Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 29

National Identity Security Strategy

Identity crime and misuse in Australia 2019

Christie Franks and Russell G Smith

ISSN 2206-7930 (Online)
ISBN: 978 1 925304 74 9 (Online)

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

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

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

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

Edited and typeset by the Australian Institute of Criminology

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

Contents

Acknowledgements

This research was undertaken with the support and assistance of representatives of Commonwealth, state and territory agencies and private sector organisations who provided data and information in response to the Australian Institute of Criminology's request for assistance. Officers of the Attorney-General's Department and the Department of Home Affairs provided guidance and assistance with the preparation of this report. The authors also gratefully acknowledge the assistance of the not-for-profit organisation IDCARE, which provided valuable reports.

Acronyms and abbreviations

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AGD	Attorney-General's Department
AIC	Australian Institute of Criminology
ANAO	Australian National Audit Office
ASIC	Australian Securities and Investments Commission
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
BOCSAR	Bureau of Crime Statistics and Research (New South Wales)
CDPP	Commonwealth Director of Public Prosecutions
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
DVS	Document Verification Service
NCA	National Crime Agency (UK)
OAIC	Office of the Australian Information Commissioner

Abstract

This report examines the nature, extent and impact of identity crime and misuse in Australia for the year 2018–19. It presents data from Commonwealth, state and territory agencies as well as from the private sector and other non-government sources. The Australian Institute of Criminology, within the Home Affairs portfolio, publishes this information as a key initiative of the National Identity Security Strategy.

The 2019 survey of identity crime and misuse found 25 percent of respondents had experienced misuse of their personal information at some time in their lives, nearly 12 percent within the previous year. These findings are consistent with those of the 2018 survey. These results, combined with data collected from stakeholders, help policymakers raise awareness of identity crime and reduce its impact throughout Australia. Government, law enforcement and private sector industry cooperation and data sharing was essential in the preparation of this report.

Executive summary

Identity crime is a ubiquitous form of criminal activity within Australia and worldwide. The financial impact of identity crime has been well documented and is further explored in an accompanying report (Smith & Franks 2020). Identity crimes are also notoriously under-reported as a result of deterrents such as victim blaming and the complexity of reporting. The emotional, physiological and socio-economic impacts faced by victims are also often overlooked. Identity crimes can have extreme and prolonged consequences for many victims.

Cost of identity crime

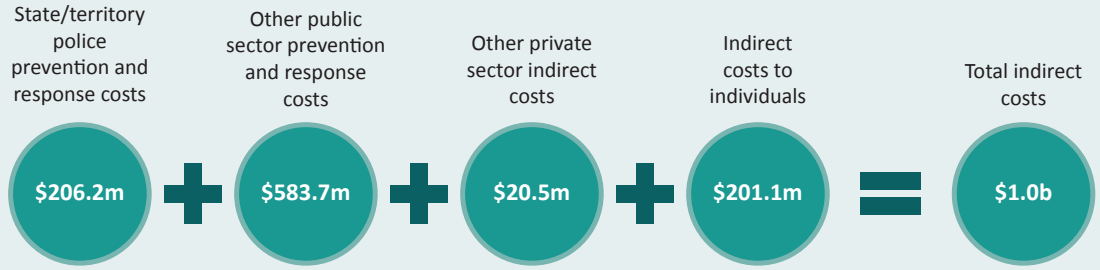
The estimated direct and indirect cost of identity crime in Australia in 2018–19 was $3.1b—17 percent more than for 2015–16. Even accounting for inflation over the three years of 5.4 percent (1.8% per year; Reserve Bank of Australia 2020), this increase is considerable. The total includes $2.1b in direct losses suffered by government agencies, Australian businesses and individuals, as indicated in Figure 1. Full details of the costing methodology are presented in the accompanying report (Smith & Franks 2020).

Figure 1: Estimated total direct cost of identity crime in Australia, 2018–19

Note: See Smith & Franks (2020) for details of the methodology used to calculate these estimates.

The indirect cost of identity crime in 2018–19 was estimated to add a further $1.0b to the $21.b in direct losses (Figure 2), bringing the total economic impact of identity crime in Australia for 2018–19 to approximately $3.1b.

Figure 2: Estimated total indirect cost of identity crime in Australia, 2018–19

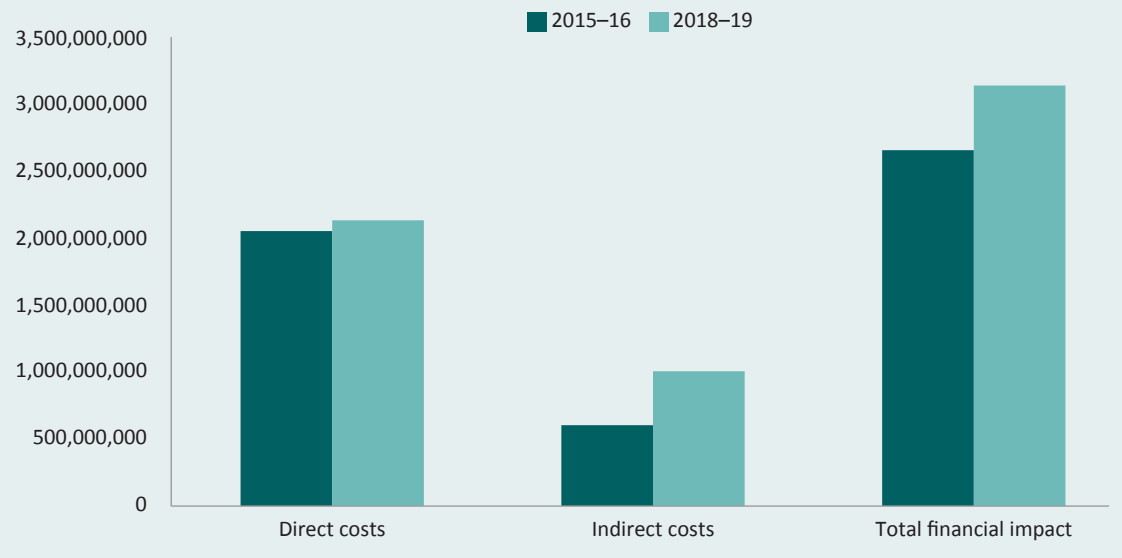


Note: See Smith & Franks (2020) for details of the methodology used to calculate these estimates

Trends in the cost of identity crime

When comparing the estimated direct and indirect costs of identity crime in 2018–19 with those of 2015–16 (Smith & Jorna 2018a), an increase is apparent across all areas. However, it should be noted that some changes in data sources and counting rules were employed to ensure all prevention costs, intangible costs, response costs and the cost of lost output were captured. Indirect costs of identity crime increased by 68 percent between 2015–16 and 2018–19, while prevention and response costs more than doubled over this period as organisations increased their investment in security strategies and monitoring. If the total costs of identity crime for the year 2015–16 are inflated to 2018–19 figures using the Reserve Bank of Australia's (2020) inflation calculator, the total cost would be $2.8b, still considerably less than the 2018–19 estimate of $3.1b (see Smith & Franks 2020 for a more specific costing breakdown).

Figure 3: Cost of identity crime and misuse in Australia report comparison ($)

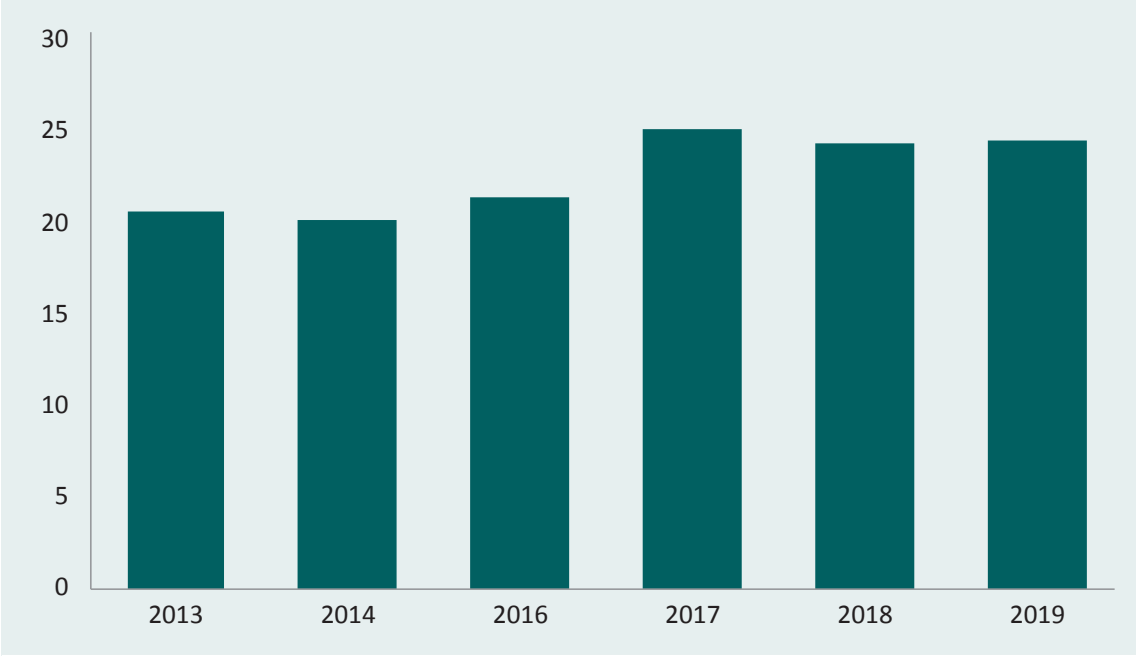


Source: Smith & Jorna 2018a; Smith & Franks 2020

Prevalence of identity crime

Identity crime continues to affect a large number of Australians, as well as businesses and government agencies. Surveys conducted by the Australian Institute of Criminology (AIC), beginning in 2013, have consistently found that over 20 percent of respondents report having experienced misuse of their personal information at some time during their lives (Franks & Smith 2020; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Smith, Brown & Harris-Hogan 2015; Smith & Hutchings 2014; Smith & Jorna 2018b). As shown in Figure 4, the proportion of people reporting lifetime victimisation increased between 2016 (21.5%) and 2017 (25.2%) with these rates staying relatively constant since then. This follows the increasing trend in online transactions and computer usage during this period.

Figure 4: Lifetime victimisation rates for misuse of personal information, 2013 to 2019 (%)

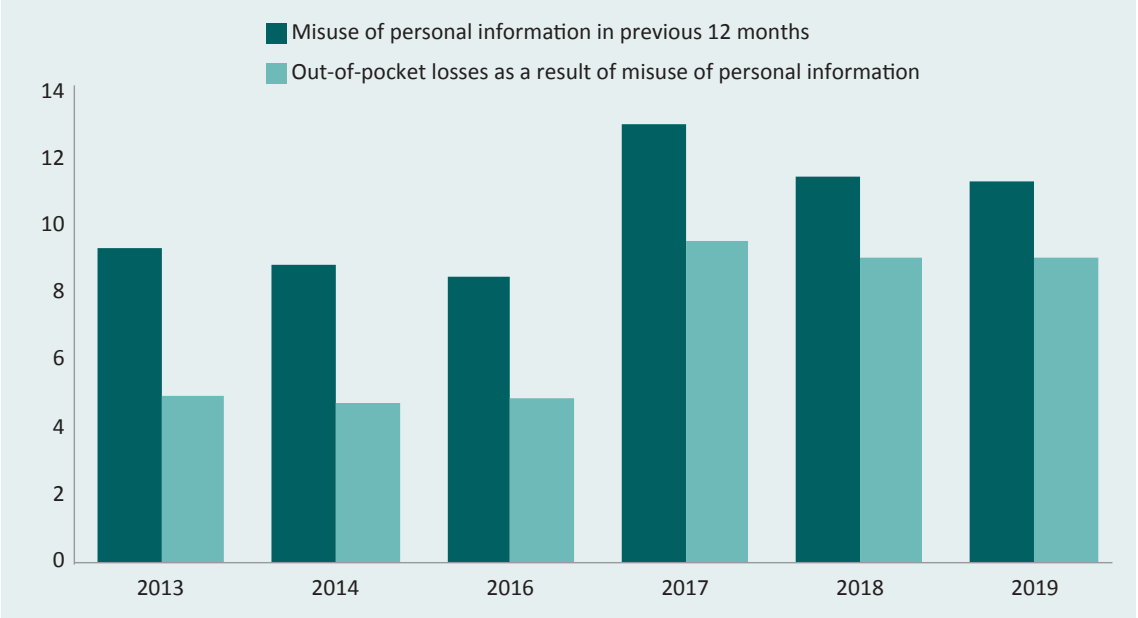


Note: 2013 and 2014 data weighted by location and 2016 to 2019 data weighted by age/gender

Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

The AIC's survey also asked respondents about their experience of misuse of personal information and associated out-of-pocket losses in the preceding 12 months. As shown in Figure 5, the 12-month victimisation rates and out-of-pocket loss rates remained relatively stable between 2013 and 2016. Both increased substantially in 2017, with 13 percent of respondents experiencing some form of misuse of their personal information in the 12 months prior to participating in the survey, and 10 percent of all respondents incurring out-of-pocket losses as a result of this misuse (Goldsmid, Gannoni & Smith 2018). In line with lifetime victimisation rates, the victimisation rates between 2018 and 2019 have remained relatively constant following a slight decline since 2017.

Figure 5: Respondents experiencing misuse of personal information and out-of-pocket losses in the preceding 12 months, 2013 to 2019 (%)



Note: 2013 and 2014 data weighted by location and 2016 and 2019 data weighted by age/gender

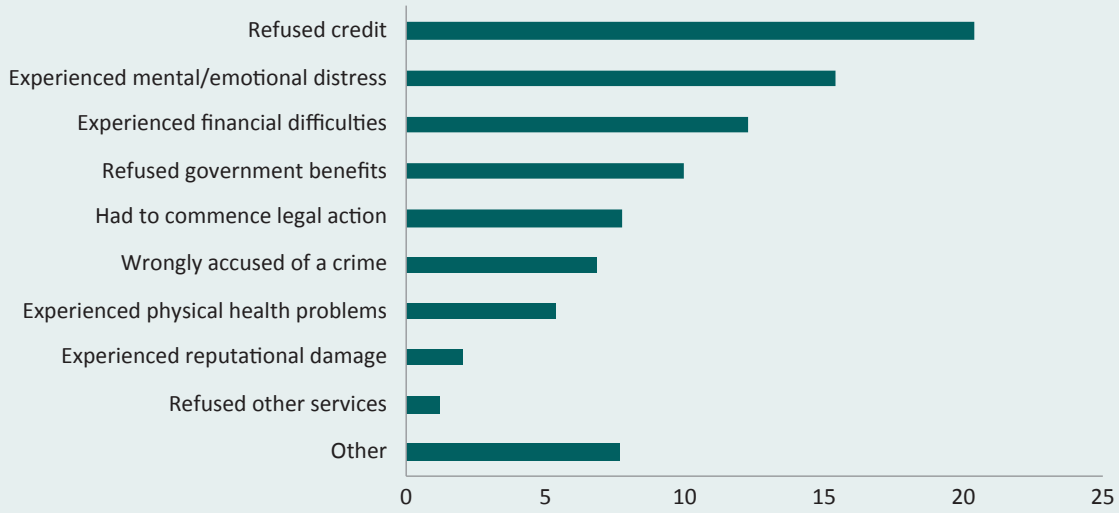
Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Misuse of personal information and identity crime remain an ongoing concern for Australians, with almost all respondents to the AIC's most recent survey (97%) indicating that misuse of personal information was, in their view, 'very serious' or 'somewhat serious' (Franks & Smith 2020).

Impact of identity crime on victims

On average, identity crime victims experience relatively low out-of-pocket losses as a result of identity crime, with a median loss of $300 reported in the AIC's 2019 identity crime survey (Franks & Smith 2020). The most common consequence of misuse of personal information was refusal of credit, with 20 percent of respondents reporting this consequence in 2019 (Franks & Smith 2020). The most pronounced change observed related to mental and emotional distress among victims of identity crime, reports of which increased nearly 12 percent between 2018 and 2019 (Franks & Smith 2020).

Figure 6: Consequences experienced as a result of personal information being misused in the previous 12 months (%)

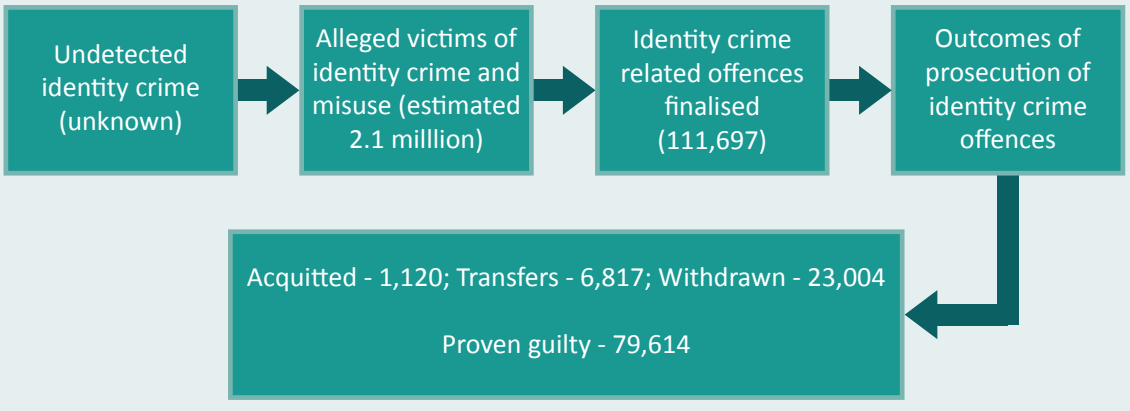


Source: Franks & Smith 2020

Criminal justice responses to identity crime

The Australian Bureau of Statistics (ABS) publishes national data on criminal justice responses to identity crime. Although large numbers of identity crimes are reported officially, a relatively small proportion of incidents result in police investigation and subsequent prosecution (Figure 7).

Figure 7: Estimated number of identity crimes 2018–19, compared with prosecutions



Source: ABS 2020 (unpublished data); Smith & Franks 2020

Document Verification Service

In 2009, the Document Verification Service (DVS) was established to allow authorised entities to verify customer identities, and in March 2015 access was expanded to additional organisations required under the Commonwealth *Privacy Act 1988* to identify their customers. Since then, take-up of the service has increased dramatically, with private sector transactions exceeding government transactions in 2017 for the first time. In 2019, however, government organisations requested five percent more verifications than private industry (Department of Home Affairs 2019).

Prevention of identity crime

Individual identity protection methods have evolved over time to deal with growing concern about identity crime. In 2019, 97 percent of survey respondents considered identity crime and misuse a serious problem in Australian society (Franks & Smith 2020). Behavioural changes in victims are common, with 46 percent of respondents admitting they are decidedly more careful when using or sharing personal information (Franks & Smith 2020). Individuals have also begun consulting with personal identity protection services, willingly paying monthly fees to organisations contracted to help them protect their information. Of the 2019 identity crime survey respondents reporting being victims of identity crime, eight percent stated they had signed up for a commercial identity theft alert/protection service as a result of the misuse of their personal information (Franks & Smith 2020).

Conclusion

This report assesses the prevalence, nature and impact of identity crime and misuse throughout Australia. The data presented indicate identity crime and misuse in Australia 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 in Australia.

Introduction

This report provides a comprehensive assessment of the nature, extent and impact of identity crime and misuse in Australia, based on surveys conducted by the Australian Institute of Criminology (AIC), and information provided by relevant Commonwealth, state and territory government agencies, business organisations and not-for-profit organisations.

Identity crime is arguably one of the most prevalent criminal activities in Australia, affecting individuals, businesses and government agencies. It is estimated that identity crime affects millions of Australians each year (Franks & Smith 2020). This is the fifth report, including a pilot study in 2013 compiled by the Identity Security Branch of the Attorney-General's Department (now part of the Department of Home Affairs) and the AIC, to assess the nature, extent and impact of identity crimes affecting Australian government organisations, businesses and individuals. Despite advances in verification of credentials and improvements in online authentication procedures, victimisation continues throughout Australia.

Case study 1: Apple account compromised

An individual purchased an iPhone and had not used their Apple account for some time, so when contacted by scammers via email and told their account would be locked in 24 hours unless account information was updated, they believed the request was genuine. The individual confirmed their full name, address, email, date of birth and driver licence details. An hour later they received a notification from Apple that their Apple ID was being used on iMessage and Facetime on a new phone. As their new phone had not yet been connected, they became worried. They contacted financial institutions and others to change passwords. They went to the police but were not issued a police report because nothing (except credentials) had been stolen. They also contacted Apple to report the compromise and were told scammers were targeting people with Hotmail accounts like the victim.

Source: ACCC 2019 (Unpublished data)

Structure of the report

This report presents findings from all data sources in respect of the 2018–19 financial year with comparisons, where appropriate, to findings of previous studies. In line with the identity crime conceptual model presented in Figure 8, the report examines:

- acquisition and use of fraudulent identities, including the cost of fraudulent credentials and how information was obtained, the number of incidents experienced by government entities and by the general public, the type of information susceptible to identity fraud and the number of prosecutions undertaken by Commonwealth, state and territory agencies involving identity crime;
- prevention and remediation of identity crime, including the number of agencies and organisations using the Document Verification Service; the online practices of individuals, businesses and government agencies; behavioural changes demonstrated by victims following victimisation; time spent dealing with the consequences of identity crime; the number of enquiries to government agencies and non-governmental organisations; and the number of people who applied for Commonwealth Victims' Certificates; and
- consequences of identity crime, including psychological and physical impacts as well as associated economic costs incurred by government, business and individuals.

Methodology

Defining identity crime

The definition of identity crime varies depending on the circumstances in which the crime occurs and the organisation and jurisdiction concerned. To ensure consistency within this report, 'identity crime' is used as a generic term to describe a range of activities in which identity credentials or personal information is fabricated, manipulated, stolen or assumed in order to commit a crime.

