identity crime survey 2018 [AIC data file]

Respondents were also asked how many hours in the previous week they had spent using a computer or device for work-related activities. Responses ranged from zero to 168 hours. However, as above, only responses less than 116 hours were included in the analysis. Therefore, the range included was 0 to 116 hours (mean=11.8, *SD*=16.2, *n*=9,897). As shown in Figure 3, the vast majority of respondents (95%) reported spending 40 hours or less using computers or devices for work in the previous week, with 77 percent of respondents reporting 20 hours or less. The average number of hours spent using a computer or device for work-related activities was the same in the 2017 and 2018 surveys (12 hours).

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



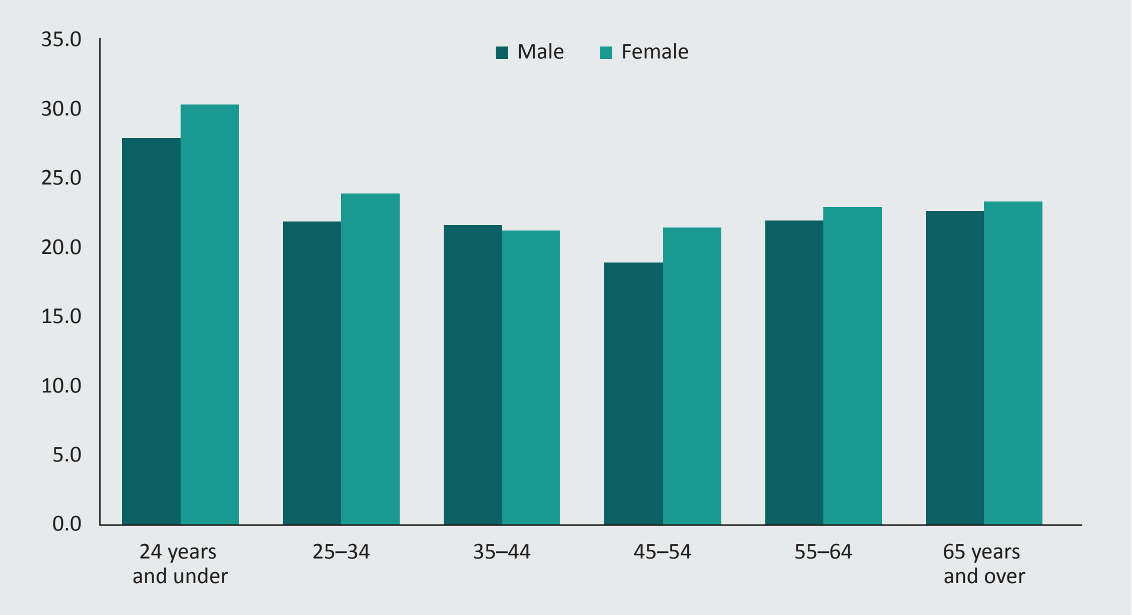
Note: Data are weighted. Excludes responses over 115 hours. *n*=9,897

Source: Identity crime survey 2018 [AIC data file]

The number of hours spent using computers or devices for work purposes was deducted from the total hours to determine the number of hours spent on non-work related activities (see Figure 4). On average, respondents reported spending 25.0 hours on computers or devices per week for non-work related activities (*SD*=20.9, *n*=9,176). This is more than double the average number of hours per week spent on the internet for personal use reported in ABS data for 2014–15 (ABS 2016a).

However, the survey finding is similar to findings from a recent global survey (using a non-probability sample) undertaken by We Are Social and Hootsuite. The global survey found Australians spent an average of 5 hours and 34 minutes a day using the internet via any device (We Are Social 2018), or roughly 27 hours a week. Respondents aged 24 years or under reported a significantly greater number of non-work related computer hours per week than all other age groups: *F*(5, 9,231)=25.26, *p*<0.001 (log transformation of computer hours).

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



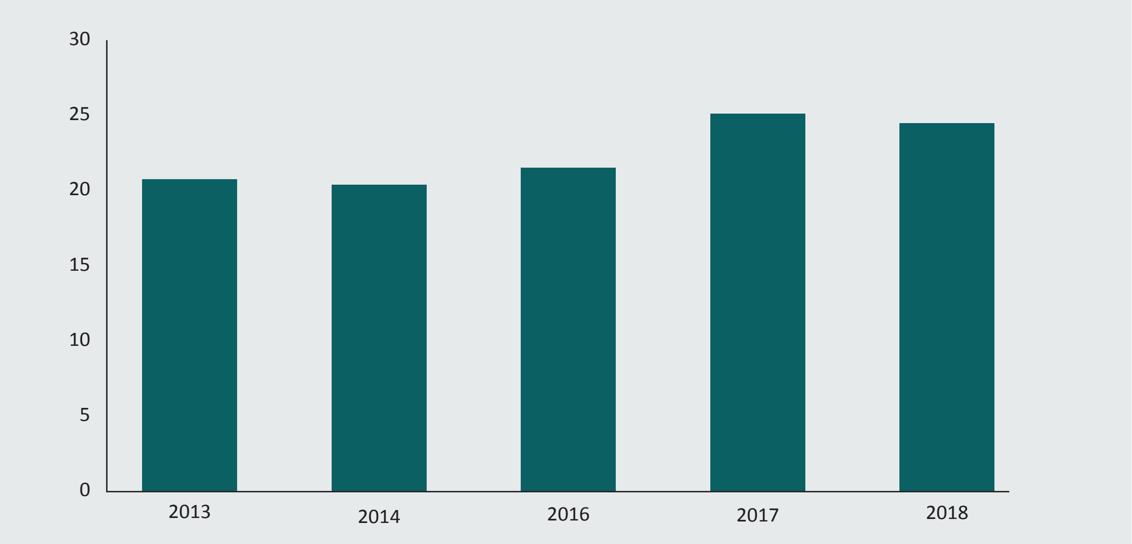
Source: Identity crime survey 2018 [AIC data file]

Prevalence of identity crime

Lifetime victimisation

One in four respondents (25%) reported they had experienced misuse of their personal information at some point in their lifetime (see Figure 5). There was a slight decrease in the number of respondents reporting lifetime victimisation between 2017 and 2018, but this decline was not statistically significant (N-1 $\chi^2(1)=1.303$, $p=0.25$). However, the 3.7 percentage point rise in lifetime victimisation between 2016 and 2018 was statistically significant (N-1 $\chi^2(1)=25.242$, $p<0.001$).

Figure 5: Lifetime victimisation rates of respondents, 2013 to 2018 (weighted data) (%)

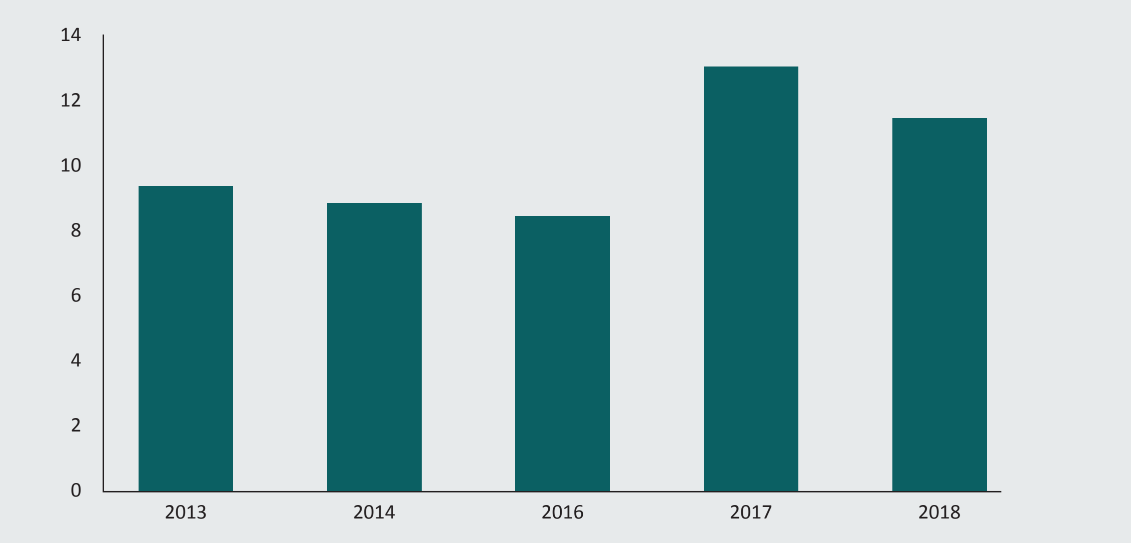


Source: Identity crime surveys 2013, 2014, 2016, 2017 and 2018 [AIC data file]

Victimisation in the last 12 months

Twelve percent of respondents (*n*=1,136) reported that they had experienced misuse of their personal information in the last 12 months (hereafter referred to as recent victimisation; see Figure 6). This was a non-significant decrease from 2017, when 13 percent of respondents (*n*=1,307) reported recent victimisation (N-1 $\chi^2(1)=1.44$, $p=0.23$). However, there was a statistically significant three percentage point increase in recent victimisation between 2016 and 2018 (N-1 $\chi^2(1)=4.76$, $p<0.05$).

Figure 6: Respondents experiencing misuse of personal information in the last 12 months, 2013 to 2018 (weighted data) (%)



Source: Identity crime survey 2013, 2014, 2016, 2017 and 2018 [AIC data file]

Geographic location

The 2018 recent victimisation data were examined against geographic location to see if the decline occurred in particular geographic locations or Australia-wide (see Table 5). There were very few significant changes in the proportion of respondents experiencing misuse of their personal information based on geographic location. Two areas showed a significant decrease in recent victimisation. One was ‘other Western Australia’, where recent victimisation reduced from 12 percent of respondents in 2017 to eight percent in 2018. A similar number of respondents from that area participated in the 2017 and 2018 surveys (*n*=183 in 2017 and *n*=199 in 2018), indicating the sample size did not influence victimisation rates.

The other area where a significant reduction in victimisation occurred was the Northern Territory. The victimisation rate for Darwin and ‘other Northern Territory’ combined decreased from 28 percent of respondents in 2017 to 15 percent in 2018. The 2018 survey included a larger number of respondents from the Northern Territory (*n*=67) than the 2017 survey (*n*=49), minimising the chances the difference in victimisation rates was due to sample size alone.

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

Location	2017	2018		% change
	%	%	*n*	
Sydney	15.2	13.2	261	-2.0
Other New South Wales	12.6	11.4	128	-1.2
Melbourne	10.8	12.2	236	+1.4
Other Victoria	14.3	12.1	71	-2.2
Brisbane	10.6	9.4	100	-1.2
Other Queensland	9.1	9.4	101	+0.3
Perth	11.3	11.4	87	+0.1
Other Western Australia	11.5	7.5	15	-4.0**
Adelaide	8.5	9.6	58	+1.1
Other South Australia	10.0	8.8	16	-1.2
ACT (including Canberra)	10.5	9.6	11	-0.9
Hobart	10.3	10.7	11	+0.4
Other Tasmania	9.5	13.2	17	+3.7
Northern Territory (including Darwin)	27.8	14.9	10	-12.9***
National	11.7	11.3	1,122	-0.4

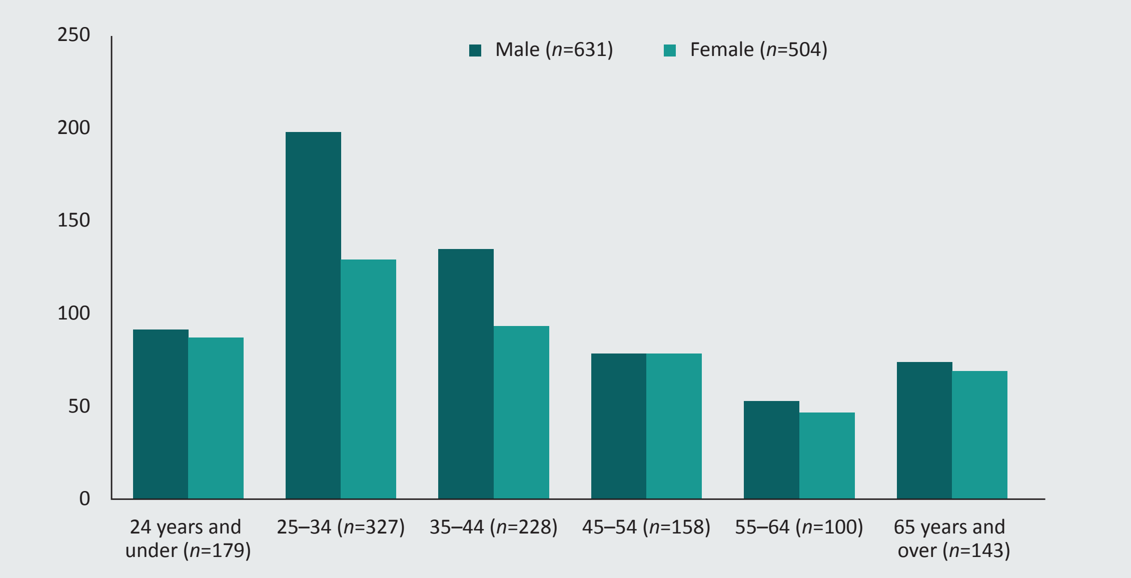
***statistically significant at *p*<0.001, **statistically significant at *p*<0.01

Source: Identity crime survey 2017 and 2018 [AIC data file]

Gender and age

Consistent with findings from 2017, males between 25 and 34 years of age were the group most likely to report recent victimisation (see Figure 7). Overall, males were significantly more likely than females to report having experienced misuse of personal information in the last 12 months ($\chi^2(1, n=9,911)=20.66, p<0.001, V=-0.03$; see Table 6). Respondents between 25 and 44 years of age were more likely to experience personal information misuse than those in other age groups ($\chi^2(5, n=9,911)=142.94, p<0.001, V=0.11$; see Table 7).

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



Source: Identity crime survey 2018 [AIC data file]

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

Gender	Recent victimisation		
	Yes	No	Total
Male	631***	4,249	4,881
Female	504	4,526	5,030
Total	**1,136**	**8,854**	**9,911**

***statistically significant at *p*<0.001

Notes: Cells may not add to totals due to weighted data and rounding

Source: Identity crime survey 2018 [AIC data file]

Table 7: Recent victimisation by age (weighted data)

Age group	Recent victimisation		Total
	n	%	*n*
24 years and under	179	14.1	1,270
25–34 years	327***	16.5	1,976
35–44 years	229***	12.1	1,887
45–54 years	158	9.6	1,647
55–64 years	100	6.0	1,661
65 years and over	143	9.7	1,470
Total	**1,136**	**11.5**	**9,911**

***statistically significant at *p*<0.001

Note: Percentages are of recent victims in each age group. Percentages may not total 100 due to rounding

Source: Identity crime survey 2018

Indigenous status

Respondents who self-identified as Aboriginal or Torres Strait Islander were more likely to report having had their personal information misused in the previous 12 months. Respondents who identified as non-Indigenous were significantly less likely to have reported recent victimisation: $\chi^2(3, n=9{,}811)=416.27, p<0.001, V=0.18$ (Table 8).

