Australian Government
Australian Institute of Criminology

Statistical Bulletin 37

December 2021

Abstract | This bulletin 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.

In 2021, 9,956 people across Australia were surveyed about their experience of victimisation over their lifetime and during 2020. Nineteen percent of respondents had experienced misuse of their personal information in their lifetime and seven percent experienced it in the past year—a decline from 2019. Seventy-eight percent of respondents who reported victimisation in the past year experienced a financial loss as a result.

Identity crime and misuse in Australia: Results of the 2021 online survey

Merran McAlister and Christie Franks

Identity crime is common in Australia and internationally, affecting millions of individuals, businesses and government agencies annually. Identity crime exploits vulnerabilities in personal identification credentials, consumer payment systems and technological advances in computing and communications, generally for financial gain. The United Nations Economic and Social Council (2007: 18) defined identity crime as 'crime which either targets identification documents, systems or data, or exploits them in the course of committing other crimes'.

In 2018–19, the estimated direct and indirect cost of identity crime in Australia was $3.1b. In 2019 alone, the total losses reported by Australian Institute of Criminology (AIC) online survey respondents was $3.6m (Franks & Smith 2020). Identity crimes are also notoriously under-reported as a result of inhibiting factors such as victim blaming and the complexity of reporting (Franks & Smith 2020). The emotional, physiological and socio-economic impacts faced by victims are often overlooked but can be extreme and prolonged (Emami, Smith & Jorna 2019).

Identity crime is often an enabler for 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 sexual abuse material. Misuse of identity has also been connected with human trafficking and the commission of terrorist acts (Australian Criminal Intelligence Commission 2017; Reichel & Randa 2018).

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). In 2012, the council reviewed and revised the strategy, concluding that an updated strategy was needed in response to the evolving nature of identity crime in Australia (Department of Home Affairs 2020). The strategy also recognised the need to quantify the nature and extent of identity crime and the misuse of personal information, particularly the victimisation experiences of Australians. It recommended the creation of a longitudinal measurement framework for identity crime and misuse that could be used to measure the effectiveness of policy and practice throughout Australia. As part of the measurement framework, the AIC has conducted a series of large-scale surveys to determine respondents' experiences of victimisation over their lifetime and during the preceding 12 months, and their perceptions of the risk of identity crime occurring in the ensuing 12 months. This bulletin presents the findings from the most recent survey, conducted in March 2021.

Methodology

Definitions

This study employed a quantitative, cross-sectional survey design, examining identity crime and misuse of personal information among a sample of Australian residents aged 15 years and over. The different types of identity crime are described by Franks and Smith (2020).

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 (e.g. 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

In March 2021, an online survey comprising 40 questions was administered to a sample of 10,000 Australians by i-Link Research Solutions, a market research company. The survey asked respondents about their experiences of identity crime and misuse in their lifetime and during the 2020 calendar year.

The survey asked respondents about the misuse of various types of personal information. This included (but was not limited to) misuse of an individual's name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (eg fingerprint), signature, bank account information, credit or debit card information, passwords, personal identification numbers (PINs), tax file numbers, shareholder identification numbers, computer or other online usernames and passwords, and student numbers.

This bulletin presents data on the types of personal information misused, how respondents believed their personal information was obtained and how the crimes were detected. The survey also collected information about respondents' views on whether the risk of identity crime would change over the next 12 months, the seriousness of identity crime, their use of and willingness to use biometric technologies as a security measure and, for victims, whether their behaviour had changed as a result of experiencing misuse of their personal information.

The questions were developed by the AIC in consultation with the Department of Home Affairs.

Sample

Sampling was completed once a quota of 10,000 respondents had been reached. No other quotas were employed as the sample was sufficiently large to ensure good representation from urban and regional areas across Australia. Data were weighted by age and gender to reflect the spread of the population in Australia. Australian Bureau of Statistics (2020) data were used to develop the weighting matrix for the sample. The total usable sample for analysis was 9,956 respondents.

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). Work-related hours using a computer or device ranged from zero to 115 hours (mean=13, standard deviation (*SD*)=17, *n*=9,950). The number of hours spent using computers or devices for work purposes was deducted from the total hours spent using devices to determine the number of hours spent on non-work-related activities. The average number of non-work-related hours using a computer or device was 23 (*SD*=21, *n*=9,163). Responses that exceeded 116 hours were excluded from these analyses. However, those participants were retained in the sample for other analyses. There were no significant associations between recent victimisation and non-work-related hours spent using a computer or device ($p>0.05$).

Limitations

The AIC's identity crime surveys use online non-probability panels to recruit respondents. Non-probability panels have been identified as less accurate than probability panels and random digit dialling recruitment (Bethell et al. 2004; Malhotra & 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. This study required participants to have internet access, a variable which may be associated with an individual's chance of being a victim of identity crime.

The limitations of human recall are also a factor in retrospective victimisation studies, given that respondents were asked to recall events over a 12-month time frame. Identity crime victimisation was identified via self-report. Given the nature of fraud, it can be difficult to determine when the crime occurred, as there may be a lapse in time between the individual's personal information being misused and the victim finding out about the misuse. 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.

