Australian Government
Australian Institute of Criminology

Statistical Bulletin 42

Abstract | This study presents findings from the Australian Cybercrime Survey related to identity crime and misuse.

Thirty-one percent of respondents experienced identity crime in their lifetime and 20 percent in the past 12 months. Almost half of identity crime victims reported that suspicious transactions appeared in their bank statements or accounts. The type of personal information most commonly misused was names, followed by credit or debit card information. While one quarter of respondents did not know how their information was obtained, 16 percent believed it to be due to the hacking of a computer or device.

Twenty-nine percent of past 12 month victims experienced a financial loss. The median amount initially lost was $300. Nineteen percent of victims had money reimbursed, the median amount being $250.

Identity crime and misuse in Australia 2023

Merran McAlister, Emily Faulconbridge, Isabella Voce and Samantha Bricknell

Identity crime, also known as identity theft, fraud or misuse, is a common cyber threat worldwide and can cause severe and long-term harm (Australian Cyber Security Centre (ACSC) 2022). Identity crime exploits vulnerabilities in personal identification credentials, consumer payment systems and technological advances in computing and communications, generally for financial gain (United Nations Economic and Social Council 2007). The Australian Competition and Consumer Commission (ACCC) states that there were over 16,000 reports of identity theft alone in 2022 (ACCC 2023). Approximately six percent of these reports resulted in losses, which totalled over $10 million (ACCC 2023). However, these crimes continue to be under-reported, often because individuals do not self-identify as victims of identity crime or due to the complexity of reporting options (Franks & Smith 2020).

Identity crime is often an enabler of other types of crime, including scams and frauds (ACCC 2023). It can be perpetrated in several ways, including through data breaches, malware and viruses (ACCC 2023; McAlister & Franks 2021). For example, Morgan and Voce (2022) found that a third of survey respondents who were notified of a data breach also reported evidence of identity crime victimisation in the previous 12 months.

The 2021–22 financial year saw an evolution in methods used by cybercriminals to target the Australian Government and community for profit (ACSC 2022). The Australian Institute of Criminology (AIC) is undertaking research to develop and inform strategies to understand, disrupt and prevent cybercrime (see Voce & Morgan 2023). As part of this research, a survey was conducted that examined a range of cyber-dependent and cyber-enabled crimes, including identity theft, compromise and misuse; malware; online scams and fraud; and online abuse and harassment.

In this study, we explore respondents' lifetime and recent experiences of identity theft, compromise and misuse. This includes the type of information misused, how the information was obtained, how it was misused, and any associated financial losses or recoveries. The findings of this research will be used to better inform policy and strategies to prevent identity crime.

Methodology

Recruitment and sampling

This study used data from the AIC's Australian Cybercrime Survey (see Voce & Morgan 2023), which was conducted by Roy Morgan Research between 8 February and 13 March 2023 using its Single Source panel as well as panels managed by PureProfile and Dynata. The survey was sent to members of these online panels aged 18 years and over who had voluntarily joined the panel to receive incentives in exchange for completing surveys.

Proportional quota sampling, a non-probability sampling method, was used to ensure the sample was broadly reflective of the spread of people living in Australia. Quotas were based on the Australian adult population stratified by sex, age and usual place of residence, derived from Australian Bureau of Statistics data (Australian Bureau of Statistics 2023a, 2023c). The data were subsequently weighted by sex, age and usual place of residence to ensure they were representative of the spread of the Australian population. Additional random iterative method weights (calculated from Roy Morgan Research's Single Source survey) were applied to correct for education level, internet use and social media use. This corrected for oversampling of people with higher levels of education and more frequent internet use, which is common among online panels.

In total, 13,887 panel members aged 18 years and over completed the survey and were included in this study. Fifty percent (*n*=6,935) of respondents identified as male, 50 percent (*n*=6,900) identified as female and less than one percent (*n*=51) identified as non-binary. Eleven percent (*n*=1,540) were aged 18–24 years, 18 percent (*n*=2,527) were 25–34 years, 26 percent (*n*=3,564) were 35–49 years, 23 percent (*n*=3,189) were 50–64 years and 22 percent (*n*=3,067) were 65 years or over.

Definitions

For the purpose of this study, we focus on each respondent's experience of identity theft, compromise and misuse (hereafter referred to as identity crime) in the previous 12 months and their lifetime (see Voce & Morgan 2023 for a detailed explanation of the Australian Cybercrime Survey). In contrast to the AIC's previous identity crime surveys, this survey adopted a bottom-up approach to measuring victimisation. This approach was taken given the difficulties respondents may have in accurately identifying whether they had been a victim of identity crime.