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

Indigenous status	Recent victimisation		
	Yes	No	Total
Aboriginal	147***	199	346
Torres Strait Islander	9	20	29
Both Aboriginal and Torres Strait Islander	20	19	39
Non-Indigenous	946	8,451***	9,397
Total	**1,122**	**8,689**	**9,811**

***statistically significant at *p*<0.001

Note: 100 respondents did not provide their Indigenous status, so analyses for this variable had a sample size of 9,811

Source: Identity crime survey 2018 [AIC data file]

Computer use

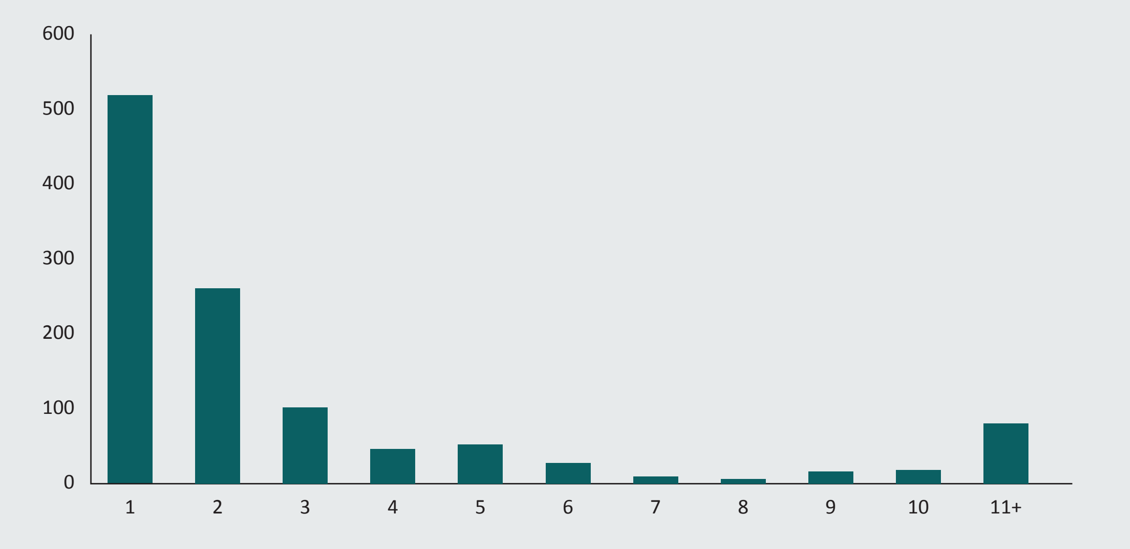
Data on the use of computers and devices were examined to see if computer use is associated with victimisation through misuse of personal information in the last 12 months. There were no significant associations between recent victimisation and either work-related or total hours spent using a computer or device. However, a significant association was found between recent victimisation and the mean number of hours spent using a computer or device for personal use. Recent victims reported using a computer for personal use fewer hours than those who did not experience misuse. As there were significant differences between the groups, Welch's *t*-test was used ($t(1155.1, 9{,}231)=-2.45, p<0.05$). Recent victims spent an average of 2.8 hours ($SD=1.14$) per week using computers or devices for non-work purposes, compared with 2.9 hours ($SD=0.9$) per week for non-victims.

Characteristics of recent incidents

Number of incidents

Forty-six percent (*n*=520) of recent victims reported that their personal information had been misused on only one occasion (see Figure 8). This proportion is slightly lower than that of the 2017 survey, where 50 percent of respondents (*n*=654) believed their personal information was misused on just one occasion (Goldsmid, Gannoni & Smith 2018). In 2018, 23 percent (*n*=262) of respondents reported misuse of personal information had occurred on two separate occasions, slightly higher than the 21 percent of respondents who reported this in 2017. On average, recent victims reported their personal information had been misused on four separate occasions (mean=4.2, *SD*=10.08).

Figure 8: Number of separate occasions on which respondents believed their personal information had been misused (weighted data) (*n*)



Source: Identity crime survey 2018 [AIC data file]

Most serious occasion of recent misuse

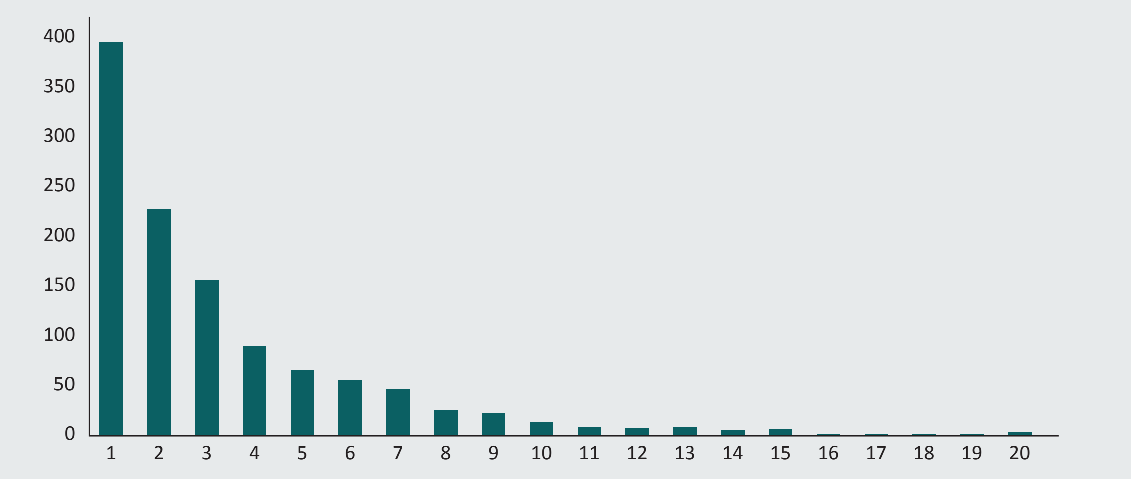
Respondents who had experienced misuse of their personal information in the last 12 months were asked to identify the most serious occasion of misuse. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the respondent. This occasion was selected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

Types of information misused on most serious occasion of misuse

Recent victims reported that between one and 20 different types of personal information had been misused on the most serious occasion of victimisation in the last 12 months (see Figure 9). On average, recent victims reported that three types of information had been misused (mean=3.3, *SD*=3.0, *n*=1,136). Only five percent of victims reported 10 or more types of personal information had been misused.

Of the 35 percent (*n*=396) of victims who reported misuse of only one type of personal information, 51 percent (*n*=200) reported that the information misused was credit/debit card details. The second most common response was misuse of a name (13%, *n*=52), followed by bank account details (10%, *n*=40).

Figure 9: Number of types of personal information misused on the most serious occasion in the last 12 months (weighted data) (*n*)



Source: Identity crime survey 2018 [AIC data file]

Among all recent victims, a person's name (47%) was the type of personal information most commonly reported as having been misused on the most serious occasion of misuse (see Table 9). This was followed by credit/debit card information (44%), then address details (32%). The 2017 survey also found names and credit/debit card details were the two most common types of information misused on the most serious occasion (45% and 36%, respectively).

Although names remained the type of personal information most commonly misused, misuse of credit/debit card information increased significantly by eight percentage points, from 36 percent in 2017 to 44 percent in 2018. This finding differs from that of the 2017 survey, which found that misuse of credit/debit card details had decreased 14 percentage points from the previous year (Goldsmid, Gannoni & Smith 2018).

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

Type of personal information	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
Name	45.2	46.8	532	+1.6
Credit/debit card information	36.2	44.2	502	+8.0***
Address	35.8	32.0	363	-3.8
Date of birth	32.2	30.5	346	-1.7
Bank account information	26.1	28.9	328	+2.8
Password	20.3	23.2	264	+2.9
Gender	18.1	20.8	236	+2.7
Online account username	10.3	13.4	152	+3.1*
Place of birth	14.6	13.2	150	-1.4
Driver licence information	14.4	12.1	137	-2.3
Computer username	8.4	9.6	109	+1.2
Personal identification number (PIN)	8.8	9.2	105	+0.8
Signature	8.2	8.5	96	+0.3
Passport	8.5	8.0	91	-0.5
Tax file number	7.9	7.9	90	0.0
Medicare information	7.5	7.5	85	0.0
Shareholder information number	2.8	2.9	33	+0.1
Biometric information (eg fingerprint)	2.8	2.5	28	-0.3
Student number	2.5	1.8	21	-0.7
Other	4.5	5.7	65	+1.2

***statistically significant at *p*<0.001, *statistically significant at *p*<0.05

Note: Respondents could select multiple responses

Source: Identity crime survey 2017 and 2018 [AIC data file]

How personal information was obtained on most serious occasion of misuse

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

The forms of access that experienced the greatest increase between 2017 and 2018 were theft or hacking of a computer or computerised device (6 percentage points) and information lost or stolen from a business or organisation (data breach—4 percentage points). The forms of access most commonly reported in 2017 decreased in 2018. Personal information being obtained via telephone (excluding text messages) decreased by six percentage points, while personal information being accessed through a face-to-face meeting decreased seven percentage points. There was also a five percentage point reduction in the number of respondents who reported their personal information was obtained via an ATM or EFTPOS machine.

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

Way of obtaining personal information	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
Theft or hacking of a computer or computerised device	18.2	24.4	277	+6.2***
Telephone (excluding text message)	24.9	19.3	219	-5.6**
Email	21.4	18.7	212	-2.7
Online banking transaction	17.1	18.4	209	+1.3
Face-to-face meeting (eg job interview or doorknock appeal)	23.2	16.5	188	-6.7***
Text message	18.8	16.0	182	-2.8
Website other than social media (eg online shopping)	11.5	12.9	147	+1.4
From information lost or stolen from a business or other organisation (ie data breach)	8.9	12.4	141	+3.5*
Social media (eg Facebook, Linked-in)	9.9	8.9	101	-1.0
From an ATM or EFTPOS transaction	11.6	6.5	74	-5.1***
From a person I know	4.0	5.3	60	+1.3
Theft of mail	3.4	3.9	44	+0.5
Theft of identity or other personal document	1.8	2.9	33	+1.1
Theft of a copy of an identity or other personal document	0.7	1.4	16	+0.7
Other	2.9	3.1	35	+0.2
Don't know	14.7	16.0	182	+1.3

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05

Note: Respondents could select multiple responses

Source: Identity crime survey 2017 and 2018 [AIC data file]

How personal information was misused on most serious occasion of misuse

The most common reason personal information had been misused on the most serious occasion of misuse, according to respondents, was to obtain money from a bank (excluding superannuation). Forty-one percent of respondents selected this reason (see Table 11). This was also the most common reason reported in 2017 (38%) and in 2016 (31%). There was a 13 percentage point rise in recent victims reporting that their personal information had been misused in multiple ways (35% in 2017 vs 48% in 2018). Recent victims reported, on average, having their personal information used in two ways (mean=1.9, *SD*=1.3).

A few statistically significant differences were found between the 2017 and 2018 surveys in how personal information was misused. There was a statistically significant increase in the misuse of personal information to purchase something (5 percentage points; N-1$\chi^2(1)=9.98$, $p<0.05$). The misuse of personal information to file a fraudulent tax return decreased six percentage points (N-1$\chi^2(1)=13.22$, $p<0.001$), while misuse for the purpose of obtaining superannuation monies also declined (4 percentage points; N-1$\chi^2(1)=8.76$, $p<0.01$). However, the reduction between 2017 and 2018 in the number of respondents reporting their personal information had been misused to file a tax return (16% in 2018 vs 22% in 2017) indicates that ATO scams in the latter half of 2018 did not affect this sample as much as the wider population (ATO 2018).

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

Purpose of misuse	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
To obtain money from a bank (excluding superannuation)	37.5	41.2	468	+3.7
To purchase something	16.4	21.4	243	+5.0**
To file a fraudulent tax return	21.8	15.9	181	-5.9***
To obtain superannuation monies	17.1	12.8	145	-4.3**
To obtain money from an investment	10.6	10.1	115	-0.5
To apply for a loan or obtain credit	9.9	8.3	94	-1.6
To apply for a job	8.8	6.1	69	-2.7*
To apply for government benefits	6.7	5.6	64	-1.1
To open a mobile phone account	7.7	5.1	58	-2.6*
To open an online account (eg Facebook, eBay)	3.0	4.1	47	+1.1
To provide false information to police	4.0	4.0	45	0.0
To rent property	2.0	2.0	23	0.0
Other	5.5	6.6	75	+1.1
Don't know	11.5	13.8	157	+2.3

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

Note: Respondents could select multiple responses

Source: Identity crime survey 2017 and 2018 [AIC data file]

Detection of most serious occasion of misuse

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

As in 2017, victims were most commonly notified of the misuse of their personal information by a bank, financial institution or credit card company (42%). The majority of respondents (73%) reported detection of the misuse of their personal information via one method, 16 percent reported two different methods and 10 percent of respondents reported three or more detection methods (mean=1.46, *SD*=0.99).

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

Detection method	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
Notified by a bank, financial institution or credit card company	40.8	42.2	479	+1.4
Noticed suspicious transactions in bank statements or accounts	33.0	37.5	426	+4.5*
Notified by police	27.5	18.0	204	-9.5***
Received a bill for which they were not responsible	11.1	11.7	133	+0.6
Was unsuccessful in applying for credit	10.1	11.1	126	+1.0
Contacted by debt collectors	4.4	5.2	59	+0.8
Notified by another company	3.5	4.1	47	+0.6
Notified by a government agency other than the police	1.8	1.0	11	-0.8
Other	10.5	15.6	177	+5.1***

***statistically significant at $p<0.001$; *statistically significant at $p<0.05$

Source: Identity crime survey 2017 and 2018 [AIC data file]

There were few significant changes between 2017 and 2018 in how victims detected the misuse of their personal information. However, the number of respondents reporting they had been notified by the police decreased by nearly 10 percentage points ($N\text{-}1\chi^2(1)=30.88$, $p<0.001$). Also, a significantly greater proportion of respondents detected the misuse themselves when reviewing their bank statements or accounts—an increase of nearly five percentage points ($N\text{-}1\chi^2(1)=5.40$, $p<0.05$).

Economic losses

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

Respondents were asked to estimate their total out-of-pocket losses from all occasions of misuse of personal information experienced in the last 12 months (see Table 13). Respondents were instructed to exclude from this estimate any money recovered or reimbursed and any costs associated with repairing any damage done.

Total out-of-pocket losses suffered by victims reduced by almost $1m between 2017 and 2018, ($2,994,786 in 2017 vs $1,968,509 in 2018). This was because the proportion of respondents who lost over $50,000 halved between 2017 and 2018.

Table 13: Summary statistics for out-of-pocket losses for all personal information misuse experienced in the last 12 months

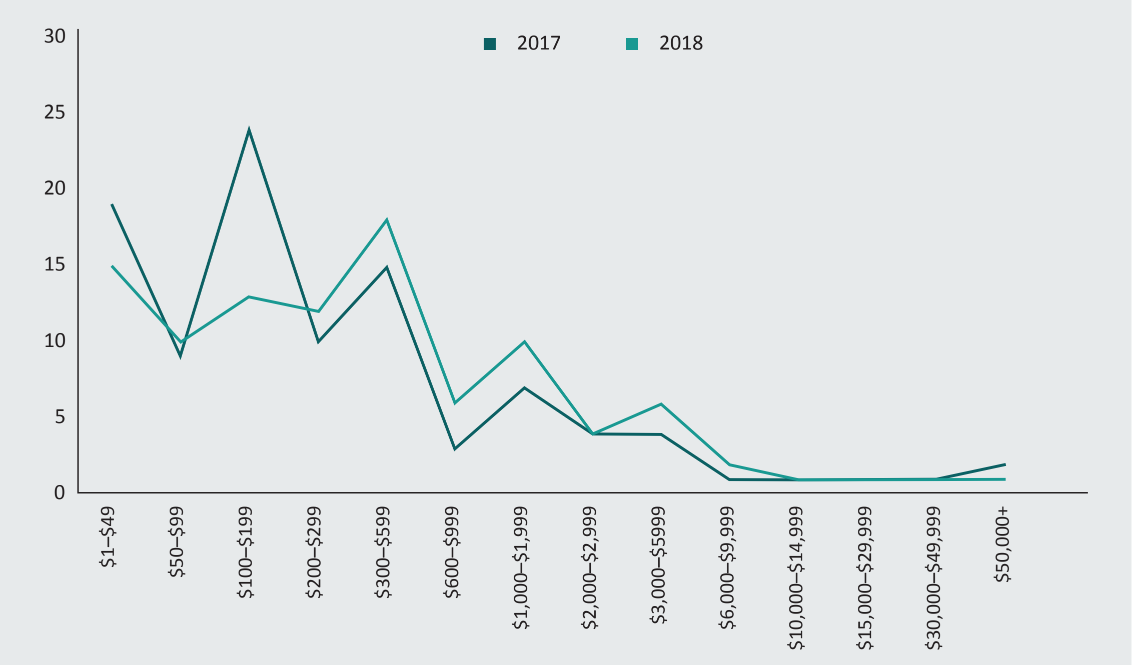
Statistic	2017	2018
Number of respondents (*n*)	950	945
Percentage of all respondents (%)	9.6	9.5
Minimum ($)	1	1
Maximum ($)	341,541	300,000
Mean ($)	3,101	2,083
Median ($)	150	300
Standard deviation ($)	20,199	13,228
25% quartile ($)	65	100
75% quartile ($)	498	1,000
Total losses ($)	**2,944,786**	**1,968,509**

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

Source: Identity crime survey 2017 and 2018 [AIC data file]

The distribution of out-of-pocket losses (see Figure 10) shows the spike in small losses ($100–$199) observed in 2017 did not occur in 2018. The 2017 and 2018 distributions of out-of-pocket losses were otherwise fairly consistent, although some of the changes were more pronounced in 2018 than in 2017. For example, in 2018 more respondents reported losses in the $300–$599, $1,000–$1,999 and $3,000–$5,999 ranges. This suggests that respondents experienced higher losses in 2018 than in 2017, when the largest difference was at the lower value of $100–$199.