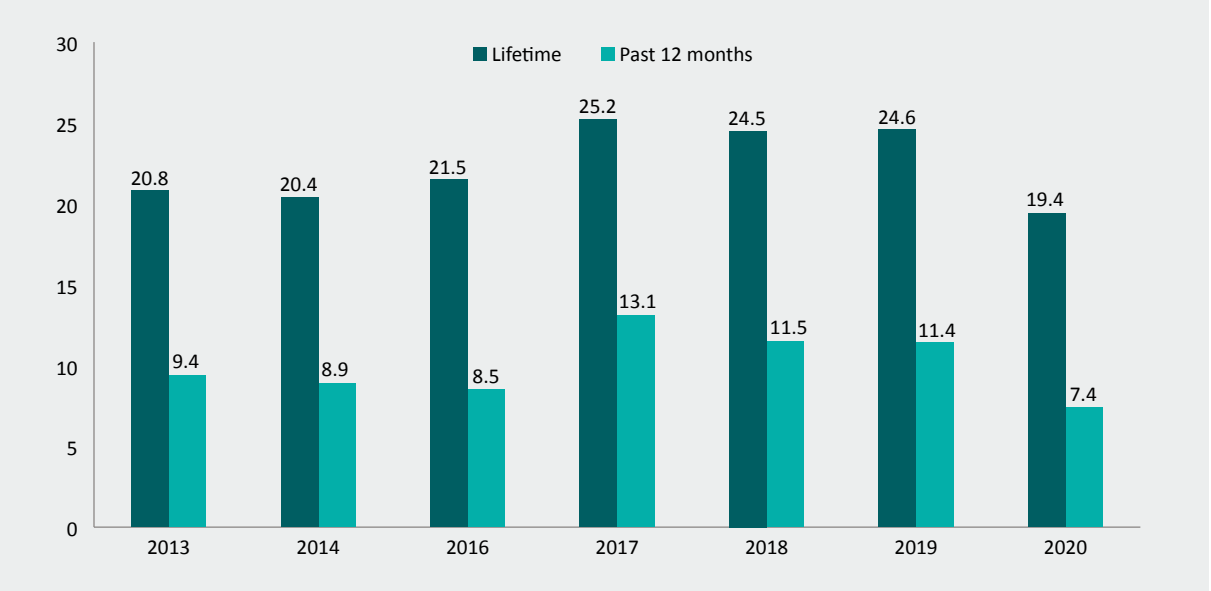
Despite these limitations, the survey results provide valuable information to inform policymakers and the public about the current extent and nature of identity crime in Australia.

Results

Prevalence of identity crime

Nineteen percent (*n*=1,930) of respondents reported they had experienced misuse of their personal information at some point in their lifetime and seven percent (*n*=741) reported experiencing misuse in 2020. This is a statistically significant decline from the 11 percent victimisation rate occurring in 2019 ($\chi^2(1)=92.93$, $p<0.01$; see Figure 1).

Figure 1: Lifetime and past-year victimisation rates of respondents, 2013 to 2020 (weighted data) (%)



Source: Identity crime survey 2013, 2014, 2016, 2017, 2018, 2019 and 2020 [AIC data file]

Forty-four percent of recent victims (*n*=326) reported that their personal information had been misused on one occasion, a decline from 48 percent in 2019. Twenty-four percent of respondents (*n*=178) reported that misuse of their personal information had occurred on two separate occasions. On average, recent victims reported their personal information had been misused on eight separate occasions (*SD*=59).

Types of personal information misused

Recent victims reported that between one and 23 different types of personal information had been misused. The 2021 survey introduced a question asking respondents about the misuse of mobile phones and email addresses, as the Australian Competition and Consumer Commission (ACCC) identified them as the top methods of obtaining personal information in 2019 (ACCC 2021b). In this survey, telephones/mobile phones (28%, *n*=207) and email addresses (22%, *n*=162) were not the primary types of personal information misused but both ranked in the top eight, as outlined in Table 1. Forty-six percent of respondents (*n*=339) reported misuse of their name, making this the most commonly misused type of personal information (see Table 1). This was not a statistically significant increase from 2019 (41%, $p>0.05$). Addresses (35%, *n*=261) and credit/debit cards (31%, *n*=233) were also commonly misused.

The misuse of bank account information significantly declined between 2019 and 2020 (32% vs 28%, $p<0.05$). The misuse of credit and debit cards also declined significantly (41% vs 31%, $p<0.001$). This could be attributed to the decreased use of physical cards in the community, leading to an increase in card-not-present fraud, which occurs primarily online (Australian Payments Network 2021).