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

Respondents to the AIC's identity crime surveys are given the following definition of identity crime and misuse:

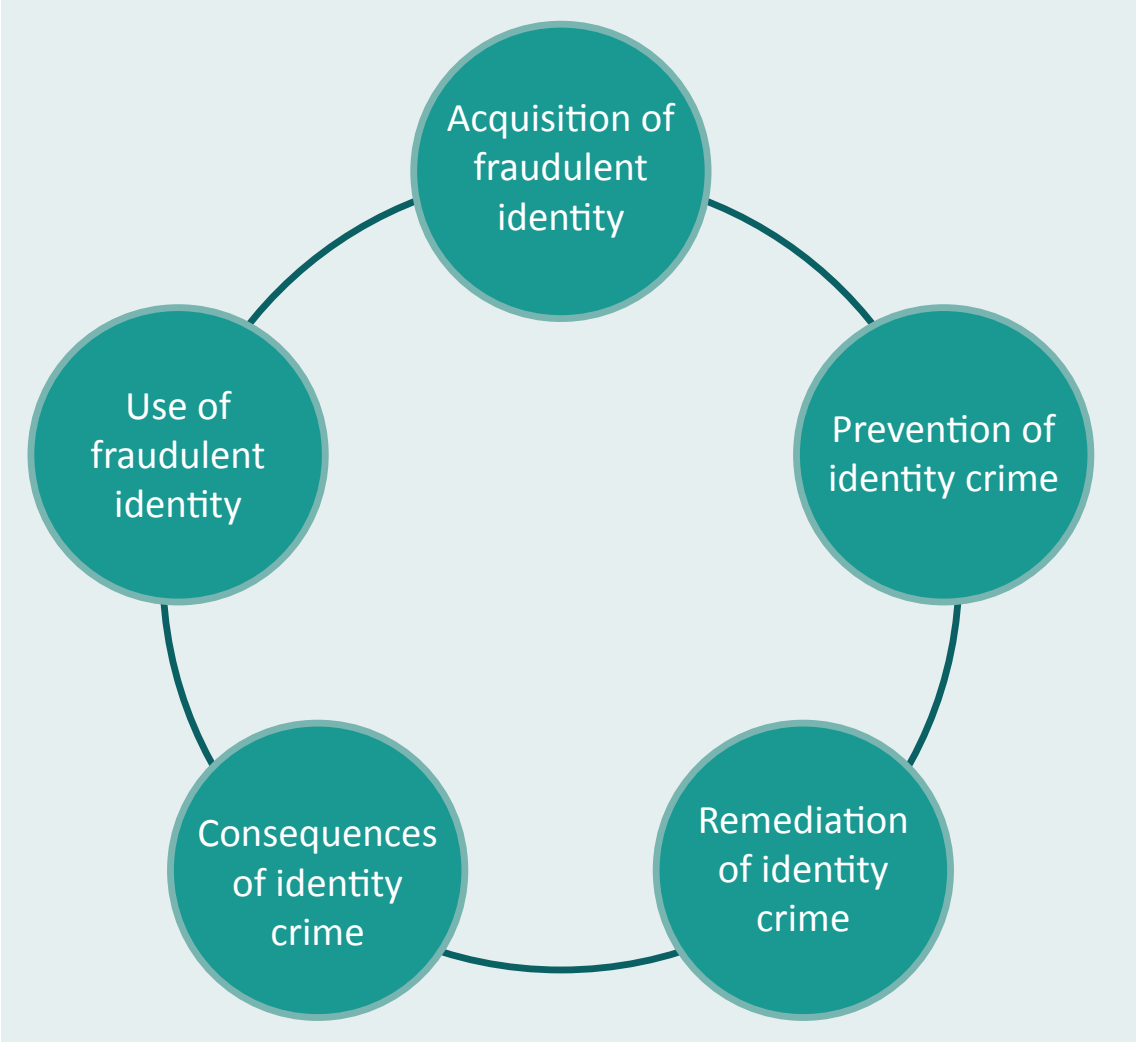
> 'Identity crime and misuse' involves someone using another person's personal information without their permission. 'Personal Information' includes: name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (eg fingerprint, voice, facial, iris recognition), signature, bank account information, credit or debit card information, password, personal identification number (PIN), tax file number (TFN), shareholder identification number (HIN), computer and/or other online usernames and passwords, student number, or other types of personal information.
>
> 'Identity crime and misuse' can also be perpetrated against government entities, corporations and businesses.

A total of 46 Commonwealth, state and territory agencies and one non-governmental organisation, IDCARE, provided information for this report. This indicates the breadth of identity crime experienced by government agencies and businesses throughout Australia. A list of the agencies invited to take part in the project is presented in *Appendix C.*

Key indicators

In quantifying the incidence and impact of identity crime and misuse, this report presents findings against a number of key indicators (Figure 8). The AGD, in collaboration with the AIC (Bricknell & Smith 2013), developed the methodology used in this and previous reports.

Figure 8: Key indicators for quantifying the incidence and impact of identity crime



Source: Bricknell & Smith 2013

Data quality and availability

Gaining a precise understanding of the prevalence and impact of identity crime in Australia remains problematic. This is due to:

- a failure to detect identity crime and misuse;
- under-reporting of identity crime by individuals and organisations;
- variable definitions of identity crime used by different agencies and organisations;
- the number of agencies and organisations that collect data pertaining to identity crime; and
- variability in legislation, recording practices, investigation and prosecution activity relating to identity crime and misuse and the inability to disaggregate identity crime from broader crime categories such as fraud.

Accordingly, the estimates presented in this report are likely to underestimate the actual incidence and cost of identity crime experienced in Australia.

Survey data

Throughout this report, survey findings have been relied on as measures of individuals' experience of personal fraud and identity crime. These include the AIC's 2019 Identity Crime and Misuse in Australia Survey (Franks & Smith 2020) and earlier surveys (see Table 1).

Identity Crime and Misuse in Australia surveys

In order to gain information on identity crime victimisation experienced by members of the Australian community, the AIC developed a questionnaire that was administered to an online panel of between 5,000 and 10,000 participants by i-Link Research Solutions, a market research company. Online panels are composed of individuals who agree to participate in surveys online. They are not necessarily representative of the entire community—although recent studies have had a large enough sample to enable analyses to be undertaken of most variables. All participants, did, however, require access to the internet and a willingness to be involved in such research.

The questionnaire included questions about demographic information, perceptions of identity crime risk and details of victimisation experienced by the respondents. Respondents were also asked to provide more detailed information on the most serious occasion of misuse of personal information within the last 12 months, including methodologies of offending, impact and response activities. Six online surveys have been conducted since 2013 (Table 1).

Table 1: Identity Crime and Misuse in Australia surveys, by year and sample size				
Year	**Analysed responses**	**Sample quota**	**Weighting of data**	**Report**
2013	4,995	Sample stratified by location. Small states and territories over-represented. (5,000)	Data weighted by location to represent the spread of population in Australia.	Smith & Hutchings (2014)
2014	5,000	Sample stratified by location. Respondents were 15 years and over. (5,000)	Data weighted by location to represent the spread of the population in Australia.	Smith, Brown & Harris-Hogan (2015)
2016	9,956	No quotas employed. Respondents aged 15–96 years. (10,000)	Data weighted by age and gender using ABS nationally representative data.	Smith & Jorna (2018b)
2017	9,947	No quotas employed. Respondents aged 15–96 years. (10,000)	Data weighted by age and gender using ABS nationally representative data.	Goldsmid, Gannoni & Smith 2018
2018	9,911	No quotas employed. Respondents aged 15–96 years. (10,000)	Data weighted by age and gender using ABS nationally representative data.	Jorna, Smith & Norman (2020)
2019	9,968	No quotas employed. Respondents aged 15–96 years. (10,000)	Data weighted by age and gender using ABS nationally representative data.	Franks & Smith (2020)

Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

In the initial surveys (2013 and 2014), respondents were randomly invited to participate in the survey using quotas relating to location, age and gender. Respondents were stratified across location so that there was an oversampling of respondents from smaller regions and territories and an under-sampling of respondents from larger jurisdictions. Age and gender were used as qualifying variables so that the respondents reflected population distributions according to demographic data from the Australian Bureau of Statistics (ABS 2013).

For the 2016 to 2019 surveys, non-probability samples consisted of 10,000 Australian residents aged 15 years and over who had internet access and who had registered with the panel provider. Quotas were not employed at the point of recruitment and sampling was completed once the target sample size of 10,000 respondents was obtained.

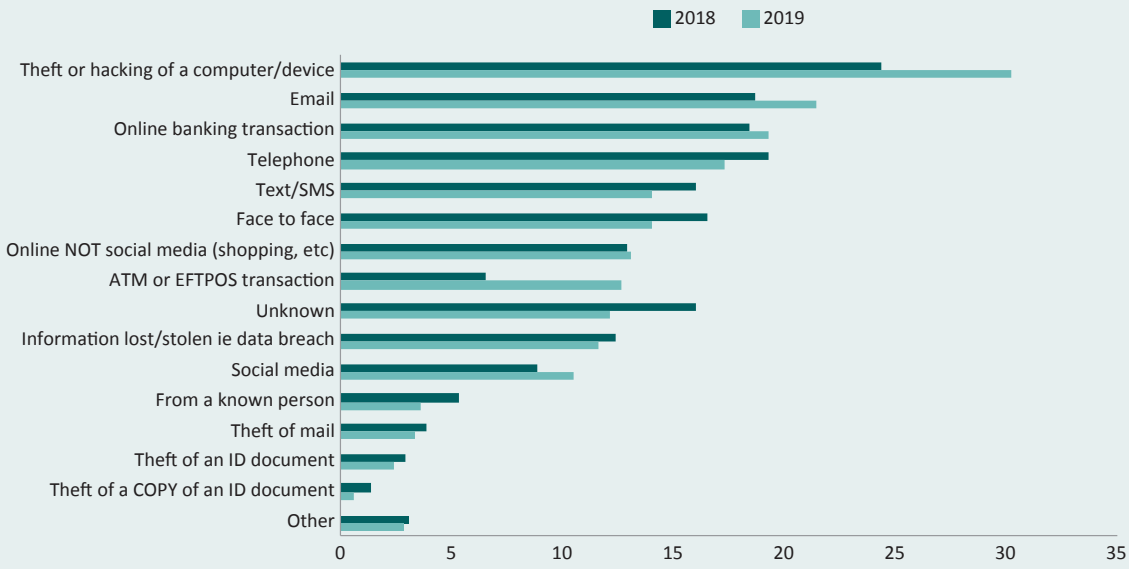
Acquisition of fraudulent identities

How personal information was obtained

Key finding: stolen and fraudulent identity credentials continue to be highly sought after by criminals, with a large amount of personal information obtained illegally online via email (phishing, malware, business email compromise), social media or through scams and data breaches. Personal information is also obtained physically by theft of documents and/or devices, through face to face methods, via text message (smishing), mobile porting or using telemarketing techniques. Social engineering has also become an established tactic criminals use to acquire personal identity information. Of most concern is the continuing trend of large proportions of identity crime victims who did not know how their personal information was illegally obtained.

The AIC's 2019 survey asked respondents how they believed their personal information had been obtained on the most serious occasion of identity crime in the 12 months preceding January 2020 (Franks & Smith 2020). Over 12 percent of respondents could not explain how their personal information had been obtained (Figure 9). Physical theft and accidental loss are still common methods used by criminals to acquire identity documents. This is now supplemented by perpetrators using social engineering techniques through telecommunications, email and social media platforms to encourage unsuspecting victims to disclose their personal details.

Figure 9: Method used to obtain personal information on the most serious occasion, 2018 and 2019 (%)



Source: Jorna, Smith & Norman 2020; Franks & Smith 2020

The Anti-Phishing Working Group (2019) reported that in 2019 phishing attacks were at their highest level in three years, steadily increasing throughout the year. An analysis of the Australian Competition and Consumer Commission's (ACCC) Scamwatch reporting system shows nearly half of all scam victims (47%) who reported were contacted by telephone or SMS (ACCC 2018).

The internet provides many opportunities to obtain personal information through unauthorised access to networks and systems. Data breaches allow substantial amounts of personal information to be accessed and used for criminal activity. Data breach was reported as the method by which personal information was obtained by 12 percent of respondents to the AIC's 2019 survey. It is likely many cases reported under the categories of social media, theft of email, online non-social media and 'unknown' also include a large proportion of data breach instances.

Symantec's (2019) *Internet security threat report* highlights a new technique used by hackers targeting organisations following a data breach. Attackers have begun 'living off the land' in an effort to prevent their network invasions being detected, using off-the-shelf tools and operating system features to conduct their attacks in the digital shadows. Keeping a low profile, they hide malicious activities among a mass of legitimate processes. By using clean system tools and inserting as few files as possible, attackers avoid being blocked or caught by traditional scanners and security measures (Symantec 2019). Of the 140 cyber attack groups monitored by Symantec (2019), nearly 75 percent used 'living off the land' techniques.

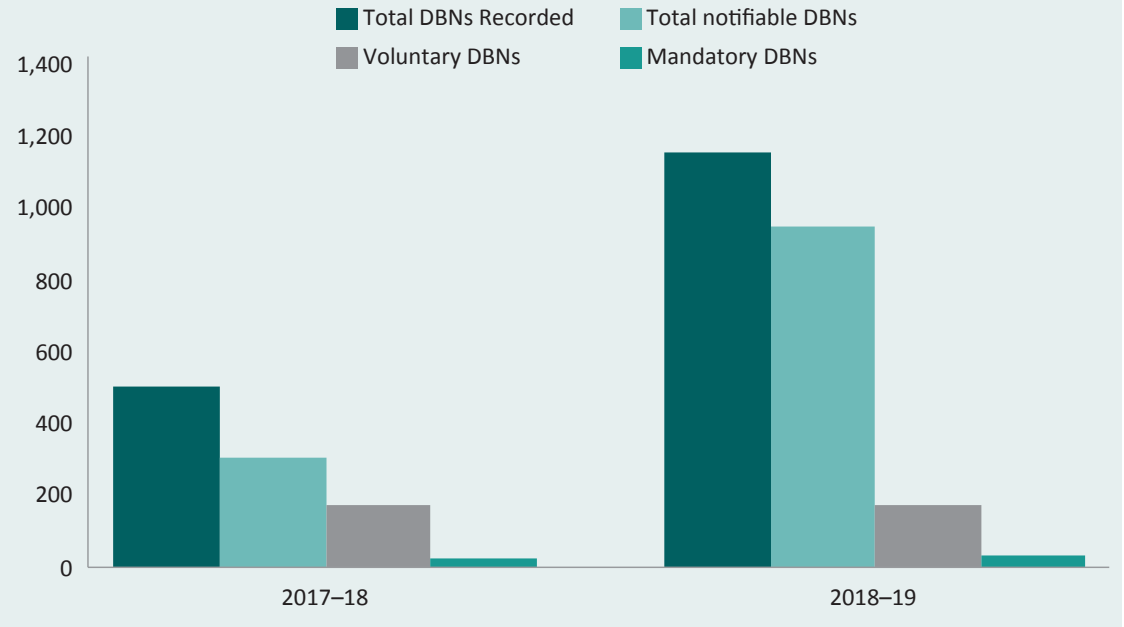
Number of reported data breaches

Key finding: in 2018–19, the Office of the Australian Information Commissioner (OAIC) received 950 data breach notifications, more than triple the number of the previous year. The annual global study undertaken by the Ponemon Institute found the average cost of a data breach for Australian companies was $3.2m in 2019, an increase of 28 percent on 2018.

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner is responsible for privacy functions conferred by the *Privacy Act 1988* (Cth) and other laws as well as collecting information on data breaches. An amendment to the *Privacy Act*, the *Privacy Amendment (Notifiable Data Breaches (NDB)) Act 2017* (Cth), established 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. The number of notifiable data breaches reported to the OAIC more than tripled between 2017–18 and 2018–19, from 305 to 950 (OAIC 2019).

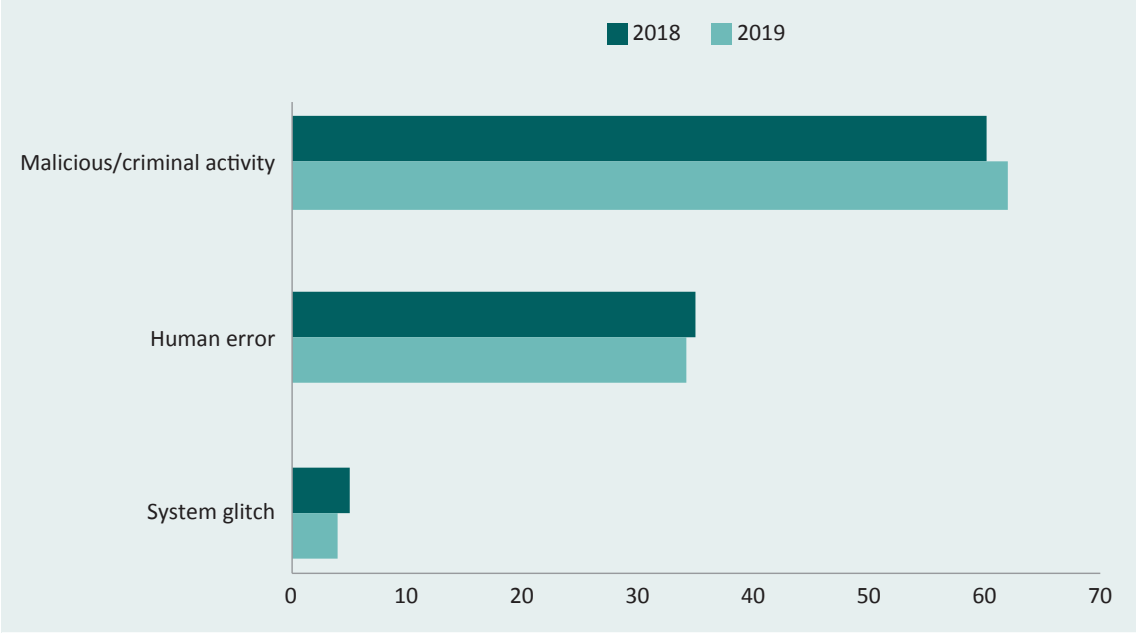
Figure 10: Data breach notifications (DBNs) received by the OAIC, 2017–18 and 2018–19 (*n*)



Source: OAIC 2019 (unpublished data)

The OAIC provided information about the sources of data breaches and how the data breaches occurred. Figure 11 shows that the majority (62%) of voluntary data breach notifications received by the OAIC in 2019 were attributable to malicious and/or criminal activity, up slightly from 2018. The remaining 38 percent were a result of a combination of human error (34%) and spontaneous system 'glitch' (4%). Because the NDB scheme came into effect on 22 February 2018, percentages shown in Figure 11 are based on the number of notifications per calendar year instead of financial year.

Figure 11: Causes of data breaches, 2018 and 2019 (%)



Source: OAIC 2018–2020; OAIC 2019 (unpublished data)

Ponemon Institute

The Ponemon Institute is a research centre in the United States with an interest in privacy, data protection and information security. The Ponemon Institute (2019) reports the global average cost of a data breach in 2018–19 was US$3.9m (A$5.7m) and that an average of 25,575 personal records were compromised per breach. The annual global study conducted by the Ponemon Institute (2019), in conjunction with IBM Security, provides further insight into the nature of data breaches experienced by Australian organisations. Twenty-five Australian organisations participated in a global study of 507 companies in 2019 as part of the *Cost of a data breach report*. Results showed that the average number of records per breach in Australia increased seven percent, from 18,556 in 2017 to 19,800 in 2019 (Ponemon Institute 2019). The study found the average cost of a data breach in Australia also increased between 2017 and 2019, from A$139 to A$166 per capita per data breach. In Australia the total average cost paid by a company increased 28 percent from A$2.5m to A$3.2m.

Key findings of the Ponemon Institute's (2019) report included the discovery of a longer overall data breach lifecycle, with malicious attacks the most common and most expensive root cause of breaches.

Breaches from random system malfunctions and human error were also still prevalent and continue to cost organisations millions each year. Worldwide numbers demonstrate the private health industry had the largest average total cost of a data breach at US$6.45m (A$9.5m). The financial industry ranks second with an average total cost of US$5.86m (A$8.6m). Please note: currency exchange rates are based on purchasing power parities (OECD 2020).

The Ponemon Institute (2019) concluded that organisations with rigorous regulatory requirements had much higher overall costs associated with a data breach, enhanced by increasing use of cloud servers, IT complexity and third-party initiated breaches.

Case study 2: Multi-party breaches

Under the Notifiable Data Breach scheme, only one entity is required to notify the OAIC in a scenario where multiple organisations were involved in a single breach. However, as an example, between April and June 2018 the OAIC received more than 50 notifications from an entity and its clients in relation to one incident. It was reported that individual consumers also received multiple notifications relating to the data breach, creating the potential for confusion.

This incident highlighted the challenges involved in multi-party breaches, in which there is a breach of data held by multiple entities, as is often the case in supplier arrangements. The incidence of multi-party breaches is expected to increase in the coming years, given continued trends towards outsourcing and the use of cloud service providers.

Source: OAIC 2019 (unpublished data)

The price of fraudulent identity credentials

Key finding: the price of Australian identity credentials in illegal online marketplaces (including those located on the darknet) varies according to the type of credential, its quality and whether it has been legitimately issued, counterfeited or altered. Prices range from around $20 for a falsified bank statement to $350 for a physical Medicare card and up to $8,000 for a certified Australian passport (IDCARE 2020).

Europol's (2019) *Internet organised crime threat assessment (IOCTA)* describes how personal identification information, including financial data, is easily monetisable through sale on the darknet or crimes of dishonesty. This makes identity theft the second most prominent cyberthreat after ransomware (Europol 2019). During the first half of 2019 the details of approximately 23m stolen credit cards were for sale on darknet markets (Europol 2019). Data compromise through server or network breaches, phishing emails and smishing text messages are the main sources of compromised credit card details, which are then misused in card-not-present fraud. When used for financial gain and combined with identity document compromise and misuse, card-not-present fraud can also facilitate illegal immigration and human trafficking by enabling the purchase of travel tickets, hotel bookings and other services.

Australian identity credentials form a critical element in the commission of many forms of financial crime. For example, the 100-point check system, introduced to control fraud, allocates points to different credentials and requires a total of at least 100 points to open an account with a bank or credit union in Australia. Full 100-point identity packages of stolen or fabricated identities are for sale on all darknet markets for as little as a few hundred dollars (IDCARE 2020).

Credentials with enhanced forms of security, such as passports and driver licences, are worth more points than other credentials such as utility bills, and command higher prices on the black market. The costliest credentials are those that have been issued legitimately using false or fabricated personal information. Physical items such as driver licences or Medicare cards are invariably more expensive to purchase than mere electronic scans of compromised credentials.

There is no 'standard' price for identity credentials. The price varies depending on the type of product, the quantity ordered, the quality of the document, the time frames, the relationship between the seller and customer and the number of hands the item passes through between the manufacturer and the end user (Bureau of Crime Statistics and Research 2019).

Use of fraudulent identities

Fraudulent identities are a key enabler of virtually all types of serious and organised crime. Financial crimes which facilitate criminal activity such as money laundering, blackmail, human trafficking, child exploitation and terrorism all rely on false identities for increased anonymity. The use of fraudulent identities facilitates benefits, taxation and other fraud against government agencies and businesses.

