Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 27

Identity crime and misuse in Australia: Results of the 2019 online survey

Christie Franks and Russell G Smith

ISSN 2206-7930 (Online)
ISBN: 978 1 925304 73 2 (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

1 in 4 of the Australians surveyed (25%) reported having been a victim at some point in their lives. This was consistent with the 25% reported in 2018.

Nearly 12% of respondents reported having their **personal information misused in the last 12 months**, also consistent with the 2018 response.

Victims of identity crime spend an average of **34 hours repairing the damage** caused, similar to the 35 hours in 2018.

Refusal of credit was the most common consequence of identity crime in 2019 **(20%)**, but occurred less than in 2018 (27%).

Names and credit/debit card details were most commonly misused **(41% each)**. Misuse of driver licences increased 25% between 2018 and 2019.

Average **out-of-pocket losses were over $4,000** per victim in 2019, much more than in 2018. Total losses grew by $700,000 since 2018, to $2.5m.

The **most common misuse** of personal information was to obtain **money from a bank (39%)**, but incidents where **mobile phone accounts** were opened increased 57%.

Personal information was most often obtained through theft or hacking of a device **(30%).**

In both **2018 and 2019, 10% of victims** 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. We gratefully acknowledge time and willingness of those who completed the survey.

Abstract

This report presents the findings of the latest survey of identity crime and misuse undertaken by the Australian Institute of Criminology as part of the Australian Government's National Identity Security Strategy. Identity crime is one of the most prevalent forms of criminal activity in Australia and can have severe and lasting consequences for victims. In 2019, 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 2019 are compared with those of the 2018 identity crime survey.

The 2019 survey found 25 percent of respondents had experienced misuse of their personal information at some time during their life, with nearly 12 percent experiencing it in the previous 12 months. Eighty percent of these identity crime victims also reported a financial loss as a result. The average amount lost in 2019 ($3,916) was noticeably larger than in 2018 ($2,234). The results from the 2019 survey will help policymakers raise awareness of identity crime and reduce its impact throughout Australia.

Executive summary

Background

Identity crime is a ubiquitous form of criminal activity worldwide and is arguably one of the most prevalent crime types in Australia, affecting millions of individuals, businesses and government agencies annually.

In April 2007, the Council of Australian Governments agreed to a National Identity Security Strategy as 'the preservation and protection of a person's identity is a key concern and a right of all Australians' (Department of Home Affairs 2020). 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). The strategy sought to enhance identification and verification processes throughout Australia and to develop other measures to combat identity crime. This included the creation of a national Document Verification Service to allow users to authenticate identity credentials and the development of reliable, consistent and nationally interoperable biometric security measures policy to be used by all jurisdictions (Attorney-General's Department 2012).

In 2012, the Council of Australian Governments revised the National Identity Security Strategy in response to the evolving nature of identity crime in Australia (Department of Home Affairs 2020). The revised strategy 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 assess the effectiveness of policy and practice throughout Australia. As part of the measurement framework, the Australian Institute of Criminology 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, undertaken in December 2019 and January 2020.

Methodology

Consistent with previous surveys, the 2019 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 (TFNs), 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:

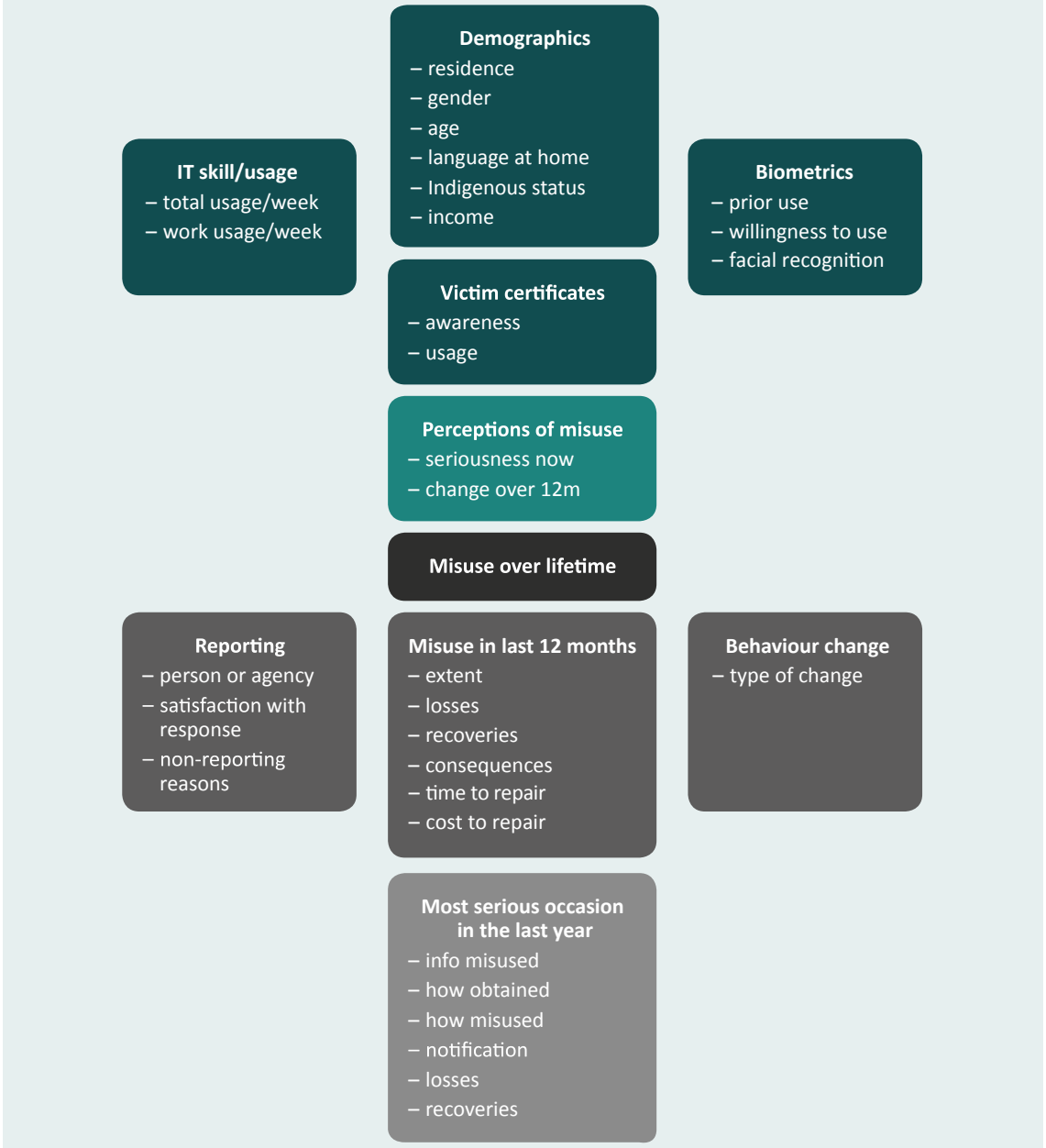
> obtaining or using your personal information without your permission, to pretend to be you, or to carry out a business in your name without your permission, or other types of activities and transactions. This does not include use of your personal information for direct marketing, even if this was done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

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

Between late December 2019 and early January 2020, a questionnaire comprising 40 questions (see *Appendix A*) was administered online to a panel of Australians drawn from all states and territories. The sampling frame of 10,000 individuals and survey hosting were provided by i-Link Research Solutions, a market research company, which then provided raw de-identified data for analysis.

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 (2013 to 2018). 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 Australian population. The total usable sample was 9,968 respondents.

Figure 1: Survey data collection plan



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 2018. Almost 12 percent of respondents (*n*=1,140) reported having had their personal information misused in the last 12 months.

Out-of-pocket losses and reimbursements

Similar proportions of respondents experienced out-of-pocket losses from the misuse of personal information during the previous 12 months in 2019 (80%) and 2018 (83%). Despite the slight reduction in the number of respondents reporting financial loss, there was a substantial 80 percent increase overall in losses that respondents experienced, from $2.0m in 2018 to $3.6m in 2019. The amount recovered was reported to be $879,463, or 25 percent of total losses. The average amount lost in 2019 ($3,916) was noticeably higher than in 2018 ($2,234)—noting that there was a single large loss of $1m reported, while the next highest loss was $530,000. These large losses are not uncommon, especially for victims who have had their bank accounts or superannuation accessed illegally. If the single $1m loss outlier is omitted from calculations, the overall loss would still be 30 percent greater than in 2018.

Impact on victims

The most common consequence of misuse of personal information was the refusal of credit (20% of recent victims), although this consequence was nearly seven percentage points less common than in 2018.

Of the 1,140 respondents who had experienced recent victimisation, 50 percent (*n*=572) incurred additional costs associated with the misuse of their personal information. Sixty-five percent of these respondents (*n*=372) spent $100 or less resolving the problem.

In addition, respondents reported spending 34 hours on average dealing with the consequences of their personal information being misused, similar to the 35 hours recorded in 2018.

Almost all respondents (94%) 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 (46%), consistent with 45 percent previous year.

Over 15 percent of respondents who reported misuse of their personal information stated they experienced mental or emotional distress as a result, an increase of 11 percent over 2018 results.

Reporting misuse of personal information

Nearly 10 percent of respondents who had experienced misuse of their personal information in the last 12 months did not report the misuse at all. Eighty percent told a family member or friend, while only 32 percent reported it to a government agency or other organisation. Of those who reported their misuse, 21 percent reported to both family/friends and an organisation/agency.

Respondents who did report to an organisation or government agency said that IDCARE (a specialised support group for identity crime victims) and financial institutions provided the most satisfactory customer service. The most common reason respondents gave for not reporting misuse of personal information was they believed their bank, credit union or credit card company had already resolved the matter (37%), followed by a belief it was not important enough to report (26%).

Risk and prevention of personal information misuse

Nearly all survey respondents (97%) believed identity crime and misuse in the Australian community was a serious issue. Nearly two-thirds (63%) of those surveyed also perceived the risk of identity crime and misuse would increase within the year.

The survey also asked respondents about their willingness to use certain security measures, particularly biometrics, to protect personal information and to engage with government and business. Passwords (97%), signatures (76%) and fingerprint recognition (63%) were the security measures most frequently used by respondents. Respondents were most willing to use facial recognition for government activities, such as identifying terrorist suspects (67%) and airport security (66%).

Conclusion

The 2019 identity crime survey found the prevalence of misuse of personal information in a large Australian sample had remained stable, with nearly 12 percent of respondents reporting they had experienced misuse in the 12 months prior to participating in the survey—the same proportion as in 2018. Names and credit/debit card details were the most commonly misused types of personal information at 41 percent each. Misuse of bank account information was the third most prevalent, at 32 percent. These figures support the most common type of direct misuse of personal information, which was to obtain money from a bank account (39%).

Misuse of personal information remains a highly prevalent crime type affecting the Australian public. Nearly a third of respondents (30%) attributed their victimisation to hacking or theft of a computerised device, an increase of six percentage points over 2018. Email remained the second highest source of compromise for the year at 19 percent, and phishing emails containing malicious links continued to enable hacking.

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 higher among victims who felt their concerns had been listened to.

Introduction

Identity crime is one of the most prevalent crime types in Australia. It 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 also an enabler of other types of crime, particularly organised economic crime (Australian Criminal Intelligence Commission 2017b).

The financial and economic impacts of identity crime have been well documented (Smith 2018; Smith & Franks 2020). Identity crimes are also notoriously under-reported as a result of inhibiting factors such as victim blaming and the complexity of reporting (Smith & Franks 2020). The emotional, physiological and socio-economic impacts faced by victims are also often over-looked and can have extreme and prolonged consequences (Emami, Smith & Jorna 2019).

Identity crime is rarely an end in itself but is an important element in a wide range of other criminal activities that include credit card fraud; superannuation and other financial frauds against individuals; welfare, tax and other frauds against government agencies; money laundering and financing of organised crime; unauthorised access to sensitive information or facilities for unlawful purposes; and the concealment of activities such as drug trafficking or the production and distribution of child exploitation material. Misuse of identity has also been connected with human trafficking and the commission of terrorist acts (Australian Criminal Intelligence Commission 2017b; Reichel & Randa 2018).

The economic impact of identity crime and misuse in Australia was most recently estimated to be $3b in 2018–19 (Smith & Franks 2020). A substantial proportion of those costs, worth an estimated $584m, relates to government actions to combat identity crime and to implement measures such as biometrics to strengthen identity security (Smith & Franks 2020).

This report assesses the prevalence, nature and impact of identity crime and misuse among a large sample of the Australian community in 2019. Where applicable, it compares the survey findings with those from previous years to discern any patterns or changes in methods, prevalence and losses. This crime type remains an ongoing concern for the Australian community. The financial and non-financial consequences experienced by victims of identity crime are considerable, highlighting the need for government, businesses and non-profit organisations to continue to work together to reduce the incidence and impact of identity crime throughout Australia.

Types of identity crime

Personal information has a wide range of uses for the criminally inclined. One of the most efficient means of obtaining personal information illegally is to hack into computer networks or make use of data exposed through data breaches. A data breach is a confirmed disclosure of data to an unauthorised party (Verizon 2019). Verizon (2019) has monitored data breaches since 2007 through voluntary reporting by organisations across the world. Its 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 the use of malware (28%). In 2019, 71 percent of breaches were financially motivated, 69 percent of attacks perpetrated by individuals external to organisations and 23 percent by state-sponsored actors (Verizon 2019).

In February 2018, in response to a series of data breaches reported in the media, the Australian Parliament enacted the *Privacy Amendment (Notifiable Data Breaches) Act 2017* to establish the Notifiable Data Breaches scheme, which came into effect on 22 February 2018. The Notifiable Data Breaches scheme requires organisations covered by the *Privacy Act 1988* (Cth) to notify any individuals likely to be at risk of serious harm relating to a data breach. This notice must include recommendations about the steps that individuals should take in response to the data breach. As a result, the number of breaches reported to the information commissioner more than tripled between 2017–18 and 2018–19, from 305 to 950 respectively (Office of the Australian Information Commissioner 2018–2020).

Verizon's (2019) top category of 'threat action' for the year was phishing, a common and effective way to access identity credentials. Verizon's (2019) second most common category involved the installation and use of backdoor or 'command and control' malware, which enables actors to manipulate systems and alter or remove data (data breach). Ransomware also remained a very prevalent method of compromising personal information (Verizon 2019).