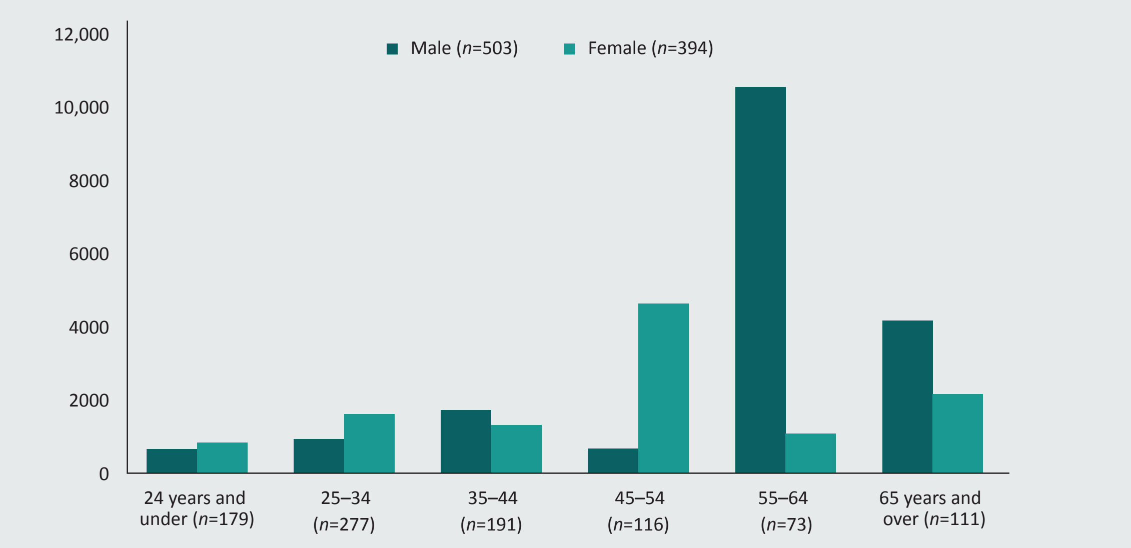
Figure 10: Distribution of total financial out-of-pocket losses, 2017 and 2018 (weighted data) (%)



Source: Identity crime surveys 2017 and 2018 [AIC data file]

Male respondents aged 55–64 years and over reported the highest mean financial losses in 2018 ($10,590; see Figure 11). This was followed by females aged 45–54 years (mean=$4,677), and then males aged 65 years and over (mean=$4,201). Females aged 24 years and under ($859 vs $691) and 25–34 years ($1,669 vs $964) reported slightly higher losses than their male counterparts. However, apart from the three oldest age categories, gender disparity was only slight, with male and female respondents aged below 45 years reporting similar levels of loss.

Figure 11: Mean total out-of-pocket losses in the last 12 months by age and gender (weighted data) ($)



Source: Identity crime survey 2018 [AIC data file]

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

Respondents were asked to report out-of-pocket losses for the most serious occasion of misuse of personal information in the last 12 months (excluding any money that they were able to recover from banks and any costs associated with repairing any damage done). The total out-of-pocket loss for 2018 was $1,786,572, a reduction of 26 percent from the out-of-pocket losses in 2017 ($2,421,433). The mean out-of-pocket loss reported was $1,974, which was lower than the $2,711 reported in 2017 (see Table 14).

Table 14: Summary statistics for out-of-pocket losses for the most serious occasion of misuse in the last 12 months (weighted data)

Statistic	2017	2018
Number of respondents (*n*)	893	905[a]
Percentage of all respondents (%)	9.0	9.1
Minimum ($)	1	1
Maximum ($)	350,000	300,000
Mean ($)	2,711	1,974
Median ($)	136	200
Standard deviation ($)	18,474	13,449
25% quartile ($)	69	77
75% quartile ($)	555	800
Total ($)	**2,421,433**	**1,786,572**

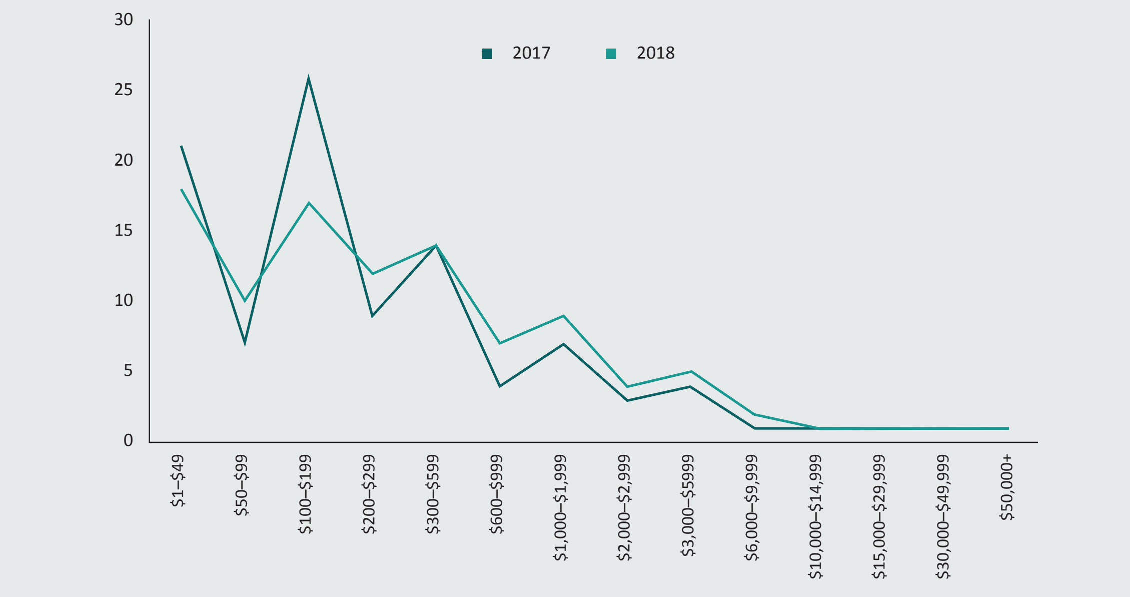
a: One respondent in 2018 advised losses from the most serious occasion of misuse of personal information were $1,500,000. Based on other responses from the respondent this loss amount was considered an outlier and was not included in the summary statistics above

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

Source: Identity crime survey 2017 and 2018 [AIC data file]

The 2018 distribution of out-of-pocket losses for the most serious occasion of misuse (see Figure 12) tends to mirror the peaks and troughs of the 2017 distribution, with the exception of losses in the $100 to $199 category, which were considerably lower in 2018 than in 2017. In higher amount categories, there were consistently more losses in 2018 than in 2017.

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



Note: Percentages may not total 100 due to rounding. One respondent in 2018 advised losses from the most serious occasion of misuse were $1,500,000; this amount was assessed as an outlier and was not included in the analysis

Source: Identity crime survey 2017 and 2018 [AIC data file]

Total losses recovered in the last 12 months

The total amount of monies recovered fell substantially, from $3,419,039 in 2017 to just $631,800 in 2018 (see Table 15). This decrease was also reflected in the mean (dropping from $3,350 in 2017, to $817 in 2018), although the median amount recovered remained the same ($200). The amounts recovered have been decreasing over the past three years. For example, the maximum amounts recovered were $4.5m in 2016, $700,000 in 2017 and $25,000 in 2018.

Table 15: Summary statistics of total losses recovered in the last 12 months (weighted data)

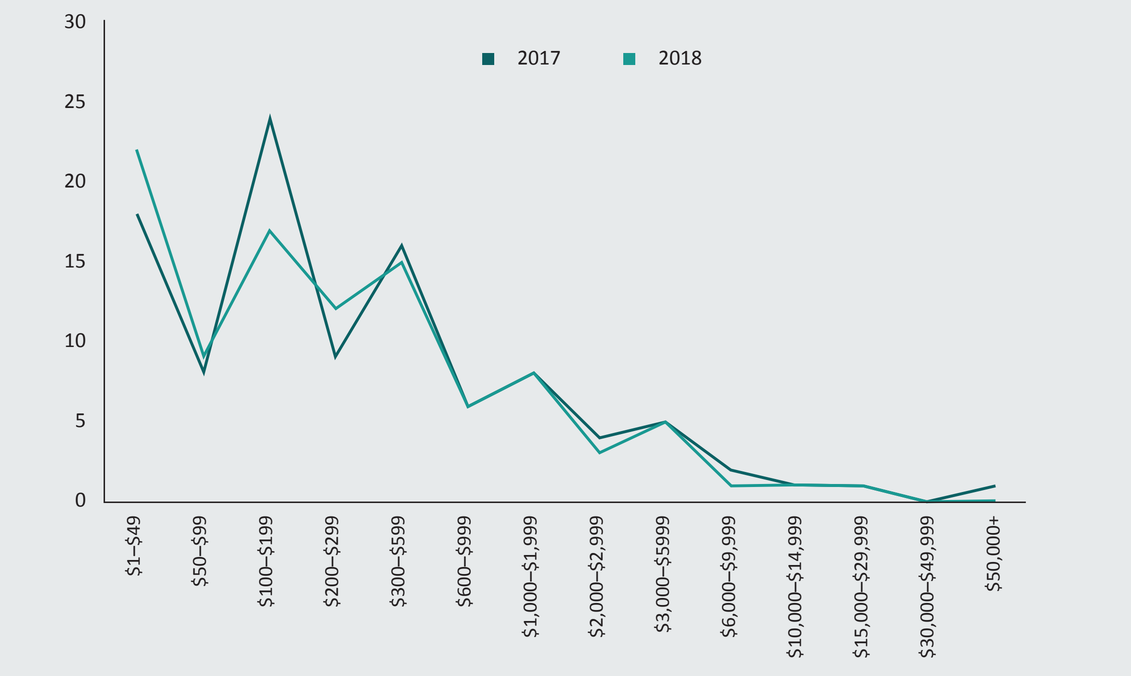
Statistic	2017	2018
Number of respondents (*n*)	1,021	773
Percentage of all respondents (%)	10.3	7.8
Minimum ($)	1	1
Maximum ($)	700,000	25,000
Mean ($)	3,350	817
Median ($)	200	200
Standard deviation ($)	36,882	2,200
25% quartile ($)	86	50
75% quartile ($)	700	600
Total ($)	**3,419,039**	**631,800**

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

Source: Identity crime survey 2017 and 2018 [AIC data file]

The distribution of total losses recovered in the last 12 months was generally similar in 2017 and 2018, apart from considerably more recoveries in the $100 to $199 category in 2017 than in 2018 (see Figure 13). This distribution follows that in Figure 12 for financial losses experienced in the last 12 months

Figure 13: Distribution of amounts recovered in the last 12 months (weighted data) (%)



Source: Identity crime survey 2017 and 2018 [AIC data file]

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

The total of amounts recovered in 2018 for the most serious occasion of personal information misuse in the last 12 months was approximately one-third of the total recovered in 2017 ($569,342 recovered in 2018 vs $1,500,352 in 2017; see Table 16). The mean amount of money recovered in 2018 was approximately half that recovered in 2017 ($730 vs $1,526 in 2017). However, the median amount recovered remained the same at $200.

Table 16: Summary statistics for recovered losses relating to the most serious occasion of misuse of personal information in the last 12 months (weighted data) ($)

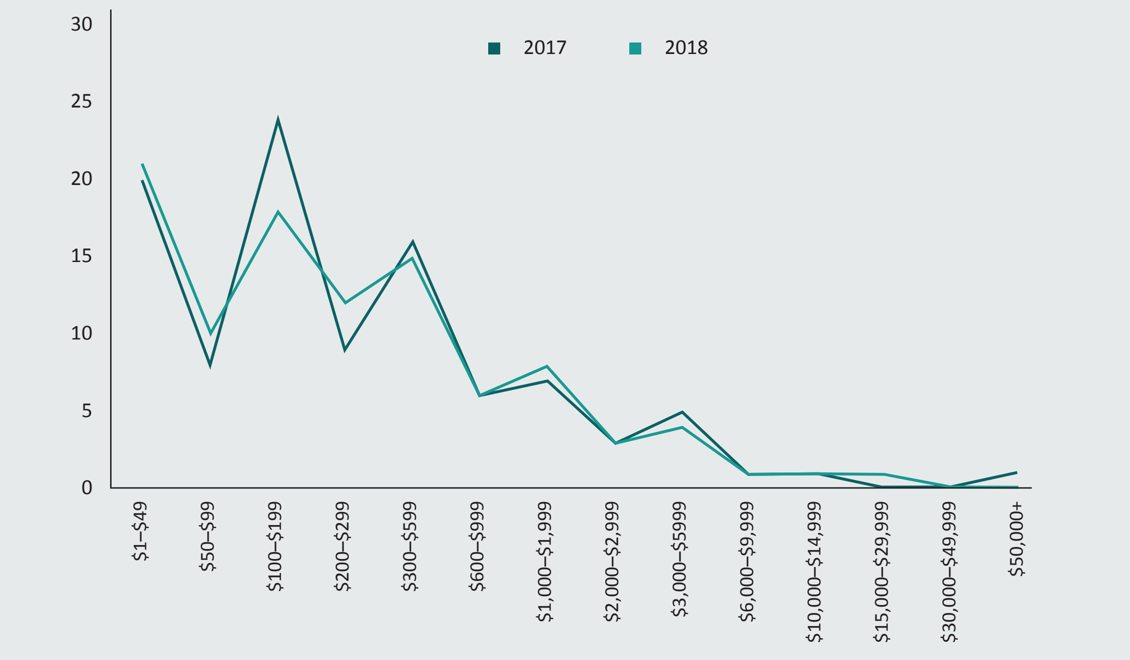
Statistic	2017	2018
Number of respondents (*n*)	983	780
Percentage of all respondents (%)	9.9	7.9
Minimum ($)	1	1
Maximum ($)	160,000	25,000
Mean ($)	1,526	730
Median ($)	200	200
Standard deviation ($)	9,719	1,930
25% quartile ($)	80	28
75% quartile ($)	600	530
Total ($)	**1,500,352**	**569,342**

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

Source: Identity crime survey 2017 and 2018 [AIC data file]

The distribution of losses recovered for the most serious occasion of misuse of personal information in the last 12 months (Figure 14) shows that recoveries in 2018 followed a similar pattern to recoveries in 2017, with two exceptions. First, the proportion of respondents who recovered between $100 and $199 decreased between 2017 and 2018, such that in 2018 the largest proportion of respondents recovered less than $50. Second, a larger proportion of respondents recovered between $200 and $299 in 2018 compared with 2017.