Fraudulent identities have been used to apply for visas, and in some cases citizenship, in order to circumvent security, criminal history or other requirements. The interdependent nature of Australia's credential-issuing authorities means that weaknesses in the process for issuing one type of identity credential can have significant downstream impacts. For instance, one fraudulent document can be used to obtain other credentials, but can also be accepted as evidence of a person's identity more broadly.

IDCARE (2020), a not-for-profit support service for victims of identity crime in Australia and New Zealand, found that its clients took, on average, 33.7 days to detect the compromise of their personal information. In comparison, it took only 6.9 days on average from the initial theft of personal and account information for criminals to commit multiple identity crimes with that information (IDCARE 2020).

Case study 3: Investment scams that mine identity credentials

An IDCARE client received an unsolicited email advertising an online trading platform (owned by a company registered in the British Virgin Islands, run out of Estonia). They clicked on a link to the registration page and filled out contact details. The client was contacted immediately and convinced to pay a deposit of €250 ($430) by credit card. This is similar to other investment scam behaviour observed by IDCARE, convincing victims to transfer small amounts, which then escalate over time as more trust is built and more exclusive benefits or opportunities are offered by scammers.

The client changed their mind the next day but was told that because of anti-money-laundering laws they would have to provide a copy of their driver licence, credit card and utility bill to close the account. The client refused but was later contacted by another cryptocurrency firm and tricked into handing over credit card details. The client's bank informed them that their money had gone to Eastern European accounts.

Another IDCARE client received continual emails from an online investment company featuring prominent Australians endorsing a Bitcoin trading platform. The client contacted the company (also based in the British Virgin Islands) and was convinced to invest an initial deposit of $400. They were immediately contacted by the trading manager via telephone and given a trading platform login and password. The client was unable to login using the provided information and allowed the trading manager remote access to their computer. The client became nervous after this and requested to close the account. The client was instructed to send copies of their driver licence and a recent utility bill with their address as part of Know Your Customer requirements. The client was informed by their bank that the platform was a scam.

Many clients report being lured to these scams by persistent and credible looking messages featuring prominent Australians or celebrities. The initial investment is around $400. IDCARE has observed many clients being asked to install trading platforms on their computer, leading to further compromise. Losses in the tens of thousands to hundreds of thousands of dollars are common. Further compromise occurs when clients attempt to withdraw money and are asked to provide copies of identity documents including driver licences, passports, utility bills and credit card details as part Know Your Customer or money laundering regulations. Misuse from these events includes the fraudulent establishment of transaction accounts, credit card accounts, personal loans and mobile phone accounts.

Source: IDCARE 2020 (unpublished data)

Identity crime incidents recorded by government agencies

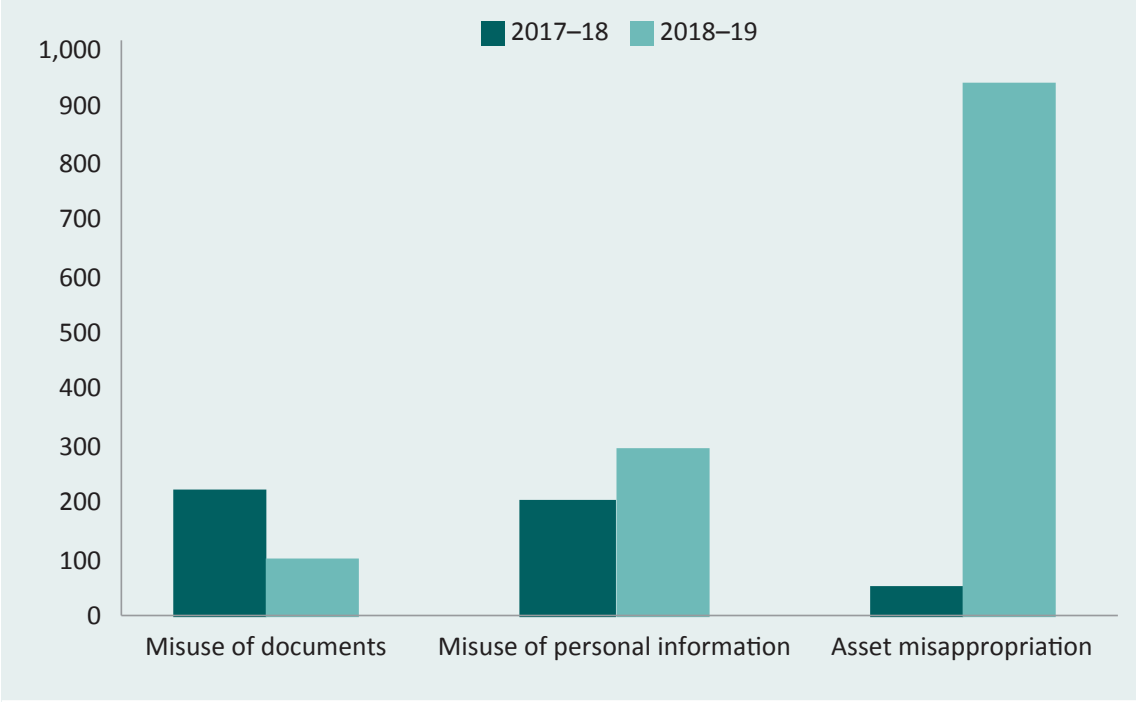
This section presents data from government entities about investigations that may have involved identity-related fraud or stolen documents. It includes information on identity crime reports made to government entities as well as identity crimes experienced by entities. Commonwealth entities are presented first, followed by state and territory agencies.

Fraud against the Commonwealth

Each year the AIC conducts a census of Commonwealth entities to assess their experience of fraud throughout the preceding financial year. The Fraud Against the Commonwealth census has found a number of fraud incidents involving the unauthorised use of another person's identification information (Figure 12).

Data on external fraud from the 2018–19 Fraud Against the Commonwealth census found a 45 percent increase in the misuse of personal information and an eighteen-fold increase in asset misappropriation, which may or may not have involved the misuse of identity credentials, between 2017–18 and 2018–19 (Teunissen, Smith & Jorna 2020). This latter increase resulted from eight entities reporting 945 investigations that involved asset misappropriation as the method of committing fraud against the Commonwealth, the majority (92%) detected through improved data analytics. Asset misappropriation involves unauthorised use of cash, assets and payment cards, but the extent to which misuse of identity credentials was involved was not specified (Teunissen, Smith & Jorna 2020).

Figure 12: External Commonwealth fraud investigations involving personal identity information, 2017–18 and 2018–19 (N)



Source: Teunissen, Smith & Jorna 2020

The AIC's Fraud Against the Commonwealth census counted finalised investigations rather than fraud incidents and, in addition, did not capture 'misuse of identity' directly but quantified specific fraud targets and misuse methods. Identity crime plays a part in numerous Commonwealth fraud typologies and because respondents to the census did not specifically identify investigations into identity crime, a general indication of the incidence of this crime type could only be estimated. This estimate was arrived at by analysing all reported Commonwealth fraud targets and misuse methods systematically, with each assigned a percentage that represented the involvement of identity crime and misuse. The estimated proportion of finalised Commonwealth fraud investigations involving identity crime was 40 percent (see Smith & Franks 2020).

Case study 4: Australian Defence Force employee's identity misused for used car sale fraud

In 2017–18, the Department of Defence was notified of six instances of a scam where a Defence Force member's identity was stolen and used on multiple online used car sales trading platforms. In one instance the scam was successful and the victim made a payment amounting to $3,000. The complainant reported the incident to the local police, their bank and Scamwatch.

In 2018–19, the Department of Defence received two additional reports about the same used car sales scam, using the same stolen identity. It appears that the perpetrator continues to repost advertisements on online trading platforms using the stolen identity. There is a possibility this Defence Force member's identity will continue to be misused in the future.

Source: Department of Defence 2019 (unpublished data)

Department of Human Services (now Services Australia)

Key finding: despite a decrease in overall fraud investigations by the Department of Human Services (DHS), there was a 25 percent increase in investigations concerning identity fraud between 2017–18 and 2018–19.

On 1 February 2020, DHS changed its name to Services Australia, but it will be referred to as DHS for the purposes of this report. In 2018–19, DHS completed 329 investigations into fraud matters concerning identity fraud, resulting in government savings of $5,568,090 for fraudulent payments. Of those identity fraud related investigations, 14 were referred to the Commonwealth Director of Public Prosecutions (CDPP). This is just over twice the $2,773,955 in total debts raised in 2017–18 (DHS 2019).

Table 2: Completed investigations into welfare and Medicare fraud, 2017–18 and 2018–19 (*n*)		
Welfare program	**2017–18**	**2018–19**
Working age[a]	1,821	1,601
Disability and carers[b]	747	677
Older Australians[c]	560	634
Students[d]	74	72
Family assistance[e]	7	12
Other welfare[f]	35	46
Medicare[g]	305	258
Total fraud matters	**4,026**	**3,312**
Total identity fraud matters	**326 (8.1% total fraud)**	**329 (9.9% total fraud)**

a: Includes Newstart, parenting payment partnered, parenting payment single, partner allowance, widow allowance, youth allowance—jobseeker

b: Includes carer payment, carer allowance, disability support pension, wife pension disability support pension, sickness allowance

c: Includes age pension, wife pension

d: Abstudy, Austudy, youth allowance—student

e: Family tax benefit

f: All other serious non-compliance

g: Child dental benefits, Medicare, pharmaceutical benefits

Source: Department of Human Services 2019 (unpublished data)

Case study 5: Investigation into compromised myGov accounts

DHS's Identity Theft and Scams Helpdesk received a referral about multiple compromised myGov accounts. These were quickly profiled by intelligence and analytics teams against the department's data holdings, leading to the identification of 277 data breaches.

An analysis of Centrelink records identified 21 victims of unauthorised payment destination updates. Tactical intelligence officers identified the alleged perpetrator and produced an intelligence product for fraud investigators within three hours of the initial referral. A search warrant was subsequently executed, leading to the seizure of a laptop and smartphone with identity information related to more than one million individuals allegedly acquired from the Null.to web forum.

The alleged perpetrator was interviewed by police officers and admitted to the alleged offending. The admission included information about a number of open source sites on which account holders can access compromised usernames and passwords. One of those sites was the aforementioned forum.

Source: Department of Human Services 2019 (unpublished data)

Australian Taxation Office

Key finding: between 2017–18 and 2018–19, the number of confirmed identity crime related fraud matters detected by the Australian Taxation Office (ATO) increased by 10 percent despite an overall decrease in potential fraud detected. Over the two-year period, the ATO saved $56.2m by thwarting fraudulent attempts to obtain benefits or avoid tax liabilities through the misuse of identity.

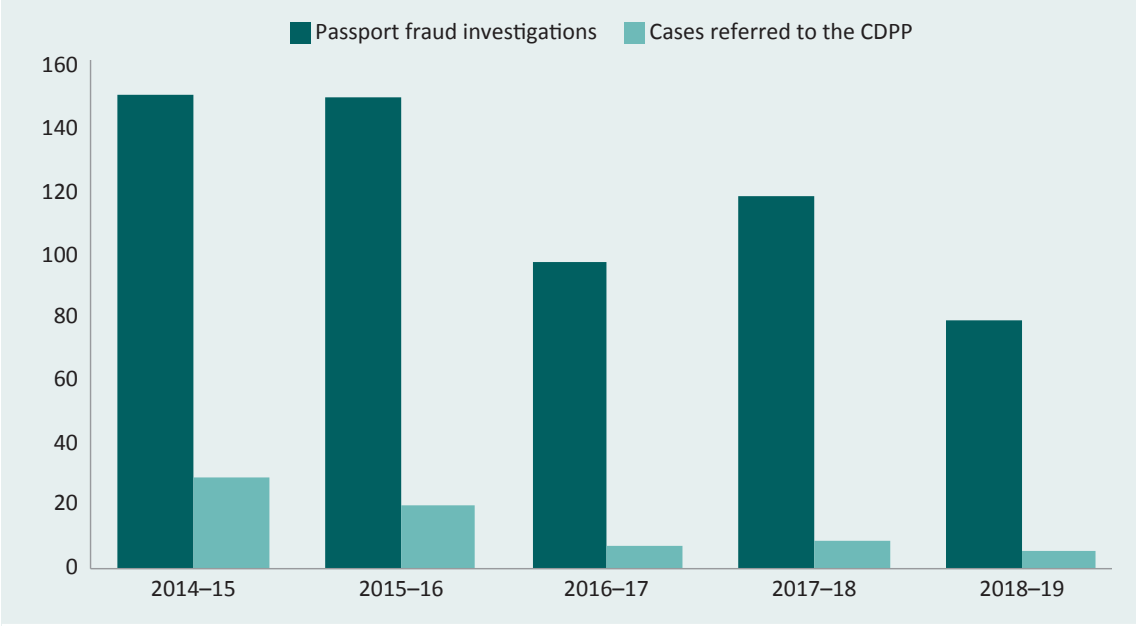
The ATO also maintains a Barred Bank Account list—a list of bank accounts identified as being used for fraudulent activity. The number of bank accounts placed on this list increased by 33 percent to 674 in 2018–19 from 507 in 2017–18. When examining identity crime incidents detected by the ATO (2019), confirmed incidents increased by 10 percent in 2018–19 (2,691) versus 2017–18 (2,450).

Department of Foreign Affairs and Trade

Key finding: in 2018–19, 79 passport fraud incidents were investigated by the Department of Foreign Affairs and Trade (DFAT), with five matters referred to the CDPP.

In October 2015, the Parliament of Australia added a new section to the *Australian Passports Act 2005*, allowing the Minister's delegate to 'refuse to process' a passport application on the grounds of fraud or dishonesty. This provision gave DFAT the scope to deal with minor cases of fraud such as forged parental consent without the need for criminal investigation and prosecution—a significant factor contributing to the decrease in the number of formal investigations.

Figure 13: Passport fraud investigations and referrals to CDPP, 2014–15 to 2018–19 (*n*)



Note: DFAT changed the way it records passport fraud investigations in 2015. Subsequent instances of minor passport fraud (not involving identity crime) were resolved by administrative action and not recorded as investigations. In 2015–16 an additional 9 cases were referred to other prosecution authorities; in 2016–17 another 3 cases were referred to other prosecution authorities

Source: AGD 2016; DFAT 2019, 2017 (unpublished data)

The number of passport fraud investigations related to identity crime and misuse is presented in Figure 14.

Figure 14: Passport fraud investigations related to identity crime, 2014–15 to 2018–19 (*n*)

Source: AGD 2016; DFAT 2019, 2017 (unpublished data)

Table 3 provides further details of the passport fraud investigations in 2017–18 and 2018–19 that may have involved identity crime.

Table 3: Identity crime related passport fraud investigations, 2017–18 and 2018–19

Case type	2017–18	2018–19
Fraudulently obtained genuine passports	12	6
Imposters	3	10
Physical alteration	6	2
Total	**21**	**20**

Source: DFAT 2019 (unpublished data)

Case study 6: Stolen Australian passports and human trafficking

DFAT received reports in 2019 indicating people smugglers operating in the Middle East would charge up to €8,500 (A$14,100) for a genuine Australian passport and airline tickets to allow a person to undertake imposter travel to Europe. There is no information available on the specific components of this cost.

Source: DFAT 2019 (unpublished data)

Lost and stolen passports

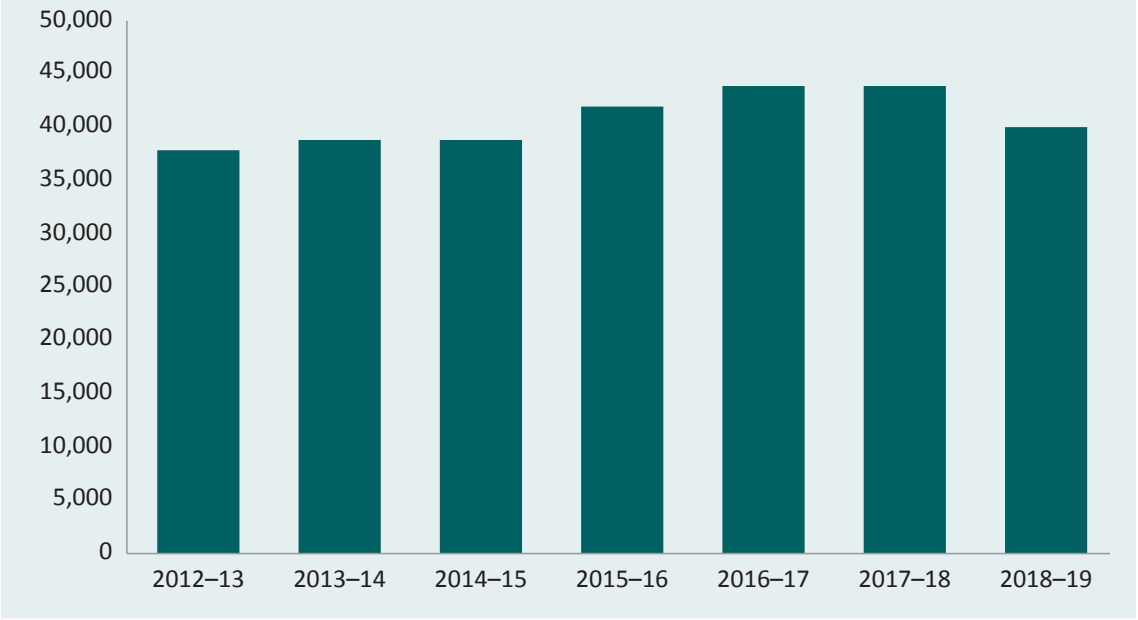
Key finding: genuine Australian passports are valuable on the black market. The number of fraudulently obtained genuine passports halved between 2017–18 and 2018–19, but the number of passport fraud investigations initiated by DFAT more than tripled over the same time.

Lost and stolen passports create opportunities for criminals to perpetrate identity-related fraud and to travel overseas without authorisation. Australia's current P series passport issued by the Department of Foreign Affairs and Trade contains world-leading security features to deter and prevent forgeries, and to detect any alterations (DFAT 2020). DFAT is on track to deliver the next generation of Australian passports, called the R series, in 2020–21. It will use new materials, construction techniques and personalisation equipment to provide greater security and durability. These features will act as further deterrents to criminals seeking to compromise these documents (DFAT 2020).

In October 2018, DFAT (2020) installed a new, more accurate face recognition algorithm and developed a new IT system to underpin its face comparison algorithms to stop fraud. All high-risk applications are individually scrutinised by specialist staff. In 2018–19, the updated systems led to 35,655 passport applications being referred to face comparison experts for manual assessment (DFAT 2020). As a result, DFAT (2020) detected six cases of passport identity fraud—two related to new applications and four involving historic applications.

Between 2017–18 and 2018–19, there was a 10 percent decline in the number of lost or stolen passports reported to DFAT (Figure 15), explanations for which are not known. Reporting and other policies relating to lost or stolen passports did not change during this period (DFAT 2019).

Figure 15: Australian passports reported lost or stolen, 2012–13 to 2018–19 (*n*)

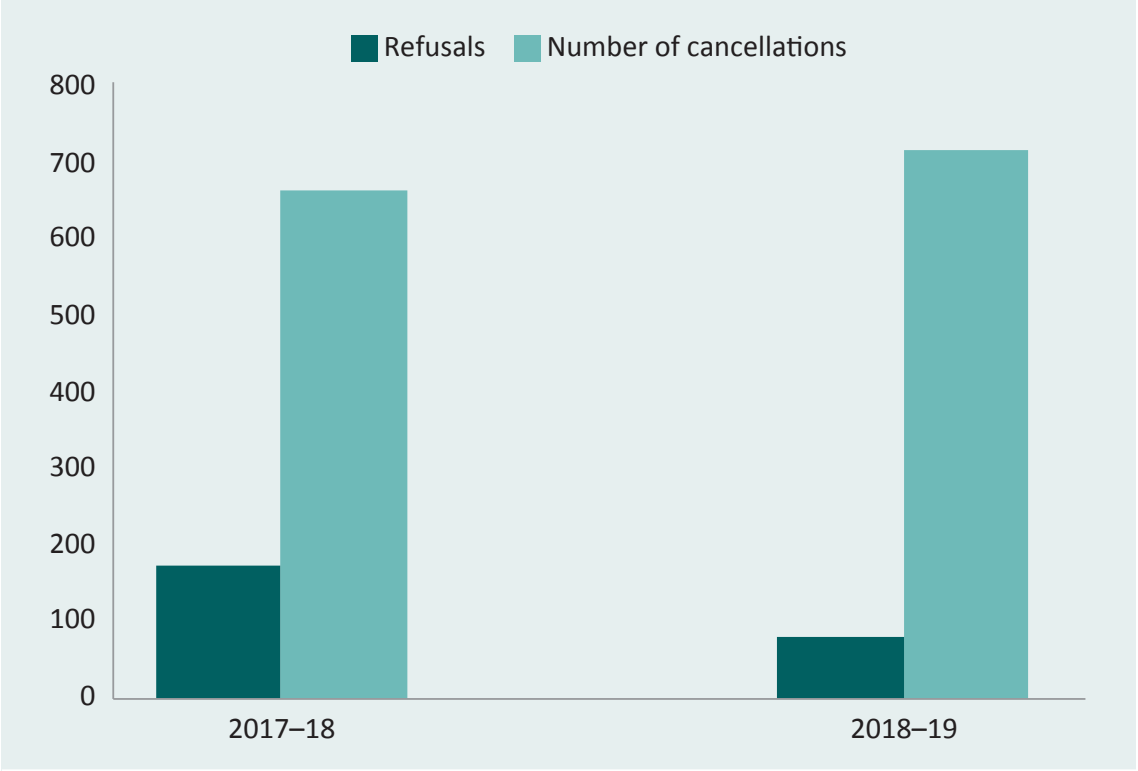


Source: AGD 2016; DFAT 2019, 2017 (unpublished data)

Visa cancellations and refusals

Key finding: there was an eight percent increase in the number of visa cancellations between 2017–18 and 2018–19. Of the 253 visa applicants refused during the same two-year period, 95 percent were also issued with a 10-year exclusion ban (Australian Border Force 2020).

Figure 16: Visa cancellations and refusals as a result of identity fraud, 2017–18 and 2018–19



Source: Australian Border Force 2020 (unpublished data)

The Department of Home Affairs also provided data on identity-related fraud involving importation and customs. In 2018–19, there were 74 instances where counterfeit credit, debit and charge cards were detected, an increase of almost 25 percent over 2017–18 numbers.