Recent reports by the Anti-Phishing Working Group have shown 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). Phishing emails and text messages that appear to be from legitimate organisations but contain malicious links are sent out daily by the millions.

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 to assess 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.

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 2019/January 2020. 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 and whether they thought the risk of identity crime would change over the next 12 months.

Methodology

Research design and definitions

This study employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information among a sample of Australian residents in varying age groups (from 15–24 years to 65 years and over). This methodology replicated that of five previous studies conducted by the Australian Institute of Criminology (AIC) in 2013, 2014, 2016, 2017 and 2018 (see Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018, Goldsmid, Gannoni & Smith 2018; and Jorna, Smith & Norman 2020 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 mix 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 court-issued Victims' Certificates;
- perceived seriousness of misuse of personal information;
- perceived risk of identity crime over the next 12 months; and
- use of security measures in the past, including biometric technologies, 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 2019 to early January 2020 (hereafter referred to as the 2019 survey).

The survey, which had 40 questions in total, took approximately 10 to 15 minutes to complete. The questionnaire is presented in *Appendix A*.

Sample characteristics

Data were weighted by age and gender to reflect the spread of the Australian population. Demographic statistics from the Australian Bureau of Statistics (ABS 2019) were used to develop the weighting matrix for the sample (see *Appendix B* for methodological details). These demographic statistics, which were based on the 2016 Census, did not allow people to list their gender as 'indeterminate/intersex or unspecified'. Accordingly, 21 respondents who selected this option or 'I'd rather not say' were excluded from analysis as weighting could not be undertaken. Seventeen respondents who did not specify their age were also excluded from the analysis. Six respondents provided neither their age nor gender, so the total number of respondents excluded was 32. This resulted in a usable sample of 9,968 respondents.

Further information on sampling and weighting, 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 by usual place of residence closely aligned with the ABS (2019) Australian demographic statistics (see Table 1). South Australia was slightly over-represented in the survey data (9% vs 7%), as was Queensland (21% vs 20%), while the Northern Territory (0.4% vs 1.0%) and New South Wales (29% vs 32%) were slightly under-represented compared with Census data. This variation in distributions is relatively minor, though, with most of the sample being within a few percentage points of the Australian population distribution.

Table 1: Respondents by usual place of residence

Source	ABS 2019	Survey sample	
Location	**%**	***n***	**%**
Sydney	31.9	1,902	19.1
Other New South Wales		1,009	10.1
Melbourne	26.0	1,946	19.5
Other Victoria		627	6.3
Brisbane	20.1	1,188	11.9
Other Queensland		917	9.2
Perth	10.3	853	8.6
Other Western Australia		179	1.8
Adelaide	6.9	710	7.1
Other South Australia		213	2.1
ACT (including Canberra)	1.7	146	1.5
Hobart	2.1	97	1.0
Other Tasmania		137	1.4
Northern Territory (including Darwin)	1.0	44	0.4
Total	**100.0**	**9,968**	**100.0**

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

Source: ABS 2019; Identity crime survey 2019 [AIC data file]

Language

Almost all survey respondents (93%) indicated that English was the language most often spoken at home (see Table 2). Another 185 respondents (2%) indicated they spoke a language not listed. These responses included a range of Eastern and Western European languages not listed (*n*=47), Afrikaans (*n*=9), Nepali (*n*=7), Bengali (*n*=11), Urdu (*n*=15), Punjabi (*n*=15), Sinhalese (*n*=24), Tagalog (*n*=13) and multiple other Middle Eastern and Asian/South-East Asian dialects.

Table 2: Respondents by language most often spoken at home (weighted data)		
Language	***n***	**%**
English	9,305	93.3
Hindi	83	0.8
Cantonese	67	0.7
Mandarin	65	0.7
Vietnamese	41	0.4
Italian	24	0.2
Arabic	22	0.2
Korean	22	0.2
Greek	20	0.2
Spanish	17	0.2
Indonesian	17	0.2
French	16	0.2
Telugu	16	0.2
Tamil	16	0.2
Russian	11	0.1
German	10	0.1
Japanese	10	0.1
Farsi	5	0.1
Swahili	1	<0.1
Other	185	1.9
I'd rather not say	15	0.2
Total	**9,968**	**100.0**

Source: Identity crime survey 2019 [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 one percentage point more than the number so identifying in the 2016 Census—the most recent national statistics available (see Table 3).

Table 3: Respondents by Indigenous status			
Source	**ABS 2016**	**Survey sample**	
Indigenous status	**%**	***n***	**%**
Aboriginal	2.5	351	3.5
Torres Strait Islander	0.1	23	0.2
Both Aboriginal and Torres Strait Islander	0.1	29	0.3
All Indigenous	2.8	403	4.0
Non-Indigenous	91.0	9,487	95.2
I'd rather not say	6.2	78	0.8
Total	**100.0**	**9,968**	**100.0**

Note: Survey data are weighed; ABS data are not. ABS Census data were used as the Australian demographic statistics for June 2019 did not contain details of Indigenous status

Source: ABS 2017; Identity crime survey 2019 [AIC data file]

Income

Respondents were asked to categorise their individual gross income (before tax had been deducted) from all sources for the year 2018–19 (Table 4). Respondents most commonly reported having income of between $37,000 and $80,000 (31%). Nine percent of respondents preferred not to divulge their income.

Table 4: Respondents by individual gross income, 2018–19		
Income	***n***	**%**
$0–$18,200	1,523	15.3
$18,201–$37,000	2,171	21.8
$37,001–$80,000	3,051	30.6
$80,001–$180,000	2,049	20.6
$180,001 and over	278	2.8
I'd rather not say	896	9.0
Total	**9,968**	**100**

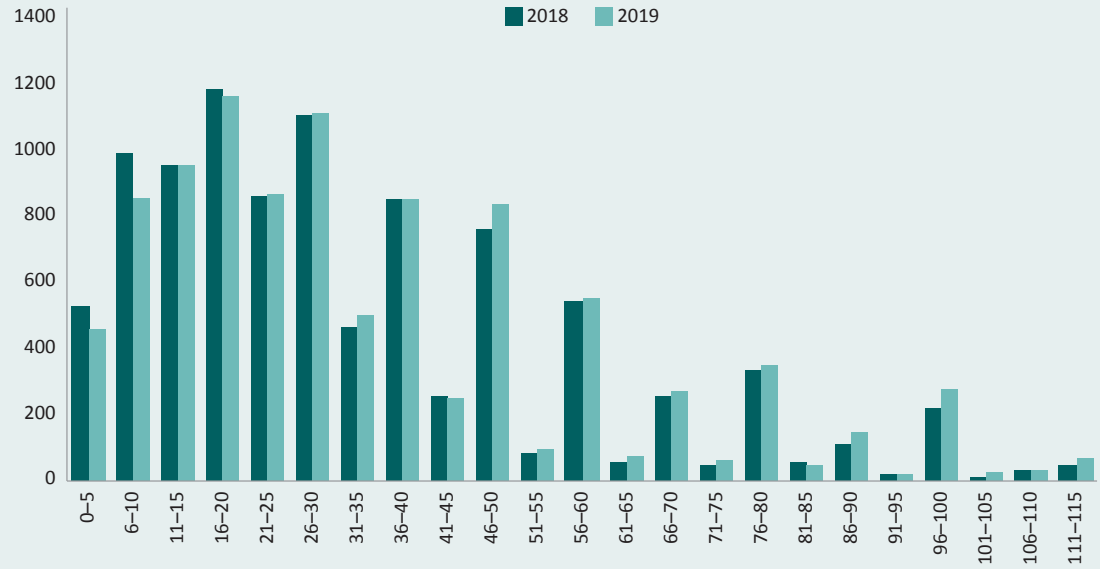
Source: Identity crime survey 2019 [AIC data file]

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=36, *SD*=25, *n*=9,853). A total of 138 respondents indicated that they used a computer or device 116 hours or more per week, which equates to over 16 hours per day. Of these, 16 respondents reported using computers or devices for 168 hours per week (24 hours a day). Such responses could, arguably, relate to the use of digital devices such as watches, activity trackers 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 a five percent increase in the average number of hours participants spent using a computer or device between 2018 (mean=34 hours) and 2019 (mean=36 hours).

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

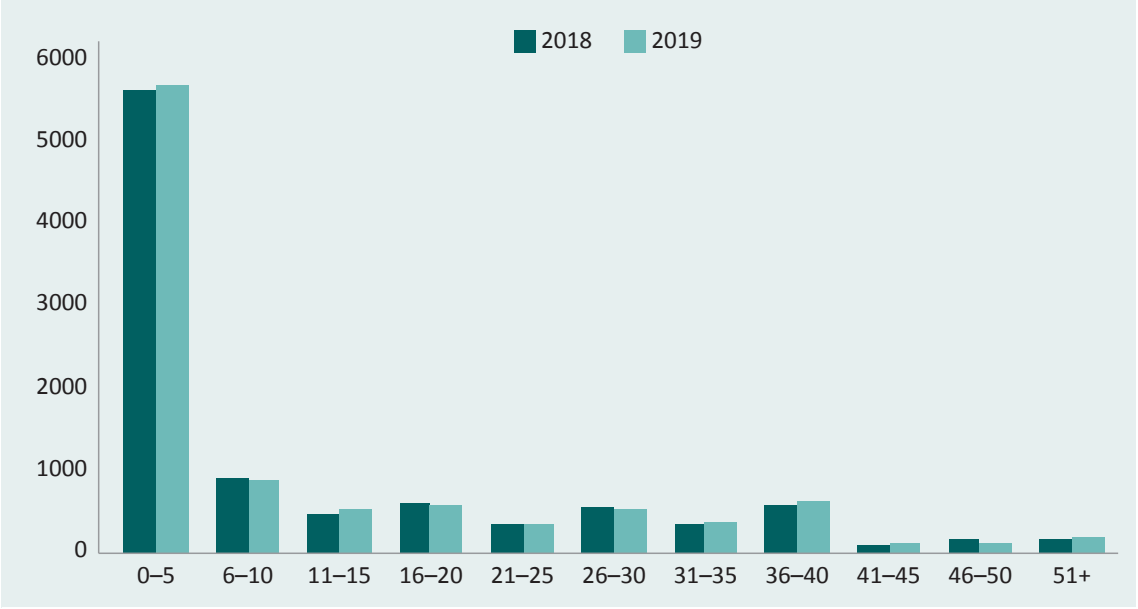


Note: Excludes responses greater than 115 hours. Weighted figures may not total 9,968 due to rounding

Source: Identity crime survey 2019 [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 under 116 hours were included in the analysis. Therefore, the range included was 0 to 115 hours (mean=12, *SD*=16, *n*=9,965). As shown in Figure 3, the vast majority of respondents (96%) 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 2018 and 2019 surveys (12 hours).

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



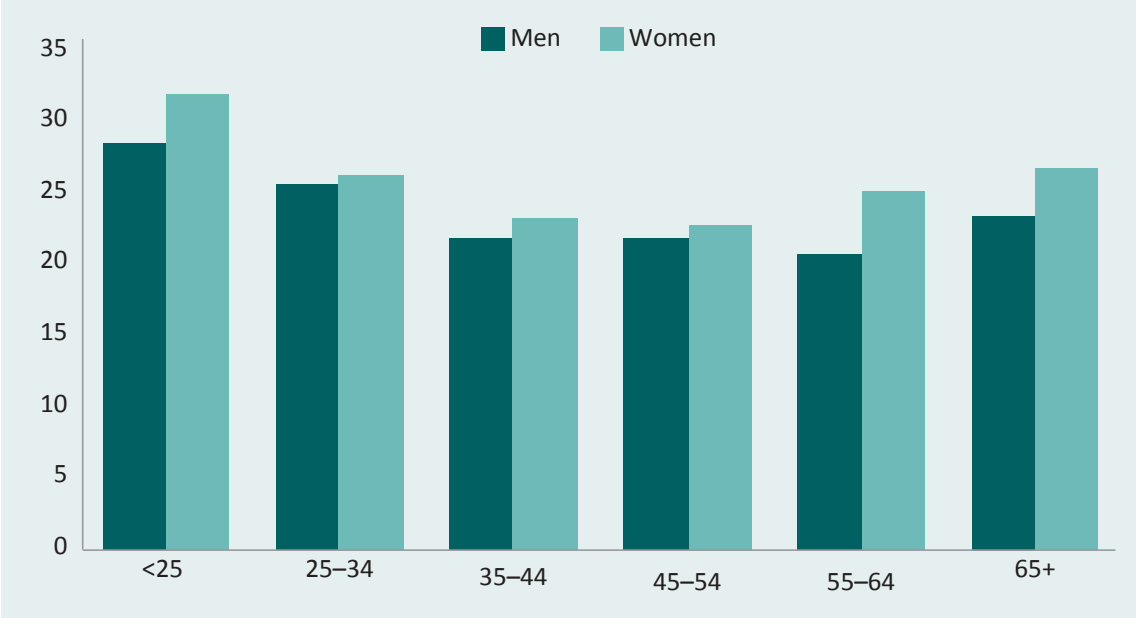
Note: Data are weighted. Excludes responses over 115 hours. *n*=9,965

Source: Identity crime survey 2019 [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 26 hours on computers or devices per week for non-work related activities (*SD*=21, *n*=9,411).

This finding is similar to that of 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 approximately 27 hours a week. Respondents aged 24 years or under reported a noticeably greater number of non-work related computer hours per week than all other age groups.