Figure 14: Distribution of losses recovered for the most serious occasion of misuse in the last 12 months (weighted data) (%)



Source: Identity crime survey 2017 and 2018 [AIC data file]

Impact on victims

Consequences of personal information misuse

Respondents who reported experiencing misuse of their personal information in the last 12 months were asked to indicate what consequences they experienced as a result of that misuse. There was a statistically significant increase in the proportion of respondents who did not experience any consequences as a result of their personal information being misused (34% in 2017 vs 47% in 2018). In line with this finding, the proportion of respondents who were refused credit as a consequence of having their personal information misused decreased by a significant margin, from 35 percent of recent victims in 2017 to 27 percent in 2018 (see Table 17). There were small but statistically significant increases in the proportion of respondents experiencing 'other reputational damage' (2% in 2017 vs 3% in 2018) and 'refusal of other services' (1% in 2017 vs 2% in 2018) as a result of their personal information being misused.

Table 17: Consequences experienced as the result of personal information being misused in the previous 12 months (weighted data)

Consequences	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
I was refused credit	34.9	27.2	309	-7.6***
I was refused government benefits	14.9	14.7	167	-0.2
I experienced mental or emotional distress requiring counselling or other treatment	12.3	13.8	157	+1.5
I experienced financial difficulties resulting in the repossession of a house, land, motor vehicle or other items	13.3	12.2	139	-1.1
I had to commence legal action to clear debts and/or to clear my name	11.2	11.8	134	+0.6
I was wrongly accused of a crime	10.6	10.3	117	-0.3
I experienced physical health problems requiring medical treatment by a doctor	5.6	5.9	67	+0.3
I experienced other reputational damage	1.9	3.2	36	+1.3*
I was refused other services	1.3	2.4	27	+1.1*
I experienced other consequences not mentioned above	7.1	8.6	97	+1.5
I did not experience any consequences as a result of the misuse of my personal information	34.4	46.6	529	+12.2***

***statistically significant at $p<0.001$, *statistically significant at $p<0.05$

Note: Respondents could select multiple responses

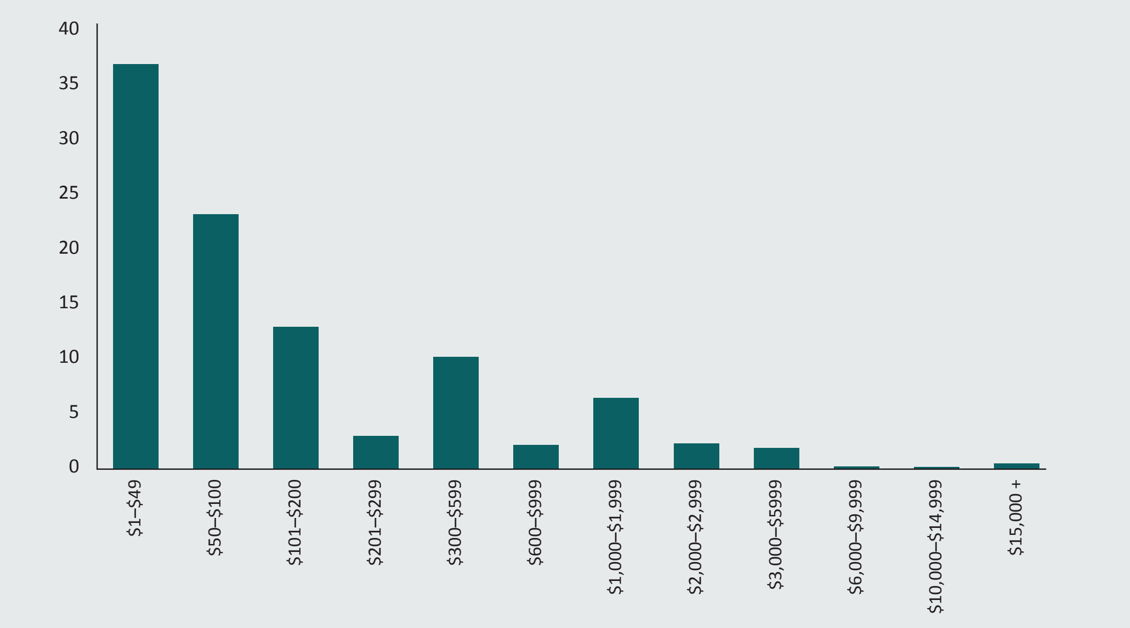
Source: Identity crime survey 2017 and 2018 [AIC data file]

Money and time spent rectifying misuse of personal information

Recent victims were asked how much money they spent dealing with the consequences of having their personal information misused. Costs associated with rectifying incidents of personal information misuse may include the cost of legal advice, the cost of obtaining a credit report, any bank fees or charges that are not reimbursed, and the costs of telephone calls made to resolve the issue or to seek advice.

Of those who had experienced misuse of their personal information in the last 12 months, 51 percent (*n*=582) incurred financial costs in dealing with the consequences. Details of the losses are presented in Figure 15. Sixty percent of these respondents spent $100 or less; however, five percent of recent victims spent $2,000 or more dealing with the misuse of their personal information.

Figure 15: Total money spent dealing with the consequences of misuse of personal information (%)



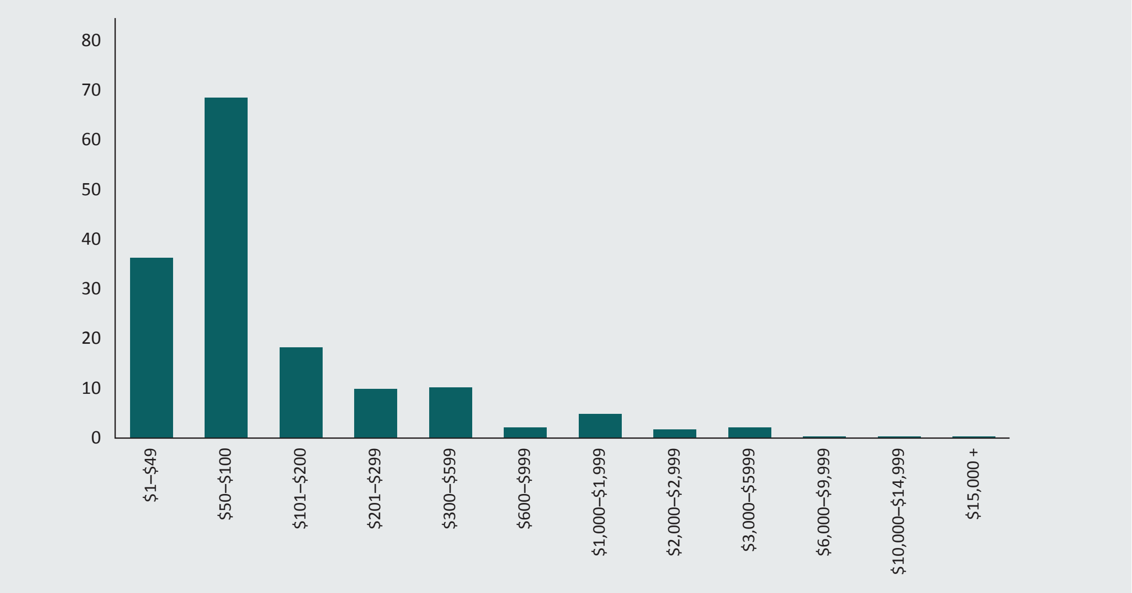
Source: Identity crime survey 2018 [AIC data file]

In addition, respondents were asked to estimate the number of hours over the last 12 months they had spent dealing with the consequences of having had their personal information misused. The mean number of hours victims spent dealing with consequences was 35—a substantial increase on the 23 hours spent in 2017. However, six respondents reported times that were more than 2.5 times the standard deviation from the mean (840, 1,000, 1,200, 2,000, 7,000 and 8,760 hours). If these outliers are excluded, the mean time was 22 hours, similar to the 2017 findings. In 2017, however, no statistical outliers were excluded from analysis.

Financial costs associated with the most serious occasion of misuse

Respondents were asked how much money they had spent dealing with the most serious occasion of personal information misuse. Estimates were provided by 568 respondents. The total amount recent victims spent dealing with the most serious occasion of personal information misuse was $407,672, but individual responses ranged from $1 to $200,000.

Figure 16: Total money spent dealing with the consequences of the most serious occasion of personal information misuse (%)



Source: Identity crime survey 2018 [AIC data file]

The 2018 survey, unlike previous surveys in the series, asked recent victims of identity crime if they had successfully resolved all of the financial, credit and other problems they suffered as a result of the misuse of their personal information. Of the 1,136 recent victims (weighted data), 815 (72%) had resolved all problems arising from the most serious occasion of personal information misuse. Sixteen percent (*n*=182) had not resolved the problems and another 12 percent (*n*=139) were unsure if the matter had been sufficiently resolved.

Behavioural changes arising from the misuse of personal information

Respondents were asked how their behaviour had changed as a direct result of their personal information being misused. As was found in previous years, most respondents (92%) reported having changed their behaviour in some way (see Table 18).

The most common behavioural change reported in 2018 was changing passwords (45%). This was also the most common behaviour change reported in 2017 (38%).

In comparison with the 2017 sample, the 2018 survey found large increases in the proportion of respondents who reported being more careful when using or sharing personal information (32% in 2017 vs 39% in 2018) and in the proportion of respondents indicating they changed their banking details (35% in 2018 vs 27% in 2017). This corresponds with the increase in credit/debit fraud victimisation among the 2018 sample compared with the 2017 sample. This finding also aligns with the statistically significant increase in the proportion of 2018 respondents who reported reviewing financial statements more carefully (34% vs 30% in 2017).

Table 18: Behavioural changes resulting from the misuse of personal information (weighted data)

Behavioural change	2017 (*n*=1,307)	2018 (*n*=1,136)		% change
	%	%	*n*	
Changed passwords	37.6	44.9	510	+7.3***
More careful when using or sharing personal information	31.8	38.5	437	+6.7***
Changed banking details	27.4	35.2	400	+7.8***
Review financial statements more carefully	29.7	33.8	384	+4.1*
Don't trust people as much	25.1	27.0	307	+1.9
Use better security for computer and other computerised devices	23.4	25.5	290	+2.1
Shred personal documents before disposing of them	17.3	19.8	225	+2.5
Changed my social media account	13.5	16.5	187	+3.0
Changed my email address(es)	15.2	14.8	168	-0.4
Lock mailbox	13.4	14.0	159	+0.6
Applied for a credit report	12.1	12.9	147	+0.8
Redirect mail when away or moving residence	11.2	12.0	136	+0.8
Changed telephone numbers	11.6	10.0	114	-1.6
Ceased all social media use	8.7	9.0	102	+0.3
Use a registered post box	10.0	8.8	100	-1.2
Avoid using the internet for banking and purchasing goods and services	7.8	7.6	86	-0.2
Changed place of residence	8.7	7.2	82	-1.5
Signed up for a commercial identity theft alert/ protection service	7.4	6.3	72	-1.1
Other	3.9	3.1	35	-0.8
Behaviour has not changed	6.5	8.4	95	+1.9

***statistically significant at *p*<0.001, *statistically significant at *p*<0.05

Note: Respondents could select multiple responses

Source: Identity crime survey 2017 and 2018 [AIC data file]

Relationship between behavioural change and method used to obtain personal information

To examine whether the method used to access personal information affected victims' behaviour, the behavioural changes of those who experienced each of the most common methods of access were compared (see Table 19). This analysis examined the eight methods of obtaining personal information reported by 10 percent of victims or more.

Table 19: Behavioural changes by method of obtaining personal information (weighted data) (%)

Behavioural change	Method by which personal information was obtained							
	Face-to-face (*n*=188)	Telephone (*n*=219)	Email (*n*=212)	Text message (*n*=182)	Theft or hacking (*n*=277)	Online banking (*n*=209)	Obtained by other website[a] (*n*=147)	Data breach (*n*=141)
Changed passwords	23.3	33.5	49.5	32.4	62.5	55.2	52.4	59.8
More careful when using or sharing personal information	23.4	35.3	36.6	30.2	62.5	52.7	55.2	58.8
Changed banking details	27.2	30.1	37.9	28.4	44.4	52.5	39.9	44.5
Review financial statements more carefully	20.1	25.2	30.8	24.6	42.3	50.8	38.3	47.2
Don’t trust people as much	15.3	27.3	27.2	22.2	38.4	34.7	36.2	39.9
Use better security for computer and other computerised devices	15.8	25.1	28.0	23.5	37.3	33.5	34.9	39.5
Shred personal documents before disposing of them	21.8	21.0	18.5	24.3	27.6	29.5	27.2	33.9
Changed email address(es)	21.5	20.7	30.5	27.1	18.6	19.4	15.2	19.1
Changed social media account(s)	17.3	24.9	24.1	26.4	23.7	24.0	26.1	28.9
Ceased all social media use	20.0	17.3	15.7	18.6	8.4	15.2	16.0	19.4
Lock mailbox	25.0	20.0	23.5	23.8	14.3	23.1	19.0	31.5
Redirect mail when away or move residence	25.4	23.2	20.0	23.5	13.8	17.8	13.7	25.0
Changed telephone numbers	21.2	18.5	19.2	22.5	11.0	18.2	11.7	18.8
Applied for a credit report	22.5	22.1	19.9	25.2	14.5	20.5	17.3	23.4
Use a registered post box	21.3	19.7	15.9	23.3	8.8	13.0	14.2	19.5
Changed place of residence	19.2	15.3	18.6	18.9	7.6	13.7	8.8	13.3
Signed up for a commercial identity theft alert/protection service	15.3	19.7	11.3	19.2	8.1	12.8	11.0	16.6
Avoid using the internet for banking and purchasing goods and services	3.5	9.1	10.8	7.5	12.9	14.7	12.0	11.1
Other	1.1	1.3	3.4	1.5	3.1	3.7	5.9	5.1
Behaviour has not changed	1.8	0.7	2.4	1.2	6.2	3.7	5.5	1.8

a: ‘Other website’ category excludes online shopping websites

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 [AIC data file]

Relationship between behavioural change and type of personal information misused

Behavioural responses to the misuse of different types of personal information were compared. This analysis examined all types of personal information that over 250 respondents reported as having been misused (see Table 20).

Table 20: Behavioural changes by type of personal information misused (weighted data) (%)

Behavioural change	Type of personal information misused					
	Name (*n*=532)	Credit/ debit card (*n*=502)	Address (*n*=363)	Date of birth (*n*=346)	Bank account (*n*=328)	Password (*n*=264)
Changed passwords	48.2	53.5	46.5	47.1	59.6	67.5
More careful when using or sharing personal information	42.4	47.8	40.0	43.3	54.2	52.0
Changed banking details	31.9	53.7	29.5	35.9	56.5	38.4
Review financial statements more carefully	34.6	50.6	31.4	33.1	52.7	40.1
Don’t trust people as much	33.2	29.8	33.6	33.6	38.4	37.0
Use better security for computer and other computerised devices	30.2	28.8	28.5	31.1	37.1	36.0
Shred personal documents before disposing of them	23.3	24.5	25.8	24.5	26.3	28.1
Changed email address(es)	21.1	11.9	21.3	23.3	21.1	25.0
Changed social media account(s)	20.7	15.6	26.5	27.4	20.3	34.8
Ceased all social media use	14.2	7.7	16.2	14.6	10.0	15.9
Lock mailbox	19.5	16.2	22.4	21.8	20.5	23.7
Redirect mail when away or move residence	17.0	11.5	21.7	21.6	14.2	20.0
Changed telephone numbers	14.3	10.3	17.7	18.4	15.1	19.4
Applied for a credit report	18.0	13.9	21.7	23.1	16.5	18.2
Use a registered post box	13.9	7.6	16.2	17.0	12.6	12.6
Changed place of residence	10.3	5.8	15.6	14.8	8.4	13.3
Signed up for a commercial identity theft alert/protection service	10.0	4.4	15.3	12.9	8.4	11.2
Avoid using the internet for banking and purchasing goods and services	8.8	11.4	9.6	9.9	11.9	10.0
Other	3.2	4.9	2.4	3.6	4.1	2.5
Behaviour has not changed	5.7	7.5	4.0	5.3	4.7	4.4

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 [AIC data file]

Reporting the misuse of personal information

Of the 1,136 respondents who experienced misuse of their personal information in the previous 12 months, 9.5 percent (*n*=108) did not report the misuse in anyway. This is similar, yet slightly lower, to the proportion of the 2017 sample that did not report the misuse (10.3%). Sixty percent of victims (*n*=676) told only a family member or friend; 12.1 percent of victims (*n*=138) told only a government agency or another organisation; and 18.8 percent (*n*=214) told an agency and a family member or friend. In 2017, 56.8 percent of victims reported the misuse to family or friends only, 7.4 percent to an agency or organisation only, and 25.5 percent to both an agency and family or friends.