Australian Securities and Investments Commission

The Australian Securities and Investments Commission (ASIC) is Australia's integrated corporate, markets, financial services and consumer credit regulator. As a financial services regulator, ASIC licenses and monitors financial services businesses to ensure they are honest and fair (ASIC 2020).

ASIC received 8,628 reports of financial misconduct relating to ASIC regulated entities and individuals in 2018–19, an increase of five percent from the 8,247 reports in 2017–18 (ASIC 2019). Data pertaining to financial losses suffered by identity crime and misuse victims and the estimated costs to ASIC in terms of investigation and compliance were not available.

Australian Transaction Reports and Analysis Centre

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is Australia's financial intelligence agency with regulatory responsibility for combating money laundering and terrorism financing. AUSTRAC's role is to identify threats to and criminal abuse of the financial system, and act to protect Australia's economy.

A major part of AUSTRAC's work involves receiving suspicious matter reports from regulated businesses such as banks and casinos. AUSTRAC supplied data for this report on the number of suspicious matters in which a false name or identity document had been used. Suspicious matter reports involving identity misuse increased by 74 percent in 2018–19 (15,040) versus 2017–18 (8,640); however, costs associated decreased slightly from $2.1m (2017–18) to $2m (2018–19) (AUSTRAC 2019).

Australian Communications and Media Authority

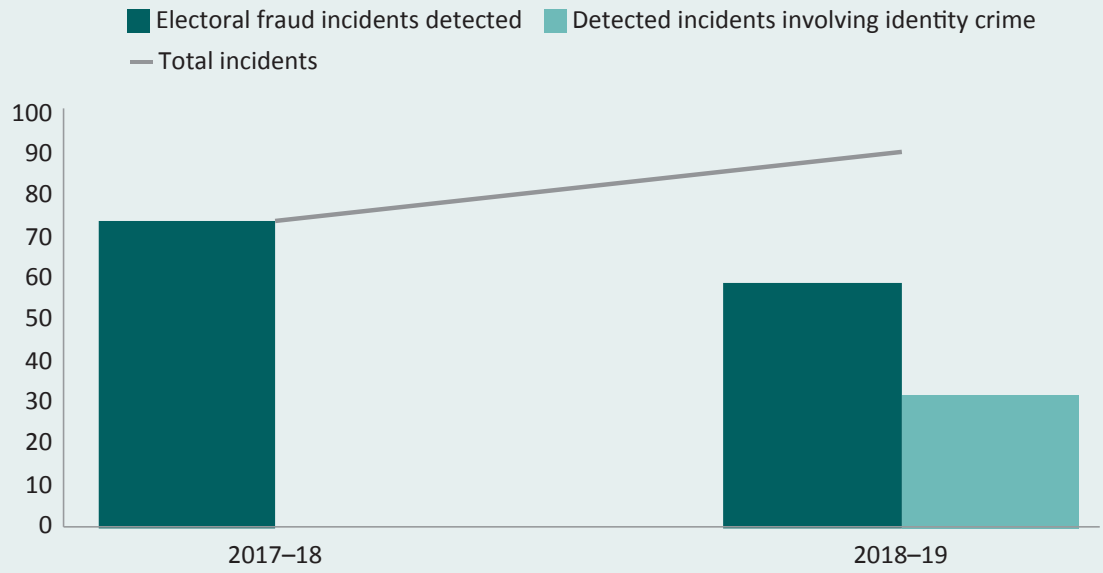
The Australian Communications and Media Authority (ACMA) receives reports of email and text message spam from a number of different sources and collates them in its Spam Intelligence Database. These data are used to identify 'phishing' activities—the use of electronic messages to acquire people's personal or financial information, often by impersonating well-known organisations such as the Australian Taxation Office, the Australian Federal Police, Australia Post, financial institutions and major brands.

In 2017–18, the ACMA received 8,620 complaints from individual victims of identity crime and misuse. That number increased to 8,703 complaints for the 2018–19 financial year (ACMA 2019).

Australian Electoral Commission

The Australian Electoral Commission (AEC) is responsible for conducting federal elections and referenda, and maintaining the Commonwealth electoral roll. The AEC also runs a range of programs relating to electoral information and education. The AEC provided data on the number of incidents of electoral fraud detected between 2017–18 and 2018–19, as well as the number of incidents that were identified as involving identity crime and misuse (Figure 17). It is important to note that the federal election held on Saturday 18 May 2019 likely had a direct effect on the overall increase in the number of incidents recorded.

Figure 17: Incidents of electoral fraud detected, and incidents involving identity crime and misuse, 2017–18 to 2018–19 (*n*)



Source: AEC 2019 (unpublished data)

ReportCyber—Australian Cyber Security Centre

ReportCyber began operating on 1 July 2019 as the successor to the Australian Cybercrime Online Reporting Network (ACORN), the national policing initiative of the Commonwealth, state and territory governments. ReportCyber is a national online system that allows members of the public to report cybercrime and related matters and is part of the Australian Cyber Security Centre (ACSC). The reports made to ReportCyber are referred to the most appropriate law enforcement agency for consideration and possible investigation.

In the first three months of ReportCyber's operation, between 1 July and 30 September 2019, 13,672 reports were made—an average of one every 10 minutes. Of these reports, 84 percent (11,461) contained sufficient information to be referred to state and territory law enforcement agencies. The ACSC responded to the remaining 2,211 cases with tailored cybersecurity advice to the person or entity who had submitted the report (ACSC 2019).

ReportCyber has logged an average financial loss per report of $6,000, with an estimated total loss of $328m annually (ACSC 2019).

Case study 7: Identity theft and online fraud

A 26 year old woman was looking for a room to rent and responded to an advertisement on a popular Australian website. The person who posted the advertisement informed her that they were currently overseas on holiday but would return to Australia in a week. In order to secure the room, she was told to provide her full name and date of birth, together with copies of her identity documents. The woman sent copies of her passport, birth certificate, driver licence and employment history. The advertiser then requested three months of rent in advance before they would provide a copy of the lease. At this point, the woman suspected that she might be the victim of a scam. A subsequent investigation discovered that the scammer had used the woman's stolen personal information to apply for a credit card in her name and purchased over $10,000 worth of airline tickets, electronics and luxury items.

Source: ACSC 2019

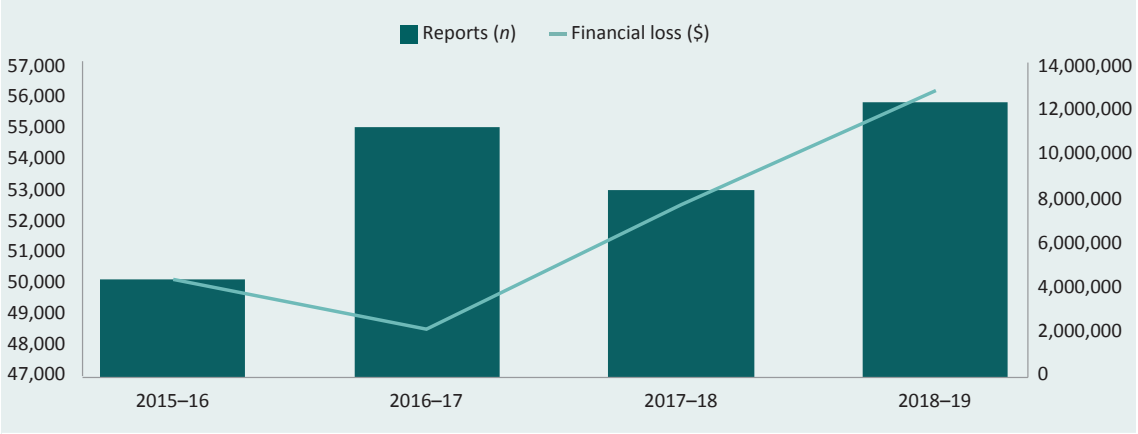
Australian Competition and Consumer Commission—Scamwatch

Key finding: financial losses recorded by the ACCC have increased substantially since the initial Scamwatch report of 2015–16. Under-reporting of cybercrime continues to undermine calculations of the true cost of identity crime in Australia and worldwide.

The role of the Australian Competition and Consumer Commission (ACCC) is to enforce the *Competition and Consumer Act 2010* and other legislation, to promote competition and fair trading for the benefit of all Australians. The ACCC also manages Scamwatch, an online resource and reporting portal that tells consumers and small businesses how to recognise, avoid and report scams. All online, face-to-face and telephone or mobile based scams can be reported to Scamwatch. The ACCC records information from individuals concerning personal information compromise and misuse across its entire range of reportable scams including romance scams, investment scams and employment scams. In 2018–19, 28,248 instances of lost identity credentials were logged, and 3,509 of these included documented financial losses totalling $19,896,167 (ACCC 2019).

The ACCC also provided data on the number of reports it received about scams involving attempts to gain personal information (eg phishing, threat-based impersonation) from people who either received or fell victim to these types of scams (Figure 18). These scams include phishing and threat-based impersonation—a scam involving a threat such as arrest, subpoena or infringement notice, and impersonation of an officer of a government agency such as the Australian Taxation Office or Australian Federal Police.

Figure 18: Scams involving attempts to gain personal information and estimated financial losses, 2015–16 to 2018–19



Source: ACCC 2019, 2017 (unpublished data)

Registries of births, deaths and marriages

Key finding: information on criminal misuse of certificates issued by Registries of Births, Deaths and Marriages is generally not available, as many people do not notify registries of loss or theft incidents. Only the New South Wales registry was able to provide data for all categories of potential identity-related crime.

The number of compromised/misused certificates issued by the New South Wales Department of Births, Deaths and Marriages nearly doubled between 2017–18 and 2018–19. A recent report by the NSW Auditor-General states there are 'significant gaps' in the controls against unauthorised access to the Registry of Births, Deaths and Marriages that could lead to identity theft and fraud (Audit Office 2020). The same report also found insufficient controls to prevent the distribution of information in the register to unauthorised third parties. Evidence also demonstrated that the NSW registry did not actively monitor user activity in the register or have sufficient assurance over the effectiveness of database security controls (Audit Office 2020). Several recommendations were made, with immediate implementation encouraged, to ensure the integrity of the registry is maintained to safeguard people's identities. The registry is working towards full implementation of all of the recommendations.

Table 4: Incidents recorded by the NSW Registry of Births, Deaths and Marriages, 2017–18 and 2018–19

Case type	2017–18	2018–19
Lost/stolen certificates	235	497
Fraudulent certificates	6	9
Unauthorised amendment of certificates	22	16
Total	**263**	**522**

Source: NSW Registry of Births, Deaths and Marriages 2019 (unpublished data)

The Queensland Registry of Births, Deaths and Marriages has proposed a national Australian Death Check register on behalf of all states. The database, designed by identity management, location intelligence and fraud prevention company Global Benefits Group, aims to fight fraud and identity crime and safeguard the reputation of individuals (Global Benefits Group 2020). Currently in a trial phase in Queensland, New South Wales, Victoria, South Australia and Tasmania with nationwide launch scheduled for mid-2020, the Australian Death Check aims to be the single source of truth for death records in Australia (Global Benefits Group 2020).

Driver licence issuing authorities

Key finding: driver licences continue to be among the most commonly targeted identity credentials as proof of identity and a source of valuable personal information such as name, address and date of birth.

Road traffic agencies in the states and territories issue and renew many millions of driver licences every year. Data available for public release were provided by only some of these agencies, with those available showing increasing numbers of cases of identity crime involving driver licences. In New South Wales, for example, the number of new driver licence numbers issued due to detected fraud increased from 12 to 44 between 2018 and 2019, and in South Australia this number increased from 18 to 105 during the same period. These numbers represent a small proportion of all licences on issue.

Identity crime involving driver licences includes reports of stolen licences being used in connection with verification of identity in online vehicles sales, and for opening bank accounts for online fraud. Genuine licences are also being digitally altered with false photographs and other details to overcome Document Verification Service checks in cases where the biographical details are genuine.

Driver licence issuing agencies continue to invest in the latest technologies to protect against tampering with genuinely-issued licences. Some states are also starting to share credential information as part of the Commonwealth's National Driver Licence Facial Recognition Solution. Licence holders also need to ensure that their personal information is held securely and that licences are not used in high-risk situations.

While all states and territories have fairly straightforward processes for replacing a physical licence that was lost or stolen, it is extremely difficult and sometimes impossible to have a new driver licence number issued in Australia (see case study 8).

Case study 8: Obtaining a new driver licence number

In January 2019, an IDCARE client received two debit cards in the mail that had not been applied for. The individual immediately spoke with the banks concerned—banks they had never previously interacted with. One bank said they could not share details about the case because of privacy concerns. The other said that someone had used the client's driver licence and Medicare card details to apply for the debit card and that the account appeared to have been used by criminals based offshore for money laundering (in the victim's name). The Department of Human Services arranged for additional security measures on their Medicare account, including a new Medicare card, and advised them to call IDCARE.

The individual reported the matter to their local police, who simply referred them to ReportCyber. Knowing their licence was being misused, and residing in one of two states that allow for driver licence numbers to be changed, the individual asked their bank for a letter to indicate that their licence had been misused to open an account. This is a requirement of the driver licence issuer, without which victims of identity theft cannot change a driver licence number. The bank initially refused. IDCARE advocated on behalf of the client to convince the bank to write an email explaining that the licence had been used to apply for an account and that this account was believed to be fraudulent. As part of their advocacy, IDCARE advised the bank that by assisting they were reducing the risk across industry and government service providers that the criminals would continue to misuse the licence.

Next, the victim asked the local police station for a police report number and a letter, again indicating that the licence had been allegedly misused to create a fraudulent account. The police initially refused, instead referring the client back to ReportCyber. An IDCARE case manager then accompanied the client to the same police station, where the same advice was given. When the police were informed that the licence issuer required the letter to change a licence number, they still refused to cooperate. At the police station, on behalf of the client, IDCARE called the manager in the licence issuing agency and asked him to speak with the local police to explain the process. Once the process had been explained, the police sergeant found a form that police complete and provide to people in this position to request a licence change. The individual then took the banking email and signed police form to the licence issuing agency.

Six weeks later a new licence with a new number was issued. This process took around 35 non-consecutive hours, time off work, the completion of around 10 different forms, and contact with Commonwealth agencies, state government agencies, banks, telecommunications companies, credit reporting bureaus and IDCARE representatives. Like many victims of identity crime, this individual never knew how their credentials had been compromised.

Source: IDCARE 2020 (unpublished data)

State and territory police

Key finding: police agencies recorded 116,643 fraud and deception offences in 2018–19, an increase of four percent from 2017–18. Only some jurisdictions were able to quantify identity fraud offences. It is estimated that 58 percent of fraud involves some element of identity misuse (Cifas 2019), which would amount to 67,523 identity-related offences recorded by police in Australia in 2018–19.

The nature of identity offences differs between Australian jurisdictions. Most states and territories (Queensland, New South Wales, Western Australia, South Australia, the Northern Territory and Victoria) have specific identity crime provisions in their criminal statutes. All jurisdictions have more general deception and dishonesty offences, a proportion of which capture identity crime, thus making inter-jurisdictional comparisons difficult. In addition, data currently collected and recorded by police agencies are primarily for operational purposes and investigative needs. A summary of the information available in each jurisdiction is presented in *Appendix D.*

Case study 9: Credit card skimming

The NSW Police Force established a strike force to investigate a syndicate believed to be involved in credit card skimming, credit card cloning and the subsequent unlawful use of the cloned credit cards and credit card data to purchase goods or gift cards from major retailers and to withdraw funds from ATMs across Sydney.

The investigation revealed the syndicate had used compromised EFTPOS devices, including a new brand of EFTPOS device that had not previously been detected in New South Wales. The syndicate stole gift cards from various retailers and encoded the details of the credit cards onto these gift cards. The syndicate would also encode the details of certain credit cards onto expired credit cards in the name of syndicate members. That way, if stopped by police or questioned by retailers, they could show their legitimate driver licence in support of the card that had been used. Syndicate members would report up to six cards lost to their respective banks each year, in order to have sufficient cards to encode with specific credit card data.

Source: NSW Police Force 2019 (unpublished data)

Prosecution of identity crime and related offences

Although large numbers of identity crimes are reported officially, only a relatively small proportion of incidents result in police investigation and prosecution. In the United Kingdom, the National Crime Agency (NCA 2018) reports that as technology continues to spread globally, cybercrime is more prevalent in countries that lack the capacity to mount an effective response. Cybercrimes are borderless, making the increasing threat a worldwide issue.

Criminal use of encryption and the darknet raise additional challenges to law enforcement in their attempts to prosecute identity crimes. The combination of encryption and anonymisation challenges law enforcement collection of intelligence and evidence (NCA 2018). Under-reporting of cybercrime is also a continuing problem, with the majority of victims (62%) lacking confidence in law enforcement response (NCA 2018). Those who do report are unlikely prepared to support prosecution.

Commonwealth Director of Public Prosecutions

Key finding: Commonwealth Director of Public Prosecutions (CDPP) cases relating to fraud, identity crime and other financial crimes declined substantially between 2017–18 and 2018–19. The Department of Human Services (DHS) continues to be the primary government agency referring matters to the CDPP. With 589 total referrals for 2018–19, DHS represents 69 percent of all referrals from government organisations.

There are several Commonwealth statutes under which people suspected of committing identity crime and fraud can be prosecuted. The specific offence provision is largely dictated by the nature, circumstances and target of the crime, rather than the method used by the offender. For instance, Part 9.5 of the *Criminal Code Act 1995* contains offences which specifically deal with identity crime, and Chapter 7 contains more general dishonesty offences relating to fraudulent conduct, forgery and falsifying documents. Identity-related offences also exist in other Commonwealth legislation such as the *Migration Act 1958*, *Customs Act 1901* and the *Trade Marks Act 1995*.

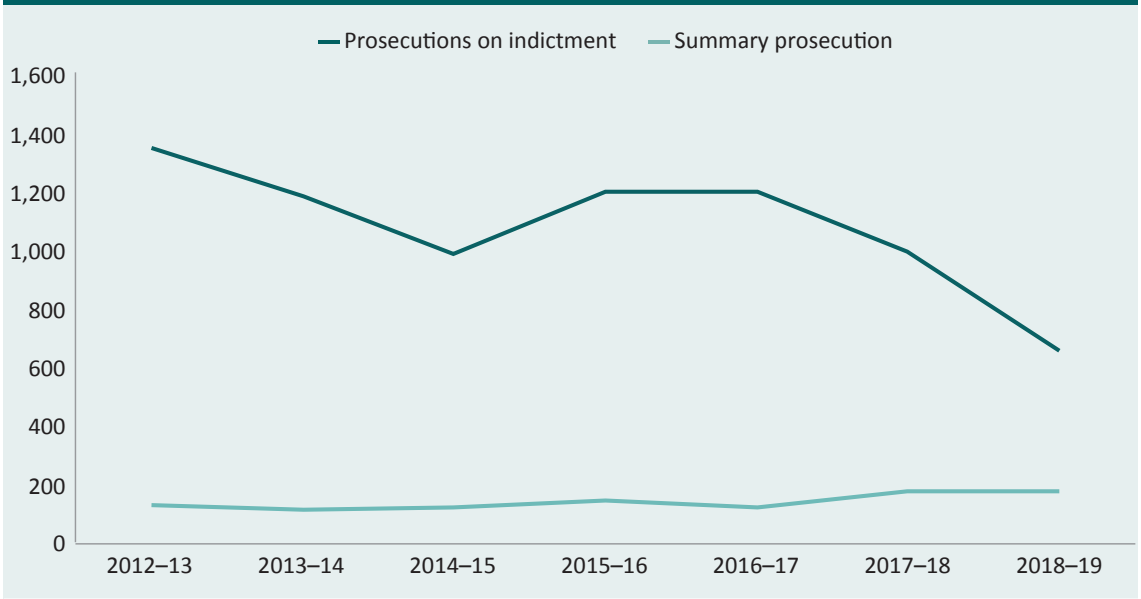
Table 5: Defendants prosecuted by the CDPP by Criminal Code Division, 2012–13 to 2018–19 (*n*)

Offence	2012–13	2013–14	2014–15	2016–17	2017–18	2018–19
Criminal Code divs 370, 372, 375—identity crime	1	3	6	4	27	25
Criminal Code divs 133–137—Fraudulent conduct	1,458	1,313	1,127	1,381	1,024	697
Criminal Code divs 144–145—Forgery	24	19	28	26	23	54
Criminal Code div 480—Financial information offences	9	3	5	0	6	0
Migration Act 1958 s 234—False documents and false or misleading information relating to non-citizens	29	10	7	11	7	12
Financial Transaction Reports Act 1988 s 24—Opening account etc in false name	9	3	2	1	1	0
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 pt 12—Offences	2	7	2	4	6	4
Criminal Code divs 400.3–400.9— Money laundering offences					135	100
Customs Act 1901 pt XIII—Penal provisions	13	38	57	0	42	33
Australian Passports Act 2005 ss 29–41—Offences					20	12
Total	**1,554**	**1,400**	**1,237**	**1,424**	**1,316**	**959**

Source: CDPP 2019 (unpublished data)

The offences regarding fraudulent conduct (*Criminal Code Act 1995* (Cth) divisions 133–137) were examined in greater detail (Figure 19). The CDPP prosecuted 1,024 fraud cases in 2017–18, most of which (*n*=891, 87%) were referred by DHS. The number of prosecutions relating to DHS declined to 81 percent between 2017–18 and 2018–19. Overall government referrals have declined in the previous three years while prosecutions on indictment have remained fairly consistent. This is likely the result of stricter monitoring and weighing of evidence.

Figure 19: CDPP fraud prosecution government organisation referrals, 2012–13 to 2018–19 (*n*)



Source: CDPP 2019, 2017 (unpublished data)

State and territory prosecutions

State and territory criminal courts hear a wide variety of matters that could potentially involve identity crime and misuse. The Australian Bureau of Statistics (2020) provided customised data on 22 offence types that potentially involve identity crime. The bureau was unable to verify that all of these offence types involved identity crime and, as such, these data should be treated with caution. Table 6 presents ABS criminal court data on the total number of offences in these categories that could involve identity crime and the number of allegations proven for 2018–19.