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



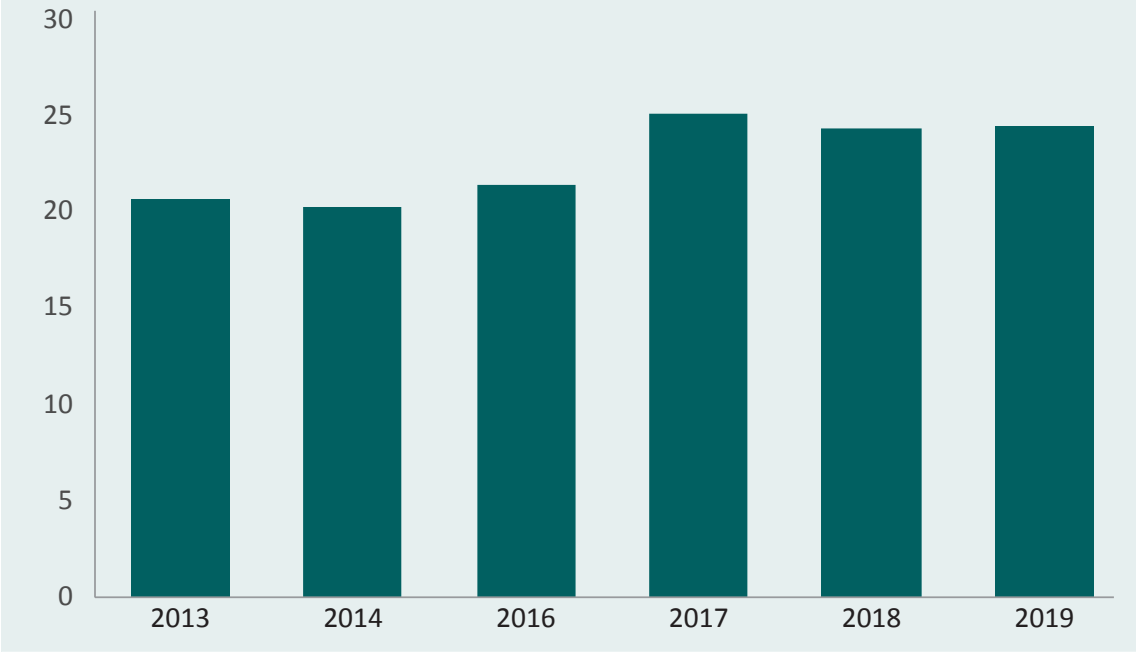
Source: Identity crime survey 2019 [AIC data file]

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). The four percentage point rise in lifetime victimisation between 2016 and 2017 was statistically significant (*N*-1 $\chi^2(1)=25$, $p<0.001$), but since 2017 the rate of victimisation has been steady.

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

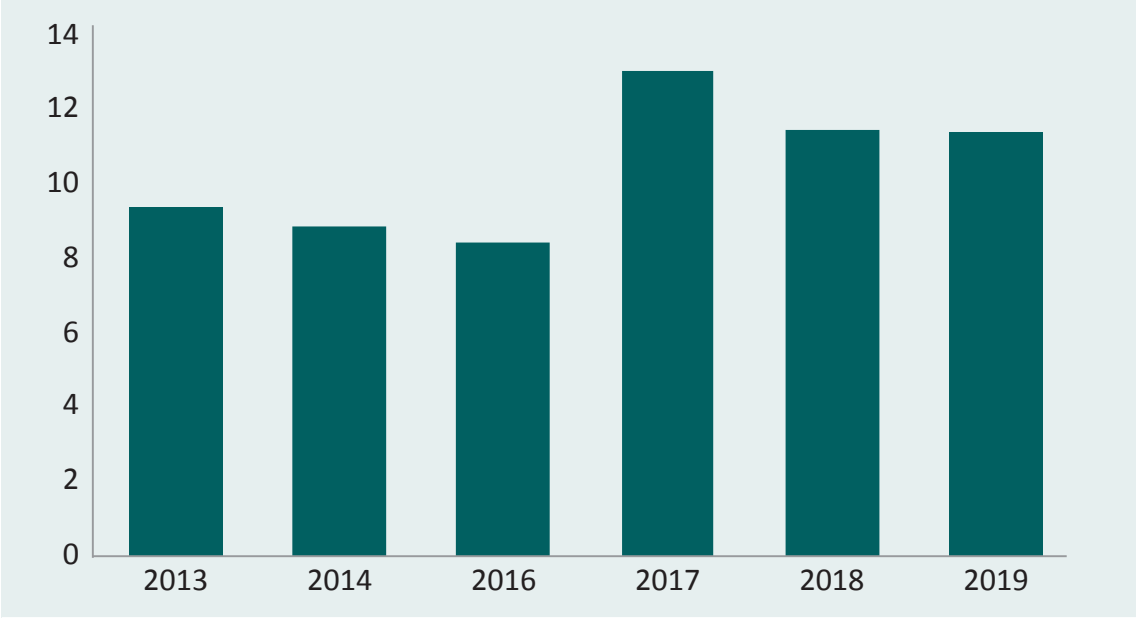


Source: Identity crime surveys 2013, 2014, 2016, 2017, 2018 and 2019 [AIC data file]

Victimisation in the last 12 months

Nearly 12 percent of respondents (*n*=1,140) 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 of 0.1 percent from 2018. However, there was a statistically significant 4.6 percentage point increase in recent victimisation between 2016 and 2017 (*N*-1 $\chi^2(1)=109$, $p<0.001$). Since then, recent victimisation rates have consistently remained above 11 percent.

Figure 6: Recent victimisation, 2013 to 2019 (weighted data) (%)



Source: Identity crime survey 2013, 2014, 2016, 2017, 2018 and 2019 [AIC data file]

Geographic location

The 2019 recent victimisation data were examined by geographic location to see if there were notable increases or decreases in misuse occurring in particular locations (see Table 5). Interestingly, misuse of personal information declined in all geographic regions of Australia except metropolitan areas of Sydney, Melbourne and Brisbane. Melbourne had the most significant increase in misuse at 10 percentage points (84% change). Sydney was a close second with an eight percentage point increase (61% change). Both Melbourne and Sydney were represented by similar numbers of survey respondents in comparison years, indicating the sample size did not influence victimisation rates. Brisbane residents experienced a two percentage point increase in misuse (22% change) with the number of survey participants slightly elevated for 2019 versus 2018 (*n*=1,179 versus *n*=1073). The increase in misuse in these three large cities alone resulted in a slight overall increase in personal information misuse in Australia (1% change).

All other regions of Australia experienced a decline in personal information misuse, with the Northern Territory (including Darwin) registering the largest decrease of 15 percentage points, resulting in a –97 percent change. The 2019 survey did, however, include a smaller number of respondents from the Northern Territory (*n*=48) than the 2018 survey (*n*=63). Other regional areas of Australia with increased numbers of survey respondents also showed declines in reported misuse of personal information. Further research is needed to explore and understand the reasons for the differences between large urban centres and regional areas.

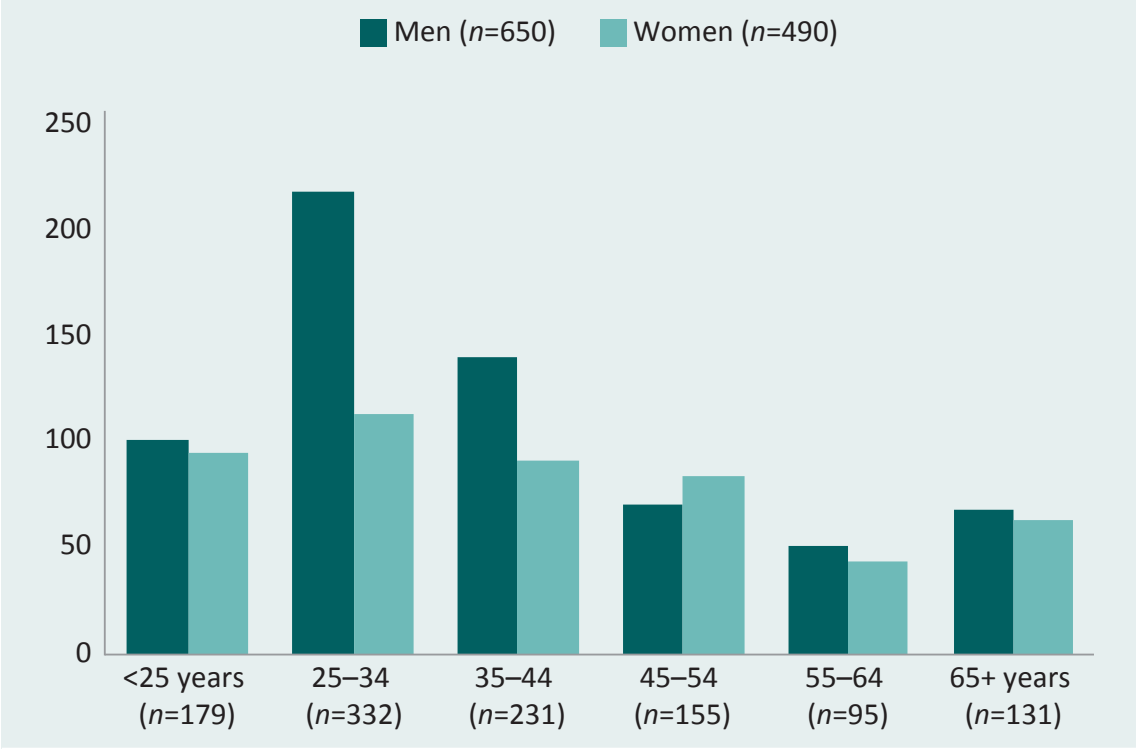
Table 5: Recent victimisation by usual place of residence (unweighted data)				
Location	2018	2019		
	%	%	*n*	% change
Sydney	13.2	21.3	242	61.1
Other New South Wales	11.4	9.3	106	–18.3
Melbourne	12.2	22.4	255	83.7
Other Victoria	12.1	6.9	79	–42.6
Brisbane	9.4	11.4	130	21.5
Other Queensland	9.4	7.3	83	–22.4
Perth	11.4	8.3	95	–26.8
Other Western Australia	7.5	1.8	20	–76.6
Adelaide	9.6	6.0	68	–37.8
Other South Australia	8.8	1.6	18	–82.0
ACT (including Canberra)	9.6	1.6	18	–83.5
Hobart	10.7	0.9	10	–91.8
Other Tasmania	13.2	0.8	9	–94.0
Northern Territory (including Darwin)	14.9	0.4	5	–97.1
National	**11.3**	**11.4**	**1,138**	**0.9**

Source: Identity crime survey 2018 and 2019 [AIC data file]

Gender and age

Consistent with findings from 2018, men between 25 and 34 years of age were the group most likely to report recent victimisation (see Figure 7). Overall, men were significantly more likely than women to report having experienced misuse of personal information in the last 12 months ($\chi^2(1, n=9{,}968)=26$, $p<0.001$, $V=–0.05$; see Table 6). Respondents aged between 25 and 44 years of age were more likely to experience personal information misuse than those in other age groups ($\chi^2(5, n=9{,}968)=137$, $p<0.001$, $V=0.12$; see Table 7).

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



Source: Identity crime survey 2019 [AIC data file]

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

Gender	Recent victimisation		
	Yes	No	Total
Male	650	4,254	**4,904**
Female	490	4,574	**5,064**
Total	**1,140**	**8,828**	**9,968**

Source: Identity crime survey 2019 [AIC data file]

Table 7: Recent victimisation by age (weighted data)

Age group	Recent victimisation		
	n	%	Total
24 years and under	196	12.4	**1,577**
25–34 years	331	18.0	**1,837**
35–44 years	231	14.2	**1,632**
45–54 years	155	10.0	**1,553**
55–64 years	95	6.7	**1,417**
65 years and over	131	6.7	**1,952**
Total	**1,140**	**11.4**	**9,968**

Source: Identity crime survey 2019 (AIC data file)

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 than non-Indigenous respondents or those who did not disclose their Indigenous status (Table 8).

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

Indigenous status	Recent victimisation			
	Yes	%	No	Total
Aboriginal	132	41.0	190	**322**
Torres Strait Islander	8	34.8	15	**23**
Both Aboriginal and Torres Strait Islander	18	62.1	11	**29**
Non-Indigenous/not disclosed	982	10.2	8,612	**9,594**
Total	**1,140**		**8,828**	**9,968**

Note: 78 respondents did not provide their Indigenous status

Source: Identity crime survey 2019 [AIC data file]

Computer usage

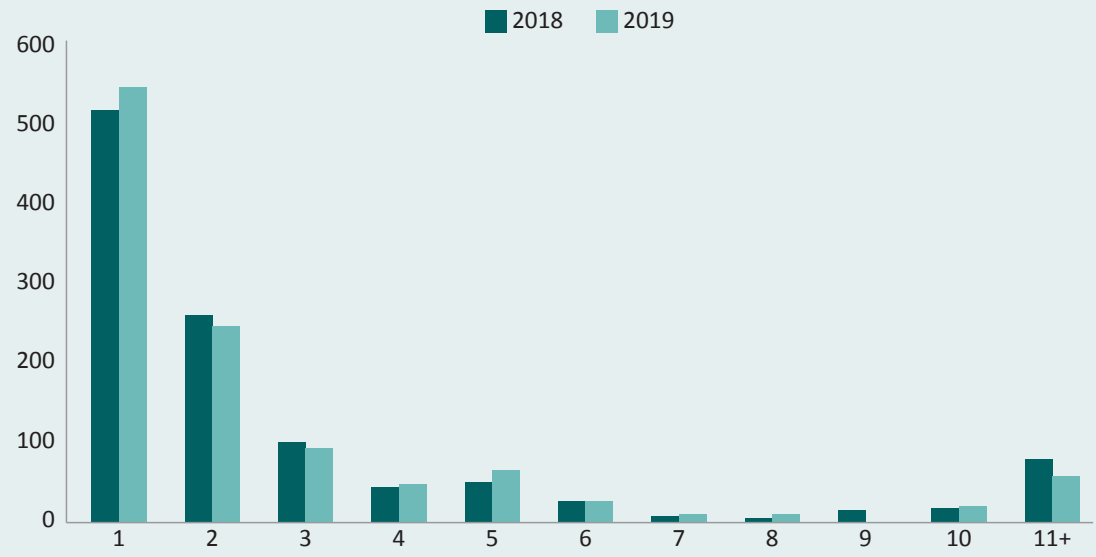
Data on the use of computers and devices were examined to see if this was associated with recent victimisation. There were no significant associations between recent victimisation and non-work related hours spent using a computer or device. However, recent victims of identity crime spent, on average, five additional hours (+3%) on a computer or device each week for work purposes. This increased computer usage for work was statistically significant in terms of total hours spent ($\chi^2(1, 10)=19$, $p<0.0001$) and total work-related hours ($\chi^2(1, 9{,}968)=44$, $p<0.0001$).

Characteristics of recent incidents

Number of incidents

Forty-eight percent (*n*=550) of recent victims reported that their personal information had been misused on only one occasion (see Figure 8). This proportion is slightly higher than that reported in 2018, when 46 percent of respondents (*n*=520) believed their personal information was misused on just one occasion (Jorna, Smith & Norman 2020). In 2019, 22 percent (*n*=247) of respondents reported misuse of personal information had occurred on two separate occasions, slightly lower than the 23 percent of respondents who reported this in 2018. On average, recent victims reported their personal information had been misused on five separate occasions (mean=6, *SD*=38).