Respondents were determined to be a victim of identity crime if they had experienced at least one of the following in their lifetime or in the past 12 months:

- someone tried to obtain money from the respondent's investment or superannuation account(s);
- someone tried to open a new bank account, apply for a new loan or obtain credit with the respondent's personal information or the respondent received credit/payment cards in the mail that they did not apply for;
- someone used the respondent's personal information to fraudulently apply for government benefits;
- someone used the respondent's personal information (including images) to create an impersonation account to extort their contacts;
- suspicious transactions appeared in the respondent's bank statements or accounts, credit card or credit report;
- someone used the respondent's personal information to purchase or order something or the respondent received unfamiliar bills, invoices or receipts;
- the respondent received calls from debt collectors asking about unpaid bills they did not recognise;
- the respondent was unsuccessful in applying for credit;
- someone used the respondent's personal information to open a mobile phone or utility account, or the respondent's current mobile phone or other utility lost service because it had been transferred to a new unknown device;
- the respondent got a medical bill for a service they did not receive, or their medical claim was rejected because they had unexpectedly already reached their benefits limit;
- the respondent was unable to file taxes because someone had already filed a tax return in their name;
- someone gained access to the respondent's cryptocurrency wallet or exchange account and made transactions or stole currency;
- someone used the respondent's personal information to create a fake cryptocurrency wallet or exchange account;
- someone used the respondent's personal information to attempt to apply for a job or rent a property; or
- someone used the respondent's personal information to attempt to give false information to police.

Personal information includes: name, address, date of birth, place of birth, sex, gender, driver's licence information, passport information, Medicare information, health records, biometric information (eg fingerprint, voice, face or iris recognition), signature, bank account information, credit or debit card information, personal identification number, tax file number, and computer and/or other online usernames and passwords.

Limitations

Online panels allow for rapid data collection from large samples. However, there are limitations to this approach (see Voce & Morgan 2023). Even though the sample in this survey was large, we are cautious not to generalise the results to the wider population, or assume the results are representative of non-respondents. Additionally, while efforts were made to ensure the questions were as comprehensible as possible for a non-technical audience, it is possible that some respondents may not have been aware they were a victim of identity crime. Similarly, some respondents may have been reluctant to disclose experiences of victimisation due to shame or embarrassment.

Results

Prevalence of identity crime

Thirty-one percent (*n*=4,360) of all survey respondents reported they had experienced identity crime in their lifetime and 20 percent (*n*=2,787) had experienced identity crime in the previous 12 months (see Table 1). There were no gender differences in previous 12 month or lifetime victimisation. However, there was a statistically significant association between age and identity crime victimisation for past 12 month and lifetime victimisation. Respondents aged 18–24 and 25–34 years were significantly more likely to report past 12 month experiences of identity crime (24%, *n*=367 and 23%, *n*=578 respectively) compared with most other age groups.

Table 1: Prevalence of identity crime by respondent characteristics, 2023 (*n*=13,887)						
	Past 12 month victimisation			Lifetime victimisation		
	n	%		*n*	%	
Gender[a]						
Male (*n*=6,935)	1,395	20.1	*F*=0.0, *p*=0.95[b]	2,186	31.5	*F*=0.0, *p*=0.84[c]
Female (*n*=6,900)	1,384	20.1		2,163	31.3	
Non-binary (*n*=51)	8	16.5		12	23.4	
Age group (years)						
18–24 (*n*=1,540)	367	23.8	*F*=7.4, *p*<0.001	499	32.4	*F*=4.5, *p*<0.01
25–34 (*n*=2,527)	578	22.9		877	34.7	
35–49 (*n*=3,564)	714	20.0		1,134	31.8	
50–64 (*n*=3,189)	589	18.5		975	30.6	
65+ (*n*=3,067)	539	17.6		875	28.5	
Income						
$0 – $18,200 (*n*=1,551)	229	14.8	*F*=9.6, *p*<0.001[d]	389	25.1	*F*=10.5, *p*<0.001[e]
$18,201 – $37,000 (*n*=2,576)	519	20.1		824	32.0	
$37,001 – $80,000 (*n*=4,361)	894	20.5		1,390	31.9	
$80,001 – $180,000 (*n*=3,631)	797	22.0		1,235	34.0	
$180,001+ (*n*=479)	131	27.4		191	40.0	
Don't know/prefer not to say (*n*=1,289)	216	16.7		331	25.7	
Language spoken at home						
English (*n*=13,209)	2,616	19.8	*F*=7.7, *p*<0.01[f]	4,128	31.3	*F*=2.1, *p*=0.15[g]
Other (*n*=632)	162	25.6		218	34.5	
Don't know/prefer not to say (*n*=46)	9	19.1		14	30.3	
Mean (median) hours of computer use[h]						
Work-related[i]	4.2 (4)			4.0 (3)		
Personal[j]	3.4 (3)			3.4 (3)		
Total (*n*)	**2,787**	20.1		**4,360**	31.4	