Table 6: Identity crime related offences in state and territory criminal courts, 2018–19			
Offence classification	**Proven guilty (*n*)**	**Total finalised (*n*)**	**% proved**
0829 Theft (except motor vehicles)	1,473	1,631	90.3
0831 Receive or handle proceeds of crime	212	312	67.9
0911 Obtain benefit by deception	64,690	90,461	71.5
0922 Forgery of documents	3,376	5,370	62.9
0923 Possess equipment to make false/illegal instrument	115	156	73.7
0931 Fraudulent trade practices	10	45	22.2
0932 Misrepresentation of professional status	3	7	42.9
0933 Illegal non-fraudulent trade practices	505	681	74.2
0991 Dishonest conversion	8,615	11,934	72.2
0999 Other fraud and deception offences, NEC	406	678	59.9
1111 Import or export prohibited weapons/ explosives	9	17	52.9
1419 Driver licence offences, NEC	N/A	N/A	N/A
1542 Bribery involving government officials	38	76	50.0
1543 Immigration offences	20	28	71.4
1559 Offences against government security, NEC	4	11	36.4
1562 Resist or hinder police officer or justice official	N/A	N/A	N/A
1569 Offences against justice procedures, NEC	13	61	21.3
1631 Commercial/industry/financial regulation	N/A	N/A	N/A
1692 Bribery excluding government officials	23	64	35.9
1694 Import/export regulations	95	154	61.7
Total	**79,614**	**111,697**	**71.3**

Note: Numbers in left column are Australian and New Zealand Standard Offence Classification codes. NEC=not elsewhere classified

Source: ABS 2020 (unpublished data)

Self-reported victimisation of identity crime or misuse

Identity crime is often difficult to detect because criminals go to some lengths to conceal their activity and remain anonymous. Modern cybercrime methods enable offenders to harvest identity credentials from databases on the darknet, using encryption to limit detection (Krone & Smith 2018). Many victims of identity crime are reluctant to report the crime to police or other authorities, believing that little can be done to investigate these crimes or recover losses. As a result, official crime statistics give only a partial picture of the nature and extent of the problem. To address this, crime victimisation surveys can be used where respondents report their experience of victimisation, the losses they suffered and how they responded. This report presents the findings of such surveys that sought to ascertain the nature and extent of identity crime in the Australian community.

Prevalence

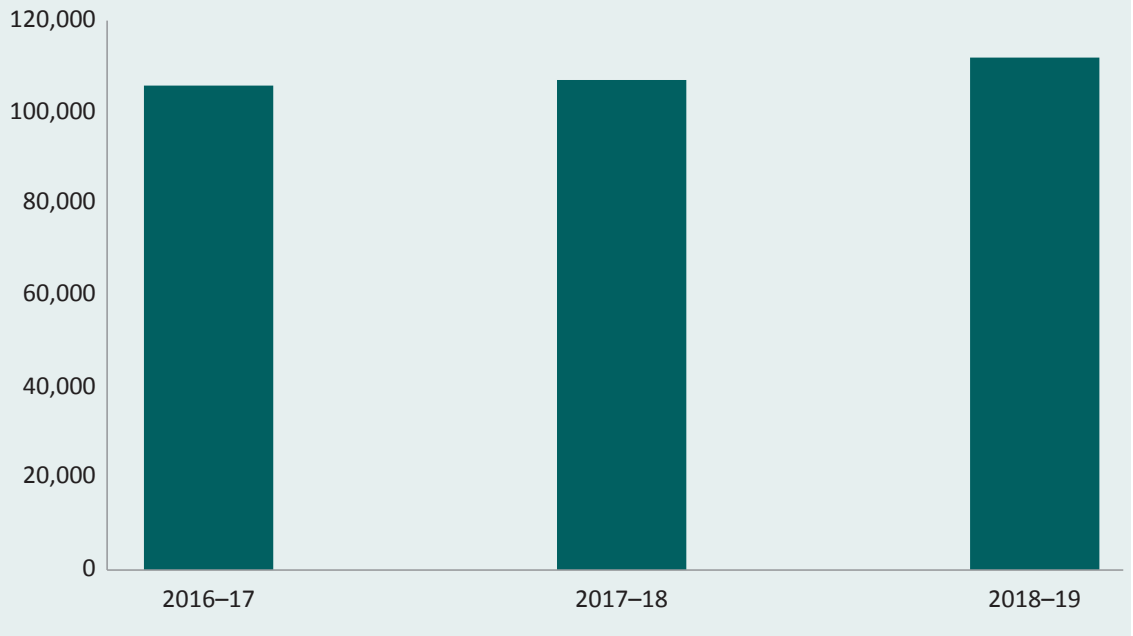
Key finding: recent Australian surveys have found a significant increase in the proportion of people experiencing and reporting identity crime and misuse of personal information. The latest Identity Crime and Misuse in Australia survey (Franks & Smith 2020) found the number of respondents experiencing misuse in the previous 12 months remained steady between 2018 and 2019, at 11.5 percent and 11.4 percent respectively.

Australian Bureau of Statistics surveys

The ABS conducted a number of Personal Fraud Surveys between 2007 and 2015. The ABS Personal Fraud Survey for 2014–15 is considered the most authoritative of its kind as it asked respondents about their experiences of card fraud, identity theft and scams in the 12 months preceding the survey—three crime types that potentially involve misuse of personal information and identity crime. However, recent surveys conducted by the AIC offer more up-to-date data on the ever-evolving world of cybercrime. The total personal fraud victimisation rate for the ABS 2014–15 survey was only 8.5 percent (ABS 2016). The most recent AIC survey found an 11.4 percent victimisation rate within the last 12 months and 24.6 percent over the person's lifetime (Franks & Smith 2020).

The number of identity crime offences finalised, as recorded by the ABS, is trending upwards, confirming that identity crimes are becoming more prevalent in Australian society (Figure 20).

Figure 20: Identity crime offences finalised, as recorded by the ABS, 2016–17 to 2018–19



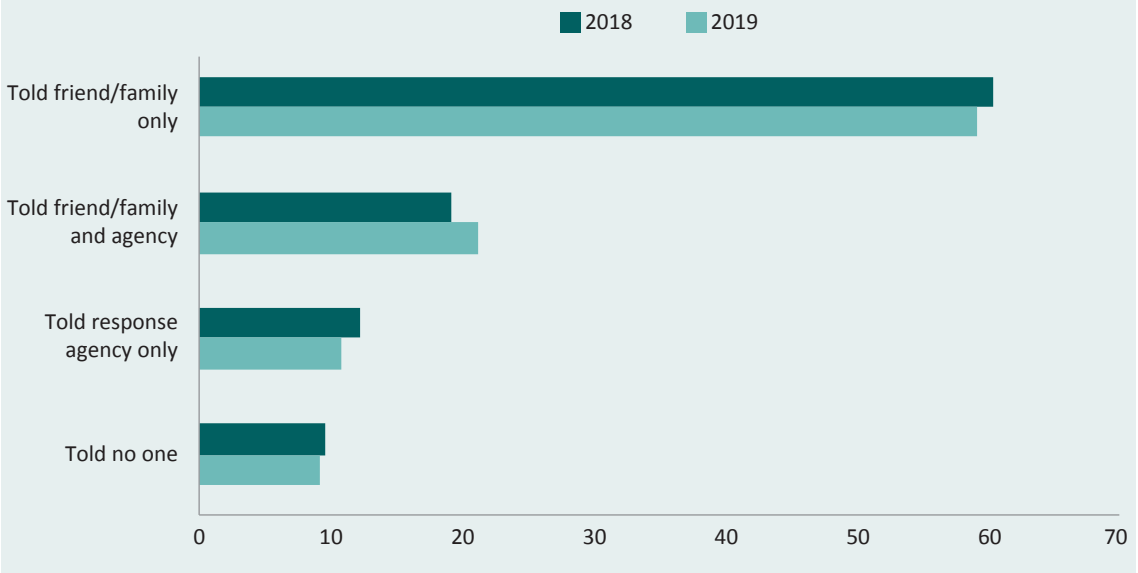
Source: ABS 2020 (unpublished data)

Reporting of identity crime

Key finding: the AIC's 2019 identity crime survey found the overall proportion of respondents who reported their victimisation experience to law enforcement, a government agency or non-government organisation stayed constant at 31 percent between 2017–18 and 2018–19 (Franks & Smith 2020). This means nearly 70 percent of victims are not officially reporting these crimes.

Under-reporting of cybercrimes obscures the true impact of those crimes, including those specific to personal information. The National Cyber Security Centre, a division of the National Crime Agency (NCA) in the United Kingdom, found under-reporting of cybercrime is a continuing problem, with the majority of victims (62%) lacking confidence in law enforcement's response to their offence claims (NCA 2018). Similar sentiment is found in Australia. The AIC's 2019 identity crime survey () found 25 percent of respondents did not report compromised credentials to law enforcement because they believed the authorities would not do anything. The majority of victims confided solely in friends and family, if anyone.

Figure 21: Respondents not reporting misuse of personal information to authorities, 2018 and 2019 (%)

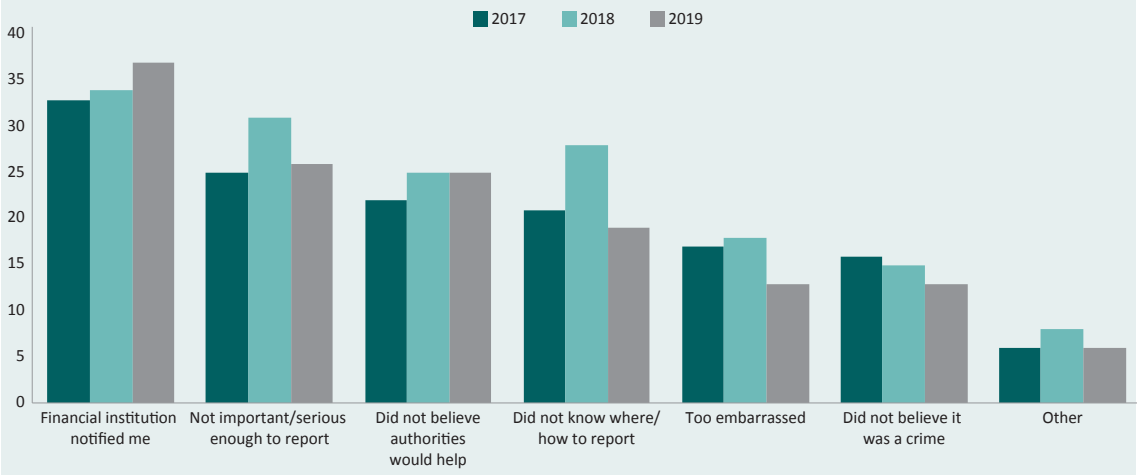


Note: Data weighted by age/gender

Source: Jorna, Smith & Norman 2020; Franks & Smith 2020

Respondents in the AIC's 2019 identity crime survey (Franks & Smith 2020) who indicated they had not reported the misuse of their personal information to police, government agencies or businesses were asked why they had not reported. The most common reason given was that their bank or other financial institution had notified them of the issue which they then felt had been resolved (37% of respondents who did not report). The next most common reason was that the respondent did not think it was important enough to report (26%). Another 19 percent of respondents stated the primary reason for not reporting was not knowing to whom they should report the incident. This difficulty in locating an organisation that could help may affect individuals' satisfaction with services and ultimately contribute to under-reporting of identity crime.

Figure 22: Reasons victims did not report misuse of personal information, 2017 to 2019 (%)

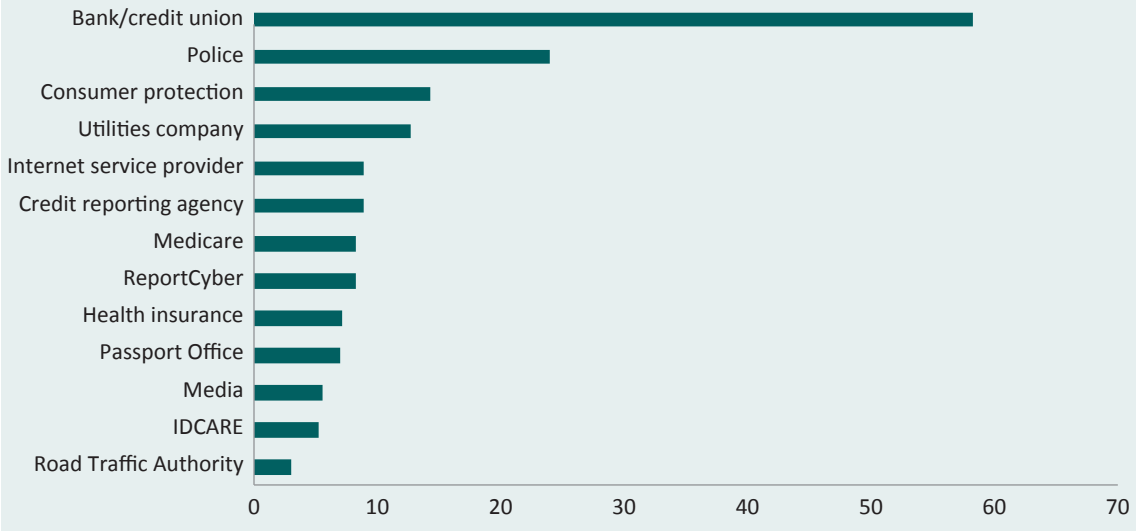


Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Respondents who did report misuse of personal information to a government agency, business or other organisation were asked to specify the entity to which they reported the misuse (Figure 23). The majority of respondents reported to a bank, credit union or credit/debit card company (58% of respondents who reported the incident). The police were the next most common agency respondents reported misuse of their personal information to (24%).

Figure 23: Respondents who reported misuse of personal information by organisation reported to, 2019 (%)



Note: Data weighted by age/gender

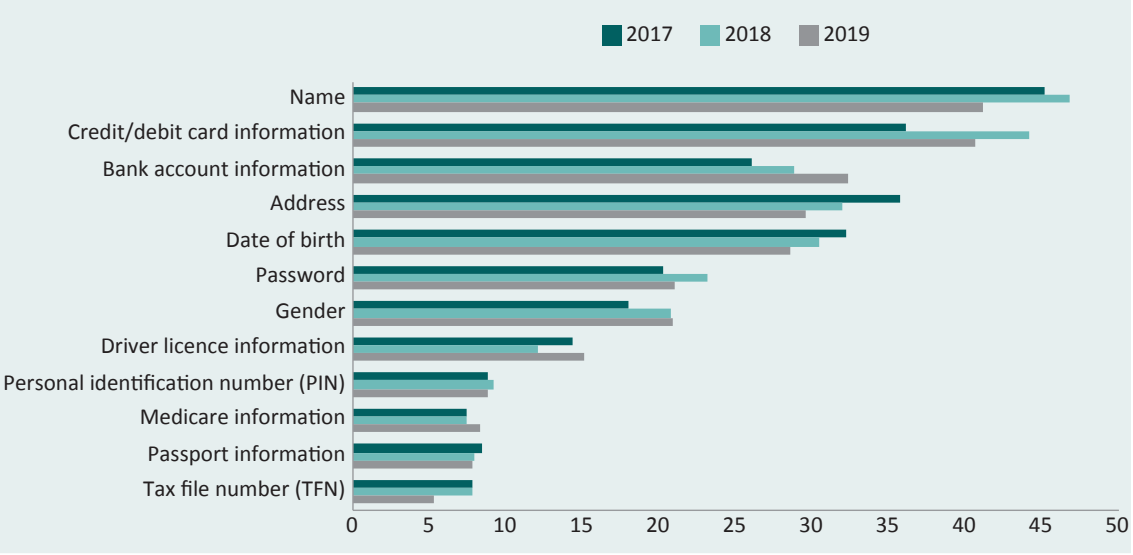
Source: Franks & Smith 2020

Personal information at risk of misuse

Key finding: survey research confirms that the types of personal information most at risk of misuse are those used in connection with financial transactions—particularly names, addresses, dates of birth and bank card or account details. Credentials issued by government agencies, such as passports and tax file numbers, were misused less than the underlying information needed to enrol with these agencies.

Respondents to the AIC's surveys were asked to indicate the types of personal information they believed had been misused on the most serious occasion of identity crime they had experienced in the preceding 12 months. In 2019, names, credit/debit card information, bank account information, addresses, and dates of birth were most often misused (Figure 24).

Figure 24: Types of personal information reported as misused on the most serious occasion in the previous 12 months, 2017 to 2019 (%)



Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Case study 10: Using security footage to detect identity crime

On 24 May 2019 a digital currency exchange reported suspicious behaviour relating to security footage of the customer not matching the identification used to withdraw funds. The exchange provider received online applications for customer accounts in the names of three women. Upon monitoring these accounts, the exchange provider recognised that these women's accounts were being used by a man, whose credentials were hidden during the transactions. The man was wearing a cap, ensuring his face could not be captured by the vending machine camera.

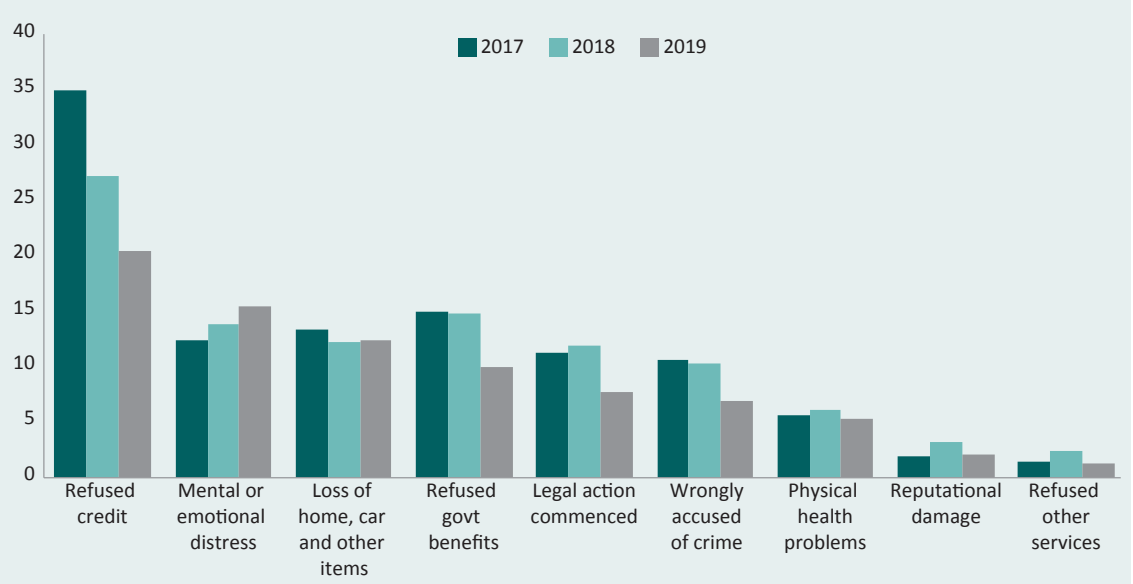
Source: AUSTRAC 2019 (unpublished data)

Non-financial impact

Key finding: the three most prevalent consequences of identity crime and misuse that victims reported in the most recent AIC survey were being refused credit, mental/emotional distress and loss of home, car or other items.

Mental and 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 process of responding to identity crime is complex and difficult to navigate and only exacerbates the psychological trauma.

Figure 25: Consequences experienced as a result of personal information being misused in the previous 12 months, 2017 to 2019 (%)



Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Remediation of identity crime

Key finding: the process of recovering misused personal information and restoring one's identity is often complex, difficult and time consuming. The amount of time victims spend dealing with the consequences of misuse of personal information has increased steadily since the AIC identity crime survey began in 2013, when respondents reported taking an average of 18 hours. In both the 2018 and 2019 surveys, the time taken was nearly double the 2013 amount.

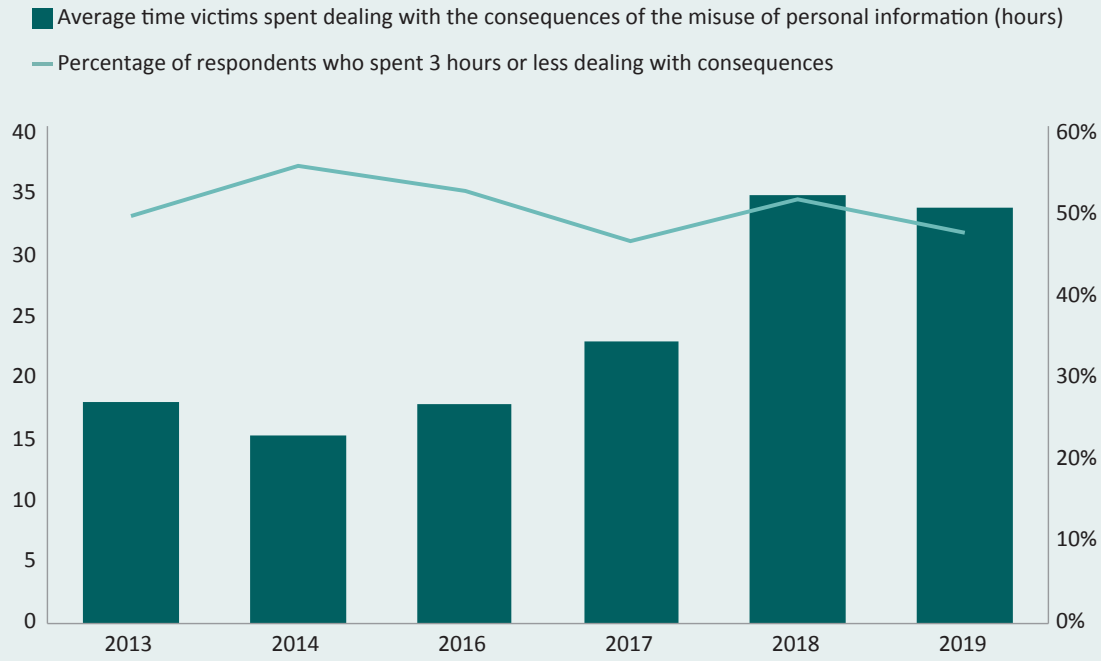
Identity crime is the only crime type that requires individuals not only to report their victimisation to a law enforcement agency but also to financial institutions, government regulators, telecommunications companies, internet service providers, utilities companies and credit reporting agencies. Victims must keep track of these reports and contact credit reporting agencies directly to apply for credit bans, which in Australia must be re-applied for every three months. A credit ban will temporarily halt all credit-issuing enquiries relating to a named individual, which temporarily stops criminals from borrowing money in the victim's name. There are also three separate credit reporting agencies that must be contacted individually to ensure all financial pathways to the criminal are closed. Victims incur not only the costs associated with the actual identity compromise and misuse but costs associated with replacing identification documents and bank cards, and the cost of other services such as identity protection as well as lost work hours and potentially medical and/or psychological treatment fees.

Time spent restoring identity information

The amount of time it takes for a victim to deal with the consequences of identity crime varies depending on the extent to which identity credentials were misused. In cases involving fraudulent credit applications or bank transactions, victims incur only minimal inconvenience and financial impost, as financial institutions generally refund losses to individual victims. Rectifying more serious cases, such as those involving a complete takeover of a victim's identity, can take many hours over a period of months or even years.