Satisfaction with reporting

Respondents who reported personal information misuse to a government agency or another organisation were asked to specify who they reported the misuse to and how satisfied they were with the responses (see Table 21).

Table 21: Government agencies and other organisations reported to and satisfaction with responses, 2018 (weighted data)

Agency/organisation reported to	Satisfied		Dissatisfied	
	n	%	*n*	%
Bank, credit union, credit/debit card company (eg Visa or MasterCard) or e-commerce provider (eg PayPal) (*n*=243)	209	85.8	34	14.2
Police (*n*=73)	44	60.6	29	39.4
ACORN (Australian Cybercrime Online Reporting Network) (*n*=22)	17	77.9	5	22.1
A consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading) (*n*=40)	27	67.8	13	32.2
Internet service provider (*n*=38)	24	63.2	14	36.8
Credit reporting agency (eg Equifax, Dun & Bradstreet) (*n*=22)	11	50.0	11	50.0
Utility company (eg gas, electricity, telephone, water) (*n*=28)	14	50.0	14	50.0
Medicare Australia (*n*=26)	18	68.5	8	31.5
Media organisation (*n*=6)	4	69.1	2	30.9
Passport Office (*n*=14)	10	75.3	4	24.7
Road traffic authority (*n*=12)	7	55.6	5	44.4
IDCARE (*n*=9)	8	88.9	1	11.1
Other (*n*=39)	27	69.2	12	30.8

Source: Identity crime survey 2018 [AIC data file]

In 2018 respondents were asked a follow-up question about why they were satisfied or dissatisfied with the response they received from the agency they reported to. Despite the range of agencies and organisations a victim of identity crime could report to, common themes were found across all organisations which contributed to a respondent feeling satisfied or dissatisfied with the response. Respondents were generally satisfied if the person they spoke to was friendly, efficient and helpful and, in some circumstances, sympathetic (for those who reported to police, IDCARE, a consumer protection agency, bank/credit union or a road traffic authority). Respondents were dissatisfied if the person taking their complaint did not respond to their query, if the matter took longer to be resolved than they expected or if they felt the person was uninterested in the complaint. For example, one respondent said they were laughed at by an officer of a government agency and another claimed the government agency they reported to 'passed the buck'.

A recurring complaint from respondents was that it seemed like what had happened to them was not a crime. One respondent commented: 'probably wrong to blame, but I thought it was a serious offence to steal your [identity] documents'. Another respondent was told that there were no laws about what had happened to them in their state. Still others found that, if their personal information had been obtained or misused online and the perpetrators were overseas, little could be done.

Respondents who indicated they had not reported the misuse of their personal information to a government agency or other organisation were asked why they had not (Table 22). Multiple reasons could be given. The most common reason given for not reporting the misuse was that the bank or other financial institution had already resolved the issue (34% of respondents who did not report). The second most common reason given was that the respondent did not think it was important enough to report (31%, a statistically significant six percentage point increase since 2017). Concerningly, the proportion of respondents who said they did not report because they did not know how or where to report the matter increased significantly, by seven percentage points. This indicates more work needs to be done by government agencies and other organisations to ensure people know how to seek help if their personal information is misused or they believe they are at risk of identity crime.

Table 22: Reasons for not reporting misuse of personal information (weighted data)

Reason for not reporting	2017 (*n*=877)	2018 (*n*=784)		% change
	%	%	*n*	
Bank, credit union or credit card company already resolved the issue	32.5	34.4	270	+1.9
Not important enough to report	25.0	30.9	242	+5.9*
I did not know how or where to report the matter	20.9	27.9	219	+7.0***
I did not believe the police or other authority would be able to do anything	21.9	25.4	199	+3.5
I was too embarrassed to report it	16.8	17.6	138	+0.8
I did not believe it was a crime	15.6	15.1	118	-0.5
Other	5.5	7.5	59	+2.0

Note: Includes the respondents who reported to no-one or who reported only to friends and family; respondents could select multiple responses

Source: Identity crime survey 2017 and 2018 [AIC data file]

Victims’ Certificates

All respondents, regardless of recent or lifetime victimisation, were asked if they were aware that a person whose personal information has been misused can apply to a court to obtain a Victims’ Certificate to prove they are a victim of identity crime (see Table 23). The proportion of respondents unaware of Victims’ Certificates significantly increased between 2017 (72%) and 2018 (77%): $N\text{-}1\chi^2(1)=62.3$, $p<0.001$. This finding differs from that of the 2017 survey, which found a statistically significant decrease in the proportion of respondents who were unaware of the certificates (Goldsmid, Gannoni & Smith 2018). This change may be explained in part by a difference in the creation of the samples. The 2018 sample only included respondents who had never participated in the survey previously, while the 2017 survey did not have this requirement.

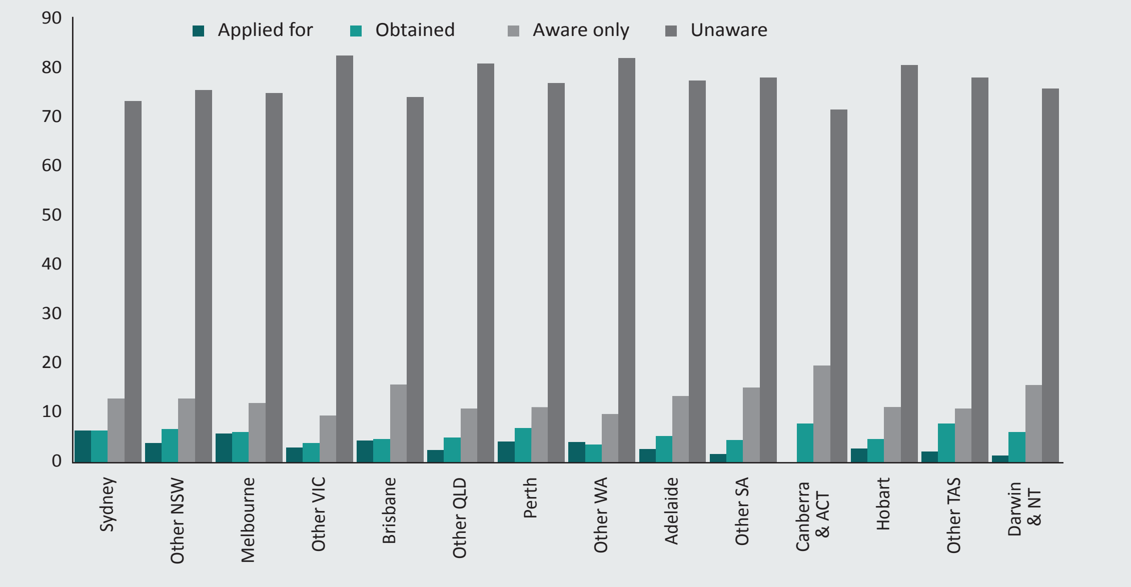
Table 23: Awareness of Victims' Certificates (weighted data)

	2017 (*n*=9,947)	2018 (*n*=9,911)	
	%	%	*n*
I am aware of such certificates, and have obtained one or more in the past	7.6	5.9	588
I am aware of such certificates, and have applied for one in the past	6.3	4.6	459
I am aware of such certificates, but have not applied for any	14.3	12.8	1,266
I am unaware of such certificates	71.8	76.7	7,598
Total	100.0	100.0	9,911

Source: Identity crime survey 2017 and 2018 [AIC data file]

In all locations, except Tasmania, awareness of Victims' Certificates was higher among respondents who lived in capital cities than among those who lived elsewhere in the state or territory (see Figure 17). The jurisdiction with the highest proportion of respondents who had obtained a Victims' Certificate was the Australian Capital Territory.

Figure 17: Awareness of Victims' Certificates by usual place of residence (weighted data) (%)



Note: Percentages may not total 100 due to rounding

Source: Identity crime survey 2018 [AIC data file]

Risk and prevention of misuse of personal information

Perceived risk of victimisation in the next 12 months

Respondents were asked whether they thought the risk of someone misusing their personal information would change over the next 12 months. Nineteen percent of respondents reported that their risk of being a victim of identity crime would 'increase greatly' over the next 12 months (see Table 24). A further 44 percent of respondents reported that they believed the risk would 'increase somewhat'.

Table 24: Perceived risk of personal information misuse in the next 12 months (weighted data)

Change in risk of misuse of personal information	2017	2018	
	%	%	*n*
Risk will increase greatly	19.7	19.3	1,916
Risk will increase somewhat	46.4	44.2	4,382
Risk will not change	32.2	34.4	3,409
Risk will decrease somewhat	0.9	1.3	132
Risk will decrease greatly	0.8	0.7	72
Total	100.0	100.0	9,911

Note: Percentages may not total 100 and weighted figures may not total 9,911 due to rounding

Source: Identity crime survey 2017 and 2018 [AIC data file]

Additional analysis was conducted to examine whether being a recent victim of identity crime was associated with a perception that the risk of victimisation would increase. A significant relationship was identified between recent identity crime victimisation and a perceived increase in the risk of victimisation in the next 12 months: ($\chi^2(4, n=9{,}911)=392.85, p<0.001, V=0.19$). Recent victims were significantly more likely than non-victims to believe the risk of identity crime would 'increase greatly' in the next 12 months (see Table 25). Respondents who had not experienced identity crime in the previous 12 months were significantly more likely than recent victims to believe the risk of identity crime would not change in the next 12 months.

Table 25: Contingency table for recent victimisation and perceived risk of personal information misuse in the next 12 months (weighted data) (*n*)

Perceived risk of personal information misuse	Misuse of personal information in previous 12 months		
	Yes	No	Total
Risk will increase greatly	443***	1,473	1,916
Risk will increase somewhat	500	3,882	4,382
Risk will not change	177	3,232***	3,409
Risk will decrease somewhat	14	118	132
Risk will decrease greatly	2	70	72
Total	**1,136**	**8,775**	**9,911**

***statistically significant at $p<0.001$

Source: Identity crime survey 2018 [AIC data file]

Perceived seriousness of personal information misuse

Respondents were asked to give their opinion as to the seriousness of misuse of personal information in terms of harm to the Australian community. The respondents were not necessarily experts in identity crime, and as such the findings should be interpreted as indicating their personal opinions. Almost all respondents (96%) believed that misuse of personal information was a 'very serious' or 'somewhat serious' issue (see Table 26). There was a small increase in the proportion of respondents who believed misuse of personal information was 'very serious'—67 percent of respondents in 2018, up from 65 percent of respondents in 2017.

Table 26: Perceived seriousness of misuse of personal information (weighted data)

Seriousness	2017	2018	
	%	%	*n*
Very serious	65.2	67.2	6,664
Somewhat serious	31.7	28.5	2,825
Not very serious	2.8	3.6	357
Not at all serious	0.3	0.7	65
Total	**100.0**	**100.0**	**9,911**

Source: Identity crime survey 2017 and 2018 [AIC data file]

Additional analysis examined whether the increase in the proportion of respondents who perceived identity crime to be 'very serious' related to experiences of personal information misuse. The perceived seriousness of personal information misuse was associated with recent victimisation: $\chi^2(3, n=9{,}911)=61.30, p<0.001, V=0.07$ (see Table 27). Recent victims were more likely to rate personal information misuse as 'very serious' than those who had not experienced victimisation. Conversely, non-victims were more likely than victims to rate personal information misuse as 'not very serious'.

Table 27: Contingency table for recent victimisation and perceived seriousness of personal information misuse (weighted data) (*n*)

Seriousness	Misuse of personal information in previous 12 months		
	Yes	No	Total
Very serious	877***	5,787	6,664
Somewhat serious	232	2,593***	2,825
Not very serious	20	337***	357
Not serious at all	7	58	65
Total	**1,136**	**8,775**	**9,911**

***statistically significant at *p*<0.001

Source: Identity crime survey 2018 [AIC data file]

Use of security measures to protect personal information

Respondents were asked whether they had ever used particular security measures and how frequently they had used those security measures in the past—that is, in any way, not just to prevent misuse of personal information. Almost all respondents (97%) had used at least one of the specified security measures at some time (see Table 28). The most common security measure was a password, with 87 percent of respondents reporting using passwords frequently. The least commonly used security measure was a computer chip implanted under the skin, although nearly 10 percent of respondents reported having used this measure.

Due to changes in the 2018 questionnaire, these data are not comparable with those from previous years. However, in 2017, a similar proportion of respondents (93%) reported using at least one of the specified security measures.

Table 28: Frequency of use of security measures in the past (weighted data)

Security measure	How frequently security measures used				% of respondents never using security measure
	Frequently	Occasionally	Rarely	Never	
Passwords	8,605	837	198	271	2.7
Signatures	3,124	2,652	1,578	2,557	25.8
Fingerprint recognition	3,159	1,476	1,170	4,106	41.4
Facial recognition	1,054	933	1,245	6,679	67.4
Voice recognition	648	1,321	1,931	6,011	60.6
Iris recognition	423	624	770	8,094	42.7
Computer chip implanted under your skin	280	376	292	8,963	90.4

Source: Identity crime survey 2018 [AIC data file]

Willingness to use security measures to protect personal information

Respondents were asked whether they would be willing to use various security measures in the future to protect their personal information—for example, at ATMs, at airports or when using a computer or entering a building (see Table 29). Ninety-eight percent (*n*=9,704) of respondents were willing to use at least one of the security measures. The security measure respondents were most willing to use in the future to protect their information was passwords (95%). In the 2017 survey respondents' willingness was measured using a five-point scale, but in 2018 a four-point scale was used. As such, these data cannot be compared.

Table 29: Willingness to use security measures to protect personal information in the future (weighted data)

Security measure	%	*n*
Passwords	94.7	9,390
Signatures	81.6	8,084
Voice recognition	72.4	7,172
Fingerprint recognition	84.7	8,390
Facial recognition	75.6	7,493
Iris recognition	68.6	6,800
Computer chip implanted under your skin	22.3	2,208
Any of the above	97.9	9,704
None of the above	2.1	207

Note: Respondents could select multiple responses

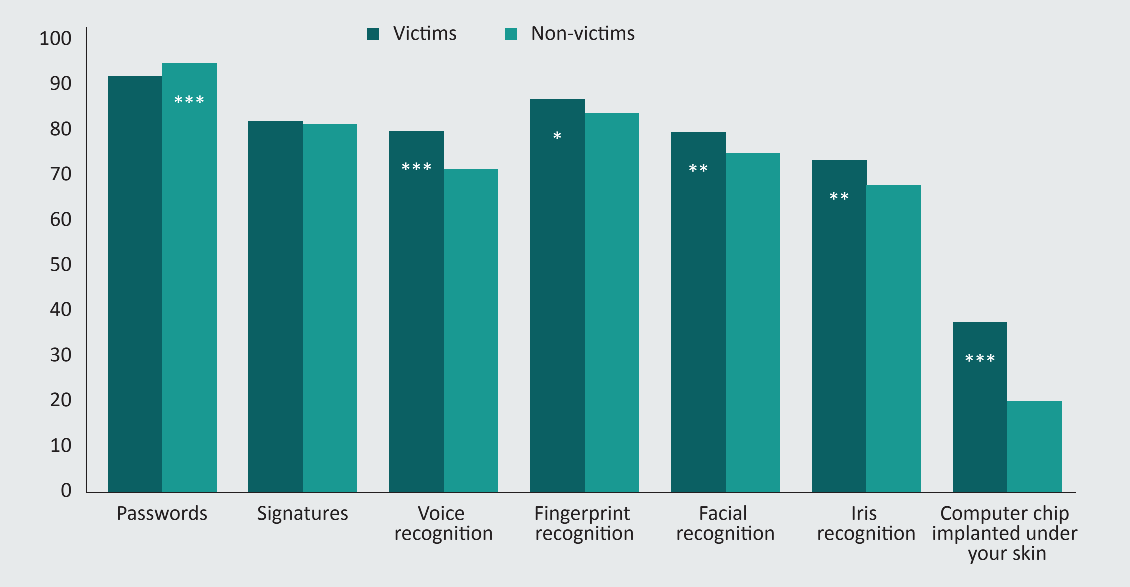
Source: Identity crime survey 2018 [AIC data file]

Additional analysis examined whether willingness to use security measures in the future to protect personal information was associated with experience of personal information misuse in the previous 12 months (see Figure 18). Recent victims were more willing than non-victims to use the following security measures:

- voice recognition (80% vs 71%; $\chi^2(1, n=9{,}911)=36.83$, $p<0.001$);
- fingerprint recognition (87% vs 84%; $\chi^2(1, n=9{,}911)=8.77$, $p<0.05$);
- facial recognition (80% vs 75%; $\chi^2(1, n=9{,}911)=12.60$, $p<0.01$);
- iris recognition (74% vs 68%; $\chi^2(1, n=9{,}911)=14.95$, $p<0.01$); and
- a computer chip implanted under the skin (38% vs 20%; $\chi^2(1, n=9{,}911)=179.95$, $p<0.001$).