Table 1: Types of personal information misused, 2019 and 2020 (weighted data)

Type of personal information misused	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
Name	41.2	45.7	339	10.9
Address	29.6	35.2	261	18.9*
Credit/debit cards	40.7	31.4	233	–22.9***
Date of birth	28.6	30.6	227	7.0
Bank account details	32.4	28.0	207	–13.6*
Telephone/mobile[a]	–	27.9	207	–
Gender	20.9	23.3	173	11.5
Email address[a]	–	21.9	162	–
Password(s)	21.1	14.8	110	–29.9***
Driver licence	15.1	14.4	107	–4.6
Place of birth	13.5	13.3	99	–1.5
Medicare information	8.4	10.1	75	20.2
Online account username	15.0	9.0	67	–40.0***
Tax file number	5.3	9.0	66	69.8**
Passport	7.8	8.7	64	11.5
Personal identification number (PIN)	8.9	7.5	56	–15.7
Computer username(s)	8.8	7.3	54	–17.0
Signature	6.8	5.9	43	–13.2
Health insurance	4.0	5.7	42	42.5
Shareholder identification number	1.9	5.1	38	168.4***
Biometric information (eg fingerprint)	2.2	3.2	24	45.5
Student ID number	1.3	2.3	17	76.9
Other	4.3	2.6	20	–39.5

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

a: This answer was not available in the 2019 survey

Note: Percentages do not total 100 as respondents could select multiple responses

Source: Identity crime survey 2019 and 2020 [AIC data file]

How personal information was obtained

Obtaining personal information via email (27%, *n*=199) and through a phone call (27%, *n*=197) were the most common methods. Second to this was theft or hacking of a computer or device (25%, *n*=183) and face-to-face meetings (25%, *n*=182). Theft or hacking of a computer or device significantly declined between 2019 and 2020 (30% vs 25%, *p*<0.01; see Table 2). There was a significant increase in the proportion of respondents reporting phone calls as the primary method of obtaining personal information between 2019 and 2020 (17% vs 27%, *p*<0.001). The increase in the use of phone calls as a method of acquisition may be attributed to the COVID-19 pandemic, which led people to spend more time at home and using their devices (ACCC 2021b).

Table 2: How the personal information of recent victims was obtained, 2019 and 2020 (weighted data)

Method of obtaining personal information	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
Email	21.5	26.8	199	24.7**
Phone call	17.3	26.6	197	53.8***
Theft or hacking of a computer/device	30.3	24.7	183	–18.5**
Face-to-face meeting	14.0	24.6	182	75.7***
Text message (SMS)	14.0	21.5	159	53.6***
Online banking transaction	19.3	20.5	152	6.2
Information placed on social media	10.5	13.9	103	32.4*
Information placed on website	13.1	13.2	98	0.8
Data breach	11.7	12.2	90	4.3
ETFPOS transaction	7.7	10.4	77	35.1**
ATM transaction	6.0	6.8	50	13.3
From a person I know	3.6	4.1	31	13.9
Theft of mail	3.3	2.7	20	–18.2
Theft of an identity document	2.4	1.8	14	–25.0
Theft of a copy of an identity document	0.6	0.9	6	50.0
Unsure	12.1	11.0	81	–9.1
Other	2.8	2.4	17	–14.3

***statistically significant at *p*<0.001, **statistically significant at *p*<0.01, *statistically significant at *p*<0.05
Note: Percentages do not total 100 as respondents could select multiple responses
Source: Identity crime survey 2019 and 2020 [AIC data file]

How personal information was misused

As in 2019, the most common reason personal information was misused was to obtain money from a bank (39% in 2019 and 41%, *n*=302 in 2020; see Table 3). This was followed by misusing personal information to open a new bank account (19%, *n*=144) and to obtain superannuation monies (19%, *n*=139), illustrating the financial motivation for identity crimes.

Table 3: How personal information of recent victims was misused, 2019 and 2020 (weighted data)

Purpose of misuse	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
To obtain money from a bank	39.4	40.7	302	3.3
To open a new bank account[a]	–	19.4	144	–
To obtain superannuation monies	10.4	18.7	139	79.8***
To file a fraudulent tax return	9.6	16.5	122	71.9***
To purchase something	18.5	15.4	114	–16.8
To obtain money from an investment (shares)	9.9	13.6	101	37.4
To apply for a job	6.8	12.1	90	77.9***
To apply for a loan or obtain credit	9.0	11.2	83	24.4
To open a mobile phone account	8.0	9.4	70	17.5
To apply for government benefits	3.9	9.0	67	130.8**
To provide false information to police	5.0	8.5	63	70.0*
To rent a property	3.0	4.6	34	53.3
False invoicing	2.7	3.2	24	18.5
To open an online account	5.5	2.6	19	–52.7**
Unknown	12.7	8.6	64	–32.3*
Other	6.0	6.9	51	15.0

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
a: This answer was not available in the 2019 survey
Note: Percentages do not total 100 as respondents could select multiple responses
Source: Identity crime survey 2019 and 2020 [AIC data file]

Detection of identity crime and misuse

Fifty-five percent (*n*=404) of recent victims were notified of the misuse of their personal information by a bank or financial institution, a significant increase from the 42 percent in 2019 ($p<0.001$; see Table 4). There was no statistically significant difference between the proportion of respondents reporting they noticed suspicious transactions on bank statements or accounts in 2020 (33%, *n*=245) and in 2019 (31%, $p>0.05$).