The AIC's surveys have found that victims of misuse of personal information spend increasingly long periods of time responding to their victimisation—varying from an average of 15 hours in 2014 to an average of 35 hours in 2018. The percentage of victims who were able to resolve the matter quickly (less than 3 hours) has remained steady at around 50 percent (Figure 26).

Figure 26: Time spent by victims dealing with consequences of misuse of personal information, 2013 to 2019

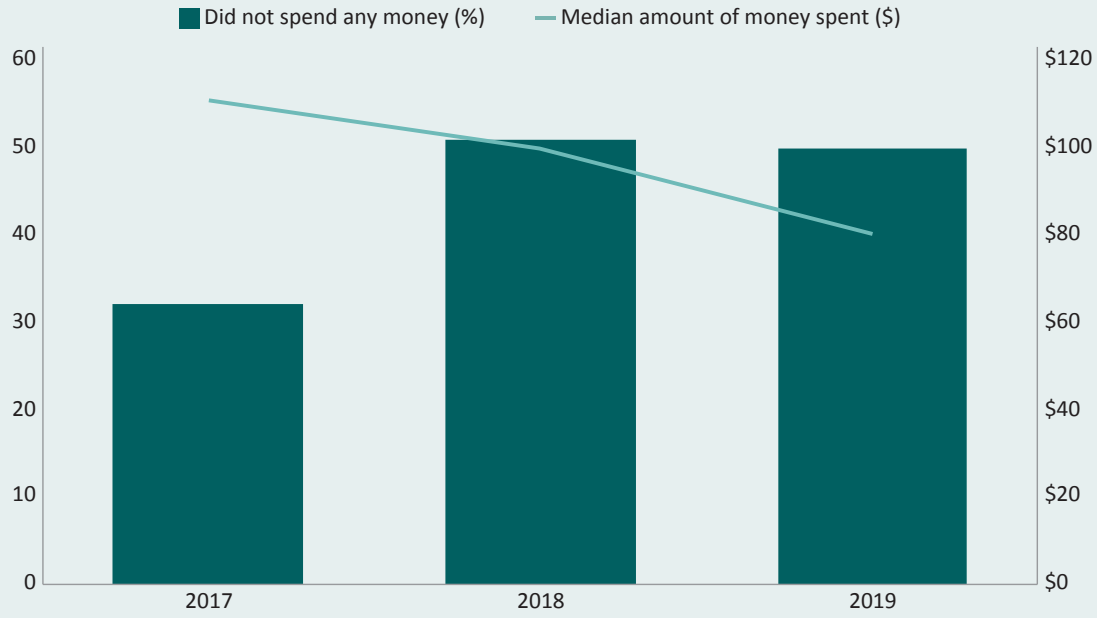


Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender

Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

The AIC surveys (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman; Franks & Smith 2020) also collected data on how much money victims spent dealing with the consequences of the misuse of personal information (Figure 27). The 2019 survey found slightly under a half of the respondents did not spend anything, while the median amount spent was $80. This amount does not include the value of victims' time spent dealing with the consequences of misuse which can equate to substantial amounts through loss of wages.

Figure 27: Amount of money victims spent dealing with the consequences of misuse of personal information, 2017 to 2019



Note: Data weighted by age/gender

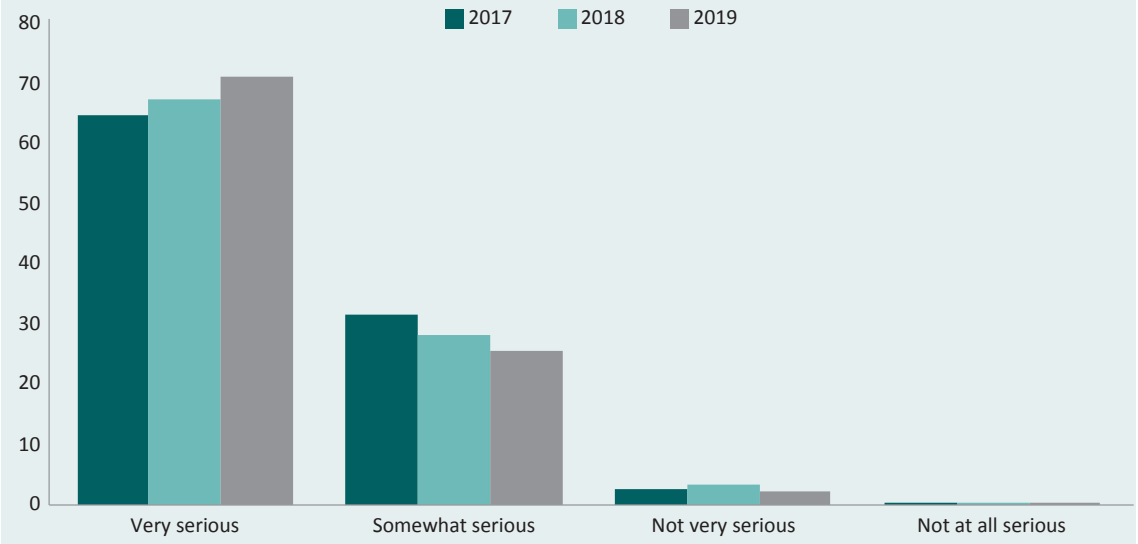
Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Perceptions of seriousness

Key finding: identity crime remains an ongoing concern for the Australian public. In 2019, 98 percent of survey respondents indicated that misuse of personal information was, in their view, 'very serious' or 'somewhat serious'.

Respondents to the AIC surveys were asked to provide their opinion as to the seriousness of misuse of personal information in terms of harm to the Australian community. Although not experts in identity crime, respondents were able to give their personal assessment of the seriousness of the problem in Australia at the time of the survey. Most respondents (over 95% each year) believed that misuse of personal information was 'very serious' or 'somewhat serious' (Figure 28).

Figure 28: Perceived seriousness of misuse of personal information (%)

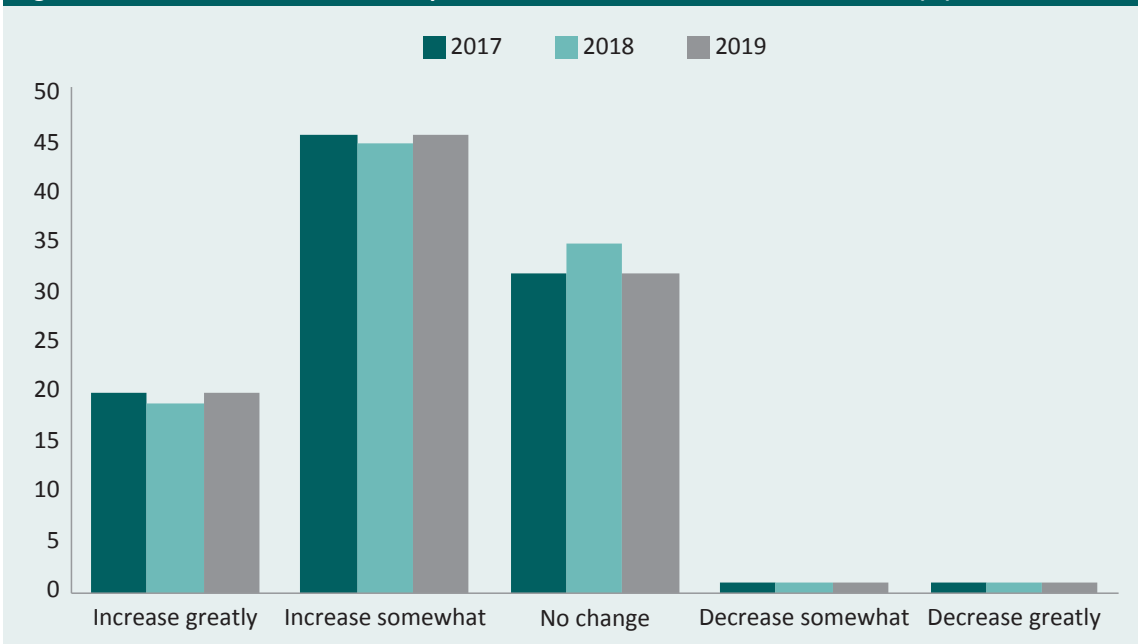


Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Respondents were also asked to indicate whether they thought the risk of someone misusing their personal information would change over the next 12 months. The majority of respondents (63%) believed their risk of becoming a victim of identity crime would increase over the next 12 months (Figure 29).

Figure 29: Perceived risk of misuse of personal information in the next 12 months (%)



Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Psychological impact of identity crime on victims

Javelin Strategy & Research's *2018 Identity fraud report* (cited in Sontiq 2019) estimates there are two new victims of identity crime every second. This report also estimates that more than one million children become victims of identity theft each year (Sontiq 2019). The financial and economic implications of identity crime have been well documented. Less focus has been placed on the emotional, psychological, physiological and socio-economic impacts that victims experience, despite long-term repercussions being apparent from prior research.

Identity theft is the only crime that requires a victim not only to report the offence to multiple organisations but also to keep track of the progress of their claims with each organisation. White-collar crime victims suffer psychological and medical issues as serious as those experienced by victims of street-level crime: anxiety, depression, distress, anger, helplessness, insecurity, betrayal, self-blame, suicidal ideation, and illness (Dodge 2020). The Identity Theft Resource Center (2018) reported emotional impacts of identity crime as having left victims with overwhelmingly negative feelings of frustration (86%), having been violated (84%), feeling lack of trust and unsafe (69%), powerless and helpless (67%) and sad and depressed (59%). These negative emotional impacts often lead to physiological consequences such as sleep problems (84%), stress reactions (77%), stomach issues (57%) and fatigue (55%) (Identity Theft Resource Center 2018).

A University of Texas at Austin (2019) report details how emotional trauma ranging from medium to high levels is the most frequently reported experience among victims of identity crime. Financial loss, property loss and reputational damage report were all less common than emotional distress (University of Texas at Austin 2019).

The journey through the victim response system also has a direct effect on the psychological and physiological health of those forced to deal with the consequences of identity crime. When a victim of identity crime contacts an organisation in an attempt to rectify their situation, the way in which the organisation responds can have either positive or negative impacts on the victim. Customer service representatives need effective training in how to recognise and respond to the complexity of identity crime to ensure victims feel their case is being well managed.

Victim support

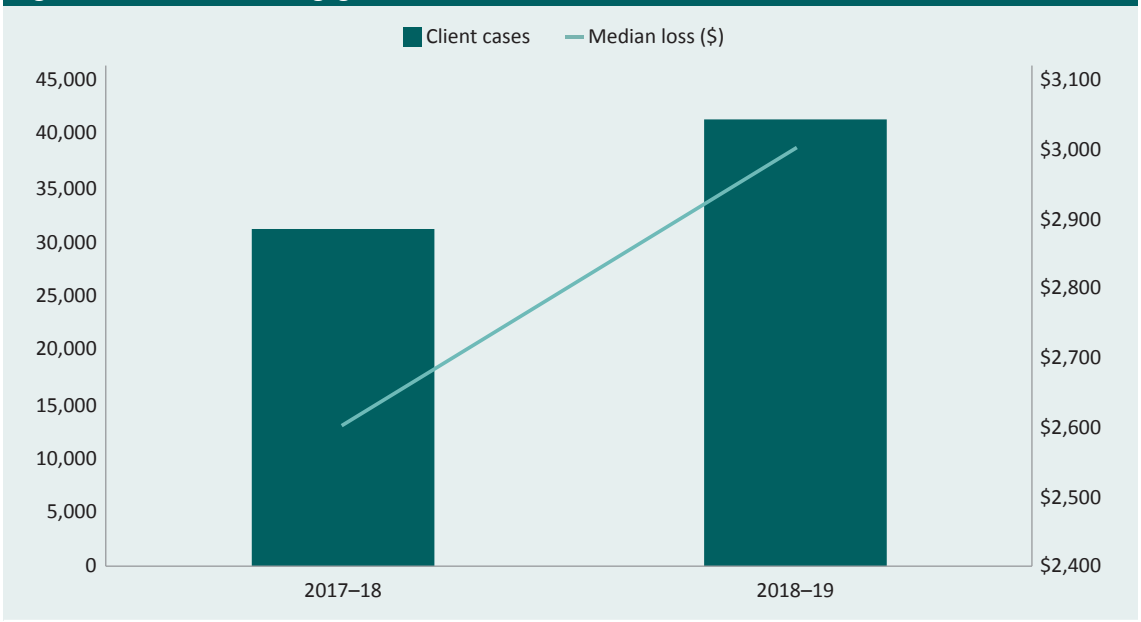
Key finding: victims of identity crime and misuse can seek assistance from a number of public and private sector agencies. Some of these agencies refer complaints to law enforcement and regulators, while others seek to support victims and help them recover funds and restore their identity credentials, some without charge and others for a one off or monthly fee.

IDCARE

IDCARE is a not-for-profit support service for victims of identity crime in Australia and New Zealand. It was launched in Australia in 2014 and New Zealand in 2015 and receives referrals from various organisations concerning victims of identity crime. It provides support in the form of counselling and assistance in recovering lost funds and identity credentials.

In 2018–19, IDCARE responded to 41,395 client engagements from individuals in Australia and New Zealand who had experienced compromise or misuse of their personal information (IDCARE 2020), an increase of 33 percent on the previous year. IDCARE (2020) found the average response time for victims was 36 days with a mean loss of $18,165 per client. The median losses, presented in Figure 30, were much lower.

Figure 30: IDCARE client engagements and median losses, 2017–18 and 2018–19



Source: IDCARE 2019 (unpublished data)

Australia's identity theft response system

A recent study examined Australia's identity theft response system based on a 12-month period of repeated engagement with 211 individual victims of identity compromise and misuse who 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 after their identities had been compromised (Wyre, Lacey & Allan 2020).

Traditional crime response agents such as law enforcement were viewed as being particularly ineffective by individuals required to gather evidence on their own behalf (Wyre, Lacey & Allan 2020). Organisations in which identities are used and potentially misused also have a role in detecting identity theft and acting against this form of crime (Cuganesan & Lacey 2003; Wyre, Lacey & Allan 2020). These organisations put effort into prevention strategies, but are frequently inadequate when responding to individual victims.

The Australian identity response system also displayed disjointed and conflicting communications, forcing victims into a response loop where industry and government actors required contrary or opposite processes (Wyre, Lacey & Allan 2020). Wyre, Lacey and Allan (2020) suggest the following improvements to Australia's identity theft response system:

- development of a national identity policy, including minimum response standards;
- A consumer-consent driven model for capture and rapid transfer of information;
- a review of credit reporting and credit ban arrangements to identify consumer driven efficiencies; and
- the establishment of an enhanced identity-cyber-scam integrated crime reporting and supporting network that streamlines data sharing.

Consumer protection agencies

The AIC's 2019 survey (Franks & Smith 2020) found that, of those respondents who had reported the misuse of their personal information, 14 percent had made a report to a Commonwealth consumer protection agency such as Scamwatch, which is operated by the ACCC.

Data were requested from all state and territory consumer affairs or fair-trading agencies about the number of suspected identity crime and misuse enquiries or complaints they had received, although responses were provided by only three organisations (Table 7). These agencies clearly received far fewer enquiries about identity crime than Commonwealth bodies and IDCARE, supporting the AIC's 2019 survey finding that 19 percent did not know who to report to.

Table 7: Enquiries to consumer protection agencies regarding identity crime and misuse, 2015–16 to 2018–19 (*n*)

	2015–16	2016–17	2017–18	2018–19
New South Wales Fair Trading	21	26	13	10
Consumer Affairs Victoria	50	61	75	64
Queensland Office of Fair Trading	0	3	1	1

Source: Consumer Affairs Victoria (unpublished data); New South Wales Fair Trading (unpublished data); Queensland Office of Fair Trading (unpublished data)

Office of the Australian Information Commissioner

The OAIC received 8,864 enquiries from the public relating to the Australian Privacy Principles in 2018–19, up from 8,093 in 2017–18 (OAIC 2019). These included complaints relating specifically to Privacy Principle 6, which is about the use or disclosure of personal information.

Case study 11: Remote access scam

An IDCARE client received an unsolicited call claiming to be from a major telecommunications carrier. The caller stated that the client's internet security had been compromised. The client was instructed to run a check on their computer that came back with supposedly compromised results. They were then told to download software to allow remote access.

The client was then locked out of their computer and received an SMS notifying them that funds had been withdrawn from their spouse's bank account. When the client questioned this, the caller said they were working with the Australian Government and it was a false transaction to try to trap hackers. The scammers then opened a cryptocurrency account online using the client's credentials and transferred money to this and other unknown accounts. The call lasted several hours and involved multiple transactions before ending abruptly. Legal documents on the client's computer had also been accessed.

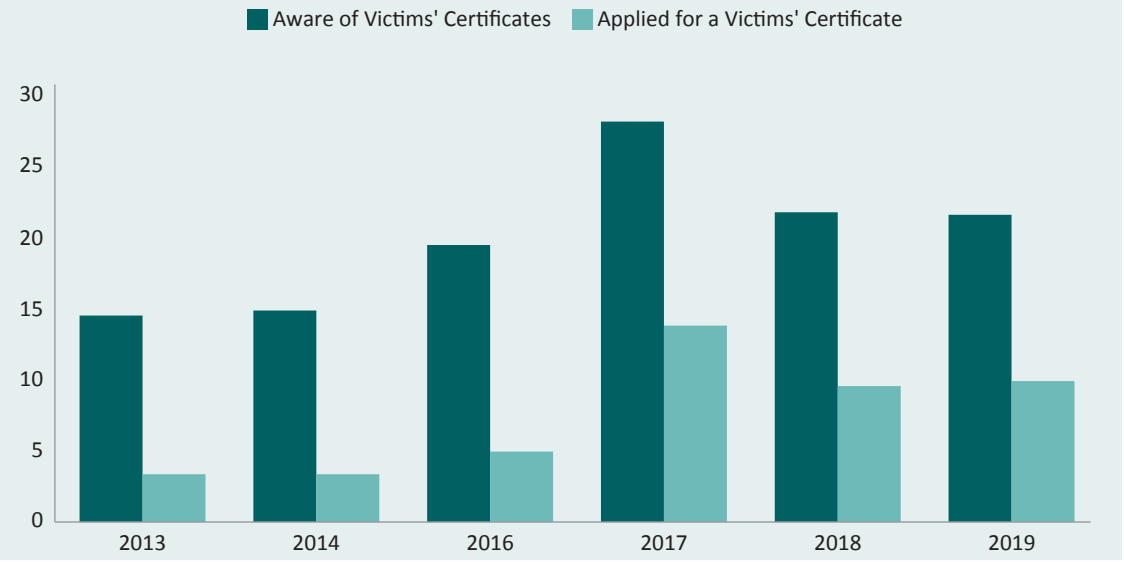
Source: IDCARE 2020 (unpublished data)

Victims' Certificates

Key finding: Commonwealth Victims' Certificates remain under-utilised, but the proportion of survey respondents who reported being aware of such certificates has increased since the AIC surveys began in 2013.

Findings of the AIC's identity crime surveys indicate awareness of Commonwealth Victims' Certificates in 2019 remained consistent with 2018 figures (Franks & Smith 2020). While not all states and territories issue certificates to victims of fraud and identity crime, there is a now a Commonwealth Victims' Certificate that victims can apply for, issued by the Federal Circuit Court. Victims can present these certificates to government agencies, financial institutions or credit agencies to prove they have been a victim of identity crime. Victims' Certificates may help individuals resolve business or personal affairs, although at present their use is minimal.

Figure 31: Awareness of Victims' Certificates, 2013 to 2019 (%)



Note: 2013 and 2014 data weighted by location and 2016 to 2019 data weighted by age/gender

Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Prevention of identity crime

Of all the AIC's 2019 survey respondents, 98 percent indicated that harm to the Australian community caused by the misuse of personal information is a serious issue whether or not they had experienced having their credentials compromised. Accordingly, preventing such crime is an important consideration for policymakers to address. A wide range of preventive measures are available to government agencies, businesses and the general public to mitigate the risk of identity crime or the misuse of personal information.

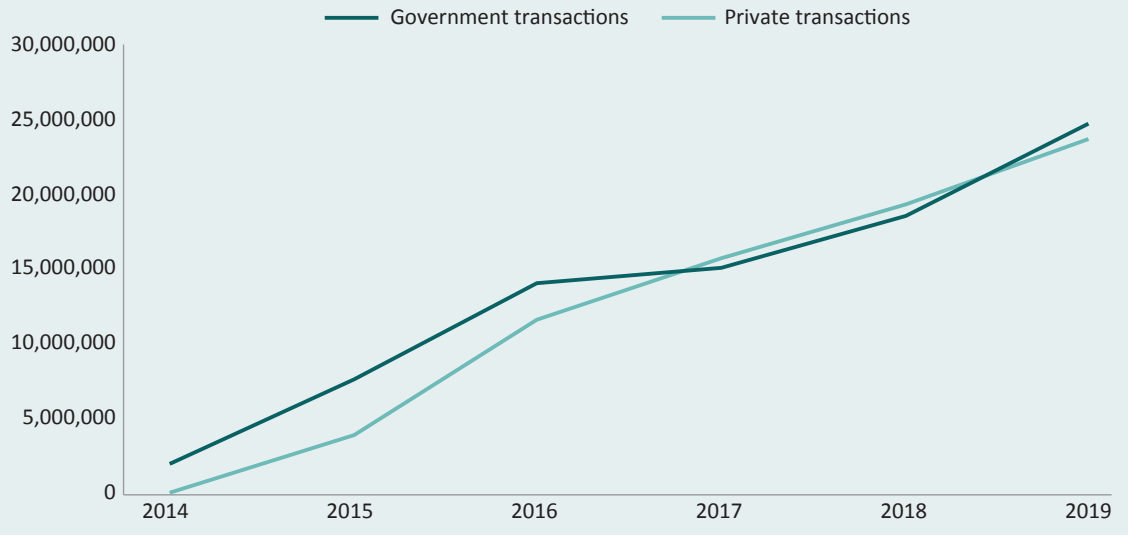
Document Verification Service

Key finding: the number of government entities and private sector agencies using the Document Verification Service (DVS) continues to increase annually, as does the number of transactions requested by those organisations.

The DVS is one of the key initiatives of the Council of Australian Governments' National Identity Security Strategy. It allows organisations to compare information from a person's identity document, with their consent, to the corresponding record of the agency that issued the document. These checks are conducted in real time to inform decisions that rely upon the confirmation of a person's identity. It is a key tool for organisations seeking to prevent the enrolment or registration of customers, clients or even staff who may be using fraudulent identities. The DVS can be used to verify information relating to most government-issued identity credentials, including the four credentials identified in this report as being most at risk of misuse: Medicare cards, driver licences, birth certificates and passports.