Conversely, recent victims were significantly less willing than non-victims to use passwords (92% vs 95%; $\chi^2(1, n=9{,}911)=16.13$, $p<0.01$).

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



***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05

Note: *n*=9,911

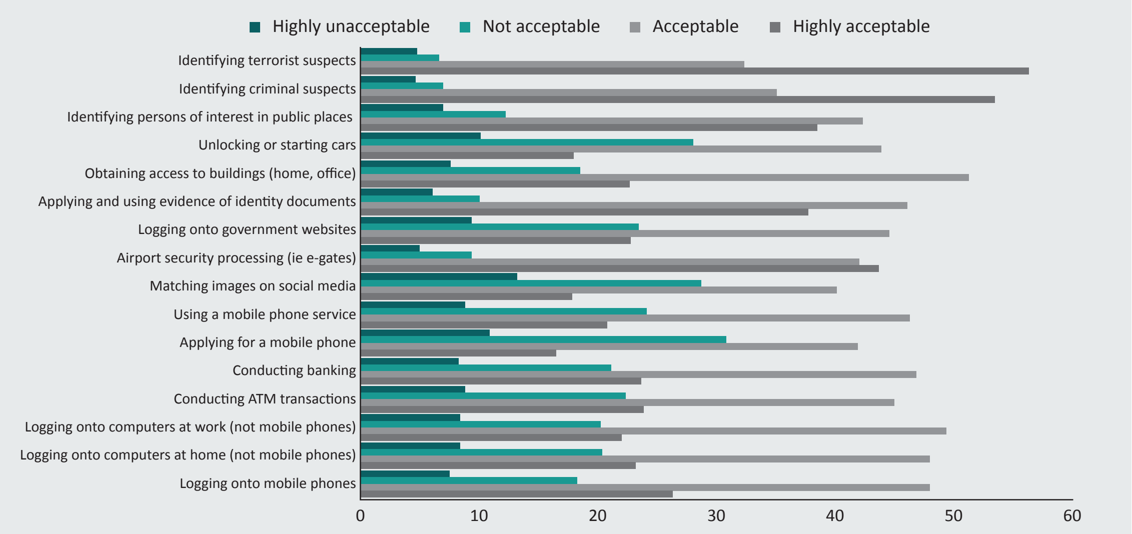
Source: Identity crime survey 2018 [AIC data file]

Facial recognition

To further explore perceptions of facial recognition, respondents were asked how willing they would be to use facial recognition technologies in various scenarios. Respondents were asked to respond to 15 facial recognition scenarios using a four-point Likert scale with response options ranging from (1) highly acceptable to use, to (4) highly unacceptable to use.

Respondents indicated it was acceptable (ie either highly acceptable or acceptable) to use facial recognition technologies for government purposes such as identifying terrorist suspects (89%), identifying criminal suspects (88%), airport security processing (85.7%) identifying persons of interest in public places (81%) and applying for and using identity documents (eg passport, driver licence) (84%; see Figure 19). The least acceptable purposes for using facial recognition technologies were for matching images on social media (58%), applying for a mobile phone (58%), and unlocking or starting a car (62%).

Figure 19: Acceptability of using facial recognition technologies for specific purposes (weighted data) (%)



Note: *n*=9,911

Source: Identity crime survey 2018 [AIC data file]

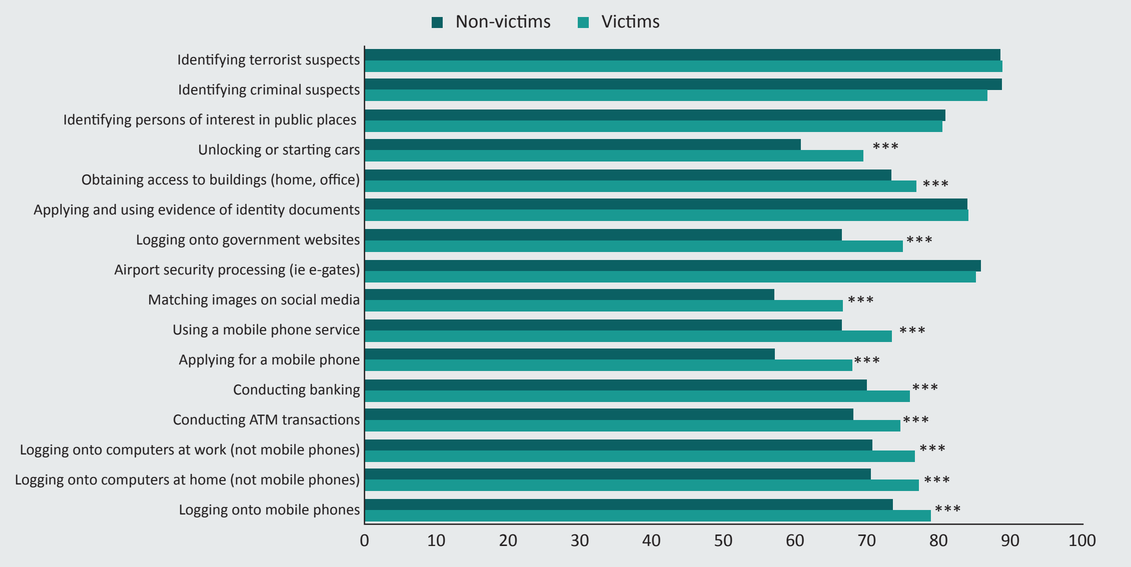
While the 2017 survey asked about willingness to use facial recognition technology (see Goldsmid, Gannoni & Smith 2018), the 2018 survey asked how acceptable it is to use facial recognition technology for specific purposes. Therefore, comparisons with previous years cannot be made.

Figure 20 explores the differences between recent victims and non-victims in the perceived acceptability of using facial recognition for various purposes. Recent victims were significantly more willing than non-victims to use facial recognition for the following purposes:

- logging onto mobile phones (79% vs 74%; $\chi^2(1, n=9{,}911)=14.66$, $p<0.001$);
- logging onto home computers (77% vs 70%; $\chi^2(1, n=9{,}911)=22.52$, $p<0.001$);
- logging onto work computers (77% vs 71%; $\chi^2(1, n=9{,}911)=17.46$, $p<0.001$);
- conducting ATM transactions (75% vs 68%; $\chi^2(1, n=9{,}911)=19.46$, $p<0.001$);
- banking (76% vs 70%; $\chi^2(1, n=9{,}911)=18.15$, $p<0.001$);
- applying for a mobile phone (68% vs 57%; $\chi^2(1, n=9{,}911)=47.16$, $p<0.001$);
- using a mobile phone service (73% vs 66%; $\chi^2(1, n=9{,}911)=23.37$, $p<0.001$);
- matching images on social media (67% vs 57%, $\chi^2(1, n=9{,}911)=38.54$, $p<0.001$);
- logging onto government websites (75% vs 66%; $\chi^2(1, n=9{,}911)=35.17$, $p<0.001$);
- obtaining access to buildings (77% vs 73%; $\chi^2(1, n=9{,}911)=15.71$, $p<0.001$); and
- unlocking and starting cars (70% vs 61%; $\chi^2(1, n=9{,}911)=32.61$, $p<0.001$).

However, there was little difference between recent victims and non-victims in the perceived acceptability of using facial recognition for government purposes such as protecting Australians and applying for and using evidence-of-identity documents.

Figure 20: Perceived acceptability of using facial recognition for specific purposes among recent victims and non-victims of personal information misuse (weighted data) (%)



***statistically significant at *p*<0.001

Note: Acceptable includes ‘Highly acceptable’ and ‘acceptable’ responses combined. *n*=9,911

Source: Identity crime survey 2018 [AIC data file]

Concerns about the use of biometric technologies

For the first time, respondents were asked how concerned they were about a range of specific issues in connection with the use of biometric technologies (voice, fingerprint, face or iris recognition). Respondents were presented with 13 issues associated with biometric technologies and asked to rate their level of their concern on a four-point scale: ‘extremely concerned’, ‘somewhat concerned’, ‘not very concerned’ and ‘not at all concerned’. Table 30 presents the findings.

Table 30: Concerns about the use of biometric technologies (weighted data) (%)

Concerns	Extremely concerned	Somewhat concerned	Not very concerned	Not at all concerned
Protection of my privacy using biometrics	48.8	34.2	13.0	4.1
Costs associated with biometrics	33.4	42.2	19.3	5.2
Risks of losing my biometric data	41.7	37.4	16.3	4.6
Risks of losing my money	43.1	35.5	16.8	4.5
Inconvenience of having to enrol in biometrics systems prior to using them for the first time	21.5	40.0	30.8	7.7
Fixing problems if biometric systems fail	41.3	41.5	13.4	3.8
Physical injury to myself through using biometrics	24.9	28.9	32.4	13.9
What to do if my biometric data are compromised	50.7	35.7	10.3	3.3
Someone using my biometric data to pretend to be me	49.2	32.1	14.2	4.4
Police taking action against me by mistake through biometric matching	40.5	35.6	19.3	5.7
Forcing me to use biometrics without my free consent	47.0	34.3	14.2	4.5
Having to use multiple different biometric systems for different purposes	31.1	44.2	19.8	4.9
Government surveillance of me	38.2	33.2	21.5	7.1

Note: Percentages may not total 100 due to weighted data and rounding. *n*=9,911

Source: Identity crime survey 2018 [AIC data file]

When respondents were asked if they had any other concerns about the use of biometrics technologies, the majority (98%, *n*=9,750) had no further concerns. Some respondents were concerned about a criminal using force to obtain personal information, the targeting of minority groups, and the requirement to update or buy new systems to be able to use biometrics. Three respondents also queried whether biometric systems would recognise them if their fingerprints were damaged or changed due to weight gain, or if their voice were altered by illness or injury.

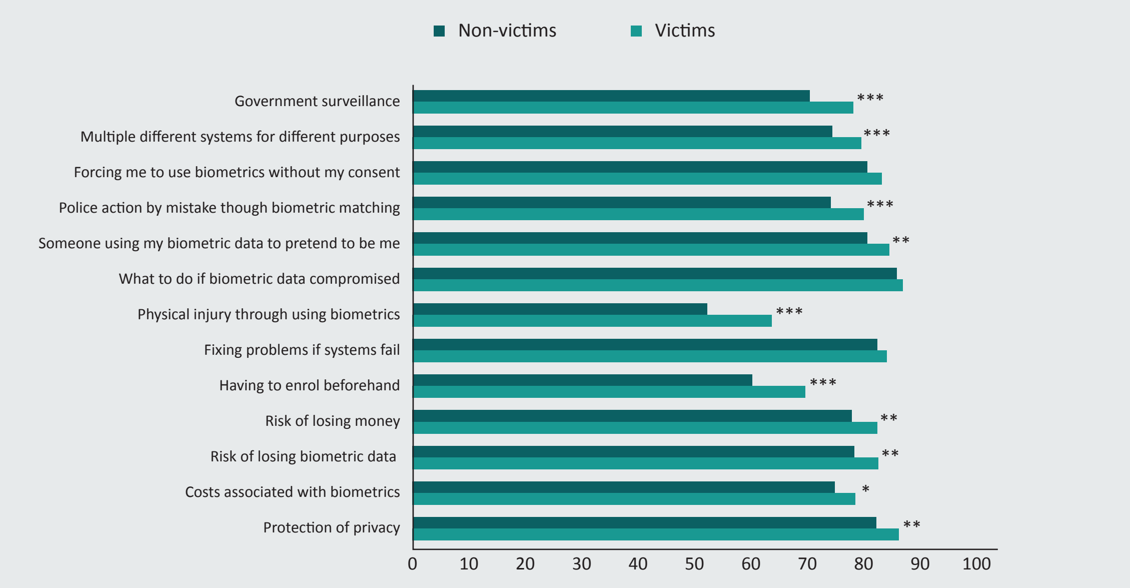
Further analyses were undertaken to examine whether respondents' concerns about the use of biometric systems were influenced by recent victimisation. Recent victims were more concerned about potential issues arising from the use of biometric technologies than non-victims (see Figure 21). There were statistically significant differences between recent victims and non-victims in their concerns about biometric technologies.

Recent victims were more likely than non-victims to be concerned about the following aspects of using biometric technologies:

- protection of privacy: $\chi^2(1, 9{,}911)=12.42$, $p<0.01$;
- the costs of implementing biometrics: $\chi^2(1, 9{,}911)=7.44$, $p<0.05$;
- the risk of losing biometric data: $\chi^2(1, 9{,}911)=11.47$, $p<0.01$;

- the risk of losing money with biometrics: $\chi^2(1, 9,911)=12.07$, $p<0.01$;
- having to enrol in biometrics before use: $\chi^2(1, 9,911)=39.57$, $p<0.001$;
- physical injury arising from the use of biometrics: $\chi^2(1, 9,911)=53.51$, $p<0.001$;
- someone using my biometrics data pretending to be me: $\chi^2(1, 9,911)=11.24$, $p<0.01$;
- police action due to mistakes with biometric matching: $\chi^2(1, 9,911)=18.56$, $p<0.001$;
- having to use multiple systems for different purposes: $\chi^2(1, 9,911)=14.00$, $p<0.001$; and
- government surveillance: $\chi^2(1, 9,911)=30.02$, $p<0.001$.

Figure 21: Concerns of recent victims and non-victims of personal information misuse about using biometric technologies (weighted data) (%)



***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05

Source: Identity crime 2018 [AIC data file]

Discussion

On the basis of this survey's findings, the prevalence of misuse of personal information in Australia has remained stable. Twelve percent of respondents reported that their personal information had been misused in the previous 12 months. This was a slight decrease on the rate of recent victimisation found in 2017, but the difference was not statistically significant. As such, prevalence of identity crime has remained constant over the last two years. Men were more likely than women to report having experienced misuse of personal information, and the highest rate victimisation occurred among male respondents aged 25 to 34 years.

The Australian Competition and Consumer Commission's recent report on the number of complaints made to Scamwatch in 2018 found identity theft remained one of the top three scam types, despite the number of complaints decreasing from 15,703 in 2017 to 12,800 in 2018 (ACCC 2019). A similar decline was found in the number of identity theft reports made to the Australian Cybercrime Online Reporting Network (ACORN). Reports of online identity theft to ACORN declined from 7,645 in 2017 (worth $43.8m in total) to 1,866 in 2018 (worth $26.7m; ACCC 2019, 2018).