a: Excludes 2 respondents who identified as 'Other' gender

b: Excludes 8 non-binary respondents from significance testing due to small cell sizes

c: Excludes 12 non-binary respondents from significance testing due to small cell sizes

d: Excludes 216 respondents from significance testing who reported that they did not know/preferred not to say

e: Excludes 331 respondents from significance testing who reported that they did not know/preferred not to say

f: Excludes 9 respondents from significance testing who reported that they did not know/preferred not to say

g: Excludes 14 respondents from significance testing who reported that they did not know/preferred not to say

h: Includes respondents who reported 24 hours of computer use for work and/or personal activities

i: Includes employed respondents who were victims of identity crime in the past 12 months (*n*=1,618) or in their lifetime (*n*=2,492) who provided a response

j: Excludes 272 past 12 month and 421 lifetime victims of identity crime who did not know or declined to answer the question

Note: Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Respondents who reported higher levels of technological literacy were more likely to be victims of identity crime (see Table 2). For example, 22 percent (*n*=685) of respondents who reported a high level of technological knowledge and 26 percent (*n*=307) of respondents who reported a very high level of knowledge were victims of identity crime in the past 12 months. Around one-third of respondents who reported high or very high levels of technological knowledge (33% *n*=1,039 and 37% *n*=431 respectively) or ability (32% *n*=1,328 and 36% *n*=607 respectively) had experienced an incident of identity crime in their lifetime.

Table 2: Prevalence of identity crime by technological literacy, 2023 (*n*=13,887)

	Past 12 month victimisation			Lifetime victimisation		
	n	%		*n*	%	
Technology knowledge						
Very low (*n*=572)	105	18.4	*F*=8.3, *p*<0.001[a]	155	27.1	*F*=6.2, *p*<0.001[b]
Low (*n*=1,958)	370	18.9		566	28.9	
Moderate (*n*=6,986)	1,305	18.7		2,149	30.8	
High (*n*=3,128)	685	21.9		1,039	33.2	
Very high (*n*=1,161)	307	26.4		431	37.1	
Don't know/prefer not to say (*n*=83)	14	17.3		20	24.1	
Technology ability						
Very low (*n*=356)	58	16.3	*F*=5.5, *p*<0.001[c]	90	25.3	*F*=5.1, *p*<0.001[d]
Low (*n*=1,237)	250	20.2		362	29.3	
Moderate (*n*=6,448)	1,197	18.6		1,951	30.3	
High (*n*=4,095)	866	21.2		1,328	32.4	
Very high (*n*=1,677)	401	23.9		607	36.2	
Don't know/prefer not to say (*n*=74)	14	18.5		23	30.6	

a: Excludes 14 respondents from significance testing who reported that they did not know/preferred not to say

b: Excludes 20 respondents from significance testing who reported that they did not know/preferred not to say

c: Excludes 14 respondents from significance testing who reported that they did not know/preferred not to say

d: Excludes 23 respondents from significance testing who reported that they did not know/preferred not to say

Note: Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: Australian Cybercrime Survey 2023 [weighted data]

Table 3 outlines the most recent incidents of identity crime respondents experienced in the past 12 months. The most commonly reported most recent incident of identity crime was suspicious transactions appearing in bank statements or accounts, credit cards or credit reports (41%, *n*=1,140). Receiving calls from debt collectors asking about unfamiliar unpaid bills accounted for one-quarter of the most recent incidents (25%, *n*=707). Combined, these accounted for 66 percent (*n*=1,847) of the most recent experiences of identity crime reported.

