Australian Government
Australian Institute of Criminology

AIC reports
Statistical Report 10

National Identity Security Strategy

Identity crime and misuse in Australia 2017

Penny Jorna
Russell G Smith

ISSN (Online) 2206-7930

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

Figures

Tables

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 information. 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

ABN	Australian business number
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACORN	Australian Cybercrime Online Reporting Network
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
APP	Australian Privacy Principle
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
CSA	Crime Statistics Agency (Victoria)
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
DIBP	Department of Immigration and Border Protection
DPFEM	Department of Police, Fire and Emergency Management (Tasmania)
DVS	Document Verification Service
NSWPF	New South Wales Police Force
NTPFES	Northern Territory Police, Fire and Emergency Services
OAIC	Office of the Australian Information Commissioner
RBDM	Registry of Births, Deaths and Marriages
TFN	tax file number
QPS	Queensland Police Service

Abstract

Identity crime involving the misuse of personal information affects a large number of Australians each year, as well as businesses and government agencies. The financial and non-financial consequences experienced by victims are considerable, and data indicate identity crime continues to increase in Australia.

This report is the fourth in a series designed to assess the prevalence, nature and impact of identity crime and misuse in Australia. 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, is responsible for compiling and publishing this information as a key initiative of the National Identity Security Strategy.

Executive summary

This report seeks to assess the nature, extent and impact of identity crime and misuse in Australia. It presents data and information from Commonwealth, state and territory agencies, as well as from the private sector and other non-government sources. The Australian Institute of Criminology (AIC), within the Home Affairs portfolio, is responsible for compiling and publishing this information as a key initiative of the National Identity Security Strategy.

Cost of identity crime

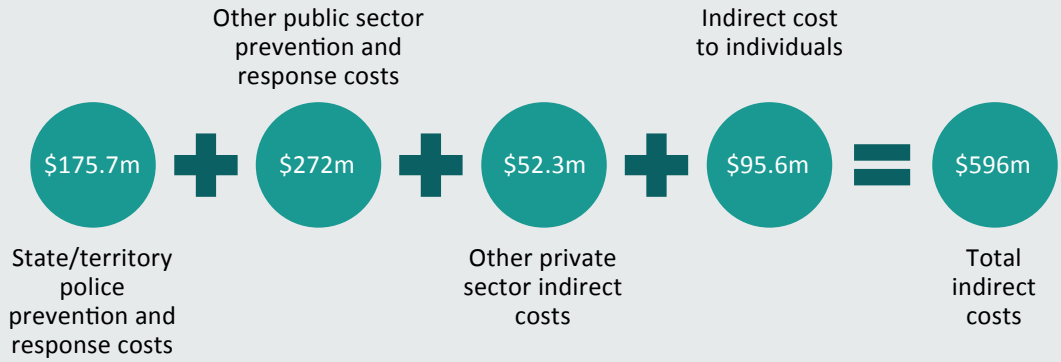
The estimated direct and indirect cost of identity crime in Australia in 2015–16 was $2.65b. This includes $2.1b in losses suffered by Australian government agencies, businesses and individuals, as indicated in Figure 1. Full details of the AIC's costing methodology are presented in the accompanying Statistical Bulletin (Smith & Jorna 2018a).

Figure 1: Estimated total direct cost of identity crime in Australia, 2015–16

Note: See Smith & Jorna 2018a for details of the methodology used to calculate these estimates

The indirect cost of identity crime in 2015–16 was estimated to add a further $596m (as indicated in Figure 2), bringing the total economic impact of identity crime in Australia for 2015–16 to approximately $2.65b.

Figure 2: Estimated total indirect identity crime costs in Australia, 2015–16

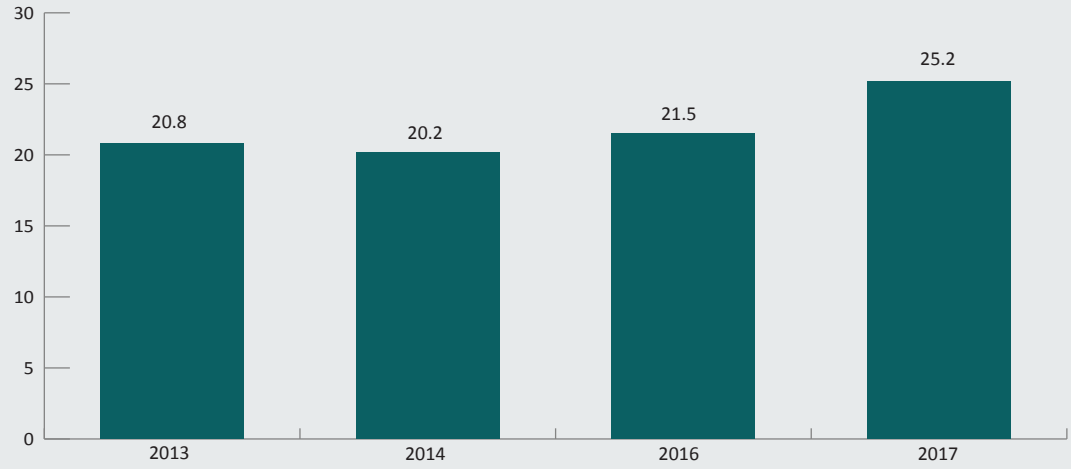


Note: See Smith & Jorna 2018a for details of the methodology used to calculate these estimates

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 AIC have found that over 20 percent of respondents each year report having experienced misuse of personal information at some time in the past (Goldsmid, Gannoni & Smith 2018; Smith, Brown & Harris-Hogan 2015; Smith & Hutchings 2014; Smith & Jorna 2018b). As shown in Figure 3, there was a significant increase in the proportion of people reporting lifetime victimisation between 2016 (21.5%) and 2017 (25.2%). This lifetime victimisation rate is, however, comparable with the 27 percent reported by respondents to the identity fraud survey conducted in 2012 for the United Kingdom's National Fraud Authority (NFA 2013: 30).

Figure 3: Lifetime victimisation rates for misuse of personal information, 2013 to 2017 (%)

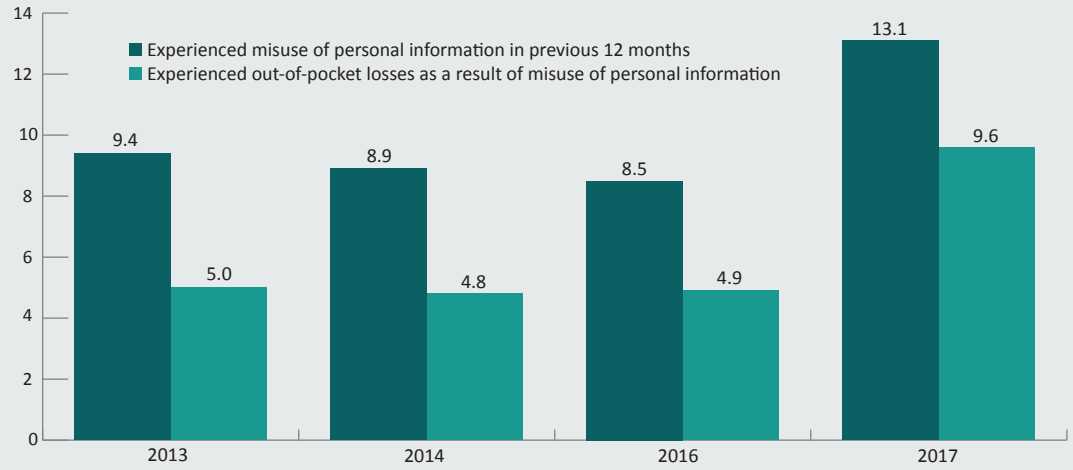


Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender. Statistically significant 3.7 percentage point rise in lifetime victimisation from 2016 to 2017: N-1 $\chi^2(1)=38.06$, $p<0.001$

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

The AIC's survey also asked respondents to report their experience of misuse of personal information and out-of-pocket losses in the preceding 12 months. As shown in Figure 4, while 12-month victimisation rates and out-of-pocket loss rates remained relatively stable between 2013 and 2016, both increased significantly in 2017, with 13.1 percent of respondents experiencing some form of misuse of their personal information in the 12 months prior to participating in the survey, and 9.6 percent of all respondents incurring out-of-pocket losses as a result of this misuse (Goldsmid, Gannoni & Smith 2018).

Figure 4: Respondents experiencing misuse of personal information and out-of-pocket losses in the preceding 12 months, 2013 to 2017 (%)



Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender. Statistically significant increase from 2016 to 2017, N-1 $\chi^2(1)=109.30$, $p<0.001$

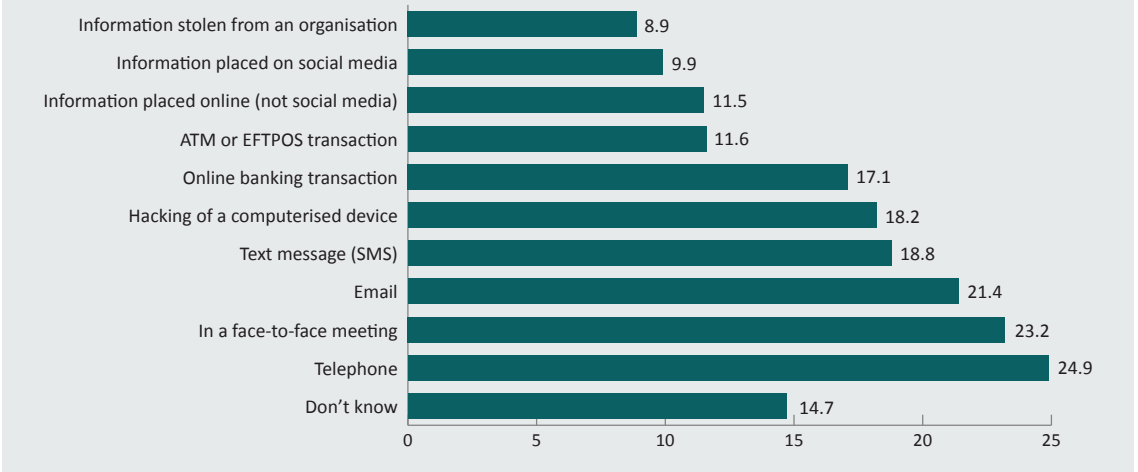
Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018

Misuse of personal information and identity crime remains an ongoing concern for Australians, with almost all respondents to the AIC's most recent survey (96.9%) indicating that misuse of personal information was, in their view, 'very serious' or 'somewhat serious' (Goldsmid, Gannoni & Smith 2018).

Acquisition of fraudulent identities

Stolen and fraudulent identity credentials continue to be highly sought after by criminals, with a large amount of personal information obtained illegally online, by email, social media or through scams or data breaches (Figure 5). Personal information was also often obtained other than through the internet, with telephone and face-to-face methods being the two most prevalent methods employed.

Figure 5: Method of obtaining personal information on the most serious occasion, 2017 (%)



Source: AIC Survey 2017 (Goldsmid, Gannoni & Smith 2018)

The price of stolen or fraudulent identity credentials varies depending on the type of product ordered, the quantity ordered, the quality of the document, the time frame requested, the relationship between the seller/customer and the number of persons/hands the item passes through between the manufacturer and end user of the document. For example, an Australian passport is estimated to cost approximately $3,000, whereas the estimated cost of a Medicare card is $350.

Although only 8.9 percent of respondents to the AIC's latest survey reported information was obtained from data breaches, the number of data breaches reported to the Office of the Australian Information Commissioner (OAIC 2017a) has continued to increase, from 123 data breaches recorded in 2015–16, to 149 data breaches recorded in 2016–17 (compared with 110 data breaches recorded in 2014–15). The OAIC also found that, between the Notifiable Data Breaches scheme coming into force on 22 February 2018 and the end of March 2018, 63 breaches were reported (OAIC 2018).

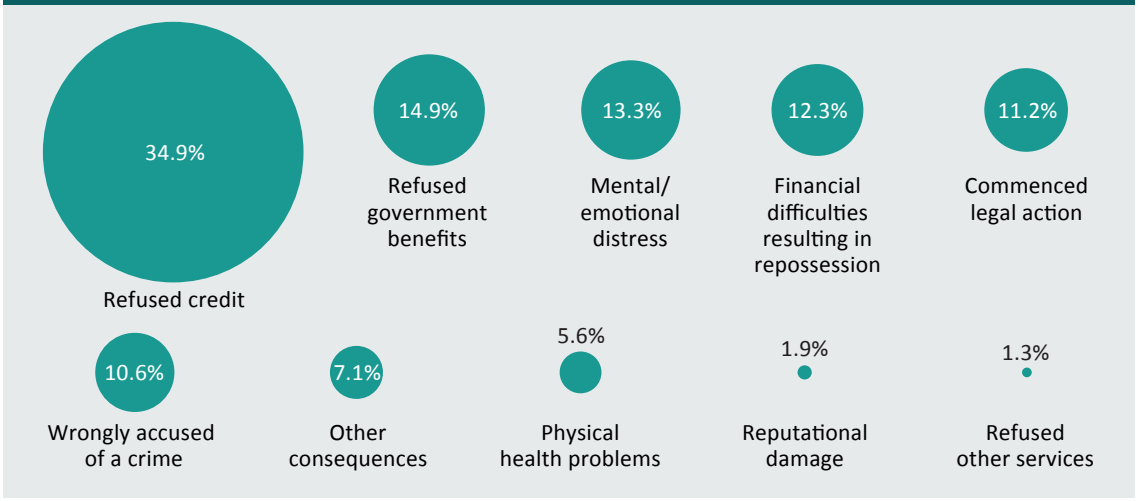
Use of fraudulent identities

IDCARE, a not-for-profit support service for victims of identity crime in Australia and New Zealand, found that it took on average 80.4 days for victims of identity crime to detect the initial misuse of their personal information, and an average of 23 days for criminals to further target victims of identity crime (IDCARE 2018b). Equifax, a leading provider of credit information and analysis in Australia and New Zealand, took over Australia's credit reference company, Veda, in 2016. Veda found identity takeover was the fastest growing type of fraud in 2015–16, up 80 percent from 2014–15 (Veda 2016). Identity takeover occurs when someone uses another person's identity or identification documents to apply for credit. Veda (2016) also found 50 percent of all credit application fraud occurred online.

Impact of identity crime on victims

Most identity crime victims experience relatively low out-of-pocket losses as a result of identity crime, with a median loss of $150. The most common consequence of personal information misuse was refusal of credit, with a statistically significant 18.7 percentage point increase in the number of reports of this consequence between 2016 and 2017 (Figure 6). There were also considerable increases in reports of being refused government benefits (a 9.6 percentage point increase from 2016) and experiencing financial difficulties resulting in repossession (an 8.1 percentage point increase from 2016).

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



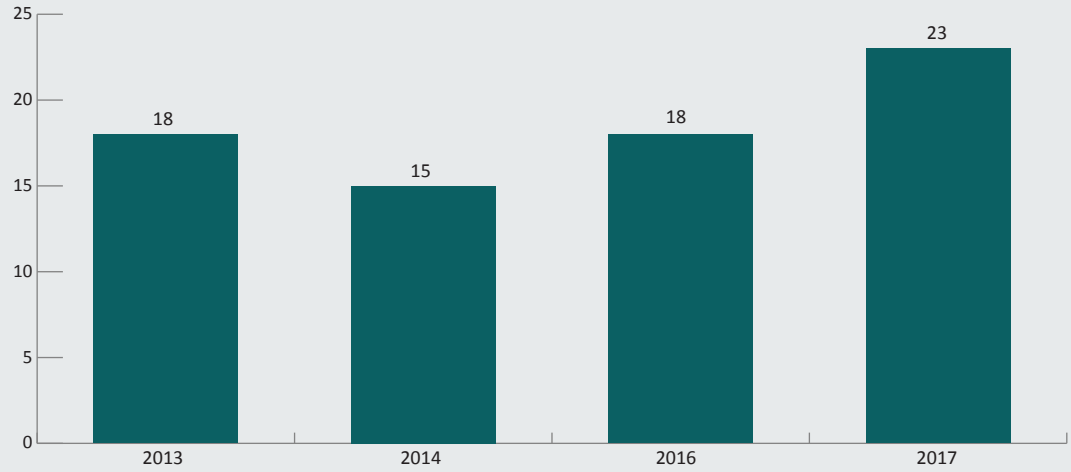
Source: Goldsmid, Gannoni & Smith 2018

Although a statistically significant reduction was found in the proportion of victims of personal information misuse who reported no adverse consequences in the last 12 months (55.9% in 2016 to 34.4% in 2017), over two-thirds of respondents (67%) who had experienced misuse of their personal information did not report the incident at all or only reported to a friend or family member.

Remediation of identity crime

The amount of time spent by victims dealing with the consequences of misuse of personal information increased from 15 hours in 2014 to 23 hours in 2017 (Figure 7).

Figure 7: Average time victims spent dealing with consequences of misuse of personal information, 2013–2017 (hours)

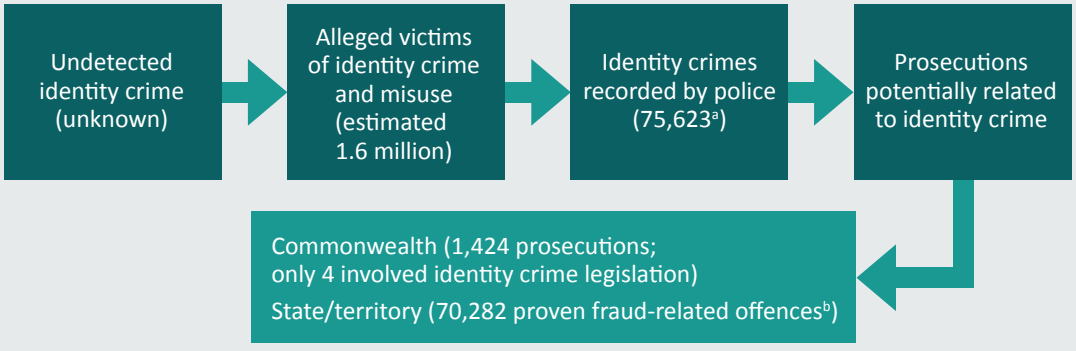


Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018

Prosecution of identity crime

Although large numbers of identity crimes are reported officially, only a relatively small proportion of incidents result in police investigation and prosecution (Figure 8).