Table 4: Method of detecting recent identity crime and misuse, 2019 and 2020 (weighted data)

Detection method	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
Notified by a bank/financial institution	42.2	54.5	404	29.2***
Noticed suspicious transactions on bank statements/ accounts	30.9	33.0	245	6.8
Received credit/payment cards in the mail not applied for	19.9	27.3	202	37.2***
Received a bill from an unknown business or company	7.8	11.4	85	46.2**
Unsuccessful in applying for credit	8.0	11.1	82	38.8*
Notified by police	5.2	6.0	45	15.4*
Contacted by debt collectors	3.5	5.4	40	54.3
Notified by a company/organisation	5.9	5.2	38	–11.9
Notified by a government agency or other authority	0.4	1.5	11	275.0
Received goods in the mail not ordered	1.3	0.5	3	–61.5
Other	12.5	7.1	53	–43.2***

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$
Note: Percentages do not total 100 as respondents could select multiple responses
Source: Identity crime survey 2019 and 2020 [AIC data file]

Impact on victims

Out-of-pocket losses and reimbursements

Respondents were asked to estimate their total out-of-pocket losses from all occasions of misuse of personal information experienced in 2020, excluding any money recovered or reimbursed and any costs associated with repairing any damage done. A single respondent reported a loss in excess of $1m. Large loss values can be recorded in identity crime and consumer fraud studies. However, this was removed as a statistical outlier as this amount exceeded the standard deviation and was outside the scope of previous survey responses and reports. Total out-of-pocket losses suffered by victims decreased between 2019 and 2020 ($3,560,266 in 2019 vs $1,514,486 in 2020; see Table 5).

Table 5: Summary statistics for out-of-pocket losses and monies recovered for all personal information misuse experienced in 2020 (unweighted data)

Statistic	Out-of-pocket losses	Monies recovered
Number of respondents (*n*)	563	503
Percentage of all respondents (%)	5.7	5.1
Minimum ($)	1	1
Maximum ($)	240,000	217,000
Mean ($)	2,690	1,494
Median ($)	200	150
Standard deviation ($)	17,174	12,111
25% quartile ($)	78	50
75% quartile ($)	700	500
Total losses ($)	1,514,486	751,425

Source: Identity crime survey 2020 [AIC data file]

The total amount of monies recovered in 2020 was $751,425, a decline from the total amount recovered in 2019 ($879,463). This corresponds with the overall decline in past-year victimisation. The total amount of monies recovered in 2020 ranged from $1 to $217,000 (see Figure 2)—a larger range than in 2019.

Figure 2: Distribution of financial losses and monies recovered by recent victims, 2020 (weighted data) (%)

Source: Identity crime survey 2020 [AIC data file]

Money and time spent rectifying misuse of personal information

Of those who experienced misuse of their personal information in 2020, 55 percent (*n*=411) incurred financial costs in dealing with the consequences. The average amount of money spent rectifying the misuse was $2,832 (median=$100, IQR=$27–$254). Sixty-one percent of these respondents (*n*=252) spent $100 or less. Seven percent (*n*=28) spent $2,000 or more and two percent of victims (*n*=7) spent more than $15,000 dealing with the consequences of the misuse.

Respondents spent an average of 49 hours (*SD*=295) dealing with the consequences of the misuse, a substantial increase from the 34 hours in 2019. However, seven respondents reported times that were almost three times the standard deviation from the mean (900, 1,000, 1,200, 2,000, 2,280, 3,000 and 3,500 hours). If these outliers are excluded, the mean time was 15 hours, slightly less than the 2019 finding (18 hours). In 2019, seven statistical outliers were excluded from the analysis.

Non-financial consequences of personal information misuse

Forty-two percent of recent victims (*n*=308) did not experience any consequences as a result of their personal information being misused—a similar proportion to that found in 2019 (46%). Of those who reported experiencing consequences, being refused credit was most common (28%, *n*=207), followed by being refused government benefits (17%, *n*=129; see Table 6). Thirteen percent of those victimised in 2020 (*n*=97) reported experiencing mental and/or emotional distress. This proportion was similar to the 2019 finding (15%) and is consistent with prior research, which has shown victims of white-collar crimes often suffer psychological and medical issues that are more serious than those experienced by victims of street-level crime (Dodge 2020).

Table 6: Consequences experienced by recent victims as the result of personal information being misused, 2019 and 2020 (weighted data)

Consequences	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
Refused credit	20.4	28.0	207	37.3***
Refused government benefits	10.0	17.4	129	74.0***
Refused other services	1.2	0.5	4	–58.3
Experienced financial difficulties	12.3	15.0	111	22.0
Experienced mental/emotional distress	15.4	13.1	97	–15.0
Had to commence legal action	7.7	12.4	92	61.0***
Wrongly accused of a crime	6.8	9.0	66	32.4
Experienced physical health problems	5.3	6.3	47	18.9
Experienced reputational damage	2.0	0.8	6	–60.0*
Other	7.6	4.8	36	–36.8*
I did not experience any consequences	45.8	42.0	308	–8.3

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

Note: Percentages do not total 100 as respondents could select multiple responses

Source: Identity crime survey 2019 and 2020 [AIC data file]

Behavioural changes arising from the misuse of personal information

As was found in previous years, most respondents (91%, *n*=678) reported having changed their behaviour in some way as a result of the victimisation. The most common behavioural change reported in 2020 was changing passwords (33%, *n*=242). There was a significant reduction between 2019 and 2020 in the proportion of people being more careful when using or sharing personal information after victimisation (46% vs 30%, $p<0.01$; see Table 7). However, these figures still suggest individuals, especially those who have experienced misuse, are becoming aware of the importance of keeping their personal identification information safe and not just their passwords.