Since 2014, there has been a large increase in use of the DVS, with 908 private sector organisations and 91 government entities using the service as of 30 June 2019 (Figure 32). This is an increase of 77 percent and 15 percent respectively.

Figure 32: DVS users and government and private sector transactions, 2014 to 2019 (*n*)

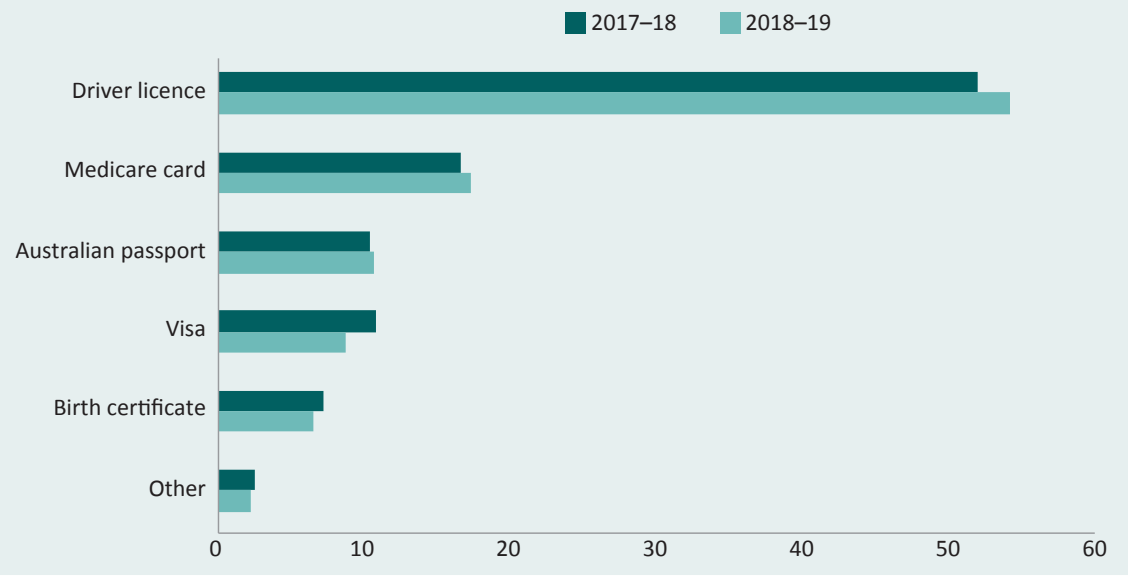


Source: Department of Home Affairs 2019 (unpublished data)

Identity credentials verifiable

Since 2014 the DVS has been available to government agencies and private sector organisations. Figure 33 presents the main types of documents verified using the DVS in 2017–18 and 2018–19.

Figure 33: Documents verified using the DVS, 2017–18 and 2018–19 (%)



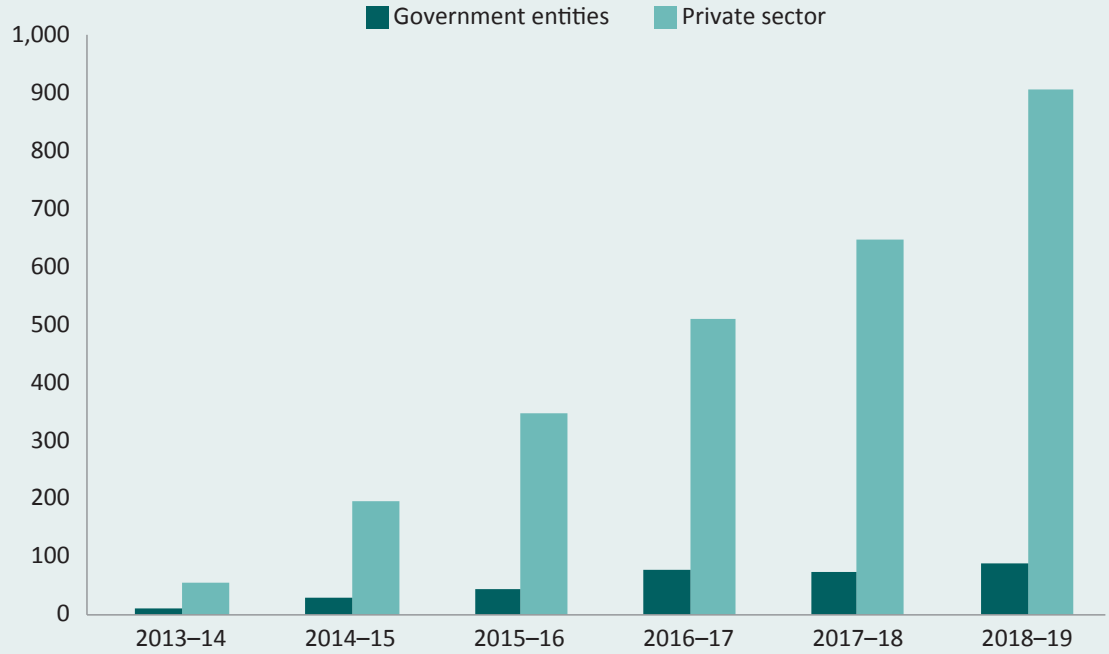
Note: 'Other' includes ImmiCards, marriage certificates, citizenship certificates, change of name certificates and registration by descent certificates

Source: Department of Home Affairs 2019 (unpublished data)

Organisations using the service

Private sector organisations were given access to the DVS from 2014, explaining the sharp increase in the number of organisations accessing the DVS in the last few years. The number of private sector agencies using the DVS increased 40 percent between 2017–18 and 2018–19, from 650 to 908 (Figure 34). That is a 77 percent increase since 2016–17, when only 513 private organisations were using the DVS.

Figure 34: Number of agencies using the DVS, 2012–13 to 2018–19 (*n*)



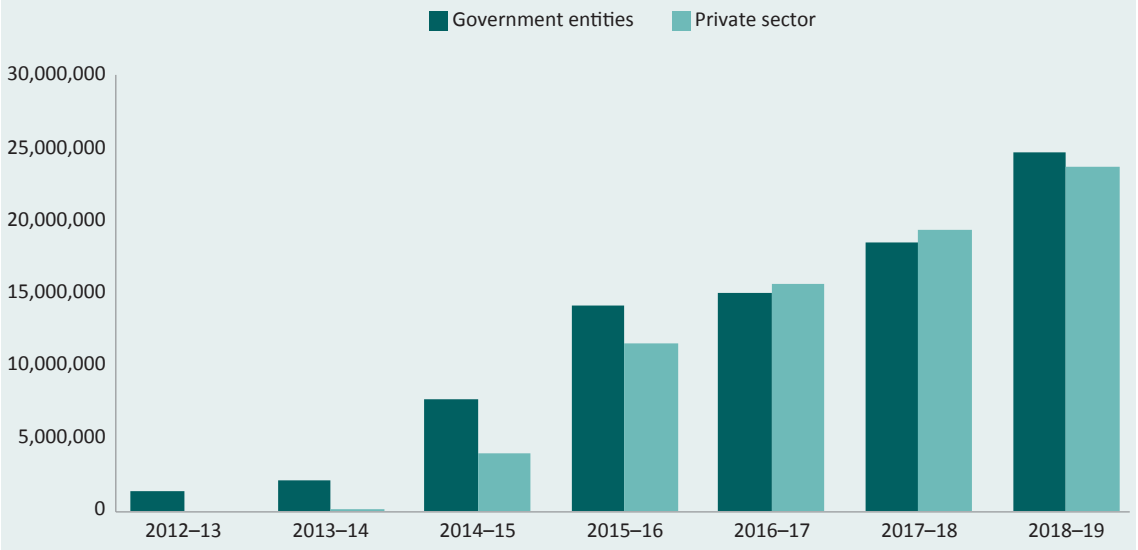
Note: Private sector access to DVS available from 2014

Source: Department of Home Affairs 2019, 2017 (unpublished data)

The number of transactions each year

In 2018–19, the number of transactions attributed to government entities was larger than the number attributed to private sector organisations for the first time since 2015–16 (Figure 35). This increase may be attributable to Australian government organisations not subject to competitive neutrality guidelines having the flexibility and convenience of a direct connection to the DVS. Government users subject to competitive neutrality and private organisations are both required to connect to the DVS through a more expensive gateway service with potential lag times.

Figure 35: DVS transactions, 2012–13 to 2018–19 (*n*)



Note: These figures include repeat transactions, for example where data entry errors occur. Some validation attempts involve numerous transactions. Private sector access to DVS available from 2014

Source: Department of Home Affairs 2019, 2017 (unpublished data)

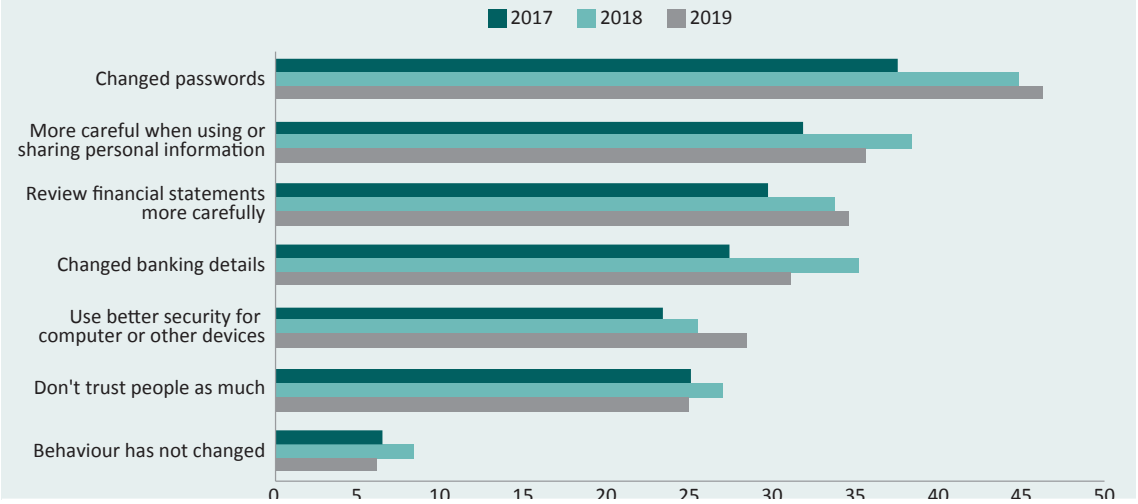
Identity crime prevention practices

Key finding: Cybercriminals have begun using a 'living off the land' technique to maintain a low digital profile, hiding illegal network access activity in a mass of legitimate processes (Symantec 2019).

Individuals

The AIC's identity crime and misuse surveys asked respondents who had experienced misuse of their personal information in the last 12 months if they had changed their behaviour following the misuse. The most common behavioural change reported was changing passwords, followed by becoming more careful when using or sharing personal information (Figure 36).

Figure 36: Behaviour changes arising from the misuse of personal information, 2017 to 2019 (%)



Note: Data weighted by age/gender

Source: Goldsmid, Gannoni & Smith 2018; Jorna, Smith & Norman 2020; Franks & Smith 2020

Businesses

Cyberthreats to organisations are becoming increasingly sophisticated and targeted. Information that organisations hold or have access to, if compromised, can provide adversaries with significant political, military or economic gains. It is important for businesses to be aware of the risks they face and implement appropriate prevention practices.

Although defences have gradually improved, cybercriminals have kept pace by adapting their tradecraft and tools to circumvent enhanced security practices (ACSC 2017). Financial institutions are still the number one target for cyber attacks and it is estimated they invest three times more in cybersecurity than non-financial institutions (McAfee 2018).

Formjacking is the use of malicious JavaScript code to steal credit card details and other information from payment forms on ecommerce sites and has been trending upward since 2018 (Symantec 2019). The surge of formjacking reinforces how the supply chain can be a weak point for online retailers, with attackers compromising third-party services such as chatbots or customer review widgets to gain access to networks (Symantec 2019). Those organisations using third-party services should consider investing in additional security tools designed for that specific risk.

PowerShell is a task automation and configuration management framework from Microsoft consisting of a command-line shell and associated scripting language. It is now a staple of both cybercrime and targeted attacks. As a result, a notable cybercrime trend that began to emerge in 2018 is the use of a 'living off the land' technique to maintain a low digital profile, hiding illegal network access activity in a mass of legitimate processes. Those 'living off the land' use off-the-shelf tools and operating system features to conduct their attacks (Symantec 2019). A method of combatting 'living off the land' cybercriminals is through maintaining up-to-date software that enables consistent and regular monitoring of dual-use tools within a network (Symantec 2019).

The popularity of business email compromise continues as criminals perfect their ability to exploit victims through their use of increasingly sophisticated techniques that combine social engineering, email phishing, email spoofing and malware (NCA 2018). Business email compromise employs identity theft as a means to impersonate a company's CEO, CFO or other staff member with accounts access to reroute financial transfers into criminal accounts. This form of identity crime is difficult for banks to detect and prevent because the transactions are submitted by a legitimate, authorised employee of the customer. Companies are reluctant to report these crimes and would rather absorb losses than lose face with their clients (McAfee 2018). Criminals are becoming more and more patient in executing business email compromise for optimum profit, inserting themselves into conversations centred around payments to gain a position of trust before rerouting funds (Verizon 2019). This is usually accomplished using 'living off the land' techniques and can be combatted with continued network maintenance. It is also imperative that organisations employ a security policy that educates their employees on the importance of recognising and deleting suspicious emails and safe practice of not clicking on unknown links or attachments.

Cybercrime as a service (CaaS) is a flourishing market of tools and services including exploit kits, custom malware, botnet rentals and ransomware distribution, which has become so popular it rates its own moniker: ransomware as a service (RaaS; McAfee 2018). The diversity and volume of cybercrime available continues to grow with no indication of slowing down. To combat these innovative criminal contractors, Biometrics as a Service (BaaS) has begun, offering smaller businesses a cost effective option for employee, contractor and client verification.

Case study 12: Business email compromise

During 2018–19, the Department of Industry, Innovation and Science became an unsuspecting, secondary victim of business email compromise. The business email of a grant recipient had been compromised. The department received an email purporting to be from the grant recipient asking for bank account details to be changed. Grant money owed was then paid to the new account. The grant recipient asked where the payment was and denied any person from their organisation had contacted the department to have bank account details changed.

Source: Department of Industry, Innovation and Science 2019 (unpublished data)

Government agencies

Australia's 2020 Cyber Security Strategy: A call for views, issued by the Department of Home Affairs (2020), recognises the continued growth in the scale and severity of malicious cyber activity in Australia. The report acknowledges the value cybercriminals place on personal information and points out the growing organisation, confidence and sophistication developing within the cyber realm. As Australia's critical systems, including energy, telecommunications and transport sectors, are becoming increasingly digitised, threats to Australia's physical safety, economic security, and the continuity of government and its services are increasing (Home Affairs 2020). It is imperative that government agencies keep up with the increased knowledge and sophistication of those who instigate malicious cyber activity.

The Australian National Audit Office (ANAO) undertook an independent performance audit of the Australian Postal Corporation, ASC Pty Ltd, and the Reserve Bank of Australia (ANAO 2019). This report found that despite the importance of cybersecurity in safeguarding the Australian government's digital information, there were ongoing low levels of cyber resilience among non-corporate Commonwealth entities and weaknesses in the regulatory framework for ensuring compliance with mandatory cybersecurity strategies (ANAO 2019). The results of this audit determined that both the Reserve Bank and ASC had effectively managed cybersecurity risks while Australia Post had not and should continue to implement a cybersecurity improvement program with key controls across all of its critical assets (ANAO 2019). This audit examined only three agencies and a third were found non-compliant. With the increased intelligence and capabilities of cybercriminals, all organisations should undertake regular audits to reduce their risk of and vulnerability to cybercrimes.

Identity Theft Protection Services

Sontiq's (2019) *Identity protection market research report* states more than 81 percent of consumers agree their identity is the most important thing they own, with nearly 75 percent willing to pay up to $25 per month for identity theft protection services. Identity resolution tops the list of 'must-have' capabilities for identity theft protection, with 98 percent of consumers surveyed stating they also employ multiple personal safety measures to shield their identity, including close review of financial statements, shredding of personal documents, identification monitoring tools, and annual credit reports (Sontiq 2019).

Identity protection services are growing in popularity as a result of victims finding themselves left to restore their own identities through a multitude of complex paperwork, emails, telephone calls and face-to-face meetings. Most consumers feel government and breached organisations should share the responsibility of managing identity recovery, but this is not the reality.

Conclusion

Identity crime and misuse of personal information remains an ongoing concern for the Australian community. The latest survey conducted by the AIC showed the percentage of respondents experiencing identity crime remained consistent with the previous year with no indication of decline. With the rapidly increasing sophistication of cybercriminals and the easy monetisation of personal information online, it is likely identity crimes will increase in frequency over the long term.

The goal of this report was to assess the nature, extent and impact of identity crime in Australia by presenting a range of quantitative and qualitative information from government, businesses and individuals. A large number of Commonwealth, state and territory government agencies provided data for the report, and it was only with the assistance of these agencies and private sector organisations such as IDCARE that the extent of the problem could be described. Further research is, however, needed to understand the true extent of identity crime, particularly through improved official statistics, increased private sector data collection, and further surveys of members of the public.

Addressing the concerns and challenges raised by identity crime requires a collaborative and sustained effort by government agencies and private sector organisations. Despite advances in the verification of credentials and improvements in online authentication procedures, victimisation continues. Financial losses also continue to rise, as do the equally harmful and ongoing non-financial consequences of psychological harm and resulting physiological manifestations of that harm. Continued monitoring of these trends will help identify changes in identity crime methodologies and assess the benefits derived from and risks associated with crime prevention initiatives.

References

URLs current as at May 2020

Anti-Phishing Working Group 2019. *Phishing activity trends report: 3rd quarter 2019*. https://apwg.org/trendsreports/

Attorney-General's Department (AGD) 2016. *Identity crime and misuse in Australia 2016*. Canberra: Attorney-General's Department

Audit Office of New South Wales (Audit Office) 2020. *Integrity of data in the births, deaths and marriages register*. New South Wales Auditor-General's Report. https://www.audit.nsw.gov.au/our-work/reports/integrity-of-data-in-the-births-deaths-and-marriages-register

Australasian Centre for Policing Research 2006. *Standardisation of definitions of identity crime terms: A step towards consistency*. Report Series no. 145.3. Adelaide: Australasian Centre for Policing Research

Australian Border Force (ABF) 2020. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Bureau of Statistics (ABS) 2020. Customised report. Data provided by National Centre for Crime and Justice Statistics. Melbourne: ABS. Unpublished data

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

Australian Bureau of Statistics 2013. *Australian demographic statistics, Dec 2012*. ABS cat. no. 3101.0. Canberra: ABS. https://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

Australian Capital Territory Policing 2019. AFP PROMIS apprehensions module: National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Capital Territory Policing 2017. AFP PROMIS apprehensions module: National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Communications and Media Authority (ACMA) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Competition and Consumer Commission (ACCC) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Competition and Consumer Commission 2018. Scamwatch online reporting service. https://www.scamwatch.gov.au/

Australian Competition and Consumer Commission (ACCC) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Cyber Security Centre (ACSC) 2019. *Cybercrime in Australia: July to September 2019*. Canberra: ACSC. https://www.cyber.gov.au/threats/cybercrime-in-australia-july-to-september-2019

Australian Cyber Security Centre 2017. *Australian cyber security centre threat report 2017.* Canberra: ACSC. https://www.cyber.gov.au/publications

Australian Electoral Commission (AEC) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Federal Police (AFP) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian National Audit Office (ANAO) 2019. *Cyber resilience of government business enterprises and corporate commonwealth entities*. https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities

Australian Securities and Investments Commission (ASIC) 2020. Our role. https://asic.gov.au/about-asic/what-we-do/our-role/

Australian Securities and Investments Commission 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Taxation Office (ATO) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Australian Transaction Reports and Analysis Centre (AUSTRAC) 2019. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

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

Bureau of Crime Statistics and Research 2019. NSW Recorded Crime Statistics July 2015 to June 2019: National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

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

Commonwealth Director of Public Prosecutions (CDPP) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Commonwealth Director of Public Prosecutions 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Consumer Affairs Victoria 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Council of Australian Governments 2007. *An Agreement to a National Identity Security Strategy.* https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-security

Crime Statistics Agency (Victoria) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

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 Defence 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Department of Foreign Affairs and Trade (DFAT) 2020. *Annual report 2018–19.* Canberra: Department of Foreign Affairs and Trade. https://www.dfat.gov.au/about-us/publications/corporate/annual-reports/Pages/department-of-foreign-affairs-and-trade-annual-report-2018-19

Department of Foreign Affairs and Trade 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Department of Foreign Affairs and Trade 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

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

Department of Home Affairs 2019. Document Verification Service: National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Department of Home Affairs 2017. Document Verification Service: National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Department of Human Services (DHS) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Department of Industry, Innovation and Science 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

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

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

Franks C & Smith RG 2020. *Identity crime and misuse in Australia: Results of the 2019 online survey.* Statistical Report no. 27. Canberra: Australian Institute of Criminology

Global Benefits Group 2020. greenID with Australian death check. https://www.gbgplc.com/apac/greenid-with-australian-death-check/

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

IDCARE 2020. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Identity Theft Resource Center 2018. The aftermath: the non-economic impacts of identity theft. California, USA: Identity Theft Resource Center.