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



Source: Identity crime survey 2019 [AIC data file]

Most serious occasion of recent misuse

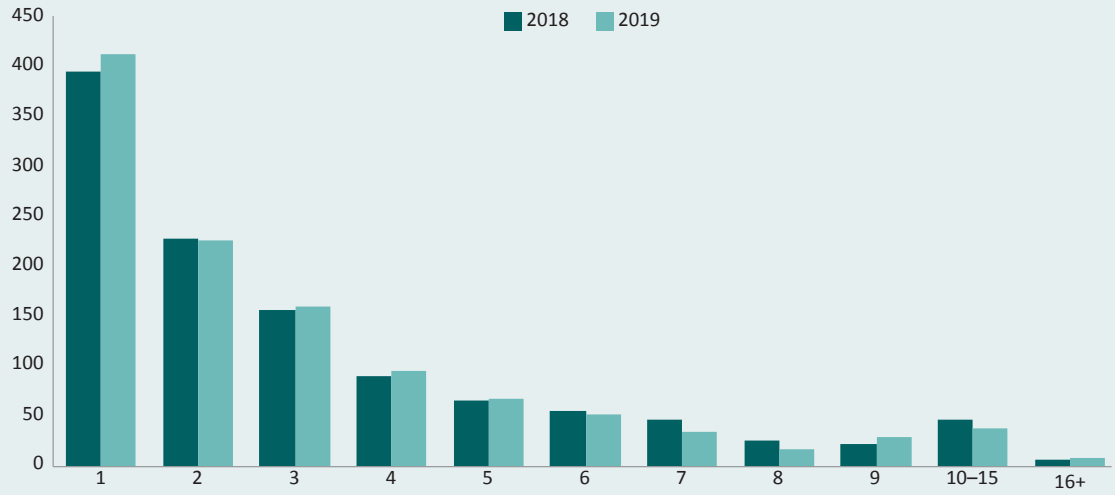
Respondents who had experienced misuse of their personal information in the last 12 months were asked to identify the most serious occasion of misuse. The most serious occasion was defined as the occasion that resulted in the largest financial or other harm to the respondent. This occasion was selected 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 in the last 12 months (see Figure 9). On average, recent victims reported that three types of information had been misused (mean=3, *SD*=3, *n*=1,138). Only three percent of victims reported 10 or more types of personal information having been misused.

Of the 36 percent (*n*=413) of victims who reported misuse of only one type of personal information, 40 percent (*n*=165) reported that the information misused involved credit/debit card details. The second most common response was bank account details (17%, *n*=68). These results confirm the primary motivation behind the theft of identity credentials is financial gain.

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 2019 [AIC data file]

Among all recent victims, the types of personal information most commonly reported as having been misused on the most serious occasion were names and credit card information (41% for each; see Table 9). The 2018 survey also found names and credit/debit card details were the types of information most commonly misused on the most serious occasion (47% and 44%, respectively).

The misuse of bank account information increased over three percentage points—a 12 percent change since the 2018 survey. Again, this demonstrates the financial motivation for identity crimes.

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	2018 (*n*=1,136)	2019 (*n*=1,140)		% change
	%	%	*n*	%
Name	46.8	41.2	470	–12.0
Credit/debit card information	44.2	40.7	464	–7.9
Bank account information	28.9	32.4	369	12.1
Address	32.0	29.6	338	–7.5
Date of birth	30.5	28.6	326	–6.2
Password	23.2	21.1	241	–9.1
Gender	20.8	20.9	238	0.5
Driver licence information	12.1	15.1	172	24.8
Online account username	13.4	15	171	11.9
Place of birth	13.2	13.5	154	2.3
Personal identification number (PIN)	9.2	8.9	101	–3.3
Computer username	9.6	8.8	100	–8.3
Medicare information	7.5	8.4	96	12.0
Passport	8.0	7.8	89	–2.5
Signature	8.5	6.8	78	–20.0
Tax file number	7.9	5.3	60	–32.9
Other	5.7	4.3	49	–24.6
Biometric information (eg fingerprint)	2.5	2.2	25	–12.0
Shareholder information number	2.9	1.9	22	–34.5
Student number	1.8	1.3	15	–27.8

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 and 2019 [AIC data file]

How personal information was obtained

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 statistically significant increases between 2018 and 2019 were ATM or EFTPOS transactions (6 percentage points/95% change; $p<0.0001$) and theft or hacking of a computer/device (6 percentage points/24% change; $p<0.01$).

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	2018 (*n*=1,136)	2019 (*n*=1,140)		% change
	%	%	*n*	
Theft or hacking of a computer or device	24.4	30.3	345	24.2**
Email	18.7	21.5	245	14.9
Online banking transaction	18.4	19.3	220	4.9
Telephone (excluding text message)	19.3	17.3	197	–10.5
Face-to-face meeting (eg job interview or doorknock appeal)	16.5	14.0	160	–14.9
Text message	16.0	14.0	160	–12.3
Website other than social media (eg online shopping)	12.9	13.1	149	1.3
ATM or EFTPOS transaction	6.5	12.7	144	95.4***
Don't know	16.0	12.1	138	–24.3**
Information lost or stolen from a business or other organisation (ie data breach)	12.4	11.7	133	–5.9
Social media (eg Facebook, LinkedIn)	8.9	10.5	120	18.3
From a person I know	5.3	3.6	41	–32.1*
Theft of mail	3.9	3.3	38	–14.5
Theft of identity or other personal document	2.9	2.4	27	–18.3
Theft of a copy of an identity or other personal document	1.4	0.6	7	–56.1
Other	3.1	2.8	32	–9.5

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

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 and 2019 [AIC data file]

How personal information was misused

On the most serious occasions of misuse, personal information was most commonly misused, according to respondents, to obtain money from a bank (excluding superannuation). Nearly 40 percent of respondents selected this reason (see Table 11). This was also the most common reason reported in 2018 (41%), 2017 (38%) and in 2016 (31%). There was a four percentage point rise in recent victims reporting that their personal information had been misused in multiple ways (48% in 2018 vs 52% in 2019). Recent victims reported, on average, having had their personal information misused in almost six different ways (mean=6), a substantial increase over 2018 figures (mean=2).

Between 2018 and 2019, a statistically significant increase was observed in the misuse of personal information to open a mobile phone account—up three percentage points, representing a 57 percent increase (p<0.01). Mobile phones are an enabling tool for criminals. Increased restrictions are being implemented in Australia and worldwide in an attempt to abolish the anonymity of prepaid mobile phones (Kampschror 2009). Prepaid phones have been a favourite of organised crime groups who, when faced with these new restrictions, have begun using stolen identities to register mobile phone accounts needed to complete their illegal activities (ACIC 2017a).

There was also a statistically significant decline between 2018 and 2019 in personal information being misused to file a fraudulent tax return (p<0.001).

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

Purpose of misuse	2018 (n=1,136)	2019 (n=1,140)		% change
	%	%	*n*	
Obtain money from a bank account	41.2	39.4	449	–4.4
Purchase something	21.4	18.5	211	–13.5
Unknown	13.8	12.7	145	–7.8
Obtain superannuation monies	12.8	10.4	118	–19.1
Obtain money from an investment	10.1	9.9	113	–1.9
File a fraudulent tax return	15.9	9.6	110	–39.3***
Apply for a loan/credit	8.3	9.0	103	8.9
Open a mobile phone account	5.1	8.0	91	56.5*
Apply for a job	6.1	6.8	78	12.2
Other	6.6	6.0	68	–9.6
Open social media account	4.1	5.5	63	34.8
Provide false information to police	4.0	5.0	57	25.0
Apply for government benefits	5.6	3.9	45	–29.5
Rent a property	2.0	3.0	34	49.1
Obtain funds from a business/false invoicing[a]	–	2.7	31	–

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

a: This response was not included in the 2018 survey

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 and 2019 [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 2018, victims were most commonly notified of the misuse of their personal information by a bank, financial institution or credit card company (42%). Most respondents (76%) reported detection of the misuse of their personal information via one method, 16 percent reported two different methods and the rest reported three or more detection methods (mean=1, *SD*=1). The only method of detection that became more common was 'notification by a company or business' (up nearly 2 percentage points). There were statistically significant decreases in several methods by which victims were notified, including 'notified by the police', which experienced a 13 percentage point decrease (–71% change; $p<0.0001$). This was closely followed by a four percentage point decline in victims being notified by a government agency (–89% change; $p<0.0001$).

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

Detection method	2018 (*n*=1,136)	2019 (*n*=1,140)		% change
	%	%	*n*	%
Notified by bank/financial institution/credit union	42.2	42.2	481	0.0
Noticed suspicious transactions on bank statements/accounts	37.5	30.9	352	–17.7***
Received credit/debit cards not applied for in the mail[a]	–	19.9	227	–
Other	15.6	12.5	143	–19.6*
Unsuccessful in applying for credit	11.1	8.0	91	–28.1*
Received a bill for services/goods not acquired	11.7	7.8	89	–33.3*
Notified by a company/business	4.1	5.9	67	43.3
Notified by the police	18.0	5.2	59	–71.2***
Contacted by debt collectors	5.2	3.5	40	–32.5
Received goods (ie mobile phones) not ordered in the mail[a]	–	1.3	15	–
Notified by a government agency	4.1	0.4	5	–89.3***

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

a: This response was not included in the 2018 survey

Source: Identity crime survey 2018 and 2019 [AIC data file]

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 increased by over $1.5m between 2018 and 2019, ($1,968,509 in 2018 vs $3,560,266 in 2019). The bulk of this increase was from a single respondent who reported a $1m loss in 2019. This was not removed as a statistical outlier because large value losses are often recorded in identity crime and consumer fraud studies and need to be taken into consideration in arriving at correct findings. Median values, however, did not change between 2018 and 2019.

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

Statistic	2018	2019
Number of respondents (*n*)	945	909
Percentage of all respondents (%)	9.5	9.1
Minimum ($)	1	1
Maximum ($)	300,000	1,000,000
Mean ($)	2,083	3,916
Median ($)	300	300
Standard deviation ($)	13,228	34,146
25% quartile ($)	100	100
75% quartile ($)	1,000	1,000
Total losses ($)	**1,968,509**	**3,560,266**

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

Source: Identity crime survey 2018 and 2019 [AIC data file]

The distribution of out-of-pocket losses was fairly consistent between 2018 and 2019, with the highest peak for each year occurring in the $300–$599 loss range (see Figure 10).

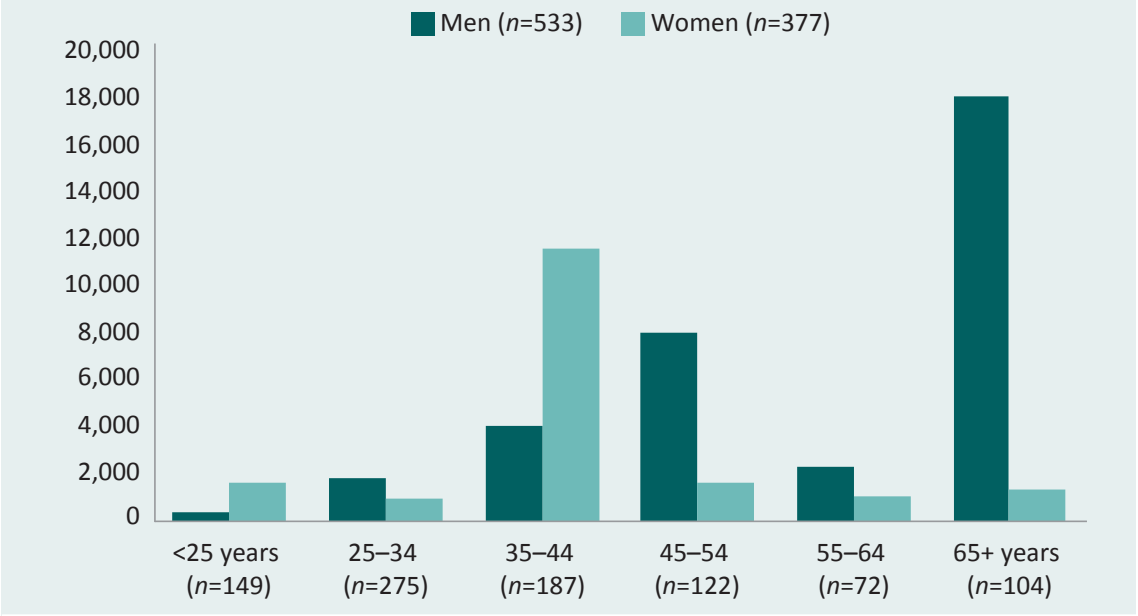
Figure 10: Distribution of total out-of-pocket losses, 2018 and 2019 (weighted data) (%)

Source: Identity crime surveys 2018 and 2019 [AIC data file]

Men aged 65 years and over reported the highest mean financial losses in 2019 ($18,115; see Figure 11). This was followed by women aged 35–44 years (mean=$11,634), and then men aged 45–54 years (mean=$8,046).

Individuals in older age brackets typically report larger financial losses as they usually have access to larger sums of money. Investment scams and dating/romance scams are consistently the two most costly types reported to the Australian Competition and Consumer Commission's (ACCC 2020) Scamwatch with the over 65 age group suffering the greatest losses.

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



Source: Identity crime survey 2019 [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 damage done). The total out-of-pocket loss for 2019 was $2,762,665, an increase of 55 percent from the out-of-pocket losses in 2018 ($1,786,572). The mean out-of-pocket loss reported was $2,802, which was a 42 percent increase over the $1,974 reported in 2018 (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	2018	2019
Number of respondents (*n*)	905[a]	861
Percentage of all respondents (%)	9.1	8.6
Minimum ($)	1	1
Maximum ($)	300,000	1,000,000
Mean ($)	1,974	2,802
Median ($)	200	250
Standard deviation ($)	13,449	29,002
25% quartile ($)	77	70
75% quartile ($)	800	800
Total ($)	**1,786,572**	**2,762,665**

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 2018 and 2019 [AIC data file]

The 2019 distribution of out-of-pocket losses for the most serious occasion of misuse tends to mirror the peaks and troughs of the 2018 distribution, with losses in the <$100, the $300–$599 and the $15,000–$29,999 categories higher in 2019 than in 2018 (see Figure 12).