Table 3: Most recent incident of identity crime experienced by victims in the past 12 months, 2023 (*n*=2,787)

	n	%
Suspicious transactions appeared in respondent's bank statements or accounts, credit card or credit report	1,140	40.9
Respondent received calls from debt collectors asking about unpaid bills they did not recognise	707	25.4
Someone used respondent's details to purchase or order something or the respondent received unfamiliar bills, invoices or receipts	259	9.3
Respondent was unsuccessful in applying for credit, and this was surprising given their credit history	104	3.7
Someone used respondent's personal details (including images) to create an impersonation account to extort their contacts	98	3.5
Someone tried to open a new bank account, apply for a new loan or obtain credit with respondent's personal details (ie in their name) or the respondent received credit/payment cards in the mail that they did not apply for	96	3.4
Someone used respondent's personal details to open a mobile phone or utility account, or the respondent's current mobile phone or other utility lost service because the service has been transferred to a new unknown device	81	2.9
Someone tried to obtain money from one of the respondent's investments or superannuation accounts	57	2.1
Respondent got a medical bill for a service they did not receive, or their medical claim was rejected because they had unexpectedly already reached their benefits limit	44	1.6
Someone used respondent's personal details to create a fake cryptocurrency wallet or exchange account	38	1.4
Someone gained access to respondent's cryptocurrency wallet or exchange account and made transactions or stole currency	37	1.3
Someone used respondent's personal details to fraudulently apply for government benefits	36	1.3
Someone used respondent's personal details (eg name, birth date) to attempt to give false information to police	30	1.1
Someone used respondent's personal details (eg name, birth date) to attempt to apply for a job or rent a property	24	0.9
Respondent was unable to file taxes because someone had already filed a tax return in their name	21	0.8
Don't know/prefer not to say	14	0.5

Note: Identity crime refers to identity theft, misuse and compromise, but does not include third-party data breaches
Source: Australian Cybercrime Survey 2023 [weighted data]

Type of information misused

Table 4 outlines the different types of personal information misused during respondents' most recent incident of victimisation in the past 12 months. The most commonly reported type of information misused was a respondent's name (37%, *n*=1,021). This was followed by credit or debit card information (36%, *n*=998), mobile phone numbers (31%, *n*=873) and addresses (21%, *n*=588). These findings show that personal details, followed by financial information, were more commonly misused than other types of information such as authentication or health information. Eight percent (*n*=232) of respondents did not know or preferred not to say what type of information was misused.

Men who experienced identity crime in the past 12 months were more likely than their female counterparts to have had their personal details stolen during the most recent incident (58%, *n*=798 vs 47%, *n*=641 respectively; *F*=25.0, *p*<0.001). Similarly, they were more likely to have their primary identity documents misused (18%, *n*=251 vs 11%, *n*=153 respectively; *F*=18.8, *p*<0.001). Women who experienced identity crime in the past 12 months were more likely than men to have had financial information stolen during the most recent incident (51%, *n*=707 vs 42%, *n*=577 respectively; *F*=19.7, *p*<0.001).

Table 4: Types of information misused in the most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772)

	n	%
Personal details		
Name	1,021	36.8
Mobile number	873	31.5
Address	588	21.2
Date of birth	541	19.5
Gender	424	15.3
Place of birth	208	7.5
Usernames		
Email address	488	17.6
Online account username	147	5.3
Computer username	82	3.0
Authentication information		
Passwords	168	6.0
Biometric information	71	2.6
Signature	71	2.6
Personal identification number	52	1.9
Photos/videos		
Photos/images of self	110	4.0
Videos of self	14	0.5
Primary identity documents		
Driver licence information	340	12.3
Passport	126	4.6

Table 4: Types of information misused in the most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772) (continued)		
	n	%
Financial information		
Credit or debit card information	998	36.0
Bank account information	540	19.5
Tax file number	75	2.7
Health information		
Medical records/Medicare information	204	7.4
Health insurance information	110	4.0
Other	**20**	**0.7**
Don't know/prefer not to say	**232**	**8.4**

Note: Respondents could select multiple types of information misused during the most recent incident of identity crime. Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Source: Australian Cybercrime Survey 2023 [weighted data]

How personal information was obtained

Personal information was obtained through a variety of means (see Table 5). During the most recent incident of identity crime in the past 12 months, 16 percent (*n*=433) of respondents reported their personal information was obtained through hacking of a computer or computerised device and 14 percent (*n*=400) reported it was the result of a data breach. Twelve percent each (*n*=330) said their personal information was obtained via online communication or an online banking transaction. Over one-quarter of respondents did not know how their personal information was obtained (28%, *n*=775).