Table 7: Behavioural changes resulting from the recent misuse of personal information, 2019 and 2020 (weighted data)

Behavioural changes	2019 (*n*=1,140)	2020 (*n*=741)		% change
	%	%	*n*	
Changed passwords	35.7	32.7	242	–8.4
More careful when using or sharing personal information	46.3	30.3	225	–34.6***
Review financial statements more carefully	34.6	29.3	217	–15.3*
Changed banking details	31.1	24.1	179	–22.5**
Do not trust people as much	25.0	22.8	169	–8.8
Use better security for computer and other computerised devices	28.5	20.3	150	–28.8***
Changed my social media account	14.6	14.9	111	2.1
Shred personal documents before disposing of them	18.4	14.6	108	–20.7*
Begun using biometric technologies more frequently[a]	–	14.2	105	–
Changed my email address(es)	13.8	14.1	105	2.2
Changed telephone number	9.0	13.2	97	46.7**
Lock mailbox	12.9	12.1	90	–6.2
Applied for a credit report	12.3	12.3	91	0.0
Ceased all social media use	8.9	9.6	71	7.9
Redirect mail when away or moving residence	9.1	9.6	71	5.5
Signed up for a commercial identity theft alert/ protection service	8.1	9.2	68	13.6
Changed place of residence	5.7	8.0	59	40.4
Avoid using the internet for banking and purchasing goods and services	7.5	6.8	51	–9.3
Use a registered post box	6.3	6.8	50	7.9
Other	3.5	4.0	30	14.3
Behaviour has not changed	6.2	8.5	63	37.1

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

a: This answer was not available in the 2019 survey

Note: Percentages do not total 100 as respondents could select multiple responses

Source: Identity crime survey 2019 and 2020 [AIC data file]

Reporting the misuse of personal information

Of the 741 respondents who experienced misuse of their personal information in 2020, 10 percent (*n*=71) did not report the misuse in any way. This is a similar proportion to the 2019 finding that nine percent did not report misuse. In 2020, 54 percent of respondents (*n*=402) told only a family member or friend, 19 percent (*n*=138) told an agency and a family member or friend, and 18 percent (*n*=130) told only a government agency or other organisation.

Satisfaction with reporting

In 2019, respondents were most satisfied with responses from the identity and cyber support service IDCARE, but in 2020 respondents were most satisfied with the assistance they received from their internet service providers (97%, *n*=19). Private health insurance ranked second, with a satisfaction rating of 86 percent (*n*=15; see Table 8).

Despite the range of agencies and organisations a victim of identity crime could report to, common themes were found across all organisations that contributed to a respondent feeling satisfied or dissatisfied with the response. Respondents were generally satisfied if the person they spoke to was professional, efficient and helpful. Respondents were generally dissatisfied if the person taking their complaint did not respond to their query or seemed uninterested in the complaint, or if the matter took longer than expected to be resolved.

Table 8: Satisfaction with responses from government agencies and other organisations reported to, 2020 (weighted data)

Agency/organisation reported to	Satisfied		Dissatisfied	
	n	%	*n*	%
Internet service provider (*n*=19)	19	96.5	1	3.5
Private health insurance company (*n*=18)	15	86.2	2	13.8
Medicare Australia (*n*=40)	32	80.9	8	19.1
Passport Office (*n*=22)	18	80.8	4	19.2
IDCARE (*n*=18)	14	76.9	4	23.1
Bank, credit union, credit/debit card company (eg Visa or MasterCard) or e-commerce provider (eg PayPal) (*n*=129)	98	76.2	31	23.8
Social media platform (*n*=27)	20	74.8	7	25.2
ReportCyber (*n*=43)	32	74.6	11	25.5
Media organisation (*n*=18)	13	72.8	5	27.3
Utility company (eg gas, electricity, telephone, water) (*n*=26)	19	72.7	7	27.3
Consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading) (*n*=39)	28	72.2	11	27.8
Road traffic authority (*n*=21)	15	70.6	6	29.5
Police (*n*=68)	46	67.9	22	32.1
Credit reporting agency (eg Equifax, Dun & Bradstreet) (*n*=34)	21	62.3	13	37.7

Note: Satisfied and dissatisfied respondent totals may not equal agency/organisation totals due to rounding of weighted data. Percentages may not total 100 as respondents could select multiple responses

Source: Identity crime survey 2020 [AIC data file]

The most common reason given for not reporting identity crime was that a bank or other financial institution had already notified the compromised individual (36%, *n*=170). This proportion was similar in 2019 (37%; see Table 9). The second most common reason was that the respondent did not believe the incident was important or serious enough to report (24%, *n*=114). Twenty-two percent (*n*=105) of respondents did not know where to report the matter—a similar proportion as in 2019 (19%).