Figure 12: Distribution of 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 2018 and 2019 [AIC data file]

Total amounts recovered in the last 12 months

The total amount of monies recovered increased from $631,800 in 2018 to $879,463 in 2019 (see Table 15). This increase was also reflected in the mean (up from $817 in 2018, to $1,217 in 2019), although the median amount recovered remained the same ($200).

Table 15: Summary statistics of total losses recovered in the last 12 months (weighted data)		
Statistic	**2018**	**2019**
Number of respondents (*n*)	773	732
Percentage of all respondents (%)	7.8	7.3
Minimum ($)	1	1
Maximum ($)	25,000	60,000
Mean ($)	817	1,217
Median ($)	200	200
Standard deviation ($)	2,200	4,297
25% quartile ($)	50	53
75% quartile ($)	600	600
Total ($)	**631,800**	**879,463**

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

Source: Identity crime survey 2018 and 2019 [AIC data file]

The distribution of total amounts recovered in the last 12 months was generally similar in 2018 and 2019, apart from increased recoveries in the $50–$99 and $300–$599 categories in 2019 (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 2018 and 2019 [AIC data file]

Amounts recovered for the most serious occasion of misuse in the last 12 months

The total of amounts recovered in 2019 for the most serious occasion of personal information misuse in the last 12 months was $803,367, 41 percent more than 2018 ($569,342; see Table 16). The mean amount of money recovered in 2019 also increased ($1,035 in 2019 vs $730 in 2018). 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	2018	2019
Number of respondents (*n*)	780	765
Percentage of all respondents (%)	7.9	7.7
Minimum ($)	1	1
Maximum ($)	25,000	52,000
Mean ($)	730	1,035
Median ($)	200	200
Standard deviation ($)	1,930	3,620
25% quartile ($)	28	60
75% quartile ($)	530	600
Total ($)	**569,342**	**803,367**

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

Source: Identity crime survey 2018 and 2019 [AIC data file]

The distribution of amounts recovered for the most serious occasion of misuse of personal information in the last 12 months shows that recoveries in 2019 followed a similar pattern to recoveries in 2018 (Figure 14).

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

Source: Identity crime survey 2018 and 2019 [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. The proportion of respondents who experienced mental/emotional distress noticeably increased, from 14 percent in 2018 to 15 percent in 2019—an 11 percent change (see Table 17). This is consistent with prior research that has shown that victims of white-collar crimes suffer psychological and medical issues that are often more serious than those of victims of street-level crime: anxiety, depression, distress, anger, helplessness, insecurity, betrayal, self-blame, suicidal ideation, and illness (Dodge 2020).

The proportion of victims being refused credit decreased seven percentage points (–25% change; $p<0.001$), and the proportion refused government benefits decreased five percentage points (–32% change; $p<0.001$). The proportion of respondents reporting no consequences remained relatively consistent between the 2018 and 2019 surveys at approximately 46 percent.

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

Consequences	2018 (*n*=1,136)	2019 (*n*=1,140)		% change
	%	%	*n*	
Refused credit	27.2	20.4	233	–24.9***
Experienced mental/emotional distress	13.8	15.4	176	11.4
Experienced financial difficulties	12.2	12.3	140	0.4
Refused government benefits	14.7	10.0	114	–32.1***
Had to commence legal action	11.8	7.7	88	–34.5*
Wrongly accused of a crime	10.3	6.8	78	–33.8*
Experienced physical health problems	6.0	5.3	60	–12.1
Experienced reputational damage	3.2	2.0	23	–35.8
Refused other services	2.4	1.2	14	–48.0*
Other	8.5	7.6	87	–11.0
I did not experience any consequences	46.6	45.8	522	–1.6

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

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 and 2019 [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*=585) incurred financial costs in dealing with the consequences. Details of the losses are presented in Figure 15. Sixty-two percent of these respondents spent $100 or less; however, eight percent of recent victims spent $2,000 or more. Two percent of victims spent more than $15,000 dealing with the consequences of the misuse of their personal information.

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

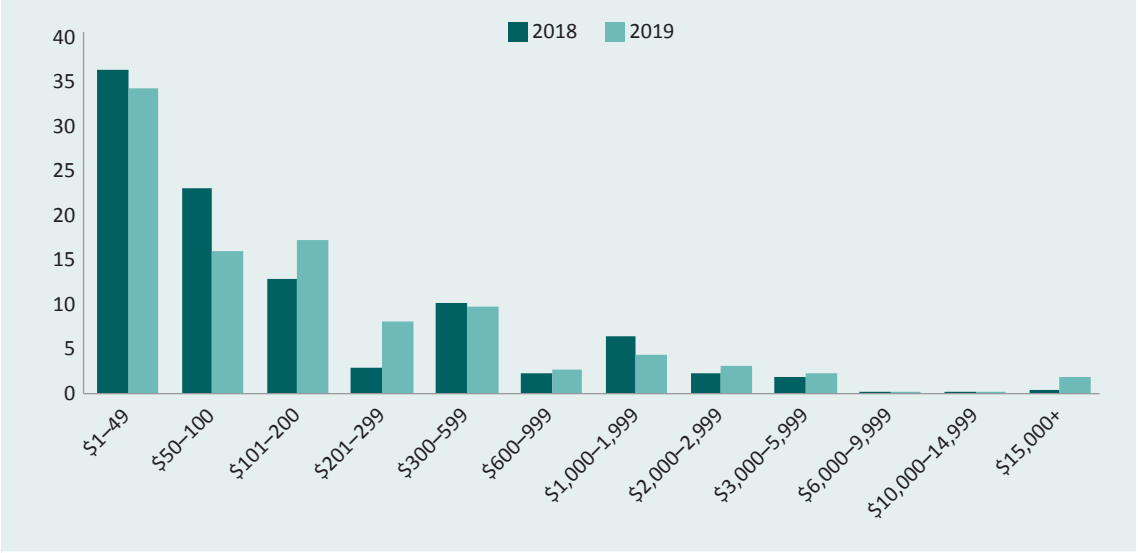
Source: Identity crime survey 2019 [AIC data file]

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 34—similar to the 35 hours reported in the 2018 survey and a substantial increase on the 23 hours spent in 2017. However, seven respondents reported times that were almost three times the standard deviation from the mean (600, 700, 800, 1,000, 2,500, 3,000 and 5,788 hours). If these outliers are excluded, the mean time was 18 hours, similar to the 2018 findings (22 hours). In 2018, six 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 498 respondents. The total amount recent victims spent dealing with the most serious occasion of personal information misuse was $862,523, but individual responses ranged from $1 to $150,000.

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



Source: Identity crime survey 2019 [AIC data file]

The 2019 survey 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 1,138 respondents, 884 (78%) had resolved all problems arising from the most serious occasion of misuse. Eleven percent (*n*=123) had not resolved the problems and the rest (*n*=131) 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 (94%) reported having changed their behaviour in some way (see Table 18).

The most common behavioural change reported in 2019 was being generally more careful when using or sharing personal information, a statistically significant increase to 46 percent in 2019 from 39 percent in 2018 (20% change; $p<0.001$). The most common behavioural change of 2018 was changing passwords (45%) which moved to second place in 2019 at 36 percent, a significant nine percentage point difference (–21% change; $p<0.001$). These figures suggest individuals, especially those who have experienced misuse, are becoming more aware of the importance of keeping all of their personal identification information safe and not just passwords.

Respondents also reported increased use of better security for computers and other devices (12% change) and signing up for commercial identity theft alert or protection services (29% change), confirming individuals are becoming extremely concerned with the safety of their credentials. Other notable behavioural changes included declines in the proportion of respondents who changed their banking details (–12% change), redirected mail when away/moving (–24% change) and used a registered post box (–28% change). However, the proportion of respondents who claimed their behaviour had not changed also decreased 26 percent, which demonstrates individuals are becoming more aware of the need to alter their behaviour to protect their identities.

Table 18: Behavioural changes resulting from the misuse of personal information (weighted data)				
Behavioural change	2018 (*n*=1,136)	2019 (*n*=1,140)		% change
	%	%	*n*	
More careful when using or sharing personal information	38.5	46.3	527	20.3***
Changed passwords	44.9	35.7	407	–20.5***
Review financial statements more carefully	33.8	34.6	394	2.4
Changed banking details	35.2	31.1	355	–11.6*
Use better security for computer and other computerised devices	25.5	28.5	325	11.8
Don't trust people as much	27.0	25.0	284	–7.4
Shred personal documents before disposing of them	19.8	18.4	210	–7.1
Changed my social media account	16.5	14.6	166	–11.5
Changed my email address(es)	14.8	13.8	158	–6.8
Lock mailbox	14.0	12.9	147	–7.9
Applied for a credit report	12.9	12.3	141	–4.7
Redirect mail when away or moving residence	12.0	9.1	103	–24.2*
Changed telephone numbers	10.0	9.0	103	–10.0
Ceased all social media use	9.0	8.9	101	–1.1
Signed up for a commercial identity theft alert/protection service	6.3	8.1	92	28.6
Avoid using the internet for banking and purchasing goods and services	7.6	7.5	856	–1.3
Use a registered post box	8.8	6.3	71	–28.4*
Changed place of residence	7.2	5.7	65	–20.8
Other	3.1	3.5	40	12.9
Behaviour has not changed	8.4	6.2	71	–26.2*

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

Note: Respondents could select multiple responses

Source: Identity crime survey 2018 and 2019 [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 is based on 383 individual responses.

Table 19: Behavioural changes by method of obtaining personal information (weighted data) (%)											
	Method by which personal information was obtained										
	Theft or hacking (*n*=353)	Email (*n*=238)	Online banking (*n*=224)	Phone (*n*=189)	Face-to-face (*n*=151)	Text (*n*=151)	All other websites[a] (*n*=144)	Data breach (*n*=129)	Social media (*n*=119)	ATM (*n*=78)	I don't know (*n*=141)
Changed passwords	62.4	45.4	51.9	30.9	28.7	34.6	58.4	51.7	52.6	37.8	49.9
More careful with personal information	45.0	33.9	49.0	32.5	30.0	33.2	50.7	52.6	49.8	38.5	36.0
Review financial statements more carefully	44.3	31.0	58.3	24.0	18.0	26.7	48.5	47.2	33.9	44.3	44.7
Changed banking details	41.4	32.3	46.3	25.0	23.1	21.2	31.5	35.5	28.9	37.3	28.5
Use better security for computerised devices	40.9	24.2	39.4	28.1	25.7	28.5	39.1	45.5	33.0	39.3	19.9
Don't trust people as much	30.7	21.1	25.4	20.3	23.5	16.8	29.5	27.7	31.4	22.3	27.5
Shred personal documents before disposing	21.4	18.1	26.1	18.4	21.1	20.2	20.6	28.9	21.2	23.4	27.6
Changed email address(es)	18.3	23.1	19.4	23.0	25.2	23.1	23.5	15.0	29.5	32.1	7.6
Changed social media account(s)	18.1	21.9	16.4	21.2	22.3	28.6	19.1	17.3	34.3	24.8	7.2
Avoid using the internet for banking or shopping	13.6	6.6	14.9	3.8	6.5	5.8	11.2	9.3	9.4	14.8	9.5
Applied for a credit report	12.6	15.9	19.3	20.5	30.1	22.3	21.8	12.8	19.5	18.8	11.3
Lock mailbox	11.1	21.8	17.5	18.0	21.1	16.2	15.7	14.0	21.5	23.6	12.3
Ceased all social media use	9.2	16.6	13.1	17.9	19.2	21.7	18.1	17.9	20.7	24.4	5.8
Changed telephone numbers	9.1	13.5	12.3	19.4	19.0	20.3	15.4	8.8	17.0	11.1	6.1
Use a registered post box	8.5	8.9	10.0	11.5	15.1	14.0	10.3	7.7	13.2	14.8	6.2
Redirect mail when away or move residence	8.2	17.1	15.2	18.7	22.4	21.9	16.0	13.4	26.2	25.8	7.6
Changed place of residence	7.8	13.0	7.3	14.4	20.3	15.3	9.2	8.1	15.3	15.3	1.8
Signed up for an identity protection service	6.4	16.7	11.1	13.8	24.5	17.8	15.4	14.1	15.0	8.2	3.5
Other	3.2	1.2	3.3	0.0	0.4	0.0	2.0	3.1	1.8	0.8	3.7
Behaviour has not changed	4.2	2.4	3.3	1.4	0.4	1.8	3.1	3.2	2.6	4.9	16.8

a: 'All other websites' category excludes online banking and social media, which are listed separately

Note: Respondents could select multiple responses

Source: Identity crime survey 2019 [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 respondents reported as having been misused (see Table 20).

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

	Type of personal information misused					
	Name (*n*=469)	Credit/ debit card (*n*=481)	Address (*n*=338)	Date of birth (*n*=319)	Bank account (*n*=383)	Password (*n*=246)
More careful when using or sharing personal information	43.0	42.8	40.1	40.1	48.7	42.8
Changed passwords	51.8	53.7	48.3	48.0	58.0	69.3
Review financial statements more carefully	34.2	50.8	34.7	33.5	47.1	40.6
Changed banking details	31.3	45.6	32.0	29.8	51.6	34.1
Use better security for computer and other devices	36.3	32.1	35.6	37.2	37.9	42.3
Don't trust people as much	30.8	29.3	32.3	33.6	34.1	32.4
Shred personal documents before disposing of them	23.5	22.1	23.6	23.2	20.8	21.6
Changed social media account(s)	21.3	10.7	19.2	20.5	15.1	22.8
Changed email address(es)	21.0	14.7	21.6	18.5	18.8	23.1
Lock mailbox	16.9	11.9	18.0	17.7	14.9	14.8
Applied for a credit report	16.9	13.9	22.0	22.3	14.3	10.9
Redirect mail when away or move residence	12.0	9.2	17.6	17.2	8.6	11.8
Changed telephone numbers	12.4	9.6	15.5	15.3	11.3	12.5
Ceased all social media use	11.6	7.3	14.2	13.8	10.0	12.8
Signed up for a commercial identity theft alert/protection service	10.5	7.2	13.3	13.6	6.9	10.3
Avoid using the internet for banking and purchasing goods and services	8.5	10.1	9.2	10.0	11.6	10.9
Use a registered post box	8.9	6.3	10.9	10.1	5.9	8.9
Changed place of residence	8.8	6.0	12.7	11.3	6.5	7.3
Other	3.2	4.9	2.8	2.3	4.1	2.0
Behaviour has not changed	4.4	6.6	3.1	3.2	4.7	2.9

Note: Respondents could select multiple responses

Source: Identity crime survey 2019 [AIC data file]

Reporting the misuse of personal information

Of the 1,140 respondents who experienced misuse of their personal information in the previous 12 months, nine percent (*n*=107) did not report the misuse in any way. This is nearly the same as the proportion who did not report the misuse in 2018 (10%). Fifty-nine percent of victims (*n*=675) told only a family member or friend; 11 percent of victims (*n*=126) told only a government agency or another organisation; and 20 percent (*n*=232) told an agency and a family member or friend. In 2018 the proportions were very similar: 60 percent of victims reported the misuse to family or friends only, 12 percent to an agency or organisation only, and 19 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). Respondents were most satisfied with the assistance they received from IDCARE, Australia and New Zealand's national identity and cyber support service (93%). Banks and financial institutions ranked second with a satisfaction rating of 82 percent. Nearly half of individuals were dissatisfied with law enforcement responses to their reports of identity crime.