Hacking of a computer or device was the most commonly reported method of obtaining authentication information during the most recent incident (36%, *n*=99; *F*=70.3, *p*<0.001). Data breaches were the most commonly reported method of obtaining personal details (19%, *n*=279; *F*=41.6, *p*<0.001), usernames (25%, *n*=141; *F*=52.1, *p*<0.001), health information (32%, *n*=82; *F*=50.9, *p*<0.001) and 'other' types of information (34%, *n*=7; *F*=4.7, *p*<0.05). Similar proportions of respondents who experienced misuse of their financial information reported their information was obtained via the hacking of a computer or device (16%, *n*=211, *p*>0.05) or via a data breach (14%, *n*=180, *p*>0.05). Thirty percent (*n*=392; *F*=5.9, *p*<0.05) of respondents who experienced misuse of financial information did not know how their financial information was obtained—one-third more than the proportion of respondents who had personal details stolen (19%, *n*=279; *F*=87.2, *p*<0.001).

Table 5: How personal information was obtained in the most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772)		
	n	%
Hacking of a computer or computerised device	433	15.6
Data breach	400	14.4
Communicating online	330	11.9
Online banking transaction	330	11.9
Email	309	11.1
ATM/EFTPOS/credit card transaction	246	8.9
From information placed on a website	240	8.7
SMS/text message	219	7.9
By telephone	214	7.7
From information placed on social media	153	5.5
From a person I know	144	5.2
Theft of mail	114	4.1
In a face-to-face meeting	100	3.6
Theft of an identity or other personal document	0	0.0
Other	63	2.3
Don't know/prefer not to say	782	28.2

Note: Respondents could select multiple methods by which their information was obtained during the most recent incident of identity crime. Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Source: Australian Cybercrime Survey 2023 [weighted data]

How identity crime was detected

Respondents' most recent incidents of identity crime were detected through various methods (see Table 6). The majority of respondents discovered the misuse themselves (61%, *n*=1,701). Equal proportions of respondents were notified online via avenues such as email or social media (16%, *n*=452) or by external agencies such as government or financial agencies (16%, *n*=435). Only one percent (*n*=30) of respondents were made aware of the misuse after being contacted by police.

Detection methods during the most recent incident were also analysed by type of information misused. Fifty-seven percent (*n*=821) of victims whose personal details were misused discovered the misuse themselves (F=18.5, p<0.001), followed by notification online via email, social media, internet browser or security software (20%, *n*=295; F=19.6, p<0.001). Seventy-three percent (*n*=938) of respondents who experienced financial information misuse discovered it themselves (F=101.1, p<0.001). This was followed by a government or financial agency informing the respondent (20%, *n*=261; F=25.8, p<0.001). Respondents discovering the misuse themselves was the most common detection method across all types of personal information misused.

Table 6: How identity misuse was detected in the most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772)		
	n	%
I discovered it myself	1,701	61.4
I was notified by email or social media account, internet browser or security software	452	16.3
A government or financial agency told me	435	15.7
Someone I know told me	202	7.3
I was contacted by police	30	1.1
Other	77	2.8
Don't know/prefer not to say	162	5.9

Note: Respondents could select multiple detection methods during the most recent incident of identity crime. Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Source: Australian Cybercrime Survey 2023 [weighted data]

Impacts and recoveries

Table 7 summarises the initial losses, money spent dealing with the consequences, and reimbursements for victims of identity crime as a result of the most recent incident. Twenty-nine percent (*n*=796) of respondents lost money due to the misuse, and 19 percent (*n*=513) had money reimbursed by banks or other organisations. Only five percent (*n*=137) spent money dealing with the consequences of the identity crime. The median amount of money stolen was $300 and the median amount recovered was $250. The median amount spent on consequences was $700. Seventy-four percent (*n*=2,057) of respondents resolved all problems associated with the misuse.