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

Krone T & Smith RG 2018. *Criminal misuse of the domain name system*. Research Report no. 3. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rr/rr03

Ludington S 2006. Reining in the data traders: A tort for the misuse of personal information. *Maryland Law Review* 66(1): 140–193

McAfee 2018. *Economic impact of cybercrime: No slowing down.* https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

National Crime Agency (NCA) 2018. *The cyber threat to UK business: 2017–2018 report.* National Cyber Security Centre. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file

New South Wales Fair Trading 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

New South Wales Police Force (NSWPF) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

New South Wales Registry of Births, Deaths and Marriages 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Northern Territory Police, Fire and Emergency Services 2019. *Annual report 2018–19*. https://pfes.nt.gov.au/corporate/publications

Northern Territory Police, Fire and Emergency Services 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

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/

Office of the Australian Information Commissioner (OAIC) 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Organisation for Economic Co-operation and Development (OECD) 2020. Purchasing power parities (PPP). https://data.oecd.org/conversion/purchasing-power-parities-ppp.htm

Ponemon Institute 2019. *Cost of a data breach report 2019.* Ponemon Institute Research Report. Michigan, USA: Ponemon Institute. https://www.ibm.com/security/data-breach

Queensland Office of Fair Trading 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Queensland Police Service (QPS) 2020. Queensland crime statistics. https://mypolice.qld.gov.au/queensland-crime-statistics/

Reserve Bank of Australia 2020. Inflation calculator. https://www.rba.gov.au/calculator/

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. 130. 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 2018a. *Counting the costs of identity crime and misuse in Australia*. Statistical Bulletin no. 15. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sb/sb15

Smith RG & Jorna P 2018b. *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

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

South Australia Police 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Symantec 2019. *Internet security threat report (ISTR)* vol 24. California, USA: Symantec Worldwide. https://www.broadcom.com/support/security-center/publications/threat-report

Tasmanian Department of Police, Fire and Emergency Management (DPFEM) 2019. *Annual report 2018–19*. https://www.police.tas.gov.au/about-us/corporate-documents/annual-report/

Teunissen C, Smith RG & Jorna P 2020. *Commonwealth fraud investigations 2017–18 and 2018–19.* Statistical Report. Canberra: Australian Institute of Criminology.

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/resources/reports/dbir/

Victoria Police 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

Western Australia Police Force 2019. National Identity Crime and Misuse in Australia 2019 Report: Data Request. Unpublished data

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

Appendix A: Measurement framework indicators

Table A1: Measurement indicators of identity crime and misuse and data sources		
Indicator	**Description**	**Data source**
Acquisition of fraudulent identities		
This component covers the activities associated with acquiring identities used in identity crime. This includes identity theft via online and other means, 'takeover' of a legitimate identity (with or without consent), and fabrication of a false identity.		
1.1 The price of fraudulent identity credentials	The cost to illicitly acquire real Australian credentials or identities, or templates of those credentials	Law enforcement and other government agencies IDCARE
1.2 Number of reported data breaches	Acts as a proxy measure of organisational cybersecurity arrangements for protecting personal information	Privacy and Information Commissioners Industry surveys
1.3 The source of the data breach or how information was accessed	Gives an idea how criminals are gaining access to personal information	ABS AIC OAIC
Use of fraudulent Identities		
This component covers activities associated with the different uses to which fraudulent identity information may be put, and the fraudulent use of legitimate (real) identities in connection with financial, taxation, immigration and identity fraud.		
2.1 Number of identity crime and misuse incidents recorded by government agencies	Estimates the known (or detected) incidence of identity crime and or misuse, based on incidents recorded in Australian government administrative and law enforcement datasets	AFP ATO DFAT Home Affairs DHS ACCC Registries of births, deaths & marriages Consumer protection agencies Police (state & territory) Privacy commissioners Road & traffic authorities

Table A1: Measurement indicators of identity crime and misuse and data sources (cont.)		
Indicator	**Description**	**Data source**
2.2 Number of prosecutions for identity crime and other related offences	Used as a proxy for the number of serious incidents of identity crime and misuse that occur in Australia	CDPP ABS Police (state & territory)
2.3 Number of people who self-report being victims of identity crime or misuse	Estimates the victimisation rate based on self-report data, collected in specialised crime victimisation or consumer surveys	AIC surveys ABS surveys
2.4 Number of people who perceive identity crime and misuse as a problem	Estimates the number and proportion of people who perceive identity crime and misuse as a problem based on data collected from attitudinal surveys	ABS Home Affairs AIC surveys
2.5 The types of personal information most susceptible to identity theft or misuse	Estimates the types of personal information and identity credentials most vulnerable to theft or misuse, based on data collected from attitudinal surveys	ABS Home Affairs AIC surveys
Impacts of identity crime		
This component includes the costs of fraudulent identity credentials and their misuse to individual victims, government agencies, business and the broader community.		
3.1 Direct costs of identity crime and misuse to government agencies	Estimates the cost of identity crime and misuse to government agencies	AFP ATO DFAT Home Affairs DHS ACCC Registries of births, deaths & marriages Consumer protection agencies Police (state & territory) Privacy commissioners Road & traffic authorities
3.2 Direct costs of identity crime and misuse to business	Estimates the cost of identity crime and misuse to businesses	Ponemon Sontiq Symantec NCA
3.3 Direct financial losses to victims of identity crime and misuse	Estimates the cost of identity crime and misuse to individuals	ABS Home Affairs AIC IDCARE

Table A1: Measurement indicators of identity crime and misuse and data sources (cont.)		
Indicator	**Description**	**Data source**
3.4 Number of identity crime victims experiencing non-financial consequences	Seeks to quantify the non-monetary harm caused by identity crime victimisation	AIC Academic literature
Remediation of identity crime		
This component covers broader activities such as support services for victims, and the time they spend recovering their identity.		
4.1 Average time spent by victims on remediation (ie recovering their identity)	Estimates the time victims (broadly individual, business and government victims) spend trying to resolve the issue of having their identity stolen or misused	ACCC ABS Home Affairs Police (state & territory) Consumer protection agencies
4.2 Number of enquiries to government agencies regarding assistance to recover identity information	Identifies the number of enquiries made to government agencies about identity recovery measures	OAIC Consumer protection agencies
4.3 Number of applications for Victims' Certificates (issued by the court)	Assesses the application rate for Victims' Certificates in each Australian jurisdiction.	Home Affairs ABS CDPP
Prevention of identity crime		
This component relates to the activities associated with preventing identity crime, including identity verification processes such as the Document Verification Service, and online security practices.		
5.1 Number of identity credentials able to be verified using the DVS	The number of identity credentials that can be validated through the Document Verification Service	Home Affairs
5.2 Number of government agencies using the DVS	The number of government agencies using the Document Verification Service to determine the validity of a document	Home Affairs
5.3 Number of private sector organisations using the DVS	The number of private sector organisations using the Document Verification Service to determine the validity of a document	Home Affairs
5.4 Number of DVS transactions each year	The number of validation transactions through the DVS each year.	Home Affairs
5.5 The proportion of individuals, business and governments that adopt robust online security practices to protect personal information	Measures the extent to which the Australian population (as individuals or by designated sector) have acted to minimise risk by using computer security protection	Home Affairs Australian Cyber Security Centre ANAO ACMA AIC Ponemon Verizon

Table A1: Measurement indicators of identity crime and misuse and data sources (cont.)		
Indicator	**Description**	**Data source**
6. Estimating the economic impact of identity crime to Australia		
This component relates to the costs associated with identity crime. These costs include the direct losses experienced by victims, the indirect costs of identity crime and the costs of preventing and responding to identity crime.		
6.1 Calculating the cost of identity crime	Estimates how much identity crime costs the Australian government and public	ATO Home Affairs DHS AIC IDCARE ABS

Appendix B: Definition of key terms

Data breach: an incident in which information is disclosed to an unauthorised party.

Forgery: the act of producing a false document with the intention of dishonestly inducing a third person to accept it as genuine. (Adapted from the *Criminal Code Act 1995* (Cth))

Fraud: dishonestly obtaining a benefit, or causing a loss, by deception or other means. (Adapted from the *Criminal Code Act 1995* (Cth) div 135; Commonwealth Fraud Control Guidelines 2011)

Identity crime: a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of a crime. (Council of Australian Governments 2007: 2)

Identity information: information relating to a person (whether living or dead, real or fictitious, an individual or a body corporate) that is capable of being used (whether alone or in conjunction with other information) to identify or purportedly identify the person. This includes the following:

(a) name or address;

(b) a date or place of birth, marital status, relatives' identity or similar information;

(c) a driver licence or driver licence number;

(d) a passport or passport number;

(e) biometric data;

(f) a voice print;

(g) a credit or debit card, its number, or data stored or encrypted on it;

(h) financial account numbers, user names or passwords;

(i) a digital signature;

(j) a series of numbers or letters (or both) intended for use as a means of personal identification; and

(k) an Australian business number.

(Adapted from the *Criminal Code Act 1995* (Cth) pt 9.5 div 370.1)

Identity theft: stealing or assuming a pre-existing identity (or significant part thereof) without consent and, in the case of an individual, regardless of whether the person is living or deceased. (Australasian Centre for Policing Research 2006: 15)

Scam: a fraudulent invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means. (ABS 2016)

Appendix C: Government data

A number of Commonwealth, state and territory agencies were asked to provide data for this report. The Commonwealth agencies are listed in Table C1.

Table C1: Australian Commonwealth entities asked to provide data

Entity	Provided data
Attorney-General's Department	Yes
Australia Post	Yes
Australian Bureau of Statistics	Yes
Australian Communications and Media Authority	Yes
Australian Competition and Consumer Commission	Yes
Australian Criminal Intelligence Commission	Yes
Australian Electoral Commission	Yes
Australian Federal Police	Yes
Australian Institute of Criminology	Yes
Australian Securities and Investments Commission	Yes
Australian Security Intelligence Organisation	No
Australian Taxation Office	Yes
Australian Transaction Reports and Analysis Centre	Yes
Commonwealth Director of Public Prosecutions	Yes
Department of Defence	Yes
Department of Foreign Affairs and Trade (Australian Passport Office)	Yes
Department of Home Affairs	Yes
Department of Human Services	Yes
Department of Industry, Innovation and Science	Yes
Department of Infrastructure, Transport, Cities and Regional Development	No
Office of the Australian Information Commissioner	Yes

State and territory police and those agencies issuing driver licences are of particular relevance to identity crime, as driver licences are a key identity document. The state and territory government agencies asked to provide data for this report are listed in Table C2.

Table C2: State/territory government agencies asked to provide data		
State or territory	**Agency name**	**Provided data**
NSW	NSW Bureau of Crime Statistics and Research	Yes
	NSW Fair Trading	Yes
	NSW Police Force	Yes
	NSW Registry of Births, Deaths and Marriages	Yes
	NSW Roads and Maritime Services	Yes
Vic	Victoria Police	Yes
	Births, Deaths and Marriages Victoria	No
	Roads Corporations Victoria (VicRoads)	No
	Consumer Affairs Victoria	Yes
Qld	Queensland Police Service	Yes
	Registry of Births, Deaths and Marriages (Department of Justice and Attorney-General)	Yes
	Office of Fair Trading	Yes
	Department of Transport and Main Roads	Yes
WA	Western Australia Police Force	Yes
	Department of Transport	Yes
	Registry of Births, Deaths and Marriages	Yes
	Department of Commerce—Consumer Protection	Yes
SA	South Australia Police	Yes
	SA Office of Crime Statistics and Research	Dissolved
	SA Births, Deaths and Marriages Registration Office	Yes
	Department of Transport and Infrastructure	Yes
	South Australia Office of Consumer and Business Services	Yes
Tas	Tasmania Police	No
	Consumer Affairs and Fair Trading	No
	Department of Justice—Births, Deaths and Marriages	Yes
	Department of State Growth (Transport)	Yes
ACT	ACT Policing	Yes
	Office of Regulatory Services	Yes
	Transport Canberra and City Services	No
	ACT Births, Deaths and Marriages	No
NT	NT Police Force	Yes
	NT Department of Transport	Yes
	NT Registry of Births, Deaths and Marriages	Yes
	NT Consumer Affairs	Yes

Appendix D: Police data

All Australian police agencies were asked to provide data on the number of recorded identity crime incidents and related offences (eg fraud, forgery and impersonation).

Australian Federal Police

The AFP (2019) recorded 70 matters involving identity crime in 2018–19, up substantially from 20 recorded instances in 2017–18. These were not the only fraud-related matters reported to the AFP but the cases specifically involving identity crime and misuse.

New South Wales Police Force

Data received from the NSW Police Force indicate that 23,009 identity crime and misuse incidents were reported during 2018–19, a slight decline (5%) from the 24,261 incidents reported in 2017–18 (NSW Police Force 2019).

(Note: The NSW Bureau of Crime Statistics and Research (BOCSAR) also supplied data on the number of incidents of identity crime recorded by the NSW Police Force. According to BOCSAR, there were 1,720 recorded incidents in 2018–19, an increase of nine percent over the 1,583 incidents recorded in 2017–18 (BOCSAR 2019). The difference between these numbers and those of the NSW Police Force reflects the definition applied. For example, NSW Police Force data include misuse incidents such as fraudulent use of a credit card, whereas BOCSAR data do not).

Victoria Police

Victoria Police recorded 27,860 identity crime related offences in 2018–19, an increase of 20 percent from 23,308 recorded in 2017–18. Victoria's Crime Statistics Agency provided further details of deception and theft offences which involved identity-related fraud (Figure D1).

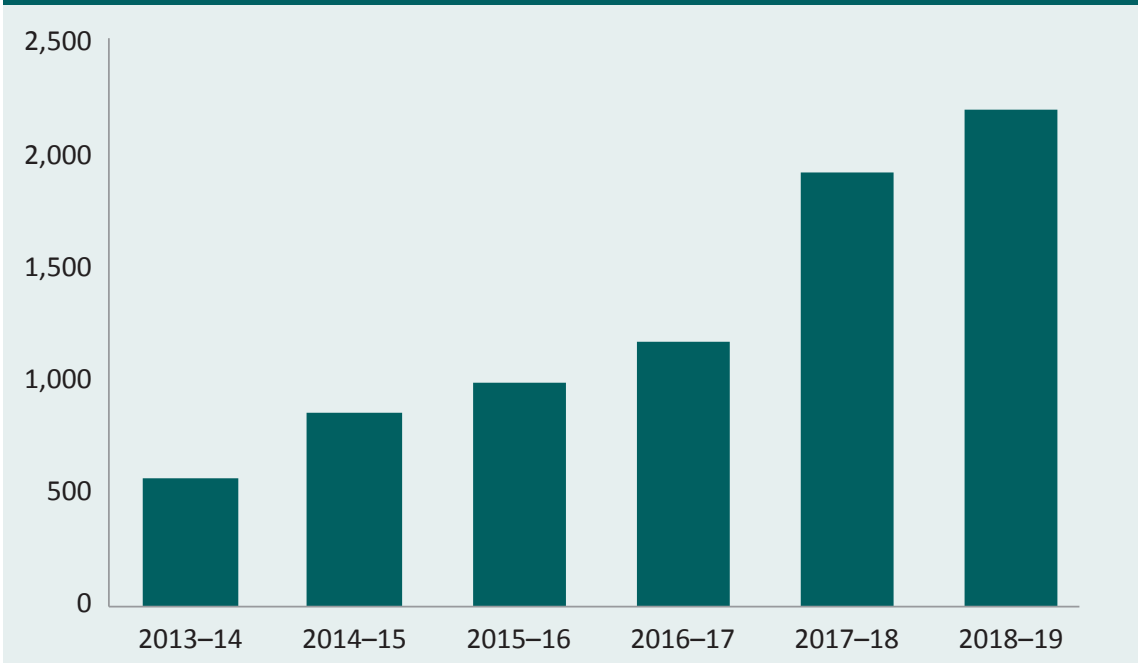
Figure D1: Identity-related fraud offences in Victoria, 2014–15 to 2018–19 (*n*)

Source: Crime Statistics Agency 2019 (unpublished data)

Queensland Police Service

In total, 28,576 fraud offences were reported to the Queensland Police Service in 2018–19. Of those offences, 2,211 involved identity fraud, while 14,606 involved credit card fraud and 773 fraud by computer. These last two types could also involve misuse of personal information. Overall, identity fraud crimes in Queensland are steadily increasing.

Figure D2: Identity fraud offences in Queensland, 2013–14 to 2018–19 (*n*)



Source: Queensland Police Service 2020

Western Australia Police Force

The Western Australia Police Force provided the following information about identity crime offences reported in 2016–17 to 2018–19 (WA Police Force 2019).

Table D1: Western Australia identity crime offences 2016–17 to 2018–19 (*n*)

2016–17	2017–18	2018–19
6	206	234

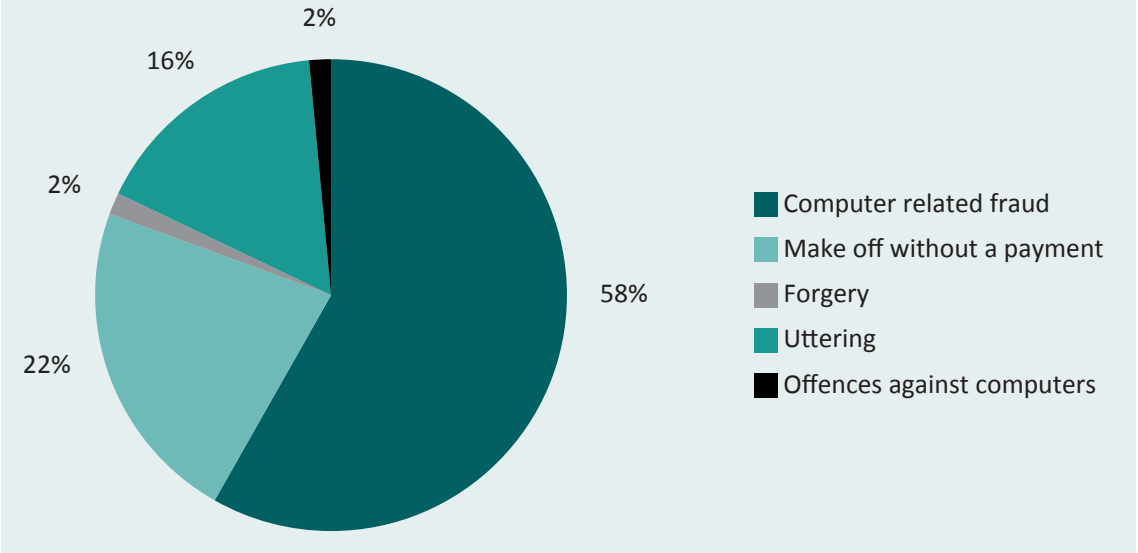
South Australia Police

During 2017–18, South Australia Police recorded 364 identity crime/misuse offences. That number increased 36 percent to 494 recorded offences in 2018–19.

Tasmania Police

Tasmania Police do not capture specific data on identity crime. However, they do publish information on fraud and similar offences in their annual report. In 2018–19, there were 949 fraud and similar offences recorded, an increase of nine percent on the 873 offences recorded in 2017–18. The distribution of fraud and similar offences in 2018–19 is provided in Figure D3.

Figure D3: Distribution of all fraud and similar offences in Tasmania, 2018–19 (%)



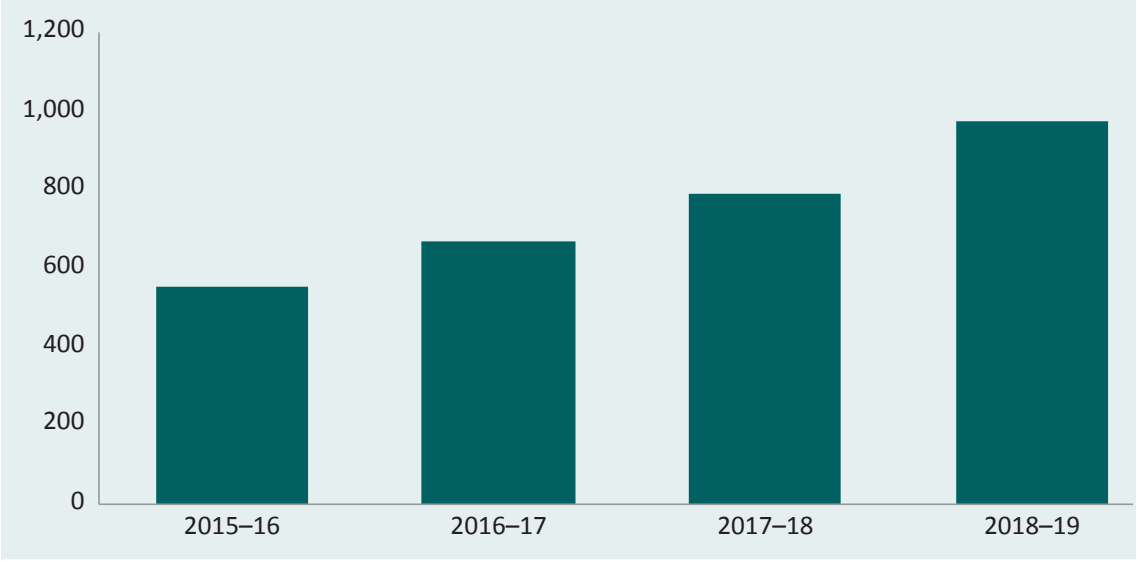
Note: 'Uttering' is the action of knowingly using a forged document with the intent to defraud

Source: Tasmanian Department of Police, Fire and Emergency Management 2019

Australian Capital Territory Policing

The Australian Capital Territory does not have legislation specifically relating to identity crime, so police record offences under more general deception and dishonesty offences. It is therefore difficult to compare the ACT's data with those of other jurisdictions. The total number of fraud offences in the ACT in 2018–19 was 975, consistent with the upward trend presented in Figure D4.

Figure D4: Identity-related apprehensions in the ACT, 2015–16 to 2018–19 (*n*)



Source: Australian Capital Territory Policing 2019, 2017 (unpublished data)

Northern Territory Police

Northern Territory Police does not currently classify data in a manner that enables reporting on identity crime. However, offence statistics, including fraud statistics, are published in the annual report of the Northern Territory Police, Fire, and Emergency Services (NTPFES). These fraud statistics provide a useful comparison with statistics from other jurisdictions. There were 404 reported cases of fraud in 2018–19, an eight percent increase from the 374 cases reported in 2017–18 (NTPFES 2019).

Figure D5: Fraud, deception related offences in the Northern Territory, 2014–15 to 2018–19 (*n*)

Source: NTPFES 2017 & 2019

Summary

Table D2 presents a summary of the number of fraud and deception related offences reported to police jurisdictions between 2017–18 and 2018–19.

Table D2: Fraud and deception related offences reported to state and territory police, 2017–18 to 2018–19 (*n*)

State or territory	Type	2017–18	2018–19	Total
NSW	All fraud offences	24,261	23,009	47,270
Vic	Deception related	23,308	27,860	51,168
Qld	All fraud offences	28,341	28,576	56,917
WA	All fraud offences	30,608	30,927	61,535
SA	All fraud offences	3,297	3,943	7,240
Tas	All fraud offences	873	949	1,822
NT	All fraud offences	374	404	778
ACT	All fraud offences	790	975	1,765
Total	**Police recorded fraud offences**	**111,852**	**116,643**	**228,495**

Source: NSW Police Force 2019; Victoria Police 2019; Queensland Police Service 2019; WA Police Force 2019; SA Police 2019; Tasmanian Department of Police, Fire and Emergency Management 2019; ACT Policing 2019; NT Police, Fire and Emergency Services 2019

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 a 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