Table 21: Government agencies and other organisations reported to and satisfaction with responses (weighted data)				
Agency/organisation reported to	Satisfied		Dissatisfied	
	n	%	*n*	%
IDCARE (*n*=18)	17	93.0	1	7.0
Bank, credit union, credit/debit card company (eg Visa or MasterCard) or ecommerce provider (eg PayPal) (*n*=211)	174	82.3	37	17.7
Passport Office (*n*=24)	19	78.6	5	21.4
Health insurance company (*n*=26)	19	73.7	7	26.3
ReportCyber (online reporting network) (*n*=29)	21	71.0	8	29.0
Utility company (eg gas, electricity, telephone, water) (*n*=46)	32	69.6	14	30.4
Consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading) (*n*=52)	36	68.9	16	31.1
Credit reporting agency (eg Equifax, Dun & Bradstreet) (*n*=32)	20	62.3	12	37.7
Medicare Australia (*n*=30)	19	62.3	11	37.7
Internet service provider (*n*=32)	20	62.1	12	37.9
Police (*n*=87)	45	51.9	42	48.1
Media organisation (*n*=20)	10	51.9	9	48.1
Road traffic authority (*n*=11)	3	29.2	8	70.8

Source: Identity crime survey 2019 [AIC data file]

In 2019 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 victims 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 basically told me tough luck.'

A recurring complaint from respondents was that those they spoke to seemed to think what had happened to them was not a crime and was their fault. One respondent commented, 'My bank tried to blame me.' Organisations are inclusively a site of identity use and potential misuse, a detector of identity theft, and a site of responsibility to act against this form of crime (Cuganesan & Lacey 2003; Wyre, Lacey & Allan 2020). Organisations invest substantial resources towards crime prevention strategies, but are often lacking in their response to individual victims.

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 reported (Table 22). Multiple reasons could be given. The most common reason given for not reporting identity crime was that a bank or other financial institution had notified the compromised individual of the misuse, making them mistakenly feel the issue had been resolved (37%). The second most common reason given was that the respondent did not think it was important enough to report (26%), closely followed by respondents believing the police or other authority would not be able to do anything about their crime (25%). Nearly 20 percent of respondents indicated they did not know how or where to report the matter, which 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. However, there were statistically significant declines in the numbers of individuals who reported they did not know how or where to report (–30% change; $p<0.001$) or who were too embarrassed to report (–28% change; $p=0.001$). This indicates that people are becoming more aware of the seriousness of identity crime as its growth rate continues.

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

Reason for not reporting	2018 (*n*=784)	2019 (*n*=775)		% change
	%	%	*n*	
Bank, credit union or credit card company notified me	34.4	36.8	288	8.1
Not important enough to report	30.9	25.9	203	–15.2*
I did not believe the police or other authority would be able to do anything	25.4	25.1	196	–0.4
I did not know how or where to report the matter	27.9	19.3	151	–30.2***
I was too embarrassed to report it	17.6	12.6	98	–27.7***
I did not believe it was a crime	15.1	12.5	98	–16.6
Other	7.5	6.1	48	–17.3

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

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 2018 and 2019 [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 could apply to a court to obtain a Victims' Certificate to prove they were a victim of identity crime. Over 78 percent of those surveyed were unaware of the existence of Victims' Certificates, again indicating work to be done by government agencies and other organisations to educate people on the assistance available to them following the compromise and misuse of identity credentials (see Table 23).

Table 23: Awareness of Victims' Certificates (weighted data)			
Level of awareness	2018 (*n*=9,911)	2019 (*n*=9,968)	
	%	%	*n*
I am aware of such certificates, and have obtained one in the past	5.9	5.6	556
I am aware of such certificates, and have applied for one in the past	4.6	4.3	429
I am aware of such certificates, but have not applied for one	12.8	11.8	1,177
I am unaware of such certificates	76.7	78.3	7,806
Total	**100.0**	**100.0**	

Source: Identity crime survey 2018 and 2019 [AIC data file]

Generally, awareness of Victims' Certificates was higher among respondents who lived in capital cities than among those who lived elsewhere (see Figure 17). The location with the highest proportion of respondents who had obtained a Victims' Certificate was Sydney (7%).

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

Source: Identity crime survey 2019 [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. Sixty-three percent of respondents believed that their risk of being a victim of identity crime would increase over the next 12 months (see Table 24). Less than two percent felt their risk would decrease.

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

Change in risk of misuse of personal information	2018	2019	
	%	%	*n*
Risk will increase greatly	19.3	17.0	1,694
Risk will increase somewhat	44.2	45.9	4,571
Risk will not change	34.4	35.4	3,524
Risk will decrease somewhat	1.3	1.3	130
Risk will decrease greatly	0.7	0.5	49
Total	**100.0**	**100.0**	**9,968**

Source: Identity crime survey 2018 and 2019 [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 statistically significant relationship was identified between recent identity crime victimisation and a perceived increase in the risk of victimisation in the next 12 months. Recent victims were more likely than non-victims (32% versus 15% respectively; $p<0.0001$) 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 (37% versus 19% respectively; $p<0.0001$). These percentages represent directly the effects of identity crime victimisation on the perception of risk.

Table 25: Contingency table for recent victimisation and perceived risk of personal information misuse in the next 12 months (weighted data)					
Perceived risk of personal information misuse	Misuse of personal information in previous 12 months				
	Yes	%	No	%	Total
Risk will increase greatly	361	31.7***	1,310	14.8***	**1,671**
Risk will increase somewhat	542	47.6	4,063	46.0	**4,605**
Risk will not change	214	18.8***	3,305	37.4***	**3,519**
Risk will decrease somewhat	14	1.2	110	1.2	**124**
Risk will decrease greatly	7	0.6	42	0.5	**49**
Total	**1,138**		**8,830**		**9,968**

***statistically significant at $p<0.001$

Source: Identity crime survey 2019 [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 (97%) believed that misuse of personal information is a serious issue (see Table 26). Between 2018 and 2019, there was a statistically significant shift in perceived seriousness from 'not at all serious', 'not very serious' and 'somewhat serious' to 'very serious'. Cumulatively, the proportion of respondents who considered the misuse of personal information 'very serious' increased by four percentage points (6% change; $p<0.001$).

Table 26: Perceived seriousness of misuse of personal information (weighted data)			
Seriousness	2018	2019	
	%	%	*n*
Very serious	67.2	71.5***	7,128
Somewhat serious	28.5	25.9***	2,579
Not very serious	3.6	2.4***	237
Not at all serious	0.7	0.2***	24
Total	**100.0**	**100.0**	**9,968**

***statistically significant at $p<0.001$

Source: Identity crime survey 2018 and 2019 [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 (see Table 27). Recent victims (n=1,140) were significantly more likely to rate personal information misuse as 'very serious' than those who had not experienced victimisation (76% vs 71%; p=0.001). Non-victims (n=8,828) were significantly more likely than victims to rate personal information misuse as only 'somewhat serious' (26% vs 22%; p=0.01).

Table 27: Contingency table for recent victimisation and perceived seriousness of personal information misuse (weighted data)					
Seriousness	Misuse of personal information in previous 12 months				
	Yes	%	No	%	Total
Very serious	863	75.7***	6,265	71.0***	**7,128**
Somewhat serious	254	22.3*	2,325	26.3*	**2,579**
Not very serious	20	1.8	217	2.5	**237**
Not serious at all	3	0.3	21	0.2	**24**
Total	**1,140**		**8,828**		**9,968**

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

Source: Identity crime survey 2019 [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 86 percent of respondents reporting using passwords frequently. The least commonly used security measure was a computer chip implanted under the skin, although 10 percent of respondents reported having used this measure.

Table 28: Frequency of use of security measures in the past (weighted data)				
Security measure	How frequently security measures used (%)			
	Frequently	Occasionally	Rarely	Never
Passwords	85.6	8.6	2.6	3.2
Signatures	28.3	29.7	17.7	24.2
Fingerprint recognition	33.4	16.8	12.6	37.3
Facial recognition	15.5	11.2	14.3	59.1
Voice recognition	7.4	16.6	21.8	54.2
Iris recognition	5.2	6.7	10.0	78.2
Computer chip implanted under your skin	3.1	3.7	3.1	90.0

Source: Identity crime survey 2019 [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=9,773) 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%). Surprisingly, 23 percent stated they would be willing to use a computer chip implanted under their skin.

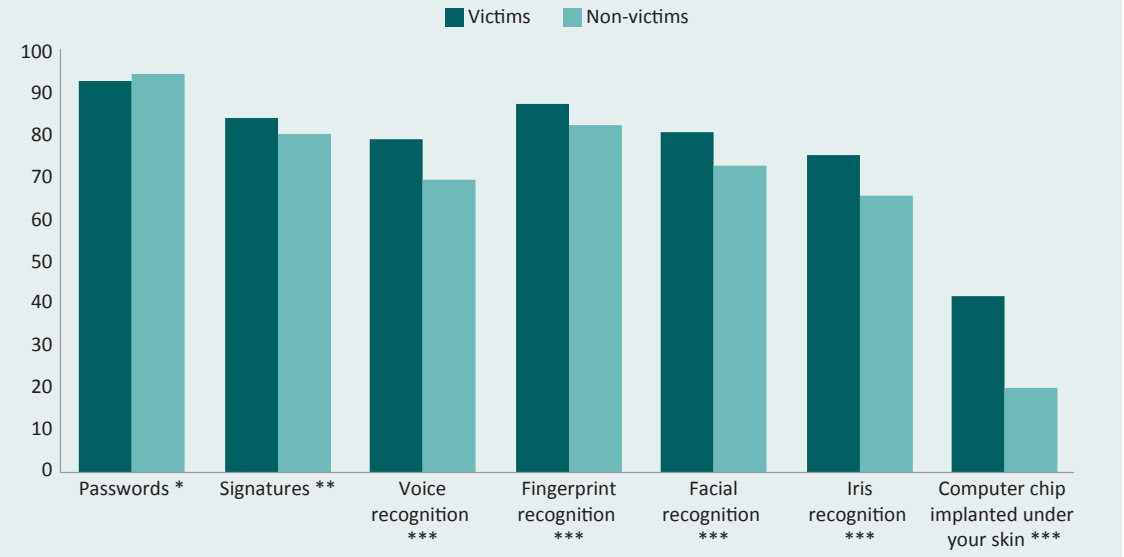
Table 29: Willingness to use security measures to protect personal information in the future (weighted data)		
Security measure	**%**	***n***
Passwords	94.7	9,438
Signatures	81.1	8,080
Voice recognition	70.8	7,056
Fingerprint recognition	83.4	8,315
Facial recognition	74.1	7,388
Iris recognition	67.3	6,705
Computer chip implanted under your skin	22.9	2,281
Any of the above	98.0	9,773
None of the above	2.0	196

Note: Respondents could select multiple responses

Source: Identity crime survey 2019 [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 (*n*=1,140) were more willing than non-victims (*n*=8,828) to use all suggested security measures with the exception of passwords. Passwords are generally the primary method of digital security for individuals. Once compromised, victims will look for alternative methods they perceive to be potentially more effective, making them significantly more willing to try technologically advanced, biometric options and computer chip implants.

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 $p<0.05$

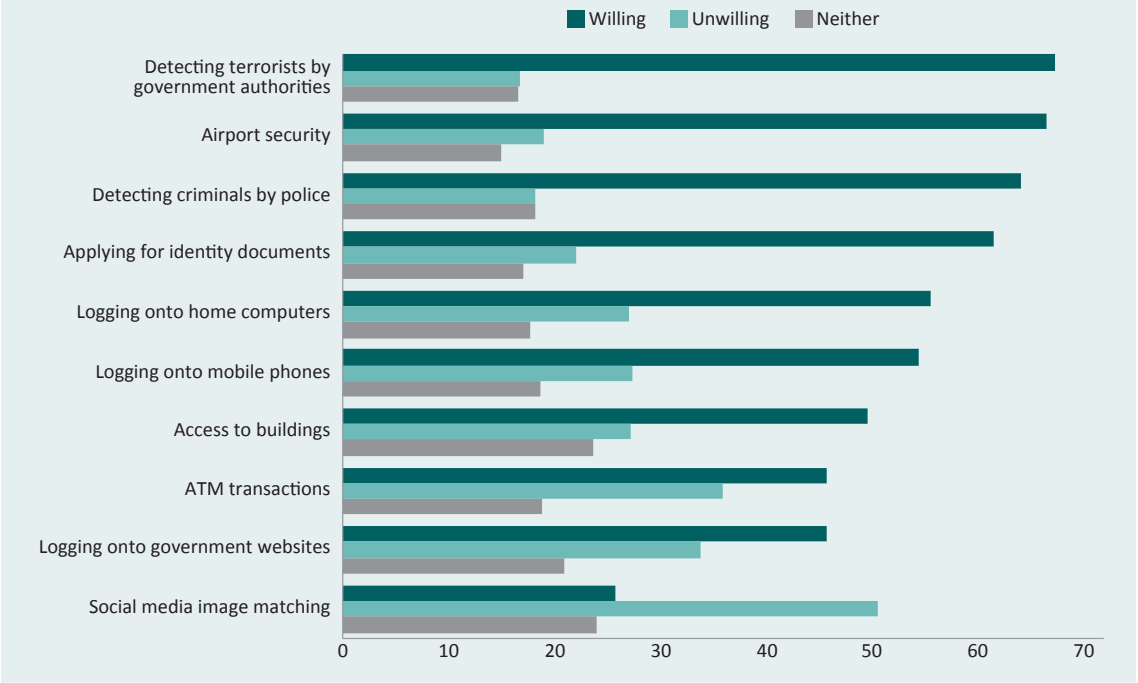
Source: Identity crime survey 2019 [AIC data file]

Facial recognition

To further explore perceptions of facial recognition, respondents were asked to rate their willingness to use facial recognition technologies in various scenarios using a five-point Likert scale with the following response options: (1) Extremely willing, (2) Willing, (3) Neither willing nor unwilling, (4) Not willing, and (5) Extremely unwilling.