Table 7: Losses and monies recovered for most recent incident of identity crime in the past 12 months, 2023			
	Initial losses[a]	Monies spent on misuse consequences	Monies reimbursed
Respondents who lost/were reimbursed monies (*n*)	796	137	513
Respondents who reported amount lost/reimbursed (*n*)	700	53	510
Percentage of respondents (%)[b]	28.7	4.9	18.5
Minimum ($)	1	30	1
Maximum ($)	275,000	34,440	275,000
Median ($)	300	700	250
Mean ($)	2,794.0	2,718.7	2,019.4
Standard deviation ($)	13,192.6	5,756.5	13,349.4
25% quartile ($)	95	100	80
75% quartile ($)	1,000	2,000	850
Total ($)	1,927,116.5	134,551.6	1,010,368.5

a: Excludes 102 respondents who reported $0 losses

b: Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Note: Analysis of monetary values excludes 11 respondents who reported greater reimbursements than losses

Source: Australian Cybercrime Survey 2023 [weighted data]

Hours spent dealing with identity crime

Respondents were asked how many hours they spent dealing with the consequences of identity crime. On average, respondents reported spending 13 hours dealing with the consequences of the most recent incident (*SD*=97.8). One respondent reported a substantially larger number of hours spent dealing with the consequences, at 2,409 hours. When this respondent is excluded, the average number of hours spent dealing with the consequences of misuse is nine (*SD*=32.8).

Behavioural changes

Respondents who experienced identity crime in the past 12 months were asked in what ways their behaviour had changed as a direct consequence of the most recent incident of their personal information being misused (see Table 8). The most common behavioural changes respondents reported were being more careful when using or sharing personal information (56%, *n*=1,542), followed by changing passwords (42%, *n*=1,169).

Being more careful when using or sharing personal information was the most commonly reported behaviour change across all types of information misuse, except for 'other' types of information. This behavioural change was found to be prevalent for username misuse (69%, *n*=385; *F*=36.0, *p*<0.001), health information misuse (67%, *n*=169; *F*=8.6, *p*<0.01), and photo/video misuse (65%, *n*=73; *p*>0.05). Changing passwords was one of the top three behavioural changes across all types of information misused, though it was most commonly reported for authentication misuse (60%, *n*=165; *F*=25.6, *p*<0.001), username misuse (58%, *n*=324; *F*=54.7, *p*<0.001) and 'other' types of misuse (53%, *n*=11). Eight percent (*n*=220) of people reported making no changes to their behaviour.

Table 8: Behavioural changes resulting from most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772)

	n	%
I am more careful when I use or share personal information	1,542	55.6
I changed my password(s)	1,169	42.2
I implemented two-factor authentication	901	32.5
I am more careful with who I add on my social media accounts	769	27.7
I review my financial statements more carefully	747	26.9
I changed my banking details	728	26.3
I don't trust people as much	497	17.9
I use biometric technologies more frequently (fingerprints, facial or voice recognition etc)	490	17.7
I made my social media accounts private and secure	401	14.5
I shred personal documents before disposing of them	360	13.0
I use better security for my computer or other computerised devices	257	9.3
I changed my social media account(s)	177	6.4
I applied for a copy of my credit report	169	6.1
I changed my email address(es)	155	5.6
I closed my social media accounts temporarily or permanently	154	5.6

Table 8: Behavioural changes resulting from most recent incident of identity crime in the past 12 months, 2023 (*n*=2,772) (continued)		
	n	%
I avoid using the internet for banking and purchasing goods and services	142	5.1
I redirect my mail when I am away or move residence	123	4.4
I lock my mailbox	120	4.3
I changed my telephone number(s)	102	3.7
I signed up for a commercial identity theft alert or protection service	90	3.2
I changed my place of residence	64	2.3
Other	83	3.0
My behaviour has not changed	220	7.9
Don't know/prefer not to say	61	2.2

Note: Respondents could select multiple behavioural changes as a result of the most recent incident of identity crime. Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Source: Australian Cybercrime Survey 2023 [weighted data]

Reporting behaviours

Table 9 shows the reporting behaviours of respondents following the most recent incident of identity crime. Respondents were asked to whom they reported the identity crime. These responses ranged from informal reporting, such as telling a family member or friend, to formal reporting through a government agency such as the police or a consumer protection agency. The most common reporting behaviour was to tell a friend or family member (45%, *n*=1,247). This was followed by reporting the misuse to a bank, credit union or credit/debit card company (42%, *n*=1,171). Only eight percent (*n*=208) of respondents reported to ACSC/ReportCyber. It was also found that almost one-fifth (17%, *n*=468) of respondents did not report, informally or formally, to any of the individuals or entities listed in the survey.

Women who experienced an incident of identity crime in the past 12 months were more likely than men to report the most recent incident to non-government entities (55%, *n*=761 vs 47%, *n*=652 respectively, F=14.0, p<0.001; see Table 9). In contrast, men who experienced an incident of identity crime in the past 12 months were more likely than women to report the most recent incident to government agencies (24%, *n*=331 vs 19%, *n*=256 respectively, F=8.6, p<0.01). There was no significant difference in informal reporting behaviours between men and women (51%, *n*=707 and 52%, *n*=712 respectively).