Table 9: Reasons for not reporting misuse of personal information, 2019 and 2020 (weighted data)

Reason for not reporting	2019 (*n*=775)	2020 (*n*=473)		% change
	%	%	*n*	
Bank, credit union or credit card company notified me	36.8	36.0	170	–2.2
I did not believe it was important or serious enough to make a report	25.9	24.1	114	–7.0
I did not know how or where to report the matter	19.3	22.1	105	14.5
I did not believe the police or other authority would be able to do anything	25.1	20.7	98	–17.5
I was too embarrassed to report it	12.6	17.5	83	38.9*
I did not believe it was a crime	12.5	13.4	63	7.2
I did not have time[a]	–	11.2	53	–
Other	6.1	4.0	19	–34.4

*statistically significant at $p<0.05$
a: This answer was not available in the 2019 survey
Note: Percentages do not total 100 as respondents could select multiple responses
Source: Identity crime survey 2019 and 2020 [AIC data file]

Victims' Certificates

All respondents, regardless of recent or lifetime victimisation, were asked if they were aware that a person whose personal information has been misused can apply to a court to obtain a Victims' Certificate to prove they have been a victim of identity crime. Seventy-six percent (*n*=7,592) of those surveyed were unaware of the existence of Victims' Certificates—a similar proportion to that found in 2019 (78%), indicating work to be done by government agencies and other organisations to educate people on what assistance is available to them following the compromise and misuse of identity credentials.

Risk and prevention of misuse of personal information

Perceived risk of victimisation in the next 12 months

Regardless of previous victimisation, 45 percent of respondents (*n*=4,515) reported that their risk of being a victim of identity crime would not change over the next 12 months. Fifty-three percent (*n*=5,230) thought their risk would increase and two percent (*n*=210) thought their risk would decrease.

There was a statistically significant relationship 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 (37%, *n*=271 vs 13%, *n*=1,198 respectively; $\chi^2(4)=382.2$, $p<0.01$) to believe the risk of identity crime would 'increase greatly' in the next 12 months. Respondents who had not experienced identity crime in the previous year were significantly more likely than recent victims to believe the risk of identity crime would not change in the next 12 months (47%, *n*=4,372 vs 19%, *n*=144 respectively; $p<0.01$).

Perceived seriousness of personal information misuse

The majority of respondents (94%, *n*=9,363) believed that misuse of personal information is a serious issue. Additional analysis examined whether the perceptions of identity crime seriousness were related to experiences of personal information misuse. Respondents who were recent victims (*n*=741) were significantly more likely to rate personal information misuse as 'very serious' than those who had not experienced victimisation (70%, *n*=520 vs 59%, *n*=5,452 respectively; $\chi^2(3)=42.7$, $p<0.01$). Non-victims (*n*=9,215) were significantly more likely than victims to rate personal information misuse as only 'somewhat serious' (35%, *n*=3,186 vs 28%, *n*=204 respectively; $p<0.01$).

Biometrics and the use of security measures

Use of security measures to protect personal information

All survey respondents had used at least one of the specified security measures at some point in their lifetime. The most common security measure was a password, with 80 percent (*n*=7,989) of respondents reporting using passwords frequently. The security measures used frequently by the fewest respondents were iris recognition (5%, *n*=463) and a computer chip implanted under the skin (4%, *n*=396; see Table 10).

Table 10: Previous use of security measures to protect personal information, 2020 (weighted data) (%)

Security measure	Frequency of security measures used			
	Frequently	Occasionally	Rarely	Never
Passwords	80.2	12.5	2.9	4.4
Signatures	28.0	31.2	18.5	22.3
Fingerprint recognition	27.2	18.4	14.0	40.4
Facial recognition	17.0	13.9	13.3	55.9
Voice recognition	7.0	17.5	20.3	55.2
Iris recognition	4.7	7.7	10.4	77.2
Computer chip implanted under your skin	4.0	5.4	3.4	87.3

Note: Percentages may not total 100 due to rounding
Source: Identity crime survey 2020 [AIC data file]

The Biometrics Institute (2020) survey found that 14 percent of respondents identified 'digital identity' as the most significant area of development for the future. In the AIC's identity crime and misuse survey, 33 percent (*n*=3,257) of respondents were registered with a digital identification service. Willingness to use a digital identification service was higher among respondents who had experienced misuse of their personal information in the past year than among those who had not (70%, *n*=522 vs 46%, *n*=4,280; $\chi^2(2)=158.2$, $p<0.01$).

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 (see Table 11). Ninety-six percent (*n*=9,566) 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 (93%, *n*=9,243). Twenty-one percent (*n*=2,124) stated they would be willing to use a computer chip implanted under their skin, a slightly smaller proportion than in 2019 (23%).