Respondents were most willing to use facial recognition technologies for government purposes such as identifying terrorist suspects (67%) and maintaining airport security (66%). The least acceptable purpose for using facial recognition technologies was for matching images on social media (50%).

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



Note: 'Willing' combines 'extremely willing' and 'willing' responses; 'Unwilling' combines 'not willing' and 'extremely unwilling' responses

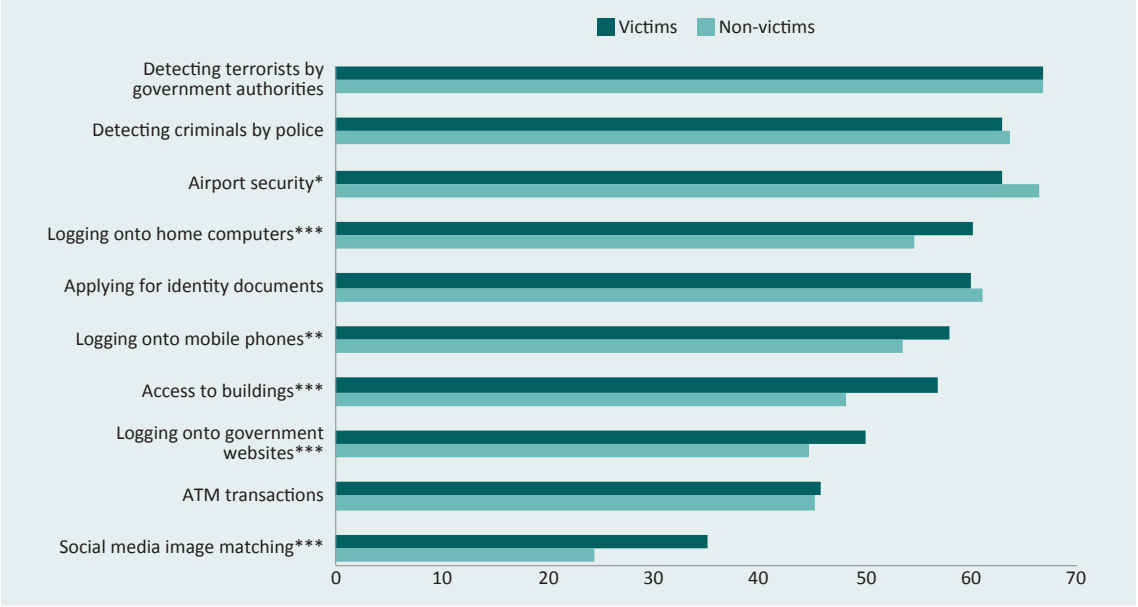
Source: Identity crime survey 2019 [AIC data file]

Figure 20 explores the differences between recent victims (*n*=1,140) and non-victims (*n*=8,828) 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 home computers (60% vs 55%; $\chi^2(1, 9{,}968)=13$, $p=0.001$)
- logging onto mobile phones (58% vs 54%; $\chi^2(1, 9{,}968)=8$, $p=0.0041$)
- access to buildings (57% vs 48%; $\chi^2(1, 9{,}968)=30$, $p<0.0001$)
- logging onto government websites (50% vs 45%; $\chi^2(1, 9{,}968)=11$, $p=0.0007$)
- social media image matching (35% vs 24%; $\chi^2(1, 9{,}968)=61$, $p<0.0001$)

Surprisingly, recent victims of identity crime were significantly less willing than non-victims to use facial recognition technology for airport security (63% versus 66% respectively; p=0.05). 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 by detecting criminals and applying for and using evidence-of-identity documents.

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



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

Note: Willingness includes 'extremely willing' and 'willing' responses combined. n=9,968

Source: Identity crime survey 2019 [AIC data file]

Discussion

On the basis of this survey's findings, misuse of personal information in Australia has remained stable with no indication of decline. Nearly 12 percent of respondents reported that their personal information had been misused in the previous 12 months. This was almost identical to the rate of recent victimisation found in 2018, indicating that the prevalence of identity crime has remained constant over the last two years. This trend is different from the increase in 'attempts to gain personal information' reported to the ACCC between 2017–18 and 2018–19. In 2018–19, Scamwatch received 55,909 such reports, a five percent increase over 2017–18 (53,055; ACCC 2019). Financial losses associated with these reports increased by 65 percent, from $8m to $13m (ACCC 2019).

In the United Kingdom, Cifas' (2019) *Fraudscape* report found identity fraud increased by eight percent between 2017 and 2018. Cifas (2019) also estimates that 58 percent of all fraud involves some element of identity misuse. These findings indicate the prevalence of identity crime is on the rise overseas. In Australia, however, although prevalence has remained stable, losses have increased.

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 Anti-Phishing Working Group (2019) reports that phishing attacks were at their highest level in three years, steadily increasing throughout 2019. An analysis of the ACCC's Scamwatch data shows nearly half of total scam victims (47%) who reported were contacted by telephone or SMS (ACCC 2018).

The 2019 survey found a slight decrease (1%) in the proportion of identity crime victims who reported their personal information was obtained via email, telephone and text message. Rather, respondents advised the most common method by which their information was obtained was via hacking or theft of a computerised device (30% of the sample). Hacking of a device is usually the direct result of a phishing email or text message. There was also an increase in credentials being compromised via social media (18% change), another result of phishing links found in online advertisements or instant messages. Nearly 12 percent of 2019 respondents reported their personal information had been obtained through a data breach, consistent with 2018 findings.

The consistency in the proportion of respondents saying that their personal information was obtained via data breach occurs in a global context. Each year, large data breaches affect tens of millions of people worldwide. For example, highly publicised data breaches have involved Facebook (Burgess 2018), Google (Leskin 2018) and—one of the most substantial data breaches thus far—Marriott 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 2018).

The increasing use of these methods of obtaining personal information aligns with the increase in the number of cybercrime incidents reported around the world. EUROPOL's (2019) *Internet organised crime threat assessment* shows how personal identification information, including financial data, is easily monetisable through sale on the darknet or through crimes of dishonesty. This makes identity theft the second most prominent cyberthreat after ransomware (EUROPOL 2019).

Results from the current survey show the types of personal information most commonly misused were names and credit/debit card information, as was the case in 2018. Financial gain was the most commonly reported motivation behind the reported identity theft, with nearly 40 percent of the cohort stating their credentials were used to obtain money from a bank account. This is directly in line with the most commonly obtained information. The personal identification document demonstrating the largest increase in popularity among criminals is the driver licence, up three percentage points in 2019. This is also in line with the misuse method which is growing the fastest and which requires driver licence information: opening a mobile phone account—also up three percentage points in 2019. Stricter regulations intended to abolish anonymous prepaid mobile phones have become the catalyst for criminals to use stolen identities to register the mobile phone accounts they need for their illegal activities.

The proportion of respondents who reported out-of-pocket losses in 2019 was similar to the figure for 2018 (10% in 2018 vs 9% in 2019), but total losses were substantially higher. When out-of-pocket losses from the most serious occasion of misuse were considered, the average loss was higher in 2019 ($2,802) than in 2018 ($1,974). This increase is explained by the fact that the single largest amount lost in 2019 was $1,000,000, compared with $300,000 in 2018. The proportion of respondents experiencing out-of-pocket losses from the most serious occasion of misuse remained similar (9% in 2018 and in 2019).

In 2019, fewer respondents reported recovering money they had lost as a result of the misuse of their personal information (732 in 2019 vs 773 in 2018). However, the total amount recovered was greater in 2019 ($879,463) than in 2018 ($631,800). This is reflected in the mean amount recovered for all misuse experienced in the last 12 months: $1,217 in 2019, compared with $817 in 2017. The maximum amount recovered by any one victim was also larger in 2019 ($60,000) than in 2018 ($25,000).

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. A larger proportion of respondents experienced mental or emotional distress (11% change), demonstrating the costs of identity crime are far greater than simply financial losses. The University of Texas at Austin's (2019) *Identity threat assessment and prediction report* details how emotional trauma ranging from medium to high levels is the most frequently reported psychological consequence victims of identity crime experience. Financial loss, property loss and reputational damage were all less common than emotional distress (University of Texas at Austin 2019).

Mental and/or emotional distress as a result of identity crime is an area that needs more research and discussion. Support for those who have had their personal information compromised and misused is scarce. The current response journey is complex and difficult to navigate and only exacerbates the psychological trauma. A study was undertaken on Australia's identity theft response system based on a 12-month period of repeated engagement with 211 individual victims of identity compromise and misuse that had contacted IDCARE for assistance (Wyre, Lacey & Allan 2020). The study found that Australia's response system relies on individual victims to perform, on average, 45 out of 67 response tasks relating to detection, disputation, protection and correction when their identities have been compromised (Wyre, Lacey & Allan 2020).

Almost all respondents to the current survey (94%) who had experienced personal information misuse in the last 12 months reported making behavioural changes as a consequence. These behavioural changes varied according to the type of information misused and the method used to access it. For example, respondents whose information was compromised via a website or hacking were more inclined to upgrade their internet security than those whose information was obtained via telephone, SMS or, oddly, email. Individuals whose bank or credit/debit accounts were misused stated they were more careful about sharing their information and spent more time reviewing financial statements. Concerningly, of the 246 respondents who reported their passwords had been misused, only 69 percent changed their passwords.

Identity crime is generally considered an under-reported crime. This research supports this, finding nearly 60 percent of victims reported the crime only to a friend or family member, and almost 10 percent did not report it to anyone. Of the 32 percent of victims who did report their experience to a government agency or organisation, satisfaction was highest among those who reported to IDCARE (93%) or to a bank or credit card company (82%). 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 survey results show the prevalence of identity crime has remained stable since 2018. Positive findings from the 2019 survey is that the vast majority of respondents (98%) considered identity crime and misuse a serious issue, and that individuals are becoming more careful when using or sharing their personal information (20% change). However, identity crimes are still very under-reported due to fear of victim shaming, and many people still lack knowledge about how to or where to report (77% unaware Victims' Certificates exist). 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, prevent further victimisation.

References

URLs correct as at June 2020

Anti-Phishing Working Group 2019. *Phishing activity trends report: 3rd quarter 2019*. 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) 2019. *Australian demographic statistics, Jun 2019*. 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 Competition and Consumer Commission (ACCC) 2020. Scam statistics. https://www.scamwatch.gov.au/scam-statistics

Australian Competition and Consumer Commission 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 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 Criminal Intelligence Commission (ACIC) 2017a. *Organised crime in Australia 2017.* Canberra: ACIC. https://www.acic.gov.au/publications/intelligence-products/organised-crime-australia

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

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 2019. *Fraudscape 2019: Identity fraud and money mules rise again*. https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019

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

Department of Home Affairs 2020. *Australia's 2020 cyber security strategy: A call for views.* https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020

Dodge M 2020. A black box warning: the marginalization of white-collar crime victimization. *Journal of White Collar and Corporate Crime* 1(1): 24–33

Emami C, Smith RG & Jorna P 2019. *Online fraud victimisation in Australia: Risks and protective factors*. Research Report no. 16. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rr/rr16

Europol 2019. *Internet Organised Crime Threat Assessment (IOCTA).* European Cybercrime Centre (EC3). https://www.europol.europa.eu/iocta-report

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

Jorna P, Smith RG & Norman K 2020. *Identity crime and misuse in Australia: Results of the 2018 online survey.* Statistical Report no. 19. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr19

Kampschror B 2009. Cell phones ideal for crime. https://www.occrp.org/en/investigations/402-cell-phones-ideal-for-crime

Leskin P 2018. The 21 scariest data breaches of 2018. https://www.businessinsider.com.au/data-hacks-breaches-biggest-of-2018-2018-12

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 2018. Starwood guest reservation database security incident. https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

Office of the Australian Information Commissioner (OAIC) 2018–2020. *Notifiable data breaches report* (various issues). Canberra: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/

Reichel P & Randa R (eds) 2018. *Transnational crime and global security.* Santa Barbara: Praeger

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 2018. *Estimating the cost to Australian businesses of identity crime and misuse*. Research Report no. 15. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rr/rr15

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 & Franks C 2020. *Counting the costs of identity crime and misuse in Australia, 2018–19.* Statistical Report no. 28. Canberra: Australian Institute of Criminology

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 2018. *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

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

University of Texas at Austin 2019. International identity theft assessment and prediction report. Austin: Center for Identity. https://identity.utexas.edu/research-projects/identity-threat-assessment-and-prediction

Verizon 2019. *2019 Data breach investigations report.* https://enterprise.verizon.com/en-au/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

Wyre M, Lacey D & Allan K 2020. The identity theft response system. *Trends & issues in crime and criminal justice* no. 592. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi592

Yeager DS , Krosnick J, Chang L, Javitz HS & Levindusky MS 2009. 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 survey 2019

Identity Crime and Misuse Survey 2019

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 licence information, passport information, Medicare/health insurance 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 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 8pm and midnight. You should contact your local police if you suspect that your identity has been stolen or misused. More information on how to report identity theft and how to protect your identity can be found at www.ag.gov.au/identitysecurity. Other advice and support is available from IDCARE on 1300 432 273 or www.idcare.org.

The results of the survey will be available from the Australian Institute of Criminology's website at www.aic.gov.au. You can obtain further information from [email] who is in charge of the study. You can also obtain further information or make a complaint about the study by contacting 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) Please indicate the postcode and place of your usual place of residence?