Table 9: Reporting behaviours of past 12 month victims of misuse during the most recent incident of identity crime, 2023 (*n*=2,772)		
	n	**%**
Informal reporting		
Told a friend or family member about it	1,247	45.0
Told someone at my workplace (manager, HR, IT etc)	264	9.5
Told a doctor, mental health worker or social worker	169	6.1
Formal reporting to government agency		
Police	248	8.9
ReportCyber/Australian Cyber Security Centre (ACSC)/cyber.gov.au/Australian Cyber Security Hotline: 1300 CYBER1	208	7.5
A consumer protection agency (eg Scamwatch, Consumer Affairs, Office of Fair Trading)	119	4.3
A government authority (eg Medicare, Australian Taxation Office)	100	3.6
Crime Stoppers	98	3.5
A road/traffic authority	59	2.1
E-Safety Commissioner	35	1.3
Office of the Australian Information Commissioner	34	1.2
Australian Passport Office	26	0.9
Formal reporting to non-government entity		
A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)	1,171	42.2
A lawyer	144	5.2
My mobile phone company	114	4.1
My internet service provider	81	2.9
IDCARE	70	2.5
The company that runs my security software (eg McAfee, Norton)	35	1.3
Someone or somewhere else	32	1.2
The manufacturer of my device(s)	28	1.0
An insurance company	27	1.0
A utility company (eg gas, electricity)	25	0.9
A media organisation	12	0.4
None of the above	468	16.9
Don't know/prefer not to say	33	1.2

Note: Respondents could select multiple methods of reporting the most recent incident of identity crime. Excludes 14 respondents who indicated they were victims of identity crime in the past 12 months but did not provide further detail

Source: Australian Cybercrime Survey 2023 [weighted data]

If respondents did not report the most recent incident to the police or ACSC/ReportCyber (*n*=2,206), they were asked what prevented them from doing so. As shown in Table 10, almost one-third (31%, *n*=687) of respondents did not report identity crime to the police or ReportCyber because they felt they could deal with the matter themselves. Twenty percent (*n*=433) of respondents did not know where to report the matter, and close to one-quarter of respondents (24%, *n*=532) did not know that reporting to the police or the ACSC/ReportCyber was an option. An additional 22 percent (*n*=486) did not think that the police or the ACSC/ReportCyber would be able to do anything.

This study also found that among respondents who experienced identity crime in the past 12 months, women were more likely than men to not know that reporting identity crime to the police or ACSC/ReportCyber was an option (27%, *n*=304 vs 21%, *n*=227 respectively; *F*=9.1, *p*<0.01). This is consistent with the finding that women who experienced an incident of identity crime in the past 12 months were less likely than men to report to government agencies (see Table 9). Women were also more likely than men to report that they did not know how or where to report the matter (22%, *n*=243 vs 17%, *n*=187 respectively; *F*=5.2, *p*<0.05).

Table 10: Reasons for not reporting the most recent incident of identity crime in the past 12 months to police/ACSC/ReportCyber, 2023 (*n*=2,206)

	n	%
Seriousness of the incident		
Felt I could deal with it myself	687	31.2
Did not regard the incident as a serious offence	477	21.6
Did not know or think the incident was a crime	201	9.1
Understanding, perceptions or past experience of reporting		
Did not know reporting to police or the ACSC/ReportCyber was an option	532	24.1
Did not think police or the ACSC/ReportCyber would be able to do anything	486	22.0
I did not know how or where to report the matter	433	19.6
Have reported before and been dissatisfied with the outcome	123	5.6
Did not trust police or the ACSC/ReportCyber	71	3.2
Worry about the reaction or consequences		
Did not want to ask for help	144	6.5
Felt ashamed or embarrassed	116	5.3
Felt I would not be believed	78	3.5
Fear of legal processes	71	3.2
Fear of the person responsible (eg fear of retaliation)	61	2.8
Did not want the person responsible arrested	43	1.9
Cultural/language reasons	30	1.4
Incident handled by someone else		
Provider involved in incident (eg financial institution or telecommunications company) was resolving or had resolved the matter	163	7.4
Workplace/on-the-job incident—internal reporting procedures followed	41	1.9
Other	78	3.6

Note: Respondents could select multiple reasons for not reporting the most recent of identity crime to police or ACSC/ReportCyber. Excludes 154 respondents who reported that they did not know or preferred not to say

Source: Australian Cybercrime Survey 2023 [weighted data]

Discussion

This study draws on data collected as part of the AIC's Australian Cybercrime Survey to explore respondents' experiences of identity crime over their lifetime and during the preceding 12 months. Almost a third of respondents had been victims of identity crime in their lifetime, and a fifth had been victims of identity crime in the previous 12 months.