In the United States, the National Crime Victimisation Survey found the percentage of the American population experiencing identity theft increased from seven percent in 2014 to 10 percent in 2016 (Harrell 2019). Similarly, in the United Kingdom, Cifas' (2018) Fraudscape report found that while most fraud decreased in 2017, the number of identity frauds increased by one percent from 2016. These findings indicate the prevalence of identity crime is on the rise in Australia and overseas.

A primary method of obtaining personal information is from phishing, either via telephone calls, such as unsolicited cold-calling, or via emails or online activity, including social media (Verizon 2019). The present study found a decline in the proportion of identity crime victims who reported their personal information was obtained via email, telephone and text message. Rather, in 2018, respondents advised the most common method by which their information was obtained was via hacking or theft of a computerised device (24% of the sample). The proportion of respondents who believed their information was accessed through a data breach increased significantly between 2017 and 2018 (12% in 2018 vs 9% in 2017).

The increasing use of these methods of obtaining personal information aligns with the increase in the number of cybercrime incidents reported around the world. Research into hacking offences reported to the police in the United Kingdom found the number of hacking incidents investigated by police rose by 14 percent between the 2016–17 and 2017–18 financial years (Parliament Street 2018).

The increase in the proportion of respondents reporting that their personal information was obtained via data breach also occurs in a global context. In 2018, large data breaches affected tens of millions of people world-wide. For example, highly publicised data breaches involved Facebook (Burgess 2018), Google (Leskin 2018) and—one of the most substantial data breaches thus far—the Marriot International's Starwood Guest Reservation Database. The latter data breach compromised the details of over 300 million guests (Sanger et al. 2018), including names, gender, dates of birth, mailing addresses, email addresses, phone numbers, passport numbers, Starwood account information, arrival and departure information, reservation dates, and communication preferences (Marriott International 2019).

The types of personal information most commonly obtained were names and credit/debit card information, as was the case in 2017. The misuse of credit/debit card information grew substantially in 2018, increasing by eight percentage points between 2017 and 2018. Misuse of online account usernames also increased.

The purpose for which the personal information was obtained relates directly to the type of information obtained. For example, in each of the last two years about four in 10 respondents reported that their personal information was misused to obtain money from a bank. To access a victim's bank account, a perpetrator would require their name and credit/debit card information—the two most commonly misused types of information. The second most common reason for misusing personal information was to purchase something, reported by 21 percent of respondents in 2018, up from 16 percent in 2017. As credit/debit card details were frequently obtained, along with an increasing number of online account usernames, it can be inferred perpetrators had sufficient information to purchase goods online.

One point of difference between the current research and overseas research was the finding regarding the misuse of personal information to open a mobile phone account. In the current study, five percent of recent victims reported their information had been misused to open a mobile account, down from eight percent in 2017. This decline contrasts with the findings of research by Cifas (2018) in which analysis of fraud reports found identity fraudsters were moving towards 'more accessible products' such as mobile phone contracts, online retail accounts (potentially reflected in the current findings) and retail credit loans. That research found the largest increases in identity fraud occurred within the telecommunications, online retail and insurance industries (Cifas 2018).

The proportion of respondents who reported out-of-pocket losses in 2018 was similar to the figure for 2017 (9.6% in 2017 vs 9.5% in 2018), but total losses were substantially lower. When out-of-pocket losses from the most serious occasion of misuse were considered, some differences in the pattern were observed. The average out-of-pocket loss was lower in 2018 ($1,974) than in 2017 ($2,711). This decrease is explained by the fact that the single largest amount lost in 2018 was $300,000, compared with $250,000 in 2017. The proportion of respondents experiencing out-of-pocket losses from the most serious occasion of misuse remained similar (9.0% in 2017 vs 9.1% in 2018).

In 2018, fewer respondents reported recovering money they had lost as a result of the misuse of their personal information (773 in 2018 vs 1,021 in 2017). This is reflected in the total amount recovered for all misuse experienced in the last 12 months: $631,800 in 2018, compared with $3.4m in 2017. This is partly because a smaller number of respondents recovered money in 2018, and partly because a higher proportion of victims recovered small losses ($1–$49). A similar pattern was found when examining monies recovered from the most serious occasion of personal information misuse. Fewer respondents reported recovering any monies in 2018 (780 respondents in 2018 vs 983 respondents in 2017), and the single largest amount recovered in 2018 was over six times lower than the largest amount recovered in 2017 ($25,000 in 2018 vs $160,000 in 2017). Ultimately, victims experienced smaller losses and recovered smaller amounts in 2018 compared to 2017.

Almost all respondents reported that misuse of personal information was ‘somewhat serious’ or ‘very serious’ in terms of harm to the Australian community, with victims more likely than non-victims to describe it as very serious. Over half of respondents (53%) who had experienced personal information misuse in the last 12 months said they had faced impacts other than financial losses. Consequences indicative of financial impacts, such as refusal of credit, declined in 2018, partly due to an eight percentage point reduction in the proportion of respondents who reported experiencing no consequences as a result of personal information misuse. Emotional and reputational impacts rose in 2018, showing that the consequences of identity crime are far greater than the financial losses (see also Golladay and Holtfreter 2017).

Almost all respondents (92%) who had experienced personal information misuse in the last 12 months reported making behavioural changes as a consequence. Examination of behavioural changes by method of access and the type of information misused showed that behavioural changes were not uniform across victims, but were tailored to the type of information misused and the method used to access it. Behavioural changes in response to credit/debit card fraud and personal information being obtained through theft or hacking were well defined, with almost half of victims reporting changing passwords, changing banking details, and reviewing financial statements more carefully. Concerningly, only two-thirds of respondents who had their password misused reported changing their password. The highest percentage of respondents who implemented better security for computer and devices were those that had information obtained via a data breach (40%) or by theft or hacking of their device (37%). This finding was the same as in 2017 (Goldsmid, Gannoni & Smith 2018).

Identity crime is generally considered an under-reported crime (ABS 2016b; Jorna & Smith 2018). The present research supports this, finding that 60 percent of victims of personal information misuse reported the crime only to a friend or family member, and other 10 percent did not report it to anyone. Of the 30 percent of victims who did report their experience to a government agency or organisation, satisfaction was highest among those who reported to IDCARE (88%) or to a bank or credit card company (85%). The high level of satisfaction with IDCARE's response is not surprising, given it is a not-for-profit organisation created for the specific purpose of assisting and supporting victims of identity crime. Respondents were satisfied with the responses of banks or credit card companies when money was reimbursed or charges reversed. Irrespective of the agency or organisation reported to, most victims were satisfied if they thought the person they spoke to had listened to them, showed empathy and, if they could not resolve the matter, offered advice on where to seek help or how to avoid becoming a victim again.

Overall, the results of the research show the prevalence of identity crime has remained stable since 2017. The methods used to obtain personal information changed somewhat, with information more often being obtained via theft or hacking of a computerised device and via data breaches. These methods were used to obtain online account usernames and credit/debit card details, which were then misused to purchase items. This reflects the increase in cybercrime experienced in Australia and the major global data breach events experienced in 2018. The different types of identity crime experienced by victims in 2017 and 2018 may also explain the smaller out-of-pocket losses experienced by victims in 2018. Although a similar number of victims experienced out-of-pocket losses in 2017 and 2018, victims lost less money in 2018 and also recovered less. This trend towards lower losses was also observed between 2016 and 2017. This may indicate that the primary aim of offenders was not to take money from individual victims but to use the personal information for other purposes or larger frauds.

A positive finding in the 2018 results is that more people are reporting the misuse of their personal information and that people are generally satisfied with the responses they receive. As identity crime remains a highly prevalent crime affecting the Australian public, it is important for government agencies, businesses and other organisations to know how they can assist victims of identity crime, and where possible, help them avoid further victimisation.

References

URLs correct as at October 2019

Anti-Phishing Working Group 2019. *Phishing activity trends report: 4th quarter 2018.* https://apwg.org/trendsreports/

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

Australian Bureau of Statistics (ABS) 2018. *Australian demographic statistics, June 2018.* ABS cat. no. 3101.0. Canberra: ABS. https://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

Australian Bureau of Statistics 2017. *Census of population and housing: Reflecting Australia – Stories from the census, 2016.* ABS cat. no. 2071.0. Canberra: ABS. https://www.abs.gov.au/ausstats/abs@.nsf/mf/2071.0

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

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

Australian Competition and Consumer Commission (ACCC) 2019. *Targeting scams: Report of the ACCC on scams activity 2018.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018

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

Australian National University (ANU) 2019. *Incident report on the breach of the Australian National University's administrative systems.* Canberra: Office of the Chief Information Security Officer, ANU. https://www.anu.edu.au/news/all-news/data-breach

Australian Taxation Office 2018. *Scammers steal over $800,000 during November.* Media release, 5 December. https://www.ato.gov.au/Media-centre/Media-releases/Scammers-steal-over-$800,000-during-November/

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

Burgess M 2018. *Here's what you need to do after the huge Facebook hack.* https://www.wired.co.uk/article/facebook-hack-data-breach-news-what-to-do

Chang L & Krosnick JA 2009. National surveys via RDD telephone interviewing versus the internet: Comparing sample representativeness and response quality. *Public Opinion Quarterly* 73(4): 641–78

Cifas 2018. *The fraudscape 2018. London: Cifas.* https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2018

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

Field A 2013. *Discovering statistics using IBM SPSS Statistics,* 4th ed. Sage, London

Goldsmid S, Gannoni A & Smith RG 2018. *Identity crime and misuse in Australia: Results of the 2017 online survey.* Statistical Reports No. 11. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr11

Golladay K & Holtfreter K 2017. The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders* 12(5): 741–60

Harrell E 2019. *Victims of identity theft, 2016.* Bureau of Justice Statistics bulletin. NCJ 251147. Washington, DC: US Department of Justice. https://www.bjs.gov/content/pub/pdf/vit16.pdf

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

Leskin P 2018. The 21 scariest data breaches of 2018. https://www.businessinsider.com.au/data-hacks-breaches-biggest-of-2018-2018-12?r=US&IR=T

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

Marriott International 2019. Starwood guest reservation database security incident. https://info.starwoodhotels.com/

Office of the Australian Information Commissioner (OAIC) 2019. *Notifiable data breaches quarterly statistics report: 1 October – 31 December 2018.* Canberra: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-october-to-31-december-2018/

Office of the Australian Information Commissioner 2007. *Community attitudes to privacy 2007.* Canberra: OAIC. https://www.oaic.gov.au/engage-with-us/research/2007-community-attitudes-to-privacy-survey/

Parliament Street 2018. *Hack attack: Police under pressure.* http://parliamentstreet.org/research/2018/new-research-hack-attack-police-pressure/

Sanders D, Clarke HD, Stewart MC & Whiteley P 2007. Does mode matter for modelling political choice? Evidence from the 2005 British Election Study. *Political Analysis* 15:257–85

Sanger DE, Perlroth N, Thrush G & Rappeport A 2018. Marriott data breach is traced to Chinese hackers as U.S. readies crackdown on Beijing. *New York Times,* 11 December. https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

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

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

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

Smith RG & Jorna P 2018b. *Counting the costs of identity crime and misuse in Australia, 2015–16.* Statistical Bulletin no. 15. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sb/sb15

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

Verizon 2019. *2019 Data breach investigations report.* https://enterprise.verizon.com/resources/reports/dbir/

We Are Social 2018. Digital in 2018 in Oceania: Essential insights into internet, social media, mobile and ecommerce use across the region part 1: west. New York: We Are Social and Hootsuite. https://www.slideshare.net/wearesocial/digital-in-2018-in-oceania-part-1-west

Yeager DS et al. 2011. Comparing the accuracy of RDD telephone surveys and internet surveys conducted with probability and non-probability samples. *Public Opinion Quarterly 75(4): 709–47*

Appendix A: Identity crime and misuse survey 2018

About the Identity Crime and Misuse Survey

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

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

'Personal Information' includes your:

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

You will be asked to answer questions about:

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

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

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

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 7pm and midnight (AEDT). You should contact your local police if you suspect that your identity has been stolen or misused. More information on how to report identity theft and how to protect your identity can be found at www.ag.gov.au/identitysecurity. Other advice and support is available from IDCARE on 1300 432 273 or www.idcare.org.

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

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

Please now answer the following questions.

Background information

Q1) Have you participated in any of our Identity Crime Surveys in the past?

□ Yes – in 2013

□ Yes – in 2014

□ Yes – in 2016

□ Yes – in 2017

□ No

□ Don't know

(If the respondent answered Yes to any of the above or Don't know – TERMINATE).

Q2) Please indicate the postcode and place of your usual place of residence?

Postcode in Australia ________________

State or Territory (please specify) ________________

I do not normally reside in Australia □ Yes □ No

(if respondent does not normally reside in Australia – TERMINATE)

Q3) What is your gender? (select one only)

□ Male

□ Female

□ Indeterminate □ Intersex □ Unspecified

□ I'd rather not say

Q4) Which age group do you belong to? (select one only)

□ 17 years and under

□ 18–24 years

□ 25–34 years

□ 35–44 years

□ 45–54 years

□ 55–64 years

□ 65 years and over

□ I'd rather not say

Q5) What language is most often spoken at your home? (select one only)

□ English

□ Mandarin

□ Cantonese

□ Korean

□ Indonesian

□ Japanese

□ French

□ German

□ Hindi

□ Italian

□ Farsi

□ Arabic

□ Swahili

□ Other (please specify) ____________________

□ I'd rather not say

Q6) 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

Q7) What is the highest educational level you have completed?

□ Postgraduate degree

□ Graduate Diploma or Graduate Certificate

□ Bachelor's Degree

□ Advanced Diploma or Diploma

□ Professional qualification without a degree

□ Certificate III or IV

□ Year 12

□ Year 11 or below

□ Other ____

□ I'd rather not say

Q8) What was your individual gross income from all sources for the year 2016–17 (ie before tax has been deducted)? (select one only)

□ $0–$18,200

□ $18,201–$37,000

□ $37,001–$80,000

□ $80,001–$180,000

□ $180,001 and over

□ I'd rather not say

Q9) Last week, how many hours did you spend using a computer or computerised devices including a desktop, laptop, smartphone and tablet?

Insert number of whole hours only ____

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

Q10) 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

(the average hours per week spent in paid employment is 35 hours)

Q11) Have you ever used any of the following technologies in the past (in any way, not just to prevent misuse of personal information) (select all that apply) For each, indicate if used frequently, occasionally, rarely or never.

Technology type	Frequently	Occasionally	Rarely	Never
Passwords	□	□	□	□
Signatures	□	□	□	□
Voice recognition	□	□	□	□
Fingerprint recognition	□	□	□	□
Facial recognition	□	□	□	□
Iris recognition	□	□	□	□
Computer chip implanted under your skin	□	□	□	□

Q12) In order to prevent misuse of personal information in the future, how willing would you be to use each of the following technologies? For each, indicate if you would be extremely willing, willing, not willing, extremely unwilling.

Technology type	Extremely willing	Willing	Not willing	Extremely unwilling
Passwords	□	□	□	□
Signatures	□	□	□	□
Voice recognition	□	□	□	□
Fingerprint recognition	□	□	□	□
Facial recognition	□	□	□	□
Iris recognition	□	□	□	□
Computer chip implanted under your skin	□	□	□	□

Q13) To what extent have you used any biometric technology (voice, fingerprint, face or iris recognition) for each of the following activities in the last 12 months?

Use of biometric technologies for:	(select one rating for each purpose)			
Activity	**Frequently**	**Occasionally**	**Rarely**	**Never**
Logging onto mobile phones	□	□	□	□
Logging onto computers at home (other than mobile phones)	□	□	□	□
Logging onto computers at work (other than mobile phones)	□	□	□	□
For ATM transactions	□	□	□	□
Opening a bank account	□	□	□	□
Applying for a mobile phone SIM card	□	□	□	□
For Airport security processing (e-gates)	□	□	□	□
Applying for a Tax File Number	□	□	□	□
For obtaining access to buildings (home, office)	□	□	□	□
For unlocking or starting cars	□	□	□	□
Other activities (please specify and rate for each)				
____________________	□	□	□	□
____________________	□	□	□	□
_____________________	□	□	□	□

Q14) How acceptable is the use of facial recognition technologies in connection with each of the following activities?