Postcode in Australia

State or Territory (please specify)

☐ I do not normally reside in Australia

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

☐ Male

☐ Female

☐ Indeterminate / Intersex / Unspecified

☐ I'd rather not say

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

- ☐ 17 years and under
- ☐ 18–24 years
- ☐ 25–34 years
- ☐ 35–44 years
- ☐ 45–54 years
- ☐ 55–64 years
- ☐ 65 years and over
- ☐ I'd rather not say

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

- ☐ English
- ☐ Mandarin
- ☐ Cantonese
- ☐ Korean
- ☐ Indonesian
- ☐ Vietnamese
- ☐ Telugu
- ☐ Tamil
- ☐ Japanese
- ☐ French
- ☐ Italian
- ☐ German
- ☐ Greek
- ☐ Russian
- ☐ Spanish
- ☐ Hindi
- ☐ Arabic
- ☐ Farsi
- ☐ Swahili
- ☐ Other (please specify) _____
- ☐ I'd rather not say

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

- ☐ Yes—Aboriginal
- ☐ Yes—Torres Strait Islander
- ☐ Yes—both Aboriginal and Torres Strait Islander
- ☐ No
- ☐ I'd rather not say

Q6) What is the highest educational level you have completed? (Select one only)

- ☐ 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

Q7) What was your individual gross income from all sources for the year 2018–19 (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

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

Insert number of whole hours only_____ (there are only 168 hours in a week, or 112 usual waking hours in a week)

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

Insert number of whole hours only_____ (the average hours per week spent in paid employment is 35 hours)

Technology	Q10) Have you ever used any of the following technologies in the past (in any way, not just to prevent misuse of personal information) (Select all that apply) Select if you PERSONALLY have ever used this technology in the past, in any way, other than in connection with pets or non-personal uses	(Q11) In order to prevent misuse of personal information in the future, would you be willing to use any of the following technologies? Select if you PERSONALLY would be willing to use this technology in the future to protect your personal information (eg at ATMs, at airports, for computers, building access etc)
Passwords	☐	☐
Signatures	☐	☐
Voice recognition	☐	☐
Fingerprint recognition	☐	☐
Facial recognition	☐	☐
Iris recognition	☐	☐
Computer chip implanted under your own skin (not pets or devices)	☐	☐

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

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

Misuse of personal information

The following questions ask about various types of 'personal information'. This could include information such as your: name, address, date of birth, place of birth, gender, driver's licence information, passport information, Medicare/health insurance 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.

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

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

- ☐ Very serious
- ☐ Somewhat serious
- ☐ Not very serious
- ☐ Not at all serious

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

- ☐ Increase greatly
- ☐ Increase somewhat
- ☐ Not change
- ☐ Decrease somewhat
- ☐ Decrease greatly

Q15) Are you aware that a person who has had their personal information misused may be able to apply to a court to obtain a victim certificate (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

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

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

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

Misuse of personal information over the last 12 months

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

Q17) In the last 12 months have you experienced misuse of your personal information? (This could include use of your information without your permission for business or personal transactions, opening accounts, taking out loans or making claims to the government, but not for direct marketing).

☐ Yes

☐ No

☐ Don't know

Q18) [If you answered Yes] On how many separate occasions over the last 12 months do you think your personal information was misused? _____ (insert number)

Q19) Over the last 12 months, how much did you pay out or did someone obtain/access or use as a result of the misuse of your personal information on all occasions combined? $_____ (insert your best estimate of the total amount you paid or was obtained/used or accessed from your bank or credit card account or elsewhere, over the 12 months in whole dollars, including any money that you were later able to recover from banks, etc. Do not include any costs associated with repairing what occurred.)

Q20) Of the amount specified in Q19, 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 over the last 12 months? $_____ (insert your best estimate in whole dollars)

Q21) Over the last 12 months, approximately how much money did you spend dealing with the consequences of having had your personal information misused? (This might include cost of getting legal advice, lost income, telephone charges, bank overdraft fees, postage and fees etc.)

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

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

☐ I was refused credit

☐ I was refused government benefits

☐ I was refused other services (please specify)_____

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

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

☐ I was wrongly accused of a crime

☐ I experienced other reputational damage (please specify)_____

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

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

☐ Other (please specify)_____

or

☐ I didn't experience any consequences

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

Please indicate how many whole hours were spent _____

Q24) Over the last 12 months, did you tell anyone about the misuse of your personal information?

☐ Yes, I told a friend or family member [skip to Q28]

☐ Yes, I told a government agency or another organisation [continue to next question]

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

☐ No, I told no-one [skip to Q28]

Q25) If you made a report to a government agency or an organisation, which of the following did you make a report to? (Select all that apply)

Q26): If you made a report to a government agency or another organisation, how satisfied are you with the outcome?

Organisation	Q27: If you made a report to a government agency or an organisation which of the following did you make a report to? (select all that apply)	Q28: Satisfied with response	Q29: Unsatisfied with response	If unsatisfied selected: why were you unsatisfied with the response?	If satisfied selected: why were you satisfied with the response	Please rate each organisational group from 1 (least favourable response) to 10 (most favourable response)
The police	☐	☐	☐	Why were you unsatisfied with the police response? _____	Why were you satisfied with the police response? _____	
ReportCyber (Australian Cyber Security Centre www.cyber.gov.au/report)	☐	☐	☐	Why were you unsatisfied with the response from the ACSC? _____	Why were you satisfied with the response from the ACSC? _____	
A consumer protection agency (eg ACCC Scamwatch, Consumer Affairs, Office of Fair Trading)	☐	☐	☐	Why were you unsatisfied with the response from the consumer protection agency? _____	Why were you satisfied with the response from the consumer protection agency? _____	
A Road Traffic Authority	☐	☐	☐	Why were you unsatisfied with the response from the Road Traffic Authority? _____	Why were you satisfied with the response from the Road Traffic Authority? _____	

Organisation	Q27: If you made a report to a government agency or an organisation which of the following did you make a report to? (select all that apply)	Q28: Satisfied with response	Q29: Unsatisfied with response	If unsatisfied selected: why were you unsatisfied with the response?	If satisfied selected: why were you satisfied with the response	Please rate each organisational group from 1 (least favourable response) to 10 (most favourable response)
The Passport Office	☐	☐	☐	Why were you unsatisfied with the response from the Passport Office _____	Why were you satisfied with the response from the Passport Office_ _____	
Medicare Australia	☐	☐	☐	Why were you unsatisfied with the repose from Medicare Australia _____	Why were you satisfied with the repose from Medicare Australia _____	
A Health Insurance organisation (other than Medicare)	☐	☐	☐	Why were you unsatisfied with the response from a health insurance organisation? _____	Why were you satisfied with the response from a health insurance organisation? _____	

Organisation	Q27: If you made a report to a government agency or an organisation which of the following did you make a report to? (select all that apply)	Q28: Satisfied with response	Q29: Unsatisfied with response	If unsatisfied selected: why were you unsatisfied with the response?	If satisfied selected: why were you satisfied with the response	Please rate each organisational group from 1 (least favourable response) to 10 (most favourable response)
A bank or credit union, a credit/ debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)	☐	☐	☐	Why were you unsatisfied with the response from your bank or credit union or credit/ debit card company or e-commerce provider? _____	Why were you satisfied with the response from your bank or credit union or credit/debit card company or e-commerce provider? _____	
A credit reporting agency (eg Equifax or Dun and Bradstreet)	☐	☐	☐	Why were you unsatisfied with the response from the credit reporting agency? _____	Why were you satisfied with the response from the credit reporting agency? _____	
Your internet service provider	☐	☐	☐	Why were you unsatisfied with the response from your internet service provider? _____	Why were you satisfied with the response from your internet service provider? _____	

Organisation	Q27: If you made a report to a government agency or an organisation which of the following did you make a report to? (select all that apply)	Q28: Satisfied with response	Q29: Unsatisfied with response	If unsatisfied selected: why were you unsatisfied with the response?	If satisfied selected: why were you satisfied with the response	Please rate each organisational group from 1 (least favourable response) to 10 (most favourable response)
A utility company (eg gas, electricity, telephone, water etc)	☐	☐	☐	Why were you unsatisfied with the response from your utility company? _____	Why were you satisfied with the response from your utility company? _____	
A media organisation	☐	☐	☐	Why were you unsatisfied with the response from the media organisation? _____	Why were you satisfied with the response from the media organisation? _____	
IDCARE (www.idcare.org)	☐	☐	☐	Why were you unsatisfied with the response from IDCARE? _____	Why were you satisfied with the response from IDCARE? _____	
Others (please specify) 1._____ 2. _____ 3. _____	☐	☐	☐	Please provide details why you were unsatisfied with reporting to the agency: _____	Please provide details why you were satisfied with reporting to the agency: _____	

Q30): Please rate each organisational group from 1 (least favourable response) to 10 (most favourable response)

Q31) If you did NOT report the misuse of your personal information to someone other than a friend or family member, please indicate why (select all that apply) [only for respondents who did not report to governments, organisations or family members or friends]

- ☐ I did not know how or where to report the matter
- ☐ I was too embarrassed to report it
- ☐ I did not believe it was a crime
- ☐ I did not believe the police or any other authority would be able to do anything
- ☐ Bank or credit union or credit card company (eg Visa, MasterCard, etc.) had already notified me and issue resolved
- ☐ Not important enough to report
- ☐ Other (please specify) _____

Q32) 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

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

☐ In a face-to-face meeting (eg a job interview or a doorknock appeal)

☐ By telephone (excluding SMS)

☐ By text message (SMS)

☐ By email

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

☐ Theft of an identity or other personal document (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 an organisation or government agency (ie a data breach)

☐ From an online banking transaction

☐ From information you placed on social media (eg Facebook, LinkedIn 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

Q34) On 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
- ☐ Health insurance information
- ☐ Biometric information (eg 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) _____

Q35) On 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)

☐ To obtain funds from a business through the use of false invoicing

☐ Other (please specify)

☐ Don't know

Q36) On this most serious occasion, how did you become aware that your personal information had been misused? (select all that apply)

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

☐ Received credit/payment cards in the mail that were not applied for

☐ Received goods in the mail, such as mobile phones, that were not ordered (please specify what goods were sent)

☐ 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) On this most serious occasion, how much money in total did you pay or did someone obtain/access or use as a result of the misuse of your personal information? $_____ (insert your best estimate of the total amount you paid or was accessed from your bank or credit card account in whole dollars, including any money that you were later able to recover from banks etc. and excluding any costs associated with repairing what occurred)

Q38) On this most serious occasion, how much money was reimbursed to you by banks or other organisations, or recovered in other ways, as a result of the misuse of your personal information? $_____ (insert you best estimate in whole dollars)

Q39) On this most serious occasion, other than the costs you have already specified above, how much, if any, additional costs did you incur as a result of the misuse of your personal information? (insert you best estimate in whole dollars, include costs for things such as legal fees, bounced cheque fees, over draft fees, and any miscellaneous expenses, such as postage, phone calls or notary fees. Do not include lost wages).

Q40) On this most serious occasion, have you been successful in clearing up all of the financial and credit problems associated with the misuse of your personal information?

☐ Yes

☐ No

☐ I 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 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 the Australian demographic statistics for June 2019 (ABS 2019).

This was consistent with the approach to weighting undertaken in the 2018 survey. The Australian Bureau of Statistics demographic statistics for June 2019 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 2019 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)

Age	ABS 2019 Demographic data	2019 Survey	
	%	%	*n*
15–24 years	15.8	9.2	917
25–34 years	18.4	23.0	2,295
35–44 years	16.4	21.2	2,114
45–54 years	15.6	14.9	1,486
55–64 years	14.2	15.0	1,500
65 years and over	19.6	16.6	1,656
I'd rather not say	–	0.6	32
Total	**100.0**	**100.0**	**10,000**

Note: Percentages may not total 100 due to rounding

Source: ABS 2019; Identity crime survey 2019 [AIC data file]

Table B2: Respondents by gender (unweighted data)

Gender	ABS 2019 Demographic data	2019 Survey	
	%	%	*n*
Male	49.0	41.0	4,097
Female	51.0	58.7	5,871
Indeterminate/intersex/unspecified	–	0.1	9
I'd rather not say	–	0.1	12
Total	**100**	**100**	**10,000**

Note: Percentages may not total 100 due to rounding

Source: ABS 2019; Identity crime survey 2019 [AIC data file]

The 2019 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 analysis (*n*=9 indeterminate/intersex/unspecified; *n*=12 'I'd rather not say'), as the data for these groups could not be weighted. The 17 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 32. This resulted in a final sample size of 9,968.

Table B3: Respondents by age and gender (*n*)							
Gender	**Age category**						
	15–24	**25–34**	**35–44**	**45–54**	**55–64**	**65+**	**Total**
Male	318	829	806	582	666	896	4,097
Female	599	1,466	1,308	904	834	760	5,871
Total	**917**	**2,295**	**2,114**	**1,486**	**1,500**	**1,656**	**9,968**

Source: Identity crime survey 2019 [AIC data file]

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

Table B4: Australian population by age and gender (n)							
Gender	**Age category**						
	15–24	**25–34**	**35–44**	**45–54**	**55–64**	**65+**	**Total**
Male	1,675,311	1,892,641	1,678,041	1,55,200	1,432,972	1,891,893	10,146,058
Female	1,586,170	1,907,561	1,698,573	1,637,657	1,500,207	2,146,452	10,476,620
Total	**3,261,481**	**3,800,202**	**3,376,614**	**3,212,857**	**2,933,179**	**4,038,345**	**20,622,678**

Source: ABS 2019

Consistent with the approach taken in the 2018 Identity Crime and Misuse in Australia Survey (Jorna, Smith & Norman 2020), the 2019 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 findings differ 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	318	2.5	810	8.1
Female	599	1.3	767	7.7
25–34 years				
Male	829	1.1	915	9.2
Female	1,466	0.6	922	9.2
35–44 years				
Male	806	1.0	811	8.1
Female	1,308	0.6	821	8.2
45–54 years				
Male	582	1.3	761	7.6
Female	904	0.9	792	7.9
55–64 years				
Male	666	1.0	693	6.9
Female	834	0.9	725	7.3
65 years and over				
Male	896	1.0	914	9.2
Female	760	1.4	1,037	10.4
Total	**9,968**		**9,968**	**100.0**

Note: Percentages may not total 100 and weighted figures may not total 9,968 due to rounding

Source: AIC identity crime survey 2019 [data file]

Comparisons with Australian demographic data show that male respondents aged 15–24 years were under-represented in the 2019 survey (3.2% of the sample vs 8.1% of 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, 2018 and 2019 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. 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. P0287A).

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 broader 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 identity crime, 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 time frame, 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 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

Christie Franks is a 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.

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

aic.gov.au