There was no statistically significant difference in lifetime or past 12 month identity crime victimisation between men and women, consistent with findings from other Australian studies (Australian Bureau of Statistics 2023b). Respondents who reported high or very high levels of technological knowledge or ability were more likely to be victims of identity crime than those with lower levels of computer literacy. Reasons for this may include increased internet usage or being better able to identify victimisation. Among the most recent incidents of identity crime respondents experienced in the past 12 months, suspicious transactions appearing in bank statements or accounts, credit cards or credit reports were the most common. Over one-third of respondents experienced misuse of their name or credit/debit card information.

Hacking of a computer or device and data breaches were the most common methods of obtaining personal information. However, more than one-quarter of respondents did not know how their personal information was obtained. Across all types of information misused, most respondents discovered the misuse themselves. Twenty-nine percent of respondents had money stolen from them in the most recent incident, the median amount being $300.

Results of this survey were consistent with evidence that cybercrimes are under-reported (ACSC 2022). Approximately one-fifth of respondents did not report the most recent incident of identity crime to any of the entities listed in the survey. Similarly, one-fifth did not know where to report the matter. Declines in reporting have been observed by ACCC's Scamwatch, which reported a 27 percent decrease in identity theft reports between 2021 and 2022 (ACCC 2023).

The high prevalence of identity crime, combined with evidence that monetary losses resulting from attempts to gain personal information are increasing (ACCC 2023), indicates the importance of addressing cybercrime in Australia. Identity crime is also recognised as a gateway to increasingly harmful crimes, including scams and fraud.

As cybercrime is rapidly evolving and becoming more difficult to detect, coordinated efforts across government and private sectors are required. Reports to government agencies are a critical component of raising awareness of cybercrime that may be occurring, as well as informing governments of relevant threats. This study highlighted the relatively low rates of reporting to government agencies, in conjunction with high proportions of respondents either not knowing where to report the misuse, or not regarding the misuse as a serious offence.

References

URLs correct as at May 2023

Australian Bureau of Statistics (ABS) 2023a. *National, state and territory population, September 2022*. Canberra: ABS. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/latest-release

Australian Bureau of Statistics (ABS) 2023b. *Personal fraud, 2021–22*. Canberra: ABS. https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release

Australian Bureau of Statistics (ABS) 2023c. *Regional population, 2021-22*. Canberra: ABS. https://www.abs.gov.au/statistics/people/population/regional-population/2021-22

Australian Competition and Consumer Commission (ACCC) 2023. *Targeting scams: Report of the ACCC on scams activity 2022*. Canberra: ACCC. https://www.scamwatch.gov.au/scam-statistics/targeting-scams

Australian Cyber Security Centre (ACSC) 2022. *Annual cyber threat report, July 2021 – June 2022*. Canberra: ACSC. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Franks C & Smith RG 2020. *Identity crime and misuse in Australia 2019.* Statistical Report no. 29. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr04749

McAlister M & Franks C 2021. *Identity crime and misuse in Australia: Results of the 2021 online survey.* Statistical Bulletin no. 37. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78467

Morgan A & Voce I 2022. *Data breaches and cybercrime victimisation.* Statistical Bulletin no. 40. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78832

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

Voce I & Morgan A 2023. *Cybercrime in Australia 2023.* Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Merran McAlister is a Research Analyst in the Statistical Collections and Indigenous Justice Research Program at the Australian Institute of Criminology.

Emily Faulconbridge is a Research Analyst in the Statistical Collections and Indigenous Justice Research Program at the Australian Institute of Criminology.

Isabella Voce is a Principal Research Analyst in the Australian Institute of Criminology's Serious and Organised Crime Research Laboratory.

Dr Samantha Bricknell is the Research Manager of the Statistical Collections and Indigenous Justice Research Program 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: www.aic.gov.au

ISSN 2206-7302 (Online) ISBN 978 1 922877 04 8 (Online)
https://doi.org/10.52922/sb77048

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