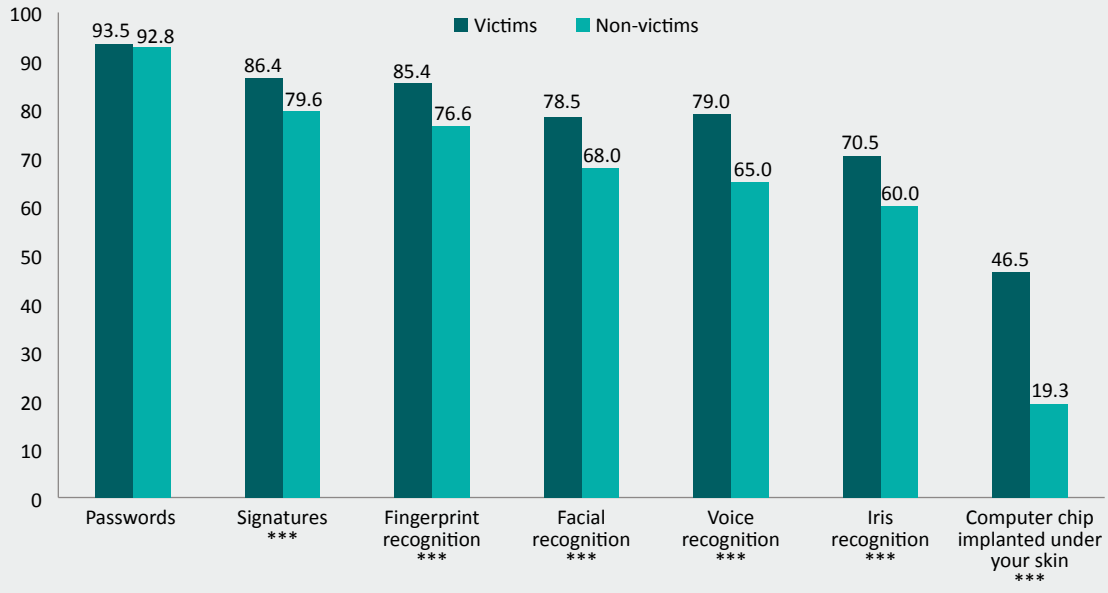
Table 11: Willingness to use security measures to protect personal information in the future, 2019 and 2020 (weighted data)

Security measure	2019 (*n*=9,968)	2020 (*n*=9,956)		% change
	%	%	*n*	
Passwords	94.7	92.8	9,243	–2.0***
Signatures	81.1	80.1	7,978	–1.2
Fingerprint recognition	83.4	77.3	7,695	–7.3***
Facial recognition	74.1	68.8	6,849	–7.2***
Voice recognition	70.8	66.1	6,577	–6.6***
Iris recognition	67.3	60.8	6,051	–9.7***
Computer chip implanted under your skin	22.9	21.3	2,124	–7.0*
Any of the above	98.0	96.1	9,566	–1.9***
None of the above	2.0	3.9	390	95.0***

***statistically significant at $p<0.001$, *statistically significant at $p<0.05$
Note: Percentages do not total 100 as respondents could select multiple responses
Source: Identity crime survey 2019 and 2020 [AIC data file]

Additional analysis examined whether willingness to use security measures in the future to protect personal information was associated with the experience of personal information misuse in the previous year (see Figure 3). Recent victims (*n*=741) were more willing than non-victims (*n*=9,215) to use each of the suggested security measures with the exception of passwords, which recent victims and non-victims were equally willing to use. This is unsurprising, as 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.

Figure 3: Willingness of recent victims and non-victims of personal information misuse to use security measures to protect personal information in the future, 2020 (weighted data) (%)



***statistically significant at $p<0.001$
Source: Identity crime survey 2020 [AIC data file]

Discussion

Increased online activity as a result of the COVID-19 pandemic greatly impacted the fraud and identity crime industry (Cifas 2021). Sontiq (2020) reported a 259 percent increase in online purchases and in-store pick-up sales, as businesses operated remotely and consumers relied on the internet to obtain goods and services. Despite the growth in online activity, identity crime and misuse significantly decreased between 2019 and 2020. Seven percent of respondents reported that their personal information had been misused in 2020, compared with 11 percent in 2019. These findings are supported by Cifas' (2021) *Fraudscape* report, which found a 17 percent decrease in identity fraud between 2019 and 2020, indicating identity crime also decreased in the United Kingdom.

As the world has become more digitally reliant, face-to-face transactions have decreased, as has the need for day-to-day use of physical identification documents (Sontiq 2020). Consumer awareness of their digital footprint and the need to protect their identity online has also increased (ACCC 2021b). Cybercriminals have adapted to this heightened awareness and have opted to increase their attempts to bring about data breaches across all levels of business but specifically targeting smaller organisations (Sontiq 2020). Poorly protected data servers, especially those that maintain comprehensive identity profiles of their customers, are desirable targets for cybercriminals (Australian Cyber Security Centre 2020) and data breaches of businesses often delay or mask notification of identity theft to the victim (Office of the Australian Information Commissioner 2021).

Contrary to the decrease in identity crime found in this survey, the ACCC's Scamwatch received 20,939 reports of identity theft in 2020, an 84 percent increase over the 11,373 reports received in 2019 (ACCC 2021a). However, the financial losses associated with identity theft reported to the ACCC decreased from $4.3m in 2019 to $3.1m in 2020 for the much larger cohort. This decrease accords with the AIC's survey results, which showed a reduction in total financial losses from $3.6m to $1.5m between 2019 and 2020.

Names (46%) and addresses (35%) were the most commonly misused types of personal information, followed by credit and debit card information (31%). These results were similar to those of the 2019 survey. However, there was a significant decrease in the misuse of credit and debit card information between 2019 (41%) and 2020 (31%, $p<0.001$). In each of the last two years, the most common reason for the misuse of personal information was to obtain money from a bank (39% in 2019 and 41% in 2020).