Figure 8: Estimated number of identity crimes 2015–16, compared with the number prosecuted (n)

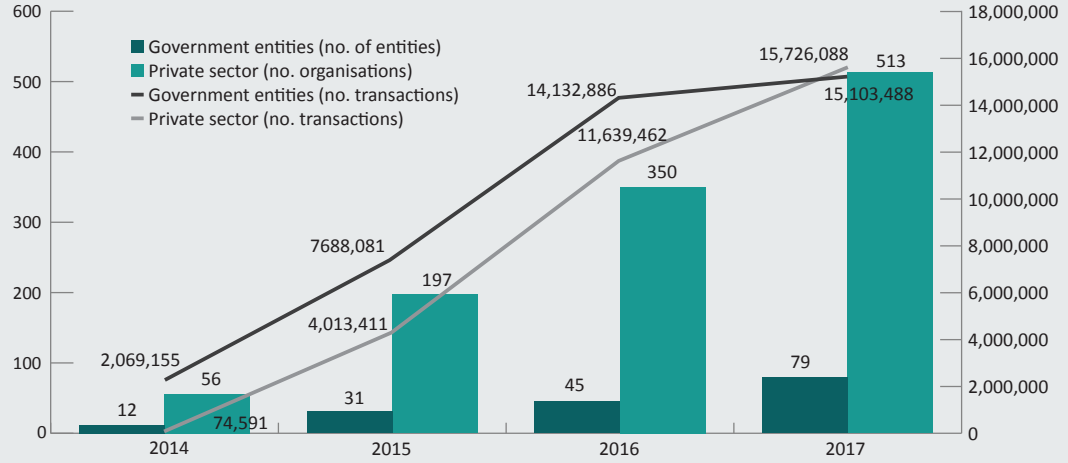


a: See Smith & Jorna 2018a
b: All fraud-related prosecutions. Data on identity crime prosecutions is not available. See Table 10 for further details
Source: AIC data; Australian police jurisdictions

Prevention of identity crime

Since 2014, there has been a large increase in use of the Document Verification Service (DVS), with 513 private sector organisations and 79 government entities using the service at 30 June 2017 (Figure 9). In 2014, the DVS was made available to private sector users with a legislative need to verify customer identities. In March 2015, access was expanded to private sector entities with a reasonable need to verify identities in accordance with the *Privacy Act 1988* (Cth). Since then, private sector take-up of the service has increased exponentially, with private sector transactions exceeding government transactions in 2017 for the first time.

Figure 9: Number of DVS users and number of government and private sector transactions, 2014–17 (n)



Source: Department of Home Affairs 2017 (unpublished data)

Conclusion

This report is the fourth in a series designed to assess the prevalence, nature and impact of identity crime and misuse in Australia. The data presented indicate identity crime and misuse in Australia remains an ongoing and increasing problem 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 work together to reduce the 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 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 hundreds of thousands of Australians each year (AGD 2016), and comparable numbers in overseas countries—although direct comparisons are difficult because of differences in definitions and data collection practices.

This is the fourth report (following a pilot study in 2013) compiled by the Attorney-General's Department (AGD) and the Australian Institute of Criminology (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 to increase.

Case study 1: The changing nature of identity crime: online and remote access

Identity thieves can steal a person's personal identification information and access email and bank accounts very easily. This became quite apparent to a family in Sydney, who had their mobile phone details, Facebook account, email account and bank details accessed and changed by identity criminals within one hour.

The family first had an inkling that something was wrong when one of their mobile phone connections stopped working. The partner of the person whose phone stopped working then received an alert on his phone from Facebook advising that his wife's password had been changed.

The family notified their bank immediately and were informed that the identity criminals were seeking to increase the daily withdrawal limit on the account. The bank quickly froze the online bank accounts, but not before the thieves had withdrawn cash from an ATM.

The family spent a considerable amount of time changing passwords and organising new passports and licences in an effort to thwart future identity theft attempts.

Source: Machado 2017

Methodology

Defining identity crime

Identity crime is a crime category with varying elements depending on the circumstances in which it 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 facilitate the commission of 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 terrorism; unauthorised access to sensitive information or facilities for unlawful purposes; and the concealment of other activities such as drug trafficking or the production and distribution of child exploitation material. Misuse of identity has also been connected with the commission of terrorist acts.

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

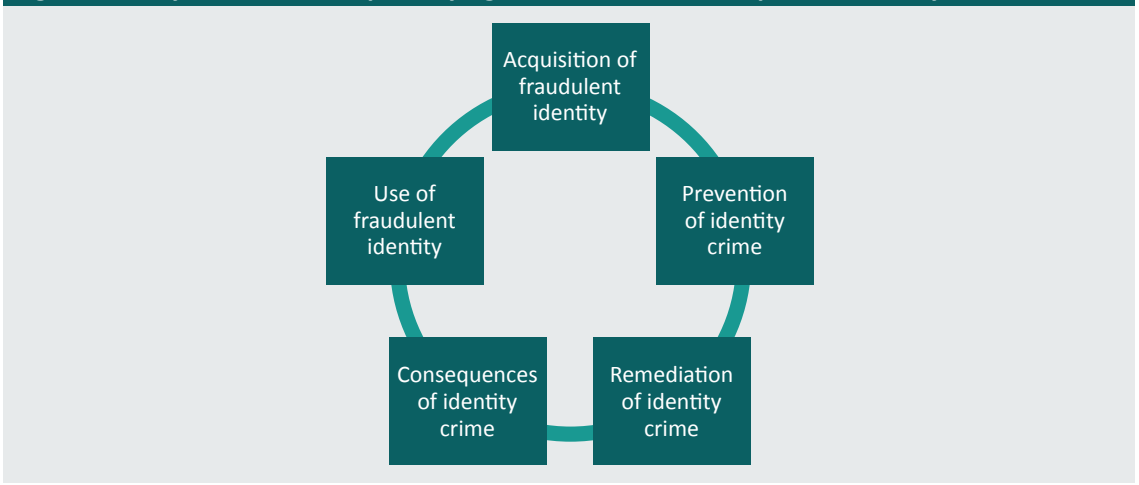
> Identity crime and misuse' involves someone using another person's personal information without their permission. 'Personal Information' includes: name, address, date of birth, place of birth, gender, driver licence information, passport information, Medicare information, biometric information (e.g.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

A total of 33 Commonwealth, state and territory agencies and one non-governmental organisation, IDCARE, provided information, which indicates the breadth of identity crime experienced by government agencies and businesses throughout Australia. A full list of the agencies invited to take part in the survey 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 10). The AGD, in collaboration with the Australian Institute of Criminology (Bricknell & Smith 2013), developed the methodology used in this and previous reports (AGD 2016, 2015, 2014, 2012).

Figure 10: Key indicators for quantifying the incidence and impact of identity crime



Source: AGD 2016

Data quality and availability

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

- failure to detect identity crime and misuse;
- under-reporting of identity crime by individuals and organisations;
- variable definitions of identity crime used by agencies and organisations;
- the proportion 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 actual incidence and cost of identity crime experienced in Australia are likely to be higher than the estimates presented in this report.

Unless otherwise indicated, information relates to the 2015–16 financial year.

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 2017 Identity Crime and Misuse in Australia Survey (Goldsmid, Gannoni & Smith 2018) and earlier surveys (see Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; and Smith & Jorna 2018b); and
- the Australian Bureau of Statistics' (ABS) Personal Fraud Survey 2014–15 (ABS 2016).

Australian Institute of Criminology identity crime 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 and are not representative of the entire community—although the current study had a large enough group to enable comparisons of most variables. All participants, did, however, require access to the internet and a willingness to be involved in such research.

The questionnaire included between 23 and 37 questions canvassing perceptions of identity crime risk and details of victimisation experienced over the preceding 12 months and throughout the respondents' lifetime. Respondents were also asked to provide more detailed information on the most serious occasion of misuse of personal information in the last 12 months, including demographic details, methodologies of offending, impact and response activities. Four online surveys have been conducted: in 2013, 2014, 2016 and 2017 (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018—Table 1).

Table 1: AIC identity crime surveys, by year and sample size

Year	Analysed responses	Sample quota	Weighting of data	Report
2013	4,995	Survey 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	Survey 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

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

In the 2013 and 2014 surveys, potential respondents were randomly selected and 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 ABS (2013) Australian demographic data.

For the 2016 and 2017 surveys, non-probability samples consisted of 10,000 Australian residents aged 15 years and over (up to 96 years, the maximum age represented in the panel) who had internet access and who had registered with the panel provider. Quotas were not employed at the point of recruitment and sampling was completed once the target sample size of 10,000 respondents was obtained.

Australian Bureau of Statistics 2014–15 Personal Fraud Survey

In 2014–15 the ABS conducted a nationally representative survey of 27,341 households in an effort to determine the prevalence of personal fraud in Australia. Personal fraud included scams, card fraud, and identity theft (ABS 2016). The survey was completed by one member of each household aged 15 years and over.

The Personal Fraud Survey collected information from individuals about their experience of selected types of personal fraud experienced in the 12 months prior to interview and whether they had incurred any financial loss. In respect of identity theft, respondents were asked if they had ever been a victim of identity theft and about experiences in the five years and 12 months prior to interview.

IDCARE Identity and Cyber Security Community Aftermath Report 2018

IDCARE also provided data about victims' experiences with identity crime. IDCARE is a non-profit organisation, supported by the Australian Government, which provides free support services to victims of identity theft to help them repair the damage to their reputation, credit history and identity.

IDCARE collected empirical information about identity crime and misuse from four sources:

- individual clients who accessed IDCARE's National Case Management Centre via either its hotline, web form, or email;
- organisational partners that work with IDCARE to respond to detected data breaches;
- independent testing conducted by IDCARE of organisational response measures that gathered critical insights from public and private sectors on what individuals may experience when having to respond to the compromise of their identifying information; and
- IDCARE's National Identity Lab, which proactively monitors illicit marketplaces online that buy and sell compromised identifying information.

Structure of the report

This report presents findings from all these data sources in respect of the 2015–16 financial year, with comparisons, where appropriate, to findings of previous studies. In line with the identity crime conceptual model presented in Figure 10, the report examines:

- acquisition of fraudulent identities, including the cost of fraudulent credentials and how information was obtained;
- use of fraudulent identities, including 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;
- remediation of identity crime, such as the 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;
- prevention of identity crime, including the number of agencies and organisations using the Document Verification Service, the online practices of individuals, businesses and government agencies, and behavioural changes demonstrated by victims following victimisation; and
- the consequences of identity crime, including economic impact of identity crime to Australia taking into account costs to government, the private sector and individuals, including actual losses suffered and the costs of preventing and responding to identity crime incurred by government, business and individuals.

Acquisition of fraudulent identities

Personal information and identity credentials can be obtained from a variety of sources. These include physical theft, such as from mailboxes or during burglaries, or accidental loss. These methods have been employed by fraudsters for centuries. With the advent of telecommunications, social engineering has been used to trick unsuspecting victims into disclosing personal information during phone calls, particularly automated telemarketing calls. The internet now provides many avenues for obtaining information either through unauthorised access to networks and systems, or by tricking users into disclosing details in response to phishing and malware attacks. Data breaches also provide access to substantial amounts of personal information that can be used for criminal activity. This section presents findings from the ABS Personal Fraud survey (ABS 2016) and the AIC Identity Crime and Misuse Surveys (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018).

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 bank statement to $350 for a Medicare card and up to $3,000 for an Australian passport.

Australian identity credentials form a critical element in the commission of many forms of financial fraud. For example, the 100-point check system, introduced to control financial 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. Credentials with enhanced forms of security, such as passports and driver licences, are worth more points than other credentials such as utility accounts, and command higher prices on the black market.

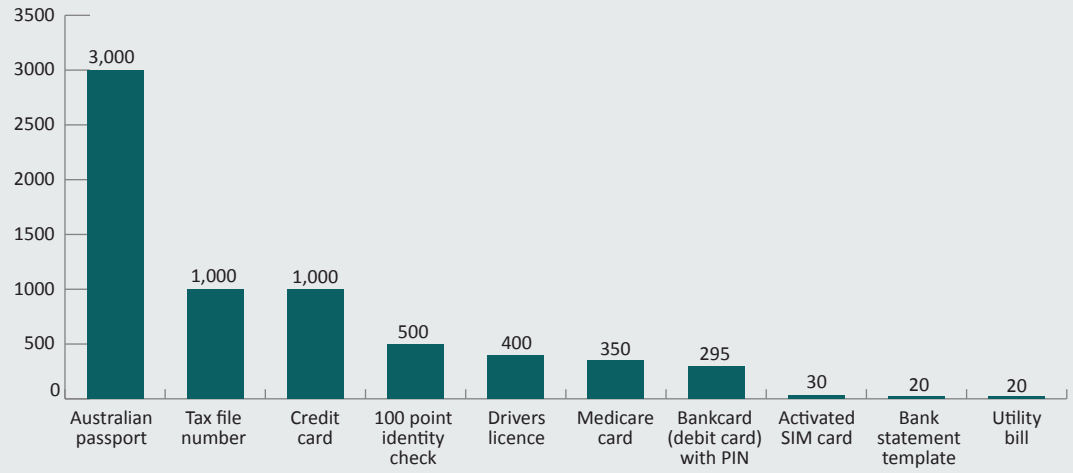
The price of Australian identity credentials varies according to the type of credential, its quality and whether it has been legitimately issued, counterfeited or altered. The most costly credentials are those that have been issued legitimately using false or fabricated personal information.

The Australian Federal Police (AFP) and the NSW Police Force (NSWPF) stated that there is no 'standard' price relating to the sale of identity credentials. The price varies depending on the type of product ordered, 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.

Victoria Police also indicated that a distinction needs to be drawn between actual identity documents and templates of identity documents, as there is a market for both in Australia and each has a different pricing structure.

Physical items, such as actual false driver licences or Medicare cards, are invariably more expensive to purchase than mere electronic scans of compromised credentials (Figure 11).

Figure 11: Price of selected Australian fraudulent identity credentials and templates of Australian identity credentials ($)



Notes: Bankcard with PIN was in US$ and converted to A$; One source reported an external agency advised them that the price of an unaltered stolen Australian passport was $35,000, although no information was supplied as to whether the passport was purchased online or through the use of a facilitator. The price of a driver licence varied, with one law enforcement agency noting a 'retailer' charged 'end users' between $1,250 and $1,500 for a driver licence or a driver licence and Medicare card

Source: Australian Federal Police 2017 (unpublished data); New South Wales Police Force 2017 (unpublished data); Victoria Police 2017 (unpublished data); Department of Home Affairs 2017 (unpublished data); Department of Foreign Affairs and Trade 2017a (unpublished data); IDCARE 2018a (unpublished report)

Recent research undertaken by IDCARE (2018a) into Australian commodities available on the darknet showed a dramatic reduction in prices of identification credentials between 2015 and 2018 (Table 2), arguably due to supply exceeding demand following some significant data breach incidents.

Table 2: Prices of Australian personal identification commodities on the darknet, 2015 and 2018 (A$)		
Australian identification credential	**2015**	**2018**
Driver licence (real but compromised)	$417–$450	Not sold
Driver licence (digital scan)	$75–$750	$12–$20
Passport (real)	$5,110	$2,000–$3,000
Passport (digital scan)	Data not available	$10–$50
100 point pack (scanned driver licence, Medicare card, bank card)	$1,170	$500
Bank account with debit card	Data not available	$120–$400
Accounts worth $100,000 or equivalent	$188–$2,107	$500
Burner SIM card	Data not available	$15–$20
Utility bill	$57	$20
Email account login/password	$6–7	$1–$10
Australia Post parcel locker/PO Box	Data not available	$47–$50
Bank/utility statements	Data not available	$23–$50

Case study 2: Victorian identity fraud arrest

A Melbourne woman was charged with 90 offences in relation to mail theft, stealing and misusing identity credentials, obtaining property by deception and retaining stolen goods after carrying out an elaborate identity crime operation from her home.

Using a laptop computer, printer and laminator, the woman was able to alter and create a range of fraudulent identification documents including NSW and Victorian driver licences, birth certificates, government concession cards and other forms of photo identification. The woman then allegedly used these false identification documents to open bank accounts, obtain credit cards, order mobile phones and set up post office boxes.

When police raided her property, they found several bank statements, car registration plates, pay slips and credit cards belonging to other people. The victims of the identity crimes were not isolated to Victoria. One victim in New South Wales was unaware that someone interstate had allegedly created a copy of her NSW driver licence and used it to open a bank account, set up a credit card and obtain four mobile phones worth $5,500 until police contacted her. The victim had no idea how her details had been obtained and how they came to be found on a USB that police confiscated from the perpetrator.

Source: Vedelago & Houston 2016

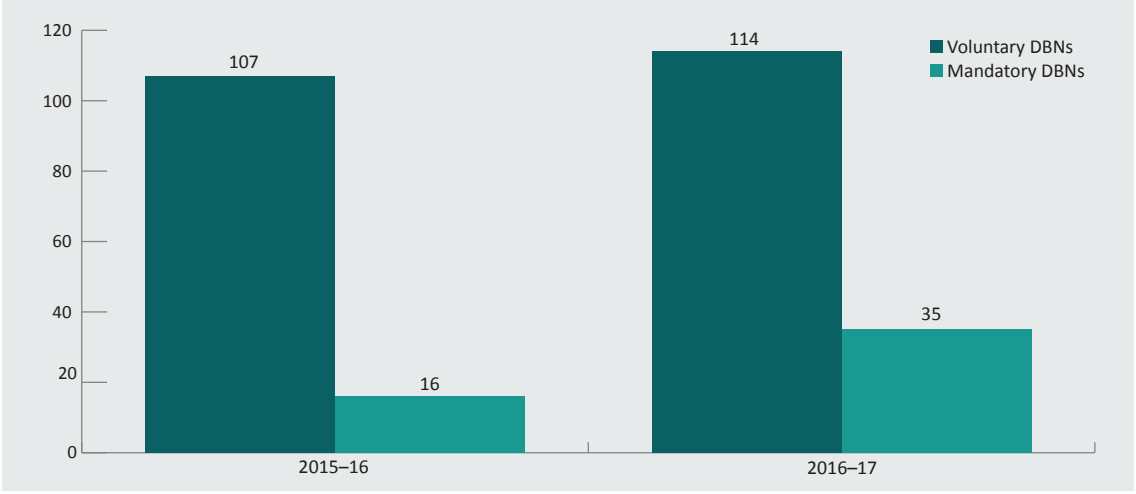
Number of reported data breaches

Key finding: In 2016–17, the Office of the Australian Information Commissioner (OAIC) received 149 data breach notifications, up 21 percent from the 123 notifications received in 2015–16. The annual global study undertaken the Ponemon Institute found the average cost of a data breach for Australian companies was $2.51m in 2017.

Office of the Australian Information Commissioner

The OAIC is responsible for privacy functions that are conferred by the *Privacy Act 1988* and other laws. The OAIC has a range of responsibilities under other laws, including laws relating to data matching, eHealth, spent convictions and tax file numbers. The OAIC also collects information on data breaches. An amendment to the Privacy Act, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* 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* 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 OIAC must also be notified (OAIC 2017a). Between 22 February 2018, when the Notifiable Data Breaches scheme came into force, and the end of March that year, 63 breaches were reported (OAIC 2018). In 2016–17, the OAIC received 149 data breach notifications, up 21 percent from the 123 notifications received in 2015–16 (Figure 12) and 110 breaches recorded in 2014–15. It is expected that the Notifiable Data Breaches scheme will result in an increase in reporting in 2017–18 and beyond.

Figure 12: Data breach notifications (DBNs) received by the OAIC, 2015–16 and 2016–17 (n)



Note: The numbers presented here are the total number of data breaches recorded by the OAIC for the financial years 2015–16 and 2016–17, not only those data breaches that the OAIC identified as possibly involving identity crime

Source: OAIC 2017b (unpublished data)

The OAIC also provided data on the total number of investigations in conducted into breaches possibly involving identity crime and misuse (Figure 13).

Figure 13: Investigations by OAIC into breaches involving identity crime, 2012–13 to 2016–17 (n)

Source: OAIC 2017b (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 (Ponemon Institute 2017). Recent research conducted by the Ponemon Institute (2017) provides further insight into the nature of data breaches experienced by Australian organisations. Twenty-five Australian organisations participated in the global study in 2017, up from 23 Australian organisations in 2015. The average number of records per breach decreased from 19,788 in 2015 to 18,556 in 2017 (Ponemon Institute 2017).

The study found the average cost of a data breach in Australia decreased between 2016 and 2017, from $142 to $139 per capita per data breach. In Australia the total average cost paid by a company also decreased, from $2.64m to $2.51m. In contrast, the total cost of data breaches in the United States rose five percent over one year, to US$7.35m. The study (Ponemon Institute 2017) noted that costs vary by industry. It found that Australian financial services and technology companies tend to have a higher per record cost than the average cost of $139. In the financial services sector, the cost per record can be as much as $232. On the other hand, organisations in the public sector, transportation and retail had a per record cost significantly below average and experienced lower rates of customer loss after a breach.

Importantly, Australian organisations were able to reduce the time taken to identify a data breach, from an average of 201 days in 2016 to 191 days in 2017. The average time taken to contain a data breach also decreased, from 70 days to 66 days (Ponemon Institute 2017).

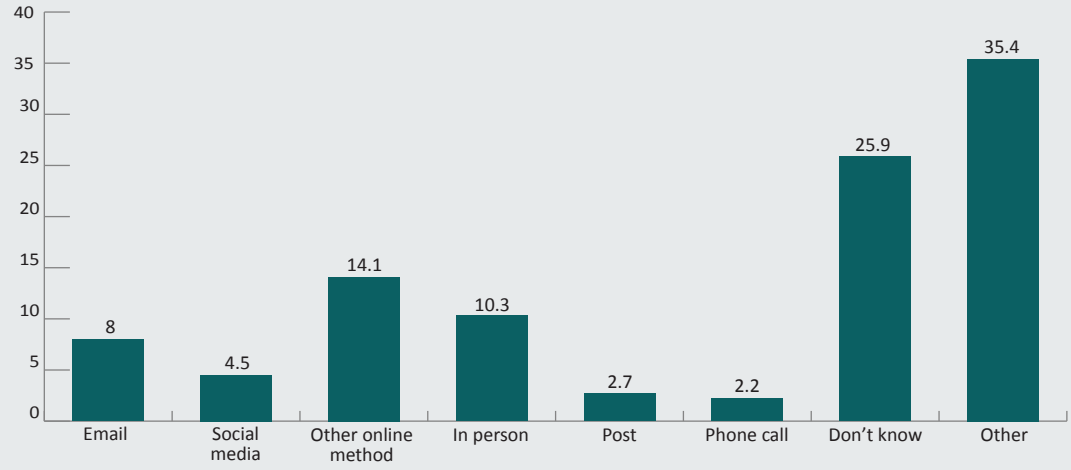
How personal information was obtained

Key finding: Personal information may be obtained by criminals in numerous ways. These include online sources such as the internet, social media or email (phishing or malware), and physical means, such as by face-to-face meetings or through stolen mail. Of most concern is the finding that a large percentage of people (26% in the ABS survey, and 15% in the AIC's 2017 survey) did not know how their personal information was illegally obtained.

The latest nationally representative Personal Fraud Survey conducted by the Australian Bureau of Statistics in 2014–15 (ABS 2016) found that in the 12 months prior to survey, an estimated 126,300 Australians experienced identity theft, or 0.7 percent of the population aged 15 years and over. The majority experienced a single incident only (103,400 or 82% of all identity theft victims).

Of those who experienced identity theft, over one-quarter (27% or 90,100) had their personal details stolen over the internet (including 5% via social media, 8% via email and 14% in another online method), while one in 10 (10% or 34,700) had their personal details obtained in person. A quarter of victims (26% or 87,300) did not know how their personal details were stolen (Figure 14).

Figure 14: Method used to obtain personal details used in identity theft, ABS 2014–15 (% of victims)

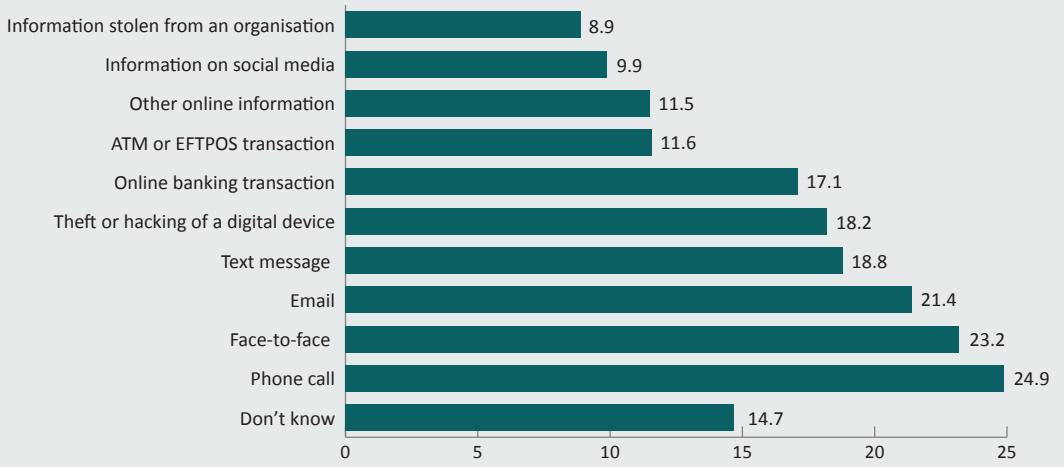


Note: 'Don't know' includes victims who experienced the subsequent misuse of their identity but could not explain how their identity was initially compromised. 'Other' includes lost or stolen items/documents, credit card purchases, and text messages

Source: ABS 2016

The latest AIC 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 July 2017 (Goldsmid, Gannoni & Smith 2018). Almost 15 percent of respondents could not explain how their personal information had been obtained prior to its subsequent misuse (Figure 15).

Figure 15: Method used to obtain personal information on the most serious occasion, AIC survey 2017 (% of victims)

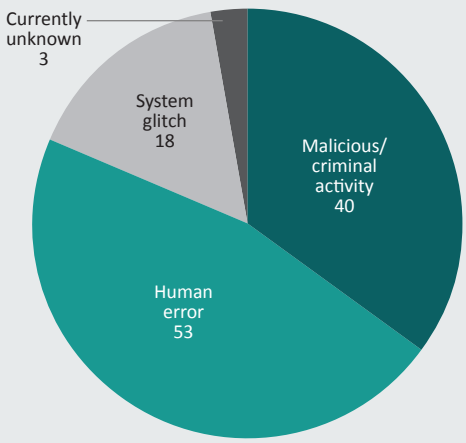


Note: The sampling method used involved an online panel, so there may be an inherent bias in the sample towards online media

Source: Goldsmid, Gannoni & Smith 2018

The OAIC also provided information about the sources of data breaches, or how the data breaches occurred. Figure 16 shows that almost half (47%) of voluntary data breach notifications received by the OAIC in 2016–17 were attributed to human error, with a further 40 percent arising from malicious or criminal activity.

Figure 16: Causes of voluntary data breaches, 2016–17 (n)



Source: OAIC 2017b (unpublished data)

Case study 3: Mobile phone porting—a method of committing identity crime

Porting is the authorised movement of a telecommunications service (ie a telephone number) to a different carrier or network. This is a legitimate process used by telecommunication companies to allow customers to retain their telephone number when moving between carriers.

The problem currently facing telecommunication companies, financial institutions and law enforcement is unauthorised phone porting. Identity crime is a central issue where unauthorised phone porting occurs. The number of reports of criminals (usually members of organised crime groups) unlawfully porting a phone or SIM card in order to commit fraud has increased. Conservatively, phone porting was estimated to have cost the community $5.8m in actual losses in the last 12 months.

NSW Police Force case study

In July 2016 the Newtown Local Area Command of NSW Police commenced Strike Force Gummum to investigate a criminal syndicate operating in the Sydney metropolitan area that was fraudulently obtaining boxes of cigarettes and other goods. The offenders targeted service stations, tobacconists, retail stores and money exchange outlets and ported the mobile phones of the managers and owners of these businesses.

The syndicate would send a text message to employees using the ported telephone, asking them to prepare stock and cigarettes for collection by a nominated courier. As the staff recognised the mobile number as belonging to the manager/owner of the store, they complied with the request. There was a very short period of time between the phone being ported and the offence being committed.

The scam was successful on no less than 25 occasions before syndicate members were arrested and charged in November 2016.

In all of these matters, the criminals were able to obtain sufficient personal identification information in relation to the manager/owner to allow the mobile phone to be ported. The victims all stated they did not receive a phone call from their telecommunications provider to verify the request prior to the porting incident.

The total value of the fraud in respect of this strike force was in excess of $1m.

Source: NSWPF 2017 (unpublished)

Use of fraudulent identities

The use of fraudulent identities is a key enabler of virtually all types of serious and organised crime, including financial crimes such as 'phoenixing' (PwC 2018) and money laundering, which both facilitate criminal activity and obscure the proceeds of crime. Money laundering can also be used to finance terrorism. The use of fraudulent identities facilitates benefits, taxation and other fraud against government agencies and businesses, and there are confirmed cases where properties in Australia have been sold by criminals using fraudulent identity documents to impersonate the property's owner.

People looking to migrate to Australia are known to have used fraudulent identities when applying for visas, and in some cases citizenship, in order to circumvent security, criminal history or other requirements that make them ineligible. Australians of security and criminal concern have also used fraudulent identities to leave the country—including some who were before the courts and charged with serious criminal offences.

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.

This section of the report presents data from government entities about investigations that may have involved identity-related fraud or stolen documents.

Identity crime incidents recorded by government agencies

Benefit/welfare fraud

Key finding: The Department of Human Services (DHS) completed 155 administrative evaluations of or investigations into identity-related fraud in 2016–17. There was a substantial increase since 2015–16 in the number of completed investigations into criminals changing the destination of online payments without the knowledge or authority of the intended recipients.

Since 1 July 2011, DHS has administered Medicare Australia, Centrelink and the Child Support Program. Each year, DHS conducts both administrative evaluations and criminal investigations into identity crime. In 2016–17, DHS completed 3,808 investigations into all forms of Centrelink-related fraud, compared with 2,777 investigations in 2015–16 (Table 3). These investigations covered a range of risks including: identity fraud, undisclosed income or assets, undeclared family relationships, residency non-disclosure and absence from Australia, and changes in study activities.

In 2016–17, 103 investigations into identity matters involving Centrelink were completed, with savings of $1,440,944 (an increase on the 39 investigations completed in 2015–16, which saved $2,380,895. The increase in Centrelink identity fraud matters can be attributed to crimes involving the hijacking of recipients' payments through unauthorised changes to payment destinations made by fraudsters online. DHS prevented 56 such unauthorised changes in 2015–16, avoiding a potential loss of $34,943, and prevented 123 unauthorised changes with a potential loss of $95,982 in 2016–17.

Table 3: DHS investigations into Centrelink fraud matters completed, 2015–16 and 2016–17 (n)

Welfare program	2015–16	2016–17
Working age[a]	1,705	1,584
Disability and carers[b]	676	634
Older Australians[c]	139	184
Students[d]	46	48
Family assistance[e]	9	13
Other[f]	202	845
Total fraud matters	2,777	3,308
Total identity fraud matters	39	103

Source: Department of Human Services 2017 (unpublished data)

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

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

c: Age pension, wife pension

d: Abstudy, Austudy, youth allowance—student

e: Family tax benefit

f: All other serious non-compliance

In 2016–17, DHS completed 499 investigations into fraud matters concerning Medicare, 473 of which related to the Medicare Benefits Schedule. In 2015–16, DHS completed 52 investigations into identity fraud involving Medicare, resulting in savings of $553,793. Data relating to fraud against Medicare were unavailable for 2015–16 due to machinery of government changes.

Case study 4: Alias used to claim multiple disability pensions

A person was suspected of receiving a disability support pension under an alias. An investigation discovered the person had used more than one name to obtain benefits to which they were not entitled over a nine-year period. In December 2016, the person was found guilty of fraud and was sentenced to a maximum three years imprisonment, with a non-parole period of 12 months. They were ordered to pay reparation in excess of $160,000 and to be of good behaviour for two years.

Source: Department of Human Services 2017 (unpublished data)

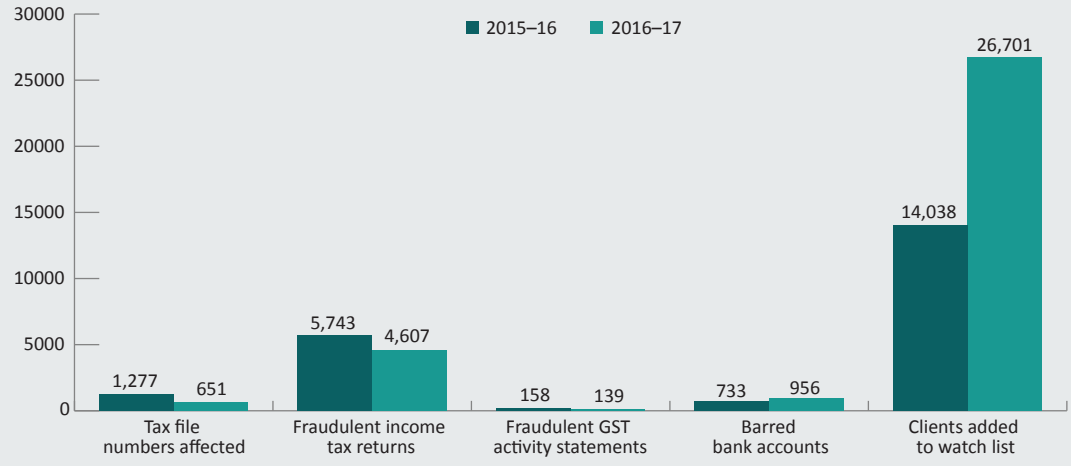
Taxation-related identity fraud

Key finding: Between 2015–16 and 2016–17, the number of tax file numbers (TFNs) added to the Client Identity Watch List increased from 14,038 to 27,701. Over the two-year period the Australian Taxation Office (ATO) saved $93.7m by thwarting fraudulent attempts to obtain benefits or avoid tax liabilities through the misuse of identity.

The ATO's Client Identity Watch List is used to monitor accounts for high-risk transactions where clients have been subject to identity crimes that pose a risk to the taxation and superannuation systems (ATO 2017: unpublished data). Two watch list levels exist: one where compromise is suspected and the other where compromise is known to have occurred.

The number of tax file numbers affected by identity crime decreased from 1,277 in 2015–16, to 651 in 2016–17 (Figure 17).

Figure 17: Potentially fraudulent incidents detected by ATO, 2015–16 and 2016–17 (n)

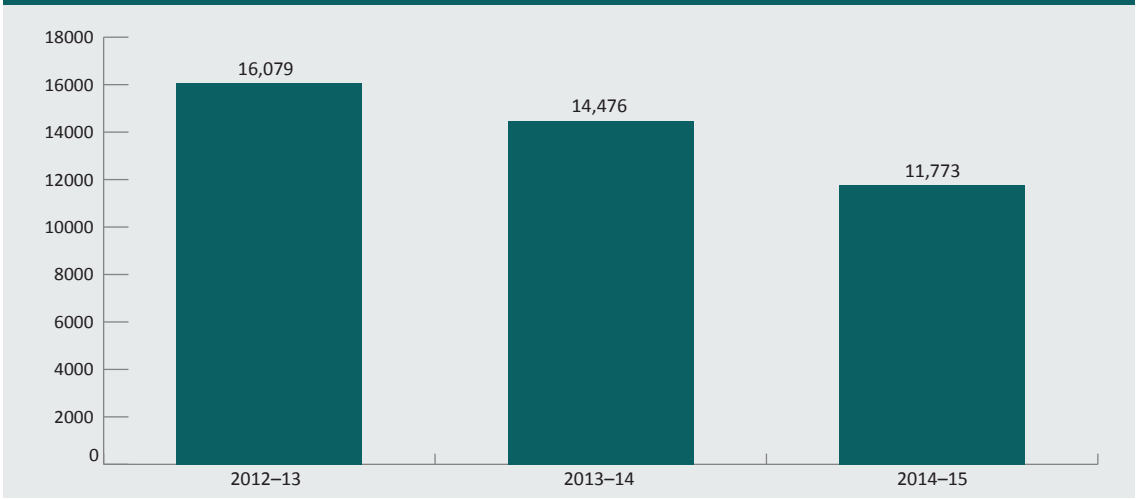


Source: Australian Taxation Office 2017 (unpublished data)

Each year the AIC conducts an annual census of Commonwealth entities to assess their experience of fraud throughout the preceding financial year. The AIC's annual Fraud Against the Commonwealth census has found a substantial number of fraud incidents involving the unauthorised use of another person's TFN or Australian business number (ABN), although these have declined over recent years (Figure 18).

The data from the 2015–16 Fraud against the Commonwealth census differed from the data presented in Figure 17 (see Figure 18). Respondents to the 2015–16 census were asked about fraud investigations finalised between 1 July 2015 and 30 June 2016, rather than suspected fraud incidents. This difference in the unit of measurement led to changes in the number of frauds included in the census. In 2015–16, no participating entities reported finalised fraud investigations involving the unauthorised use of another person's TFN or ABN (Jorna & Smith 2018a).

Figure 18: External Commonwealth fraud incidents involving unauthorised use of another person's TFN or ABN, 2012–13 to 2014–15 (n)



Source: Jorna & Smith 2018b

In addition to the fraud incidents perpetrated against the ATO, the ATO also experienced its name and reputation being misused via impersonation and threat-based scams. The ATO estimated that between January and August 2017, 29,000 reports of ATO scams were received, with $1.6m in losses recorded (Robertson 2017). The losses arose in relation to phishing scams, and criminals lodging false tax returns using a victim's personal identification details obtained via social media, data breaches and other sources. In June 2017, more than one thousand taxpayers reported to the ATO that their personal information had been compromised.

Case study 5: False income tax refunds received using stolen personal information

In June 2017, a Canberra man was sentenced to three years and two months imprisonment with a non-parole period of one year and seven months following conviction on 302 charges of obtaining a financial benefit by deception.

The man had stolen the personal identity information of over 1,000 foreign students and lodged over 400 false income tax returns. The false refunds were issued to over 250 separate bank accounts.

The man first appeared in court in 2011 charged with obtaining in excess of $1.06m from this fraudulent behaviour. The court found that it was an 'elaborate, planned and sophisticated fraud over several years'.

Source: Australian Taxation Office 2017 (unpublished data)

Immigration, customs and transport security related identity fraud

Key finding: The Department of Immigration and Border Protection (DIBP) received 402 allegations of possible visa-related identity fraud in 2016–17.

DIBP, now the Department of Home Affairs, recorded 402 allegations of possible visa-related identity fraud in 2016–17. This was a substantial decrease from the 572 allegations recorded in 2015–16 (Figure 19).

Figure 19: Allegations of possible visa-related identity fraud, 2012–13 to 2016–17 (n)

Source: DIBP 2017 (unpublished data)

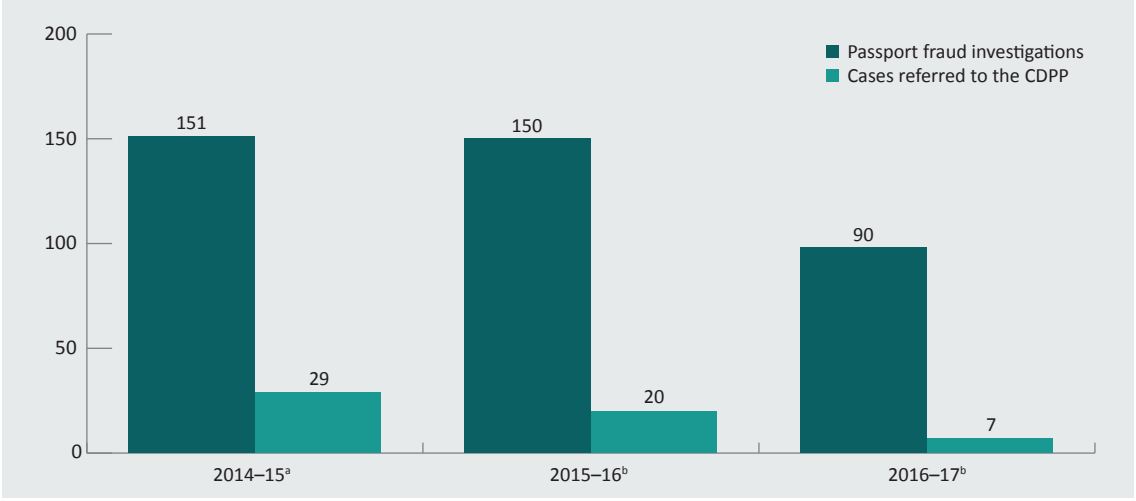
The DIBP also provided data on identity-related fraud involving importation and customs. In 2015–16, there was one importation of blank credit cards, and another in 2016–17. This is consistent with the prohibited importation findings from 2014–15.

Passport identity fraud

Key finding: In 2016–17, 98 passport fraud incidents were investigated by the Department of Foreign Affairs and Trade (DFAT), with seven matters referred to the Commonwealth Director of Public Prosecutions (CDPP).

In October 2015 the parliament introduced a new section into 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. This was a significant factor contributing to the decrease in formal investigations (see AGD 2016 for investigations relating to earlier years). The number of passport fraud cases referred to the CDPP also decreased, from 29 referrals in 2014–15 to just seven referrals in 2016–17 (Figure 20).

Figure 20: Passport fraud investigations and referrals to CDPP, 2014–15 to 2016–17 (n)



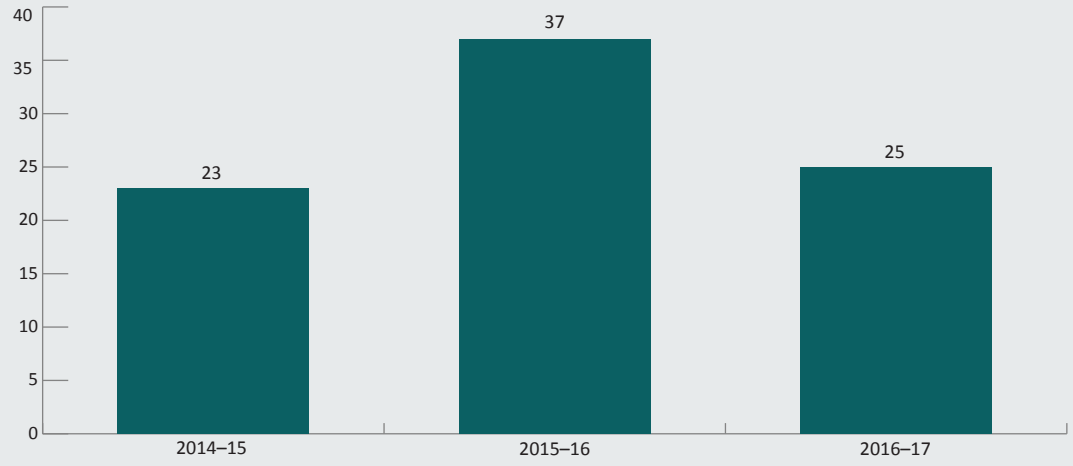
a: DFAT changed the way it records passport fraud investigations in 2015. Subsequent instances of minor passport fraud (not involving identity crime) were resolved by administrative action and not recorded as investigations

b: 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 2017a (unpublished data)

The number of passport fraud investigations related to identity crime and misuse are presented in Figure 21.

Figure 21: Passport fraud investigations related to identity crime, 2014–15 to 2016–17 (n)



Source: AGD 2016; DFAT 2017a (unpublished data)

Table 4 provides further details of the 37 passport fraud investigations in 2015–16 and the 25 investigations in 2016–17 that may have involved identity crime.

Table 4: Identity crime related passport fraud investigations, 2015–16 and 2016–17

Case type	2015–16	2016–17
Fraudulently obtained genuine passports	27	17
Imposters	5	4
Physical alteration	5	4
Total	37	25

Source: DFAT 2017a (unpublished data)

Case study 6: Facial recognition technology detects attempted passport fraud

In February 2016, while on conditional bail for significant intellectual property offences, an offender (Mr D) attempted to obtain an Australian passport in the name of another person (Mr R). Facial recognition technology identified the anomaly, which was confirmed by a facial recognition expert. Mr D was arrested. Through subsequent joint enquiries with police, Mr R was identified as complicit in the passport offence and was subsequently charged, along with another co-accused. All parties pleaded guilty to a range of offences. Mr D was sentenced to 4½ years imprisonment for the intellectual property and passport offences.

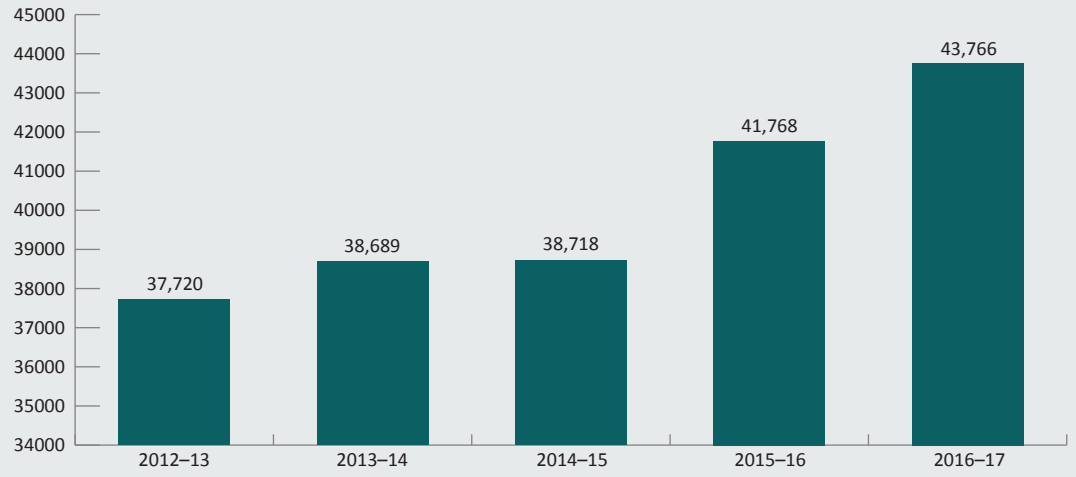
Source: DFAT 2017a (unpublished data)

Lost and stolen passports

Key finding: The number of Australian passports reported lost or stolen has increased by 16 percent since 2012–13.

The number of Australian passports reported lost or stolen has increased by 16 percent since 2012–13 (Figure 22). While these numbers seem large, they represent a small percentage of the total number of passports the Australian government issues each year. In 2016–17, for example, over two million passports were issued (DFAT 2017b). Lost and stolen passports, however, create opportunities for criminals to perpetrate identity-related fraud and to travel overseas without authorisation.

Figure 22: Lost or stolen Australian passports, 2012–13 to 2016–17 (n)



Note: Cancelled passports cannot be verified via the Home Affairs Document Verification Service
Source: AGD 2016; DFAT 2017a (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.

Each year, Registries of Births, Deaths and Marriages issue large numbers of certificates, which are important credentials used for identification and authentication of identity. However, statistics on the number of certificates reported lost or stolen, or altered or fabricated, are generally not collected. Only the New South Wales, Western Australian and Tasmanian registries were able to provide some relevant data (Table 5).

In 2016–17, the NSW registry referred 48 cases of suspected identity crime involving birth certificates, marriage certificates and/or change of name certificates to police for investigation. The majority of all crime and misuse associated with certificates issued by the NSW registry involved birth certificates.

Table 5: Identity crime and misuse associated with certificates issued by RBDMs, 2016–17 (n)

Registry	Lost	Lost/stolen	Unauthorised change	Fraudulent	Referred to police
NSW	22	90	25	4	48
Vic		Unavailable/not recorded			
Qld		Unavailable/not recorded			
WA	Not recorded	1	1	3	
SA		Unavailable/not recorded			
Tas	Not recorded	3	0	0	0
ACT		Unavailable/not recorded			
NT		Unavailable/not recorded			

Source: NSW RBDM 2017, Tasmania RBDM 2017 and WA RBDM 2017 (unpublished data)

Due to the limited data available on the misuse of birth certificates, IDCARE (2018c) examined reports they received during April, May and June 2018. During that period IDCARE responded to 207 individual matters where a birth certificate was compromised, and found 39 percent of the individuals affected experienced further misuse of their personal information (IDCARE 2018c). Figure 23 shows the state/territory distribution of those incidents of identity misuse involving a birth certificate.

Figure 23: State/territory distribution of contact with IDCARE about misuse of birth certificates, April–June 2018 (%)

Source: IDCARE 2018c

Driver licence fraud

Key finding: Driver licences continue to be among the most commonly targeted identity credentials, partly because of their widespread use in the community as proof of identity, and partly because they are a source of highly sought after personal information such as name, address and date of birth.

Road traffic agencies in the states and territories issue and renew large numbers of driver licences every year. For example, VicRoads undertook 800,000 licence renewals in 2016–17 (VicRoads 2017). Three road traffic agencies responded to questions concerning the misuse of driver licences. Only two (Western Australia and Queensland) were able to provide data on the number of suspected identity crime incidents they had detected. These two agencies reported a total of 93 cases of suspected identity crime in 2015–16, and 111 cases in 2016–17. These cases did not include licences recorded as lost or stolen.

One of the agencies estimated that it took 7.25 hours (approximately one day's work) on average to investigate a case of suspected identity crime, with some fraudulent driver licence cases taking months to investigate.

IDCARE's *Identity and cyber security community aftermath report* (2018b), found that driver licences were the most targeted credential misused by criminals in 2017, involving over 20 percent of IDCARE's clients. The AIC's identity crime surveys, however, found that fewer than 15 percent of respondents reported driver licence information being misused (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Goldsmid, Gannoni & Smith 2018).

Case study 7: Syndicate specialises in fabricated identity credentials

As part of Project Birrie, New South Wales Police Force and AFP officers identified 1,710 falsified documents on a computer hard drive in a Sydney home used by a syndicate specialising in fabricating identity credentials. Customers of the syndicate sent photos of themselves to the group, who then printed the photos onto cards imported from China.

Police traced the fabricated credentials to determine the manner in which they were being used in serious crimes. Several other computers were also seized from the premises and these also contained a number of false identity documents.

The credentials had been used by 29 organised crime groups and 13 outlaw motorcycle gang members to move $57m in illegal money offshore. The documents had also been used to facilitate hundreds of scams involving online marketplaces such as eBay. A number of falsified credentials were also found to have been used by suspected terrorists and individuals who had overstayed their visas.

Police involved in Project Birrie noted that false identity credentials are used to facilitate serious and organised crime in a number of ways. They enable criminals to lease properties, purchase products for drug manufacturing and hire cars and trucks to transport drugs. False credentials also command a high price on the black market, with a set comprising a driver licence, Medicare card and credit card selling for between $1,600 and $2,500.

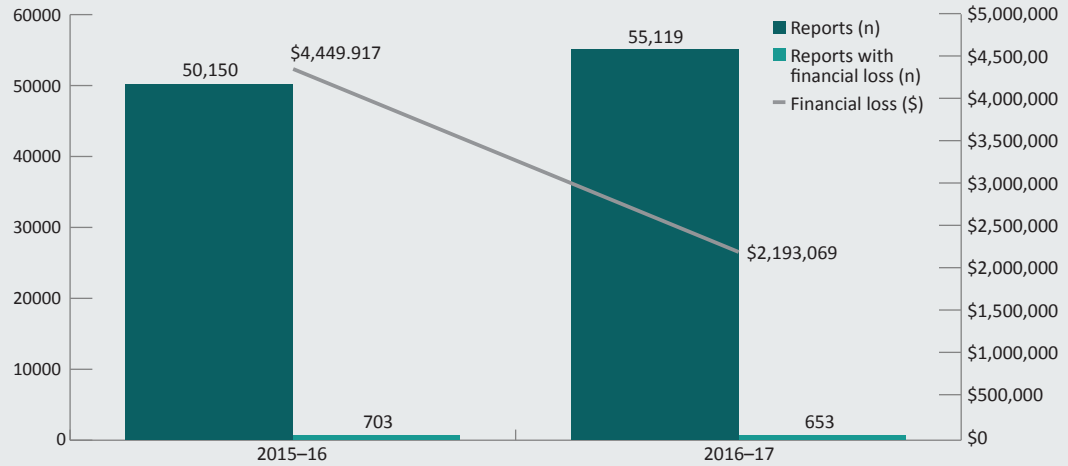
Source: Adapted from Morri 2017

Identity fraud targeting consumers

Key finding: the number of people reporting scams involving identity crime and misuse increased from 50,150 reports in 2015–16 to 55,119 reports in 2016–17 (ACCC 2017b: unpublished data). However, the number of reports involving a financial loss declined slightly, from 703 to 653. The total losses victims experienced also decreased from $4.4m to just under $2.2m (Figure 28).

The role of the Australian Competition and Consumer Commission (ACCC) is to enforce the *Competition and Consumer Act 2010* (Cth) and other legislation, to promote competition and fair trading and to regulate national infrastructure for the benefit of all Australians. As part of its role to protect the interest and safety of consumers, the ACCC manages Scamwatch, an online resource and reporting portal that tells consumers and small businesses how to recognise, avoid and report scams. The ACCC provided data on the number of contacts it received about phishing, identity theft and threat-based impersonation scams from people who reported receiving or falling victim to these types of scams in 2015–16 and 2016–17 (Figure 24).

Figure 24: Number of reports of phishing, identity theft and threat-based impersonation scams recorded by the ACCC and estimated financial losses, 2015–16 to 2016–17



Note: Threat-based impersonation scam is defined as 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, Department of Immigration and Border Protection, or Australian Federal Police

Source: ACCC 2017b (unpublished data)

Case study 8: Threat-based impersonation scam involving a tax audit

One day Stuart[a] arrived home to find a message on his answering machine stating that he needed to call the ATO or go to court for failure to respond to letters sent by registered post. Stuart was concerned as he had not received any correspondence from the ATO. Stuart called the number left on his answering machine and spoke to someone who claimed to be from the ATO's auditing department. The scammer told Stuart that they had done a tax audit of his finances for the last five years and found some discrepancies in payments and that he owed the ATO money.

The scammer told Stuart an officer had sent him a notice, but as it had not been answered someone would be coming to arrest him and take him to court. This would happen unless he agreed to settle the amount owed straightaway. The scammer told Stuart to buy $5,000 worth of preloaded payment cards and said that, once he had done this, the ATO officer would visit him at his house the next day and go through the audit to help Stuart identify where the error in his tax payments had occurred.

Stuart told the scammer he was unaware he owed any money to the ATO as he always paid his tax on time. The scammer assured Stuart that he would explain everything the next day when he visited. The scammer then asked Stuart to call him back and read out the card numbers and PIN so they could clear his debt. Stuart did as requested. At the end of the phone call Stuart was told not to contact anyone before their visit the next day. Stuart had given the scammer $5,000 for a debt he never owed.

a: Name changed to preserve anonymity

Source: ACCC 2017b (unpublished data)

Identity fraud incidents recorded by police

Key finding: Police agencies recorded 130,474 fraud and deception offences in 2016–17, a decrease of three percent from 2014–15. Only some jurisdictions were able to identify numbers of identity fraud offences. It is estimated that 46.5 percent of all fraud involves some element of identity misuse, which would amount to 60,670 identity-related offences recorded by police in Australia in 2016–17.

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 introduced specific identity crime provisions into 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*.

Table 6 presents summary statistics on the number of fraud offences recorded by police jurisdictions between 2014–15 and 2016–17 (and identity fraud offences where available). Over these three years the number of reported fraud offences decreased by three percent.

Table 6: Fraud and identity-related fraud offences reported to state and territory police, 2014–15 to 2016–17 (n)

State or territory	Type	2014–15	2015–16	2016–17
NSW	Fraud	51,137	51,935	47,934
	ID fraud			15,639 (33%)
Vic	Fraud	36,668[a]	36,988[a]	34,605[a]
	ID fraud	882	6,071	5,972 (17%)
Qld	Fraud	23,382	22,054	27,258
	ID fraud	858	1,000	1,179 (4%)
WA		19,290	22,212	16,154
SA	Fraud	2,757	2,909	2,753
	ID fraud		560	462 (17%)
Tas		646	750	825
ACT	Fraud	1,195	553	668
	ID fraud		26	18 (3%)
NT	Fraud	317	316	277
	ID fraud[b]		41	26 (9%)
Total	Fraud	133,967	137,717	130,474

a: The Victorian Crime Statistics Agency collects data for the calendar year, not financial year

b: NT identity fraud component includes 'forgery of documents' data published in the NTPFES annual report

Note: Numbers in parentheses are the percentage of all fraud offences that are identity-related offences in each jurisdiction. Definitions of identity-related offences differ between jurisdictions

Source: NSW BOCSAR 2017 (unpublished data); Tas DPFEM 2017; NTPFES 2017; Crime Statistics Agency (Vic) 2017 (unpublished data); QPS 2018; SA Police 2018 (unpublished data); SA Office of Crime Statistics and Research 2017 (unpublished data); AFP (unpublished data); WA Police Force 2018

Australian Cybercrime Online Reporting Network

The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of the Commonwealth, state and territory governments. It is a national online system that allows members of the public to report most types of cybercrime. It also provides advice to help people recognise and avoid common types of cybercrime (ACORN 2018). The reports made to ACORN are referred to the most appropriate law enforcement agency for consideration and possible investigation (Table 7).

Between 1 July 2016 and 30 June 2017, 6,789 identity crime reports categorised as 'online identity theft' were submitted to ACORN. Not all victims reported financial losses, but the total amount lost by those who did estimate a loss was $415.6m (ACIC 2018: unpublished data).

The reports made to ACORN showed that the most common accounts compromised were bank (43.6%), email (39.8%), social media (18.9%) and PayPal (8.0%) (ACIC 2018: unpublished data).

Table 7: Reports made to ACORN, 2015–16 and 2016–17 (n)

Year	Jul–Sep	Oct–Dec	Jan–Mar	Apr–Jun	Total
2015–16	9,340	9,291	11,900	10,810	41,341
2016–17	11,556	12,691	11,775	Not available	36,022

Source: ACCC 2017b (unpublished data)

Other

Criminal misuse of identity also occurs in a variety of other business environments and a number of regulatory authorities collect information on the nature and extent of the problem. These include financial services and market regulators, business and corporate regulators, financial transaction regulators, and electoral system regulators. These regulatory entities provided information on risk and experience of identity crime and misuse for 2015–16 and 2016–17.

Australian Securities and Investments Commission

The Australian Securities and Investments Commission (ASIC) is Australia's integrated corporate, markets, financial services and consumer credit regulator. ASIC ensures fair and efficient markets by maintaining and improving the performance of the financial system and the entities in it. As a financial services regulator, ASIC licenses and monitors financial services businesses to ensure they are honest and fair (ASIC 2018).

ASIC received 9,802 reports of misconduct in 2015–16, and 8,941 reports in 2016–17. In 2015–16, 58 (0.6%) related to identity theft and, in 2016–17, 70 (0.8%) related to identity theft (ASIC 2017: unpublished data).

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 when there is doubt about the identity of a person using a designated service, or if the person is suspected of avoiding tax obligations or committing a crime. AUSTRAC supplied data on the number of suspicious matter reports involving suspicions that a false name or identity document had been used (Table 8).

Table 8: Suspicious matter reports involving identity misuse and associated costs, 2015–16 to 2016–17

Financial year	Reports (n)	Costs associated[a] ($)
2015–16	2,834	210,078,192
2016–17	4,792	1,238,961,389

a: Costs are indicative only and cannot be attributed solely to the victims. Reports are not always accurate due to the way they were recorded. Reports can be made about failed attempts to defraud, so the value includes potential losses, not only actual losses

Source: AUSTRAC 2017 (unpublished data)

As a government agency, AUSTRAC can also be a victim of identity crime. During the period 2015–16 to 2016–17, there were six instances in which AUSTRAC's name was misused or where the agency was targeted by criminals. Five of the six (attempted) instances involved 'whaling', also known as CEO fraud. This type of identity crime involves targeting senior management figures who hold power in a company, such as the Chief Executive Officer, Chief Financial Officer, or other executives who have complete access to sensitive data and financial accounts.

Australian Communications and Media Authority

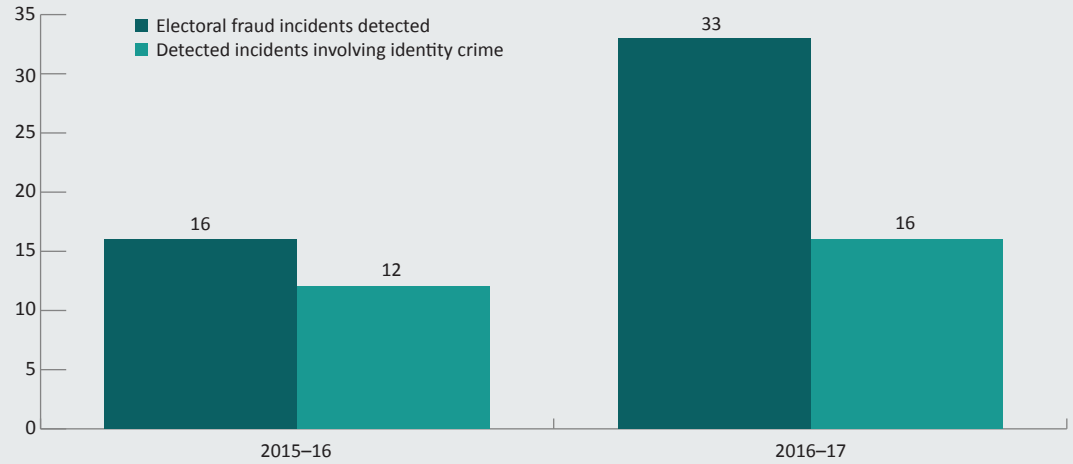
The Australian Communications and Media Authority (ACMA) receives reports of email and text message spam from a number of different sources and collates them in its Spam Intelligence Database. These data are used to identify 'phishing' activities—the use of electronic messages to acquire people's personal 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 2015–16, a monthly average of 3,689 phishing notifications were received, compared with 3,627 in 2014–15. (No data were available for 2016–17.) A trend observed during the reporting period was the increasing use of text messages to facilitate phishing campaigns, often supported by fabricated replicas of mobile banking websites and other sophisticated online forms (ACMA 2017).

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 and activities relating to electoral information and education. The AEC provided data on the number of incidents of electoral fraud detected in 2015–16 and 2016–17, as well as the number of incidents that were identified as involving identity crime and misuse (Figure 25).

Figure 25: Incidents of electoral fraud detected, and incidents involving identity crime and misuse, 2015–16 to 2016–17 (n)



Source: AEC 2017 (unpublished data)

Prosecution of identity crime and related offences

Commonwealth prosecutions

Key finding: CDPP prosecutions relating to fraud, identity crime and other financial crimes declined between 2012–13 and 2016–17. However, the number of fraud prosecutions referred by Centrelink increased 21 percent between 2015–16 and 2016–17. The number of prosecutions referred by other Commonwealth entities also increased.

There are several Commonwealth statutes for which people 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* (Cth) (Criminal Code) 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* (Cth), *Customs Act 1901* (Cth) and the *Trade Marks Act 1995* (Cth).

Offenders who commit identity-related offences against Australian Government entities may be prosecuted by the Commonwealth Director of Public Prosecutions. The CDPP provided a suite of prosecution statistics relating to identity crime offences under the Criminal Code (Table 9).

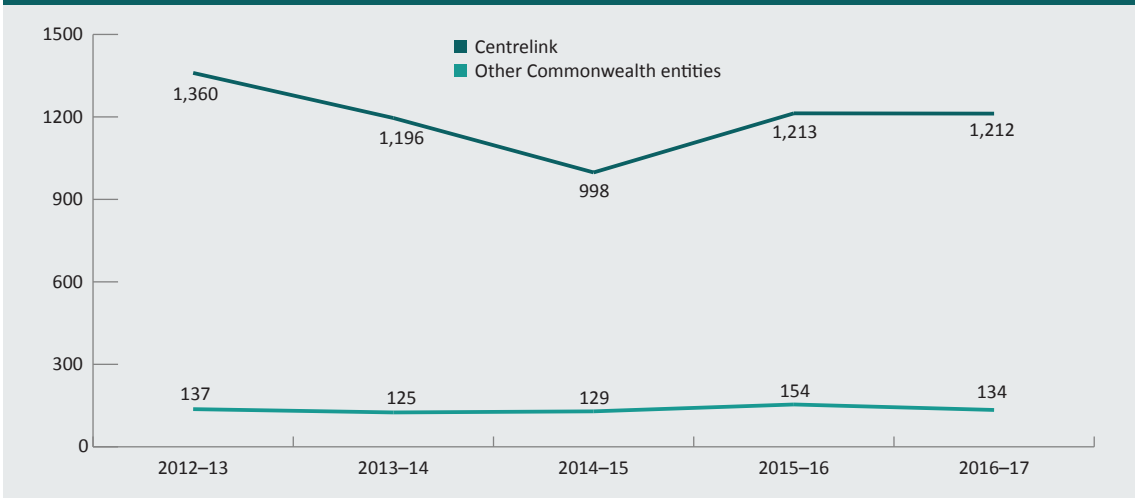
Table 9: Defendants prosecuted by the CDPP by Criminal Code Division and year, 2012–13 to 2016–17 (n)

Offence	2012–13	2013–14	2014–15	2016–17
Criminal Code divs 370, 372, 375—identity crime	1	3	6	4
Criminal Code divs 133–137—fraudulent conduct	1,458	1,313	1,127	1,381
Criminal Code divs 144–145—forgery	24	19	28	26
Criminal Code div 480—financial information offences	9	3	5	0
Migration Act 1958 s 234—False documents and false or misleading information relating to non-citizens	29	10	7	11
Financial Transaction Reports Act 1988 s 24—Opening account etc. in false name	9	3	2	1
Anti-Money Laundering and Counter-Terrorism Financing Act 2006 pt 12—Offences	2	7	2	4
Customs Act 1901 pt XIII—Penal Provisions	13	38	57	0
Trade Marks Act 1995 pt 14—Offences	9	4	3	1
Total	1,554	1,400	1,237	1,424

Source: CDPP 2017 (unpublished data)

The offences regarding fraudulent conduct (*Criminal Code Act 1995* divs 133–137) were examined in greater detail (Figure 26). The CDPP prosecuted 1,346 fraud cases in 2016–17, most of which (1,212; 90%) were referred by the Centrelink division of the Department of Human Services. The number of prosecutions relating to Centrelink matters declined by 27 percent between 2012–13 and 2014–15 but increased by 21 percent between 2014–15 and 2016–17.

Figure 26: CDPP fraud prosecutions by referring entity, 2012–13 to 2016–17 (n)



Source: CDPP 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 ABS (2017b) provided customised data on 22 offence types that were classified as potentially involving identity crime. The bureau was unable to give an assurance that all of these offence types involved identity crime and, as such, these data should be treated with caution. Table 10 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 2015–16. (Data for other years were unavailable.)

Table 10: Identity crime related offences proved in state and territory criminal courts, 2015–16

Offence classification	Proven guilty (n)	Total Finalised (n)	% proved
Obtain benefit by deception (911)	58,781	74,786	78.6
Dishonest conversion (991)	7,427	9,670	76.8
Forgery of documents (922)	2,170	4,660	46.6
Illegal non-fraudulent trade practices (933)	700	937	74.7
Theft (except motor vehicles) (829)	429	462	92.9
Other fraud and deception offences NEC (999)	201	297	67.7
Driver licence offences NEC (1419)	169	205	82.4
Offences against government security NEC 1559	24	202	11.9
Fraudulent trade practices (931)	700	937	74.7
Import/export regulations (1694)	80	140	57.1
Possess equipment to make false/illegal instrument (923)	48	90	53.3
Bribery involving government officials (1542)	76	80	95.0
Receive or handle proceeds of crime (831)	50	68	73.5
Immigration offences (1543)	17	24	70.8
Import or export prohibited weapons/explosives (1111)	3	20	15.0
Resist or hinder police officer or justice official	0	19	0.0
Bribery excluding government officials	11	17	64.7
Misrepresentation of professional status (932)	6	8	75.0
Resist or hinder government official (1541)	0	5	0.0
Commercial/industry/financial regulation (1631)	5	5	100.0
Transport regulation offences (1624)	4	4	100.0
Offences against justice procedures NEC (1569)	3	3	100.0
Total	70,282	91,880	76.5

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

Source: ABS 2017b (Customised report); ABS 2011

Self-reported victimisation of identity crime or misuse

Identity crime is often difficult to detect, because those committing it go to some lengths to conceal their activity and remain anonymous. Modern cybercrime methodologies enable offenders to harvest identity credentials from databases on the darknet, where encryption limits the chances of detection (Krone & Smith 2018). Many victims of identity crime are reluctant to report the crime to police or other official agencies, believing that little can be done to investigate these crimes and to 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 in which respondents report their experience of victimisation, the losses they suffered and how they responded to the occurrence. This report presents the findings of a number of such surveys that sought to ascertain the nature and extent of identity crime in the Australian community.

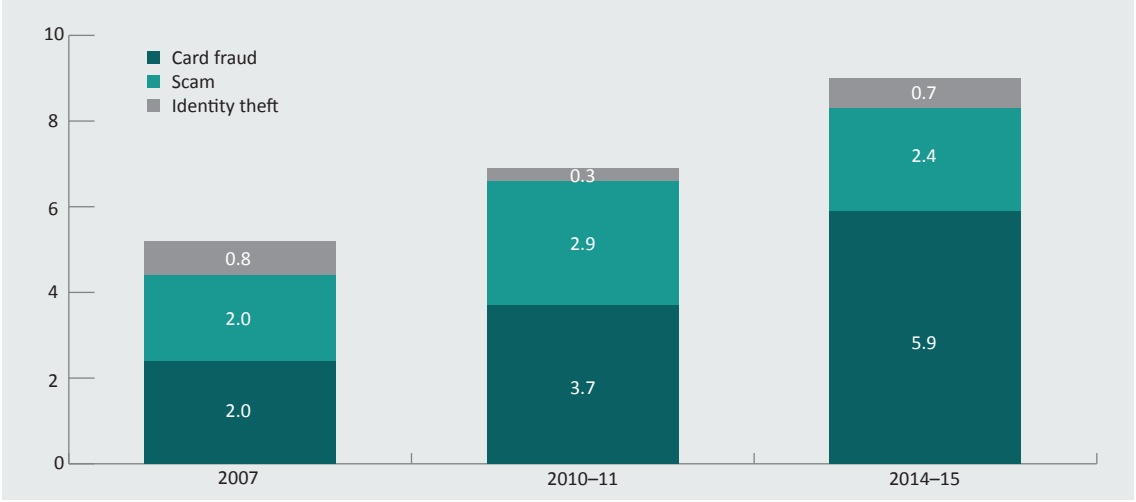
Prevalence

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 AIC identity crime and misuse survey (Goldsmid, Gannoni & Smith 2018) found the number of respondents experiencing misuse in the previous 12 months increased five percent between 2016 and 2017 (8.5% in 2016 vs 13.1% in 2017).

Australian Bureau of Statistics surveys

The most authoritative survey research in Australia was undertaken by the ABS (2016) in its Personal Fraud Survey for 2014–15. The ABS conducted multiple Personal Fraud Surveys between 2007 and 2015. The surveys ask respondents about their experiences of card fraud, identity theft and scams in the 12 months preceding the survey. It should be noted that all three of these incidents may involve misuse of personal information and identity crime. The latest survey found that 6.6 percent of the Australian population aged 15 years and over reported being victims of identity fraud (including both card fraud and identity theft) in the preceding 12 months (Figure 27). This rate is more than double that found by the ABS in its 2007 survey (ABS 2008). If scam victimisation is added to card fraud and identity theft recorded by the ABS in 2014–15, the total personal fraud rate for 2014–15 was 8.5 percent.

Figure 27: Respondents reporting personal fraud victimisation, 2007, 2010–11 and 2014–15 (%)



Note: Due to changes in the survey questionnaire wording regarding experience of identity theft, data from 2014–15 and 2007 are not comparable with those from 2010–11

Source: ABS 2008, 2012 and 2016

This annual victimisation rate is much higher than for other crime types. For example, the ABS (2017a) national Crime Victimisation Survey found that in 2015–16 less than five percent of persons in Australia aged 15 years and over experienced one of four major crime types (and only 0.4 percent of persons aged 18 years and over experienced at least one sexual assault). In the same year, 6.6 percent of persons aged 15 years and over reported experiencing identity crime. This is largely due to the high-volume nature of identity crime, in which a large proportion of internet users are targeted by criminals.

Australian Institute of Criminology surveys

Survey research conducted by the AIC has also found high rates of victimisation, both over a lifetime and during the preceding 12 months. The AIC's surveys have found that over 20 percent of respondents each year reported having experienced misuse of their personal information at some time in the past (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018). As shown in Figure 3 (above), the 2017 rate of 25.2 percent represents a statistically significant 3.7 percentage point rise in lifetime victimisation from 2016, when 21.5 percent of respondents (n=9,956) reported lifetime victimisation (N-1 $\chi^2(1)=38.06$, $p<0.001$).

The AIC's surveys also asked respondents to report their experience of misuse of personal information and out-of-pocket losses in the preceding 12 months. As shown in Figure 4 (above), both 12-month victimisation rates and out-of-pocket loss rates, while remaining relatively stable between 2013 and 2016, increased significantly in 2017, when 13.1 percent of respondents experienced some form of misuse of their personal information in the 12 months prior to participating in the survey, and 9.6 percent of all respondents incurred out-of-pocket losses as a result of this (Goldsmid, Gannoni & Smith 2018).

Equifax (Veda) surveys

Equifax, one of four credit reporting agencies in Australia, took over Australia's credit reference company, Veda, in 2016. Veda regularly conducted research about consumers' views on cybercrime and identity theft and in 2016 found 11 percent of Australians reported having been a victim of identity theft in the past 12 months, an increase from the six percent who reported victimisation in 2015 (Veda 2016).

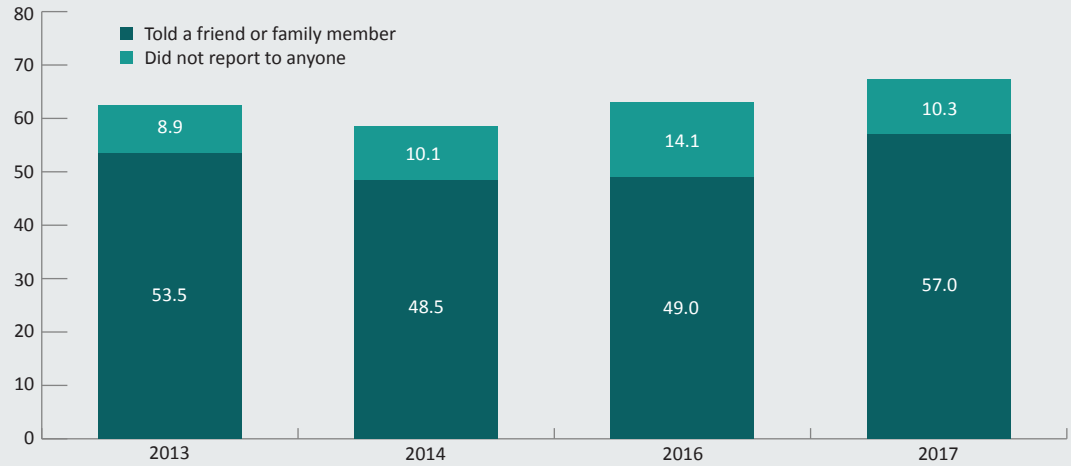
Reporting

Key finding: The AIC's 2017 identity crime survey found an increase in the proportion of respondents who reported their victimisation experience, from 86 percent in 2016 to 90 percent in 2017 (Goldsmid, Gannoni & Smith 2018). However, the ABS (2016) Personal Fraud Survey found a small decline in the percentage of people reporting identity theft, from 31 percent in 2010–11 to 25 percent in 2014–15. The main reasons people did not report incidents were a belief that nothing could be done (22%), followed closely by not knowing to whom the report should be sent (21%) (Goldsmid, Gannoni & Smith 2018).

The rate of reporting misuse of personal information and identity crime is low throughout Australia. A primary reason for the low reporting rate is that people do not know to whom they should report the incident. For example, IDCARE found that the majority of clients were referred by Commonwealth agencies (58.6%), a further 11.4 percent were referred by telecommunications carriers and 11.3 percent by state or territory government agencies. On average it took clients 2.3 contacts before they were directed to IDCARE (IDCARE 2018b). This difficulty in locating an organisation that could help may affect individuals' satisfaction with services and ultimately may contribute to under-reporting of identity crime.

Respondents to the AIC surveys who reported experiencing misuse of personal information were asked if they had reported the crime to anyone or if they had reported the incident officially, such as to a bank, credit card company, law enforcement agency, regulatory office, internet service provider or government agency. Figure 28 shows the proportion of respondents who told only a friend or family member and the proportion who did not report to anyone. Between 2016 and 2017, there was a four percentage point increase in the number of people who made any report, and an eight percentage point increase in the number who reported to friends or family (Goldsmid, Gannoni & Smith 2018).

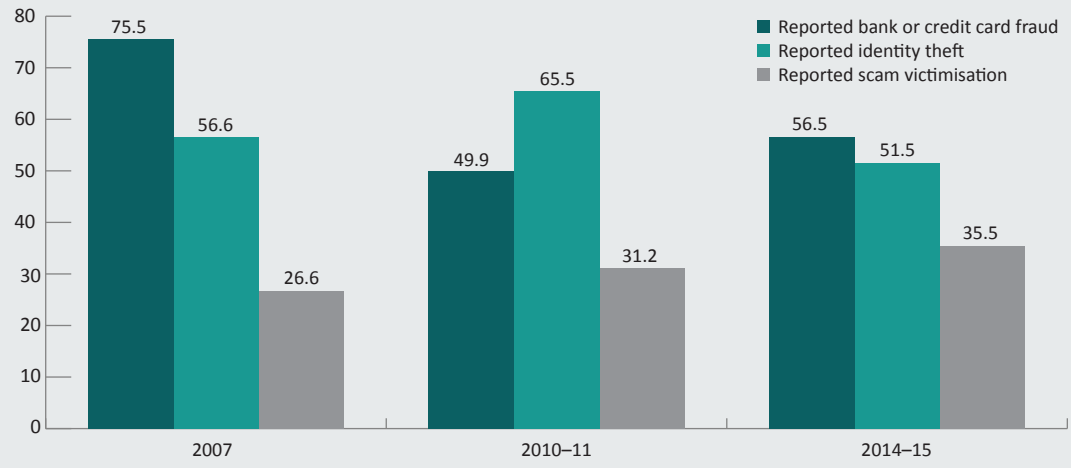
Figure 28: Respondents who did not report misuse of personal information to authorities, 2013 to 2017 (%)



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

The ABS Personal Fraud Surveys, while not comparable with the AIC's misuse of personal information surveys, also asked respondents if they had reported any of the three types of victimisation to various authorities—including police, financial institutions, other businesses and other government agencies. Figure 29 shows the percentage of respondents who reported identity theft, scam victimisation or bank and credit card fraud to authorities in each year covered by the survey.

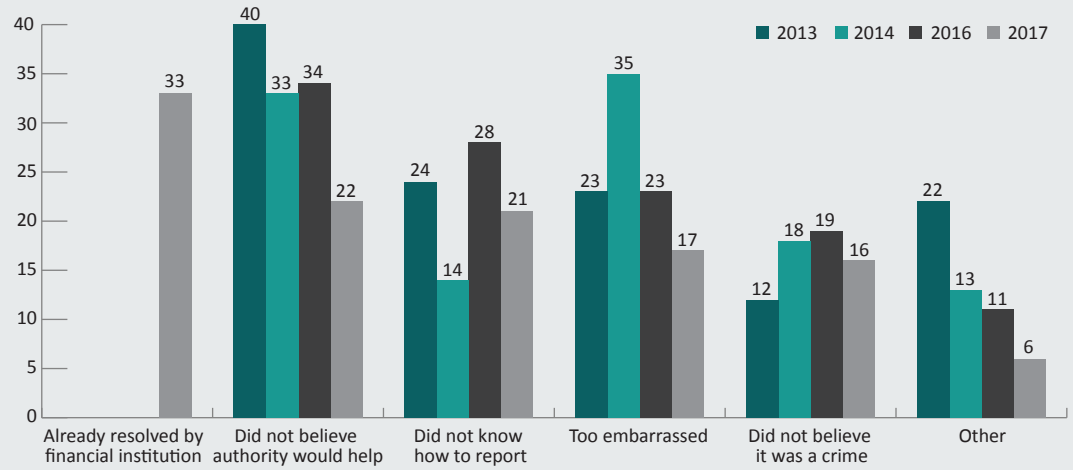
Figure 29: ABS Personal Fraud Survey respondents who reported personal fraud to authorities, 2007 to 2014–15 (%)



Note: Due to changes in the questionnaire wording regarding experience of identity theft, data from 2007 and 2014–15 are not comparable with those from 2010–11. In 2007, not all scam types had data pertaining to reporting to authorities.
Source: ABS 2008, 2012 and 2016

Respondents in the AIC's 2017 identity crime survey (Goldsmid, Gannoni & Smith 2018) who indicated they had not reported the misuse of their personal information to police, a government agency or business were asked why they had not. The most common reason given was that the bank or other financial institution had already resolved the issue (32.5% of respondents who did not report the misuse). The next most common reasons were that the respondent did not think it was important enough to report (22%), and the respondent did not know where to report the matter (21%).

Figure 30: Reasons for not reporting misuse of personal information by year (% of victims)

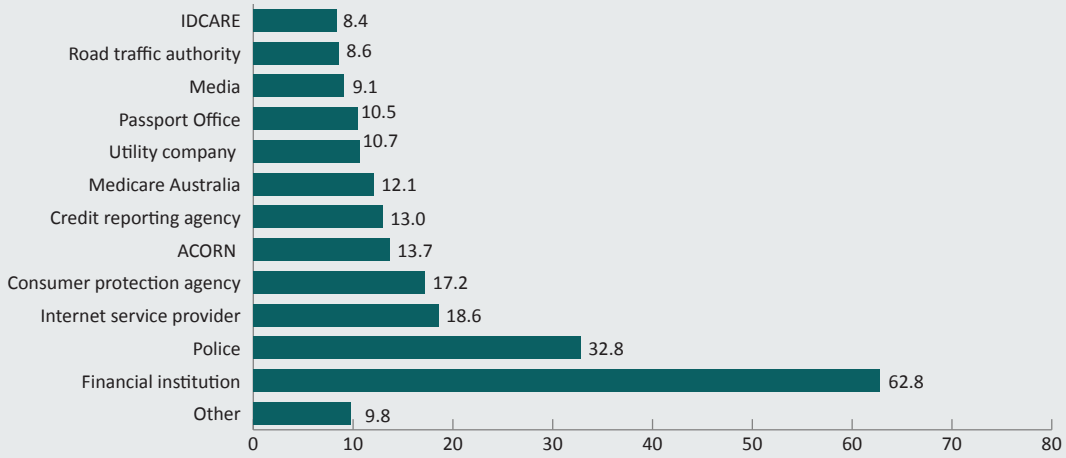


Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender

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

Respondents who did report personal information misuse to a government agency, business or other organisation were asked to specify which specific entity they reported the misuse to (Figure 31). The majority of respondents reported to a bank, credit union or a credit/debit card company (63% of respondents who reported the incident). The police were the next most common agency respondents reported misuse of their personal information to (33%).

Figure 31: Respondents who reported misuse of personal information by organisation reported to, 2017 (%)



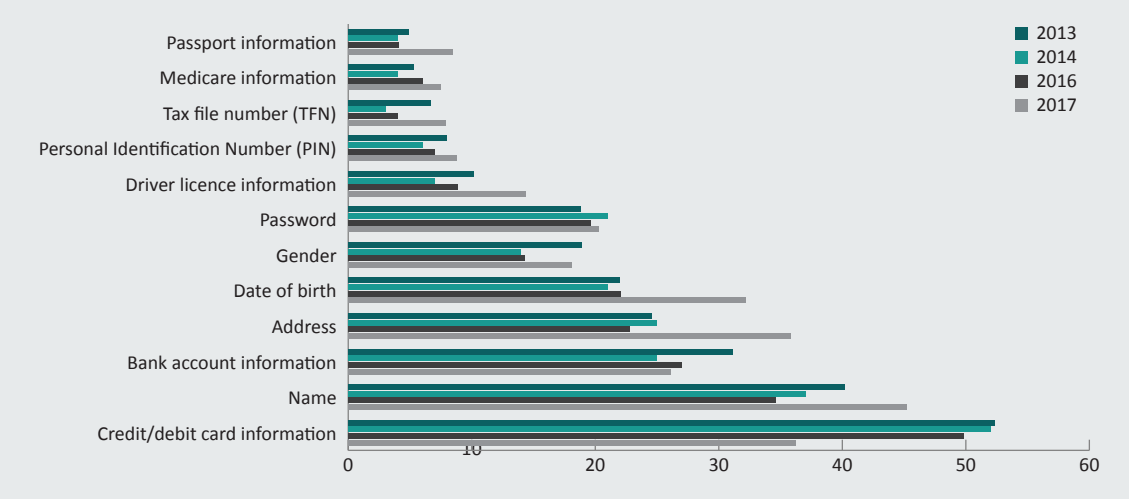
Note: Data weighted by age/gender
Source: Goldsmid, Gannoni & Smith 2018

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 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 type 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 2017, names, addresses, dates of birth and credit card details were most often misused (Figure 32). Comparing 2016 and 2017 data shows a significant increase in reported misuse of address details (13 percentage points), name (11 percentage points), and date of birth (10 percentage points).

Figure 32: Types of personal information that respondents reported as having been misused on the most serious occasion in the previous 12 months, 2013 to 2017 (%)



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

Case study 9: Medicare numbers for sale on the darknet

In July 2017, a journalist for the Guardian Australia revealed that he had been able to purchase his own Medicare details from an auction site on the darknet. While government agencies regularly monitor the darknet to ensure that personal information held by government departments is not being accessed illegally and sold online, a darknet trader had been illegally selling Medicare numbers after identifying and exploiting vulnerabilities in a government computer system. This unauthorised access to government information had gone undetected.

The darknet trader reportedly advertised his products using the logo of the Department of Human Services, naming his business the 'Medicare machine'.

Once made aware of the breach, the Minister for Human Services referred the matter to the Department of Human Services and the Australian Federal Police for further investigation. The chief information officer at DHS stated that the breach was not due to hacking activity but traditional criminal activity.

Medicare card information is valuable among crime syndicates as a means of identification that can be used to facilitate identity fraud. In 2015, police arrested a criminal group that was using Medicare card information to channel Medicare rebate payments into fraudulent bank accounts.

Source: Farrell 2017

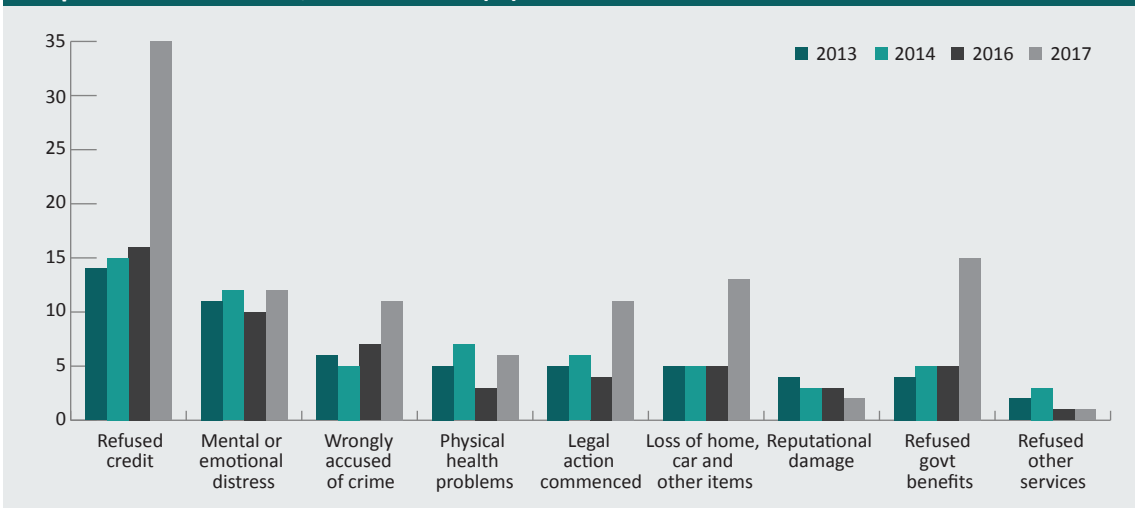
IDCARE's *Identity and cyber security community aftermath report* (2018b) found that driver licences were the most targeted credential misused by criminals in 2017, associated with over 20 percent of IDCARE's cases. IDCARE also found that a combination of driver licence and bank account information was three times more likely than any other combination of identity credentials to result in further misuse of identity (IDCARE 2018b).

Non-financial impact

Key finding: The three most prevalent consequences of identity crime and misuse that victims reported were being refused credit, being refused government benefits and experienced financial difficulties resulting in the repossession of a house, land, motor vehicle or other item.

The AIC's most recent survey found that, aside from being refused credit, the consequences experienced by victims changed between 2016 and 2017. The number of victims who reported having been wrongly accused of a crime increased substantially in 2017 (Figure 33). The majority of other consequences reported by victims were also greater in 2017 than in 2016.

Figure 33: Consequences experienced as a result of personal information being misused in the previous 12 months, 2013 to 2017 (%)



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

Case study 10: Stolen mail leads to fraudulent loan applications

Identity criminals successfully applied for 18 loans in an unsuspecting victim's name. The victim was alerted to possible anomalies with her mail by the local postman. The postman of the small country town had noticed that some Telstra bills were being addressed to a house that the victim had previously lived at. The postman was aware that the victim had moved and delivered the mail to the woman's new address. It was then that the victim discovered the identity theft.

The woman's identity information had been obtained through her driver licence. Criminals used the victim's identity information to apply for 18 loans online. The victim's credit rating was significantly damaged by the fraudulent loans and she was unable to obtain a new driver licence until she could prove she had been a victim of identity crime.

The victim called for changes to the way in which loan applications can be made online. Specifically, more stringent identification processes are needed to ensure the person applying for the loan is truly who they say they are.

Source: Wakatama 2017

Remediation of identity crime

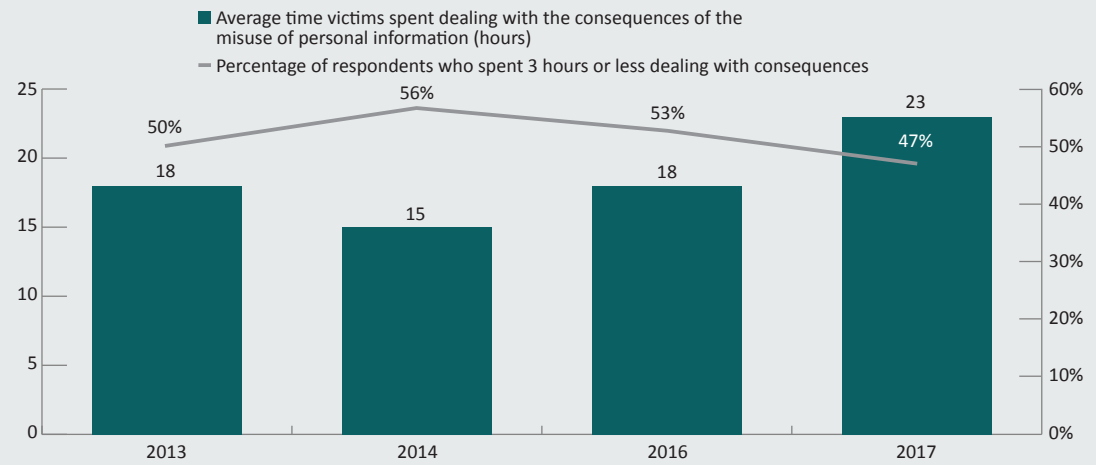
The amount of time it takes for a victim to deal with the consequences of identity crime varies depending on the extent to which identity credentials have been misused. In cases involving fraudulent credit applications or bank transactions, victims incur only minimal inconvenience and financial impost, as financial institutions generally refund losses to individual victims who have not contributed to those losses. In more serious cases, such as those involving a complete takeover of a victim's identity, it can take many hours to rectify the problem.

Time spent restoring identity information

Key finding: The process of recovering misused personal information and restoring one's identity is often complex, difficult and time consuming. The average time victims spent dealing with the consequences of identity crime in 2017 was 23 hours—an increase on the 18 hours reported by victims in 2016 (Figure 34).

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 23 hours in 2017. The percentage of victims who were able to resolve the matter quickly (less than 3 hours) has continued to decline (Figure 34).

Figure 34: Time spent by victims dealing with consequences of misuse of personal information, 2013 to 2017

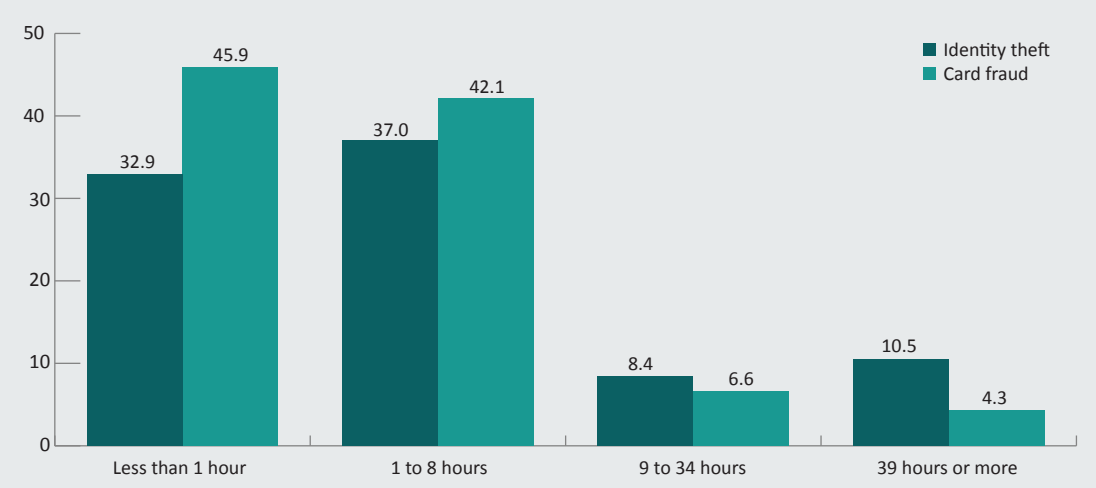


Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender

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

The ABS surveys also found that victims of personal fraud spent many hours dealing with the consequences of their victimisation. Although most took less than eight hours, some spent days restoring information. This includes not only attempting to recover financial losses but also dealing with non-financial consequences such as loss of reputation and damage done to one's credit rating. The ABS Personal Fraud Survey 2014–15 (ABS 2016) found victims of identity theft spent more time dealing with the consequences than victims who experienced card fraud (Figure 35).

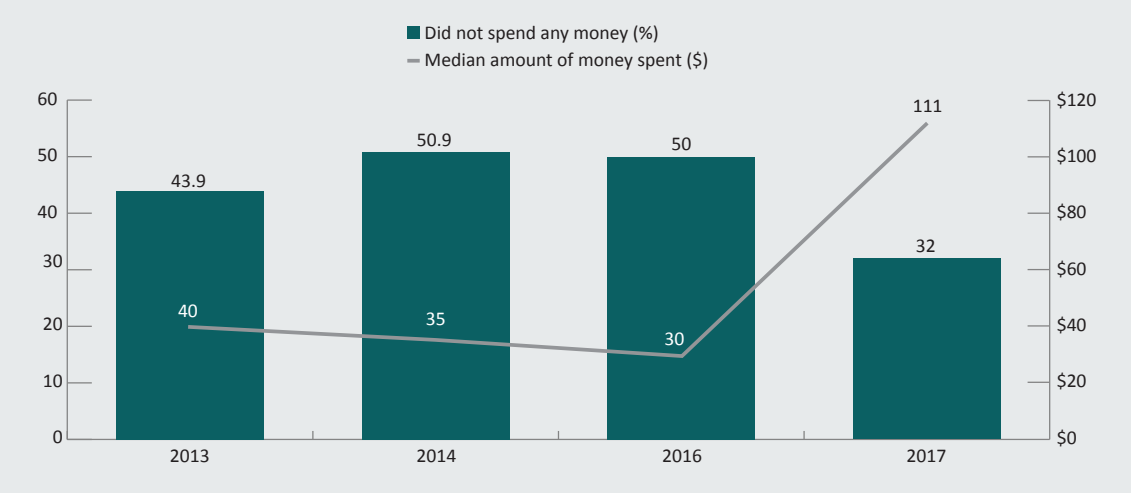
Figure 35: Time victims spent dealing with the consequences of personal fraud, 2014–15 (%)



Source: ABS 2016

The AIC surveys (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018) also collected data on how much money victims spent dealing with the consequences of the misuse of personal information (Figure 36). The 2017 survey found slightly under a third of the respondents did not spend anything, while the median amount spent was $111. This was a substantial increase from previous years; however this is in line with the increase in the losses found in the 2017 survey and the increase in the percentage of people reporting being victims of identity crime in the 12 months prior to completing the survey. This amount does not include the value of victims' time taken to deal with the consequences of misuse.

Figure 36: Amount of money victims spent dealing with the consequences of misuse of personal information, 2013 to 2017



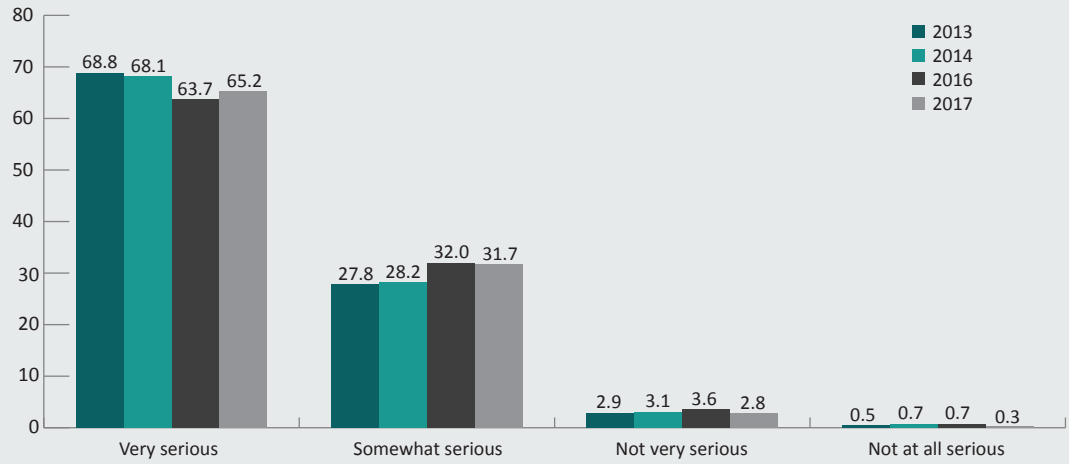
Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender
Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018

Perceptions of seriousness

Key finding: Identity crime remains an ongoing concern for the Australian public. In 2017, almost 97 percent of respondents to the AIC's most recent survey indicated that misuse of personal information was, in their view, 'very serious' or 'somewhat serious'.

Respondents to the AIC surveys (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan 2015; Smith & Jorna 2018b; Goldsmid, Gannoni & Smith 2018) 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 90% each year) believed that misuse of personal information was 'very serious' or 'somewhat serious' (see Figure 37).

Figure 37: Respondents' perceptions of the seriousness of misuse of personal information (%)

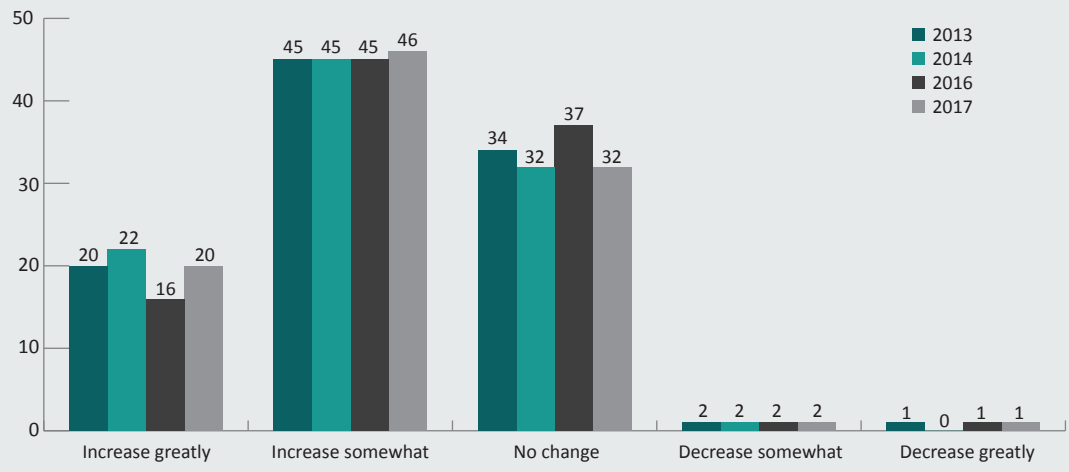


Note: 2013 and 2014 data weighted by location and 2016 and 2017 data weighted by age/gender

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

Respondents were asked to indicate whether they thought the risk of someone misusing their personal information would change over the next 12 months. One in five respondents (19.7%) indicated that they believed their risk of becoming a victim of identity crime would 'increase greatly' over the next 12 months (Figure 38).

Figure 38: Respondents' perceptions of the risk of misuse of personal information in the next 12 months (%)



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

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. During 2017, IDCARE (2018b) responded to over 35,000 enquiries from across Australia and New Zealand, while the Office of the Australian Information Commissioner received 1,765 enquiries concerning Australian Privacy Principle no. 6, which deals with the use or disclosure of personal information.

IDCARE

IDCARE is a Trans-Tasman identity and cyber support service for the community. It was launched in Australia in 2014 and New Zealand in 2015 and receives referrals from different organisations concerning victims of identity crime. It provides support in the form of counselling and assistance in recovering lost funds and identity credentials (IDCARE 2018b).

Between January and December 2017, 35,013 individuals aged 15 years and over in Australia and New Zealand sought assistance from IDCARE. IDCARE (2018b) found it took, on average, 27.5 hours in total to respond to an incident of identity crime. The process involved an average of 8.2 different organisations (with some organisations being contacted on multiple occasions).

Consumer protection agencies

The AIC's 2017 survey (Goldsmid, Gannoni & Smith 2018) found that 17.2 percent of respondents who had experienced having their personal information misused, and had reported the incident to family, friends or an organisation, had made a report to a consumer protection agency. Examples of consumer protection agencies include Scamwatch (operated by the ACCC), the Office of Fair Trading in relevant states and territories and Consumer Affairs agencies. The ABS Personal Fraud Survey for 2014–15 (ABS 2016) found that a lower proportion of respondents had reported their experience of personal fraud to a consumer protection agency. This may be due to people not understanding what the different agencies do or to whom they should be reporting.

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 in 2015–16 and 2016–17. Data were provided by New South Wales Fair Trading, Consumer Affairs Victoria and the Queensland Office of Fair Trading (Table 11). These agencies clearly received far fewer enquiries regarding identity crime than Commonwealth bodies and IDCARE.

Table 11: Enquiries to consumer protection agencies regarding identity crime and misuse, 2015–16 and 2016–17 (n)		
Enquiry or complaint	**2015–16**	**2016–17**
New South Wales Fair Trading	21	26
Consumer Affairs Victoria	50	61
Queensland Office of Fair Trading	0	3

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

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner received at total of 8,001 enquiries from the public relating to the Australian Privacy Principles (APPs) in 2015–16 and 6,825 in 2016–17. These included 2,228 in 2015–16 and 1,765 in 2016–17 relating specifically to APP 6, which is about the use or disclosure of personal information (Table 12).

Table 12: Enquiries related to the APPs received by the OAIC, 2015–16 and 2016–17 (n)						
Privacy Principle	2015–16			2016–17		
	Enquiries	Complaints	Investigations	Enquiries	Complaints	Investigations
APP 1: open and transparent management of PI	135	33	2	76	8	5
APP 2: anonymity and pseudonymity	13	6	0	27	11	0
APP 3: collection of solicited PI	1,271	254	3	1,182	271	3
APP 4: dealing with unsolicited PI	10	4	0	7	7	0
APP 5: notification of the collection of PI	673	96	0	538	71	2
APP 6: use or disclosure of PI	2,228	729	4	1,765	800	10
APP 7: direct marketing	345	121	0	299	108	0
APP 8: cross-border disclosure of PI	120	4	0	88	5	3
APP 9: adoption, use or disclosure of government related identifiers	10	3	1	6	4	0
APP 10: quality of PI	138	173	1	108	212	0
APP 11: security of PI	1,432	444	12	1,214	492	19
APP 12: access to PI	1,519	345	1	1,362	424	2
APP 13: correction of PI	107	48	0	153	35	0
Total	8,001	2,260	24	6,825	2,448	44

Note: PI=personal information
Source: OAIC 2017b (unpublished data)

Case study 11: A data breach of personal information

In October 2016, the Australian Red Cross Blood Service notified the Australian Privacy Commissioner's office of a data breach involving the DonateBlood website. A file containing information relating to approximately 550,000 prospective blood donors was saved to a publicly accessible portion of a webserver managed by a third-party provider. This was an inadvertent error by an employee of the third-party provider. Upon discovering the error, the Australian Red Cross Blood Service took immediate steps to contain the breach and notify affected individuals. On 25 October 2016, an individual scanning the internet for security vulnerabilities located, accessed and made a backup of the data file. The personal information consisted of all information collected about these individuals via the website, and included contact information and answers to questions about their eligibility to donate blood. Some of the information collected was sensitive health information. The categories of personal information collected via the Donate Blood website included:

- identifying particulars: first and last name, gender, date of birth and donor ID (optional)
- contact details: physical address, email address and phone number
- appointment preferences: postcode or suburb for donation, preferred date range and preferred time of day
- yes or no responses to donor eligibility questions: for example, whether or not the prospective donor was taking antibiotics, if they had engaged in risky sexual behaviour, or if they were or had been pregnant in the last nine months.

The circumstances of this incident and the Blood Service's response mean that it is unlikely that there will be adverse consequences for affected individuals. All copies of the database backup have now been destroyed. The Blood Service has enhanced its information handling practices since the incident. The commissioner believes the community can have confidence in the Blood Service's commitment to the security of their personal information. To assure the commissioner and the Australian community that the Blood Service would continue to address the issues identified in the investigation, the Blood Service offered, and the Commissioner accepted, an enforceable undertaking on 28 July 2017.

Source: Coyne 2016

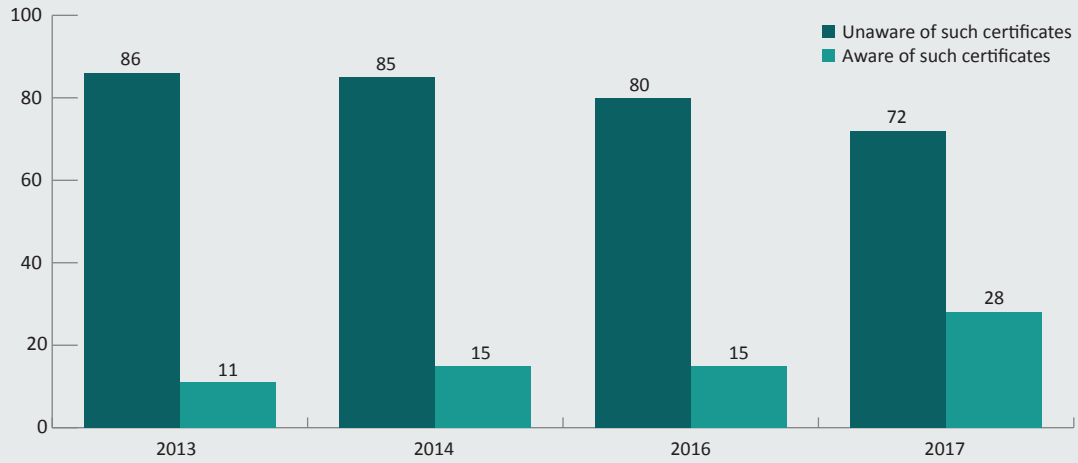
Victims' Certificates

Key finding: Commonwealth Victims' Certificates remain under-utilised, but the proportion of survey respondents who reported being aware of such certificates significantly increased between 2013 (11%) and 2017 (28%).

Findings of the AIC's identity crime surveys indicate a significant increase in awareness of Commonwealth Victims' Certificates—from 11 percent of respondents in 2013 to 28 percent in 2017 (Goldsmid, Gannoni & Smith 2018; see Figure 39). While not all jurisdictions have state-based victim certificates for fraud and identity crime, there is a now a Commonwealth Victims' Certificate that victims can apply for.

Victims' Certificates are issued by magistrates' courts. Victims can present them to government agencies, financial institutions or credit agencies to support their claim that they have been a victim of identity crime. These certificates may help victims resolve business or personal affairs with the organisation in question, although their use is, at present, minimal. IDCARE (2018b) found only three clients out of approximately 35,000 had successfully applied for a Commonwealth or state identity crime victim certificate.

Figure 39: Respondents' awareness of Victims' Certificates, 2013 to 2017 (%)



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

Prevention of identity crime

Almost all of the AIC's survey respondents indicated that harm to the Australian community caused by the misuse of personal information was 'somewhat serious' or 'very serious'. 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 private sector agencies using the Document Verification Service (DVS) increased 47 percent, from 350 in 2016 to 513 in 2017. The number of government entities using the DVS also increased, from 45 entities in 2015–16 to 79 entities in 2016–17.

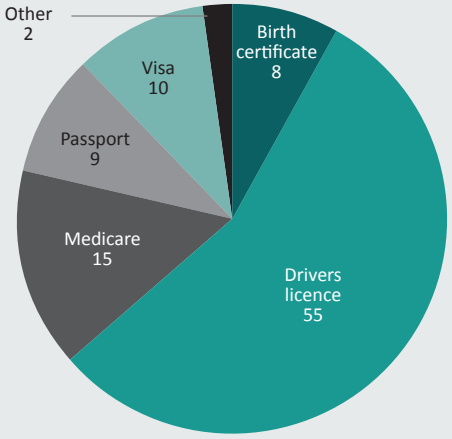
The Document Verification Service is one of the key initiatives of the Council of Australian Governments' National Identity Security Strategy. It allows organisations to compare information from a person's identity document, with their consent, with the corresponding record of the agency that issued 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. From 31 March 2015, the DVS was extended to a wider range of businesses with a reasonable need to verify a client's identity (Department of Home Affairs 2018).

The DVS can be used to verify information relating to most government-issued identity credentials. This includes four credentials identified in this report as being most at risk of misuse (Medicare cards, driver licences, birth certificates and passports).

Identity credentials verifiable

Since 2014 the DVS has been available to government agencies and private sector organisations. Figure 40 presents the main types of documents verified using the DVS in 2016–17.

Figure 40: Documents verified using DVS, by document type, 2016–17 (%)



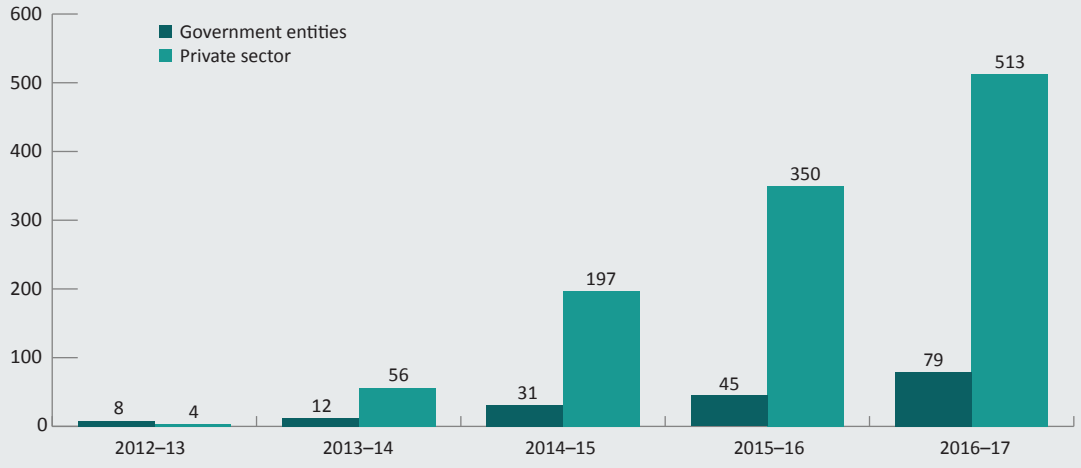
Note: 'Other' includes ImmiCards, marriage certificates, citizenship certificates, change of name certificates and registration by descent certificates. Percentages may not total 100 due to rounding

Source: Department of Home Affairs 2017 (unpublished data)

Organisations using the service

Private sector organisations were given access to the DVS from 2014, explaining the sharp increase in the number organisations accessing the DVS in the last few years. In 2017 the number of private sector agencies using the DVS increased 47 percent, from 350 in 2016, to 513 in 2017 (Figure 41).

Figure 41: Number of agencies using the DVS, 2012–13 to 2016–17 (n)



Note: Private sector access to DVS available from 2014

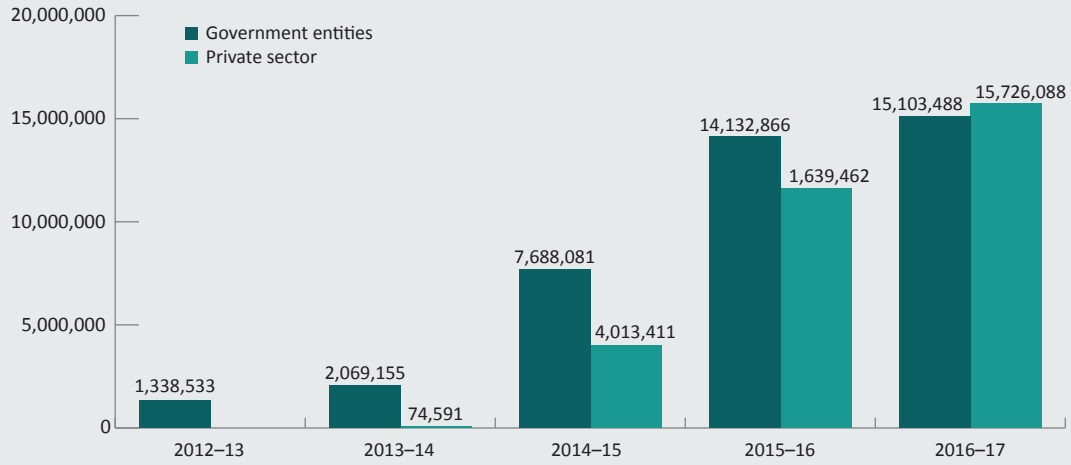
Source: Department of Home Affairs 2017 (unpublished data)

The number of transactions each year

In 2017, the number of transactions attributed to private sector organisations was higher than the number of transactions initiated by government entities (Figure 42).

Once private sector organisations were given access to the DVS in 2014, their uptake was swift. In 2017 government agencies verified over 15 million identity documents and private sector organisations verified over 15.7 million documents through the DVS.

Figure 42: DVS transactions, 2012–13 to 2016–17 (n)



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

Source: Department of Home Affairs 2017 (unpublished data)

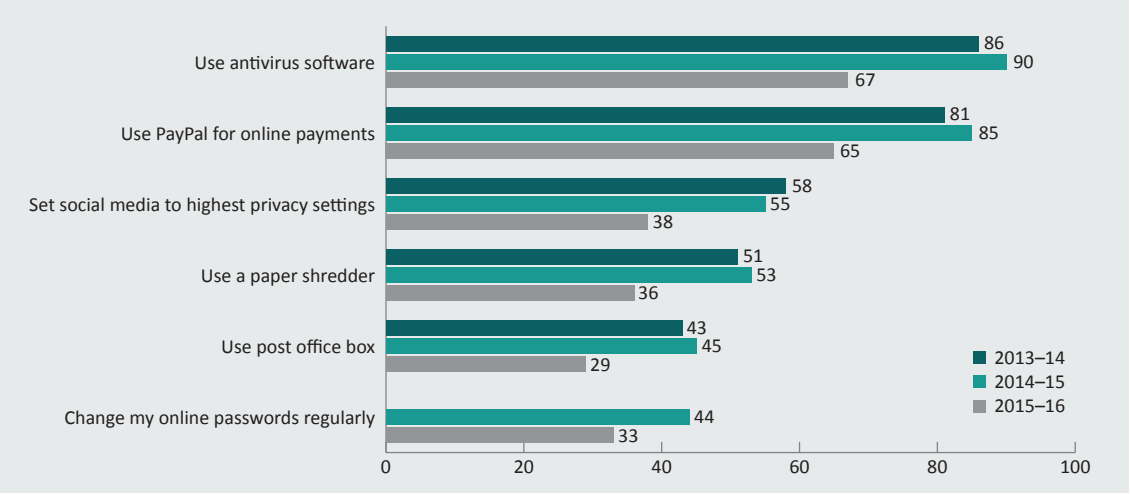
Identity crime prevention practices

Key finding: The Australian Cyber Security Centre (ACSC 2017) found that 90 percent of organisations faced some form of attempted or successful cybersecurity compromise during the 2015–16 financial year. The AIC's survey research has found the most common behavioural change reported by individual respondents is changing passwords once they had experienced misuse of their personal information.

Individuals

Each year more and more people use information technologies for work purposes, for personal administration such as paying bills or applying for government services, and for shopping and entertainment. This reliance on the internet is the principal contributing factor to online identity crime, making it important for users to limit their exposure to identity crime by maintaining adequate computer and telecommunications security. Equifax (formerly Veda), a national credit reference organisation, reports on insights into consumers' views and concerns about identity theft and cybercrime in general. Veda (2016) found in a recent review of cybercrime prevention measures that use of most measures declined between 2013–14 and 2015–16. This could be because of user complacency, barriers to ease of use or a perception that computer security has become automated (Figure 43).

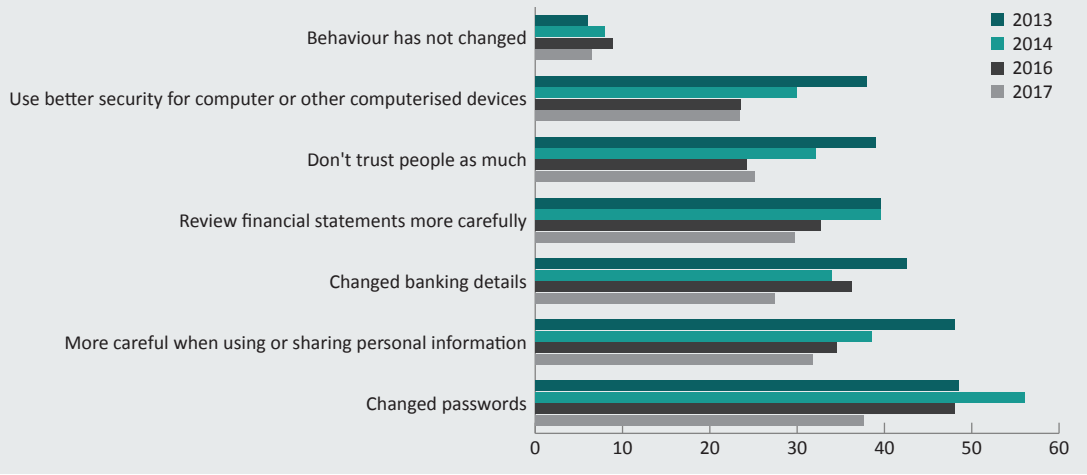
Figure 43: Methods used to prevent identity crime, 2013–14 to 2015–16 (% of respondents)



Source: Veda 2016

The AIC's identity crime and misuse surveys asked respondents if they had changed their behaviour following the misuse of their personal information. The most common behavioural change reported by respondents was changing passwords, followed by becoming more careful when using or sharing personal information (Figure 44).

Figure 44: Behaviour changes arising from the misuse of personal information, 2013 to 2017 (% of respondents)



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

Businesses

Cybercrime remains a persistent threat to most Australian businesses. The Australian Cyber Security Centre (ACSC 2017) found in a review of Australian organisations that 90 percent faced some form of attempted or successful cybersecurity compromise during the 2015–16 financial year. Organisations face numerous malicious cyberthreats daily. Some businesses receive hundreds of spear phishing emails each day (see Smith 2018).

The Australian Competition and Consumer Commission's (ACCC 2017a) eighth annual report on scam activity included data on scams targeting Australian businesses. These totalled 5,953 in 2016, with 356 businesses losing $3,784,779. This represents 3.8 percent of the total number of 155,035 scam reports made to Scamwatch, or 4.5 percent of the total losses of $83,563,599. Of the $3.8m total amount lost by businesses, over $2m was reported lost by micro and small businesses. The average loss was $10,631.

Although cyber defences have gradually improved, adversaries have kept pace by adapting their tradecraft and tools to circumvent enhanced security practices (ACSC 2017). Small and medium-sized enterprises are at continuing risk of victimisation, because they have limited resources available for investment in cybersecurity measures. Organised cybercriminals are also broadening their scope by targeting professional practices in law and accountancy with phishing attacks and CEO fraud (Smith 2018).

Case study 12: Ransomware and identity misuse

The Australian private sector continues to be a target for malicious activity, ranging from low impact incidents such as website vandalism through to high impact intrusions that result in the loss of valuable intellectual property.

Credential-harvesting malware poses an increasing threat to Australian