Use of facial recognition technology in connection with verification and authentication of identity when:	(select one rating for each purpose)			
Activities	Highly acceptable	Acceptable	Not acceptable	Highly unacceptable
Logging onto mobile phones	□	□	□	□
Logging onto computers at home (other than mobile phones)	□	□	□	□
Logging onto computers at work (other than mobile phones)	□	□	□	□
Conducting ATM transactions	□	□	□	□
Conducting banking	□	□	□	□
Applying for and using a mobile phone	□	□	□	□
Matching images on social media	□	□	□	□
Airport security processing (e-gates)	□	□	□	□
Logging onto government websites	□	□	□	□
Applying and using evidence of identity documents (such as a passport or driver licence)	□	□	□	□
Using a driver licence Identity verification using passport or driver licence images)	□	□	□	□
Obtaining access to buildings (home, office)	□	□	□	□
Unlocking or starting cars	□	□	□	□
Identifying persons of interest in public places (e.g. airports, shopping centres, sports arenas, etc.)	□	□	□	□
Identifying criminal suspects	□	□	□	□
Identifying terrorist suspects	□	□	□	□
Other activities (please specify and rate for each)				
____________________	□	□	□	□
____________________	□	□	□	□
_____________________	□	□	□	□

Q15) How concerned are you about each of the following issues in connection with biometric technologies (voice, fingerprint, face or iris recognition)?

	(select one rating for each issue)			
Issues	**Extremely concerned**	**Somewhat concerned**	**Not very concerned**	**Not at all concerned**
Protection of my privacy	□	□	□	□
Cost involved	□	□	□	□
Risks of losing my biometric data	□	□	□	□
Risks of losing my money	□	□	□	□
Having to enrol beforehand	□	□	□	□
Fixing problems if systems fail	□	□	□	□
Physical injury to myself through using biometrics	□	□	□	□
What to do if my biometric data are compromised	□	□	□	□
Someone using my biometric data to pretend to be me	□	□	□	□
Police taking action against me by mistake through biometric matching	□	□	□	□
Forcing me to use biometrics without my free consent	□	□	□	□
Having to use multiple different systems for different purposes	□	□	□	□
Government surveillance of me	□	□	□	□
Other issues (specify which and rate for each)				
______________________________	□	□	□	□
______________________________	□	□	□	□
______________________________	□	□	□	□

Misuse of personal information

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

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

Q16) 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

Q17) 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

Q18) 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 (either a Commonwealth or state/territory victims' certificate) to prove what occurred? (select one only)

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

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

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

□ No, I am unaware of such certificates

Q19) 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 [continue to next question]

□ No, I have not had my personal information misused in the past [skip to end of survey]

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.

Q20) In the last 12 months 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 [continue to next question]

□ No [skip to end of survey]

□ Don’t know [skip to end of survey]

Q21) [If you answered Yes] On how many separate occasions over the last 12 months do you think your personal information was misused?

(insert number) ____

Q22) Over the last 12 months, how much money was taken from you as a result of the misuse of your personal information on all occasions combined?

$ ____

(insert your best estimate of the total amount of money taken over the 12 months in whole dollars, including any money that you were later able to recover from banks, other organisations, or recovered in other ways. (Do not include any costs associated with dealing with the consequences of having had your personal information misused such as getting legal advice, obtaining victim certificates, credit reports, lost income, telephone charges, bank overdraft fees, postage and fees etc.).

Q23) Of the amount specified in Q22, 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 committed over the last 12 months?

$ ____

(insert your best estimate in whole dollars)

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

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

Q25) 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

Q26) 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, change accounts etc.)

Please indicate how many whole hours were spent ______

Q27) Over the last 12 months, did you tell anyone about the misuse of your personal information?

□ No, I told no-one [skip to Q30]

□ Yes, I told a friend or family member [skip to Q30]

□ Yes, I told a government agency or a business organisation [continue to next question]

□ Yes, I told a friend or family member and a government agency or another organisation [continue to next question]

Q28: If you made a report to a government agency or another organisation, to which of the following did you make a report?		Q29: Were you satisfied with the response you received?		If unsatisfied selected: why were you unsatisfied with the response?	If satisfied selected: why were you satisfied with the response?
Organisation	(select all that apply)	Yes	No	Unsatisfied	Satisfied
The police	□	□	□		
ACORN (Australian Cybercrime Online Reporting Network)	□	□	□		
A consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading)	□	□	□		
A Road Traffic Authority	□	□	□		
The Passport Office	□	□	□		
Medicare Australia	□	□	□		
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)	□	□	□		
A credit reporting agency (eg Veda or Dun and Bradstreet)	□	□	□		
Your internet service provider	□	□	□		
A utility company (eg gas, electricity, telephone, water etc.)	□	□	□		
A media organisation	□	□	□		
IDCARE (www.idcare.org)	□	□	□		
Others (please specify)					
1. ______________________	□	□	□		
2. ______________________	□	□	□		
3. ______________________	□	□	□		

Q30) If you did NOT report the misuse of your personal information to a government agency or another organisation over the last 12 months, please indicate why you decided not to make such a report (select all that apply) [only for respondents who did not report to government or organisation]

□ 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

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

□ It was not important or serious enough to make a report

□ Other (please specify) ____________________

Q31) As a direct result of having had your personal information misused in the last 12 months, in what ways has your behaviour changed? (select all that apply)

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

□ I changed my password(s)

□ I changed my social media account(s)

□ I ceased all social media use

□ I changed my email address(es)

□ I changed my banking details

□ I changed my telephone number(s)

□ I changed my place of residence

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

□ I lock my mailbox

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

□ I use a registered post box/post office box

□ I shred personal documents before disposing of them

□ I review my financial statements more carefully

□ I applied for a copy of my credit report

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

□ I don’t trust people as much

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

□ Other (please specify) ____________________

□ My behaviour has not changed

Q32) In respect of all the occasions of misuse of your personal information in the last 12 months, have you been successful in resolving all of the financial, credit and other problems associated with the misuse of your personal information?

□ Yes

□ No

□ I don’t know

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).

Q33) In respect of this most serious occasion, please indicate which of the following types of personal information you think were misused.

□ Name

□ Address

□ Date of birth

□ Place of birth

□ Gender

□ Driver’s licence information

□ Passport information

□ Medicare information

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

□ Signature

□ Bank account information

□ Credit/debit card information

□ Password

□ Personal Identification Number (PIN)

□ Tax File Number (TFN)

□ Shareholder Identification Number (HIN)

□ Computer username

□ Online account username

□ Student number

□ Other (please specify) ______________________________

Q34) In respect of this most serious occasion, how do you think that your personal information was obtained? (select all that apply)

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

□ By telephone (excluding SMS)

□ By text message (SMS)

□ By email

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

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

____

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

____

□ Theft of your mail

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

□ From an online banking transaction

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

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

□ From an ATM transaction

□ From an EFTPOS transaction

□ From a person that I know

□ Other (please specify) ____ or

□ I don't know how my information was obtained

Q35) In respect of this most serious occasion, in which of the following ways do you think your personal information was misused (select all that apply)

□ To file a fraudulent tax return

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

□ To obtain superannuation monies

□ To obtain money from an investment (eg shares)

□ To apply for a job

□ To provide false information to police

□ To rent a property

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

____

□ To apply for government benefits

□ To apply for a loan or obtain credit

□ To open a mobile phone account

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

□ Other (please specify) ____________________

□ Don't know

Q36) In respect of 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) ____________________

Q37) In respect of n this most serious occasion, how much money was taken from you as a result of the misuse of your personal information?

$ ______________________________

Insert your best estimate of the total amount of money taken in respect of this most serious occasion only in whole dollars, including any money that you were later able to recover from banks, etc. (Do not include any costs associated with dealing with the consequences of having had your personal information misused such as of getting legal advice, obtaining victim certificates, credit reports, lost income, telephone charges, bank overdraft fees, postage and fees etc.)

Q38) In respect of 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?

$ ______________________________

(insert you best estimate in whole dollars)

Q39) In respect of this most serious occasion, 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, obtaining victim certificates, credit reports, lost income, telephone charges, bank overdraft fees, postage and fees etc. Please insert your best estimate (in whole dollars only)

Q40) In respect of this most serious occasion, have you been successful in resolving all of the financial, credit and other problems associated with the misuse of your personal information?

□ Yes

□ No

□ Don’t know

Thank you for your time in answering these questions.

Appendix B: Methodological details

Sampling

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

The non-probability sample consisted of 10,000 Australian residents aged 15 years and over (up to 96 years, the maximum age represented in the panel) who had internet access and who had registered with the panel provider. (Limitations associated with panel non-probability samples are discussed below.) Demographic quotas were not employed at the point of recruitment. However, the panel provider screened the participants to ensure no respondent had participated in earlier surveys. Sampling was completed once the target sample size of 10,000 respondents had been obtained.

Respondents received incentives for completing the survey. They could select the type of reward they wished to receive from a range of incentives offered by the external provider (no incentives were provided by the AIC). Examples of the incentives offered included:

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

Weighting of data

Data were weighted by age and gender to represent the distribution of the Australian population in terms of age and gender (either male or female only) based on population data from the Australian demographic statistics for June 2018 (ABS 2018).

This was consistent with the approach to weighting undertaken in the 2017 survey. The Australian Bureau of Statistics demographic statistics for June 2018 for age and gender were used to develop the weighting matrix. The process of weighting involved applying a formula to data provided by each respondent who specified their gender and age category, to make each response proportionate in relation to the broader population of Australians.

The tables below show the 2018 Australian demographic data and the unweighted distribution of survey respondents by age (Table B1) and gender (Table B2).

Table B1: Respondents by age (unweighted data)

	ABS 2018 Demographic data	2018 Survey	
Age	**%**	**%**	***n***
15–24 years	16.0	12.8	1,278
25–34 years	18.0	19.9	1,986
35–44 years	16.0	19.0	1,895
45–54 years	16.0	16.5	1,651
55–64 years	14.0	16.6	1,662
65 years and over	19.0	14.7	1,472
I'd rather not say	–	0.6	56
Total	**100.0**	**100.0**	**10,000**

Note: Percentages may not total 100 due to rounding

Source: ABS 2018; Identity crime survey 2018 [AIC data file]

Table B2: Respondents by gender (unweighted data)

	ABS 2018 Demographic data	2018 Survey	
Gender	**%**	**%**	***n***
Male	49	40.4	4,040
Female	51	59.1	5,905
Indeterminate/intersex/unspecified	–	0.1	12
I'd rather not say	–	0.4	43
Total	**100**	**100.0**	**10,000**

Source: ABS 2018; Identity crime survey 2018 [AIC data file]

The 2018 Australian demographic statistics are based on the 2016 Census, which did not allow respondents to identify as indeterminate/intersex/unspecified or allow non-responses. Those not identifying as male or female were therefore excluded from the survey analysis (*n*=12 indeterminate/intersex/unspecified; *n*=43 'I'd rather not say'), as the data for these groups could not be weighted. The 56 respondents who declined to indicate their age were removed from the sample for the same reason. Some respondents declined to provide both their age and gender, so the total number of respondents removed was 89. This resulted in a final sample size of 9,911.

Table B3: Age and gender of respondents, 2018 identity crime survey (*n*)

Gender	Age category						
	15–24	25–34	35–44	45–54	55–64	65+[a]	Total
Male	380	697	668	610	749	919	4,023
Female	890	1,279	1,219	1,037	912	551	5,888
Total	**1,270**	**1,976**	**1,887**	**1,647**	**1,661**	**1,470**	**9,911**

a: The range for this age group was 65–97 years

Source: Identity crime survey 2018 [AIC data file]

Table B4 presents the nationally representative age and gender distribution of the Australian population.

Table B4: ABS age and gender data at 30 June 2018

Gender	Age category						
	15–24	25–34	35–44	45–54	55–64	65+[a]	Total
Male	1,655,870	1,862,605	1,651,132	1,567,888	1,411,373	1,820,990	9,969,858
Female	1,575,033	1,877,533	1,665,139	1,631,171	1,477,355	2,049,174	10,275,405
Total	**3,230,903**	**3,740,138**	**3,316,271**	**3,199,059**	**2,888,728**	**3,870,164**	**20,245,263**

a: The range for this age group was 65–97 years

Source: ABS 2018

Consistent with the approach taken in the 2017 Identity Crime and Misuse in Australia Survey (Goldsmid, Gannoni & Smith 2018), the 2018 survey responses were weighted to align with the Australian population gender and age distributions (see Table B5). Under-represented categories were assigned a multiplier larger than one, and over-represented categories were assigned a multiplier smaller than one, as determined by a mathematical formula. The method used to calculate weights involved finding the percentage of the population for each age and gender category using ABS data and then performing the same calculations on the survey data, and then dividing the ABS data percentages by the survey data percentages for each of the age and gender categories.

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

Table B5: Respondents by age and gender (unweighted and weighted data)

Age/gender	Unweighted	Multiplier	Weighted	
	n		*n*	%
24 years and under				
Male	380	2.1	811	8.2
Female	890	0.9	771	7.8
25–34 years				
Male	697	1.3	912	9.2
Female	1,279	0.7	919	9.3
35–44 years				
Male	668	1.2	808	8.2
Female	1,219	0.7	815	8.2
45–54 years				
Male	610	1.3	768	7.7
Female	1,037	0.8	799	8.1
55–64 years				
Male	749	0.9	691	7.0
Female	912	0.8	723	7.3
65 years and over				
Male	919	1.0	891	9.0
Female	551	1.8	1,003	10.1
Total	**9,911**		**9,911**	**100.0**

Note: Percentages may not total 100 and weighted figures may not total 9,911 due to rounding

Source: AIC Identity Crime survey 2018 [data file]

Comparisons with Australian demographic data show that male respondents aged 15 to 24 years were under-represented in the 2018 survey (3.8% in the AIC sample vs 8.2% in the Australian population). Overall, male respondents were under-represented in the survey (41%) compared to the Australian population (49%).

Analysis

Analysis undertaken was largely descriptive, centring on the characteristics of the sample and reported experiences of misuse of personal information. Bivariate analysis was undertaken to further examine the relationship between identity crime and particular variables where a notable association was identified through descriptive analysis.

Where appropriate, 2017 and 2018 survey data were compared, with statistical significance of any differences calculated using MedCalc statistical software (https://www.medcalc.org/calc/comparison_of_proportions.php).

Ethical considerations

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

- the need for research respondents to remain anonymous;
- the need to reach a large number of respondents;
- the need for informed consent;
- the presence of rewards for participation;
- the ability for respondents to withdraw from participation;
- the inclusion of respondents under 18 years old; and
- the potential for the survey questions to cause psychological discomfort, particularly as they related to victimisation experiences.

To maintain the anonymity of participants, no identifying information was collected from respondents unless they agreed to participate in a follow-up study. The dataset was then provided to the AIC in a de-identified format.

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

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

This research was approved by the AIC's Human Research Ethics Committee (approval no. P0279A).

Limitations

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

The limitations of human recall are also a factor in retrospective victimisation studies. Identity crime victimisation was identified via self-report. Given the nature of fraud, it can be difficult to determine when the crime occurred, as there may be a lapse in time between the individual's personal information being misused and the victim finding out about the misuse. Respondents were asked to recall events over a 12-month timeframe, so it is possible that respondents had forgotten when incidents occurred or could not recall all the consequences of incidents accurately. Another limitation is that some respondents may not have identified themselves as a victim of identity crime despite having had their personal information misused if no financial loss was incurred.

Despite these limitations, the 2018 identity crime survey results provide valuable information to inform policymakers and the public about the current extent and nature of identity crime in Australia.

AIC reports

Statistical Report

Ms Penny Jorna is a former Research Analyst at the Australian Institute of Criminology.

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

Katherine Norman is a Senior Research Editor at the Australian Institute of Criminology.

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

aic.gov.au