In 2019, the largest proportion of respondents attributed their victimisation to hacking or theft of a computerised device (30%). In 2020, most respondents believed that their data had been obtained through a phone call (27%) or email (27%). Hacking or theft was the next highest source of compromise, at 25 percent. Given that phishing emails containing malicious links are an enabler of hacking (Sontiq 2020), this is unsurprising.

Additional analysis of the ACCC's Scamwatch data also suggested phone calls and emails were the most common ways victims were contacted and personal information obtained (ACCC 2021b). While 12 percent of respondents believed their personal information was obtained through data breaches, internationally, data breaches are one of the biggest sources of identity data on the darknet (Sontiq 2020). Identity crime is generally considered an under-reported crime. Often, individuals will not realise their identity data has been compromised, as cybercriminals instead target business databases for identity information. For instance, Sontiq (2020) found that one-third of data breaches in 2020 involved small businesses.

This survey's results support other recent research on under-reporting (ACCC 2021b; National Crime Agency 2018), as over half of recent victims (54%) only told a family member or friend and 10 percent told no-one. Those who reported to a government agency or organisation were most satisfied with the assistance they received from their internet service providers (97%) and their health insurance providers (86%). Of those who did not make a report, 24 percent believed the incident was not important or serious enough to warrant reporting.

The survey found that 96 percent of respondents were willing to use at least one security measure, regardless of previous victimisation. Similarly, Sontiq (2019) found that more than 81 percent of consumers agree their identity is the most important thing they own and nearly 75 percent were willing to pay monthly for identity theft protection services.

The decline in reported identity misuse in 2020 could be partially attributed to the increase in cybercriminals obtaining identity data by breaching business databases, as outlined by Sontiq (2020). Despite the decline in identity misuse, it remains a highly prevalent crime affecting the Australian public.

Acknowledgements

This study was undertaken as part of the Department of Home Affairs' National Identification of Identity Crime and Misuse project, pursuant to the National Identity Security Strategy. The survey was developed with input and advice from the Department of Home Affairs. Data collection was undertaken professionally and efficiently by i-Link Research Solutions, a market research consultancy firm that provided a panel of individuals drawn from across Australia. The time and willingness of those who completed the survey are gratefully acknowledged.

References

URLs correct as at November 2021

Australian Bureau of Statistics (ABS) 2020. *National, state and territory population, June 2020*. ABS Canberra: ABS. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/jun-2020

Australian Competition and Consumer Commission (ACCC) 2021a. Scam statistics. https://www.scamwatch.gov.au/scam-statistics

Australian Competition and Consumer Commission (ACCC) 2021b. *Targeting scams: Report of the ACCC on scams activity 2020*. Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2020

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

Australian Cyber Security Centre (ACSC) 2020. *Cyber security and Australian small businesses: Results from the Australian Cyber Security Centre Small Business Survey.* Canberra: ACSC. https://www.cyber.gov.au/acsc/small-and-medium-businesses/small-business-survey-results

Australian Payments Network 2021. *Australian payment fraud 2021*. Sydney: Australian Payments Network. https://www.auspaynet.com.au/resources/fraud-statistics/2020-Calendar-year

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. https://doi.org/10.2196/jmir.6.1.e2

Biometrics Institute 2020. *Biometrics Institute industry survey 2020*. London: Biometrics Institute

Cifas 2021. *Fraudscape 2021.* https://www.fraudscape.co.uk/

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. https://doi.org/10.1177/2631309X19888501

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://www.aic.gov.au/publications/rr/rr16

Franks C & Smith R 2020. *Identity crime and misuse in Australia: Results of the 2019 online survey*. Statistical Report no. 27. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr04732

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. https://doi.org/10.1093/pan/mpm003

National Crime Agency (NCA) 2018. *The cyber threat to UK business: 2017–2018 report*. National Cyber Security Centre. https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report

Office of the Australian Information Commissioner (OAIC) 2021. *Notifiable data breaches report.* Canberra: ACSC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021

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. https://doi.org/10.1093/pan/mpl010

Sontiq 2020. *Protecting what matters most v4.0: Combatting vulnerabilities & risks in your connected world.* https://www.sontiq.com/protecting-what-matters-most-v4/

Sontiq 2019. *Identity protection market research report*. https://www.sontiq.com/2019-identity-protection-market-research-report/

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

Yeager DS et al. 2011. Comparing the accuracy of RDD telephone surveys and internet surveys conducted with probability and non-probability samples. *Public Opinion Quarterly* 75(4): 709–47. https://doi.org/10.1093/poq/nfr020

Merran McAlister is a Research Analyst at the Australian Institute of Criminology.

Christie Franks is a former Research Analyst at the Australian Institute of Criminology.

General editor, Statistical Bulletin series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology.
For a complete list and the full text of the papers in the Statistical Bulletin series, visit the AIC website at: aic.gov.au

ISSN 2206-7302 (Online) ISBN 978 1 922478 46 7 (Online)
https://doi.org/10.52922/sb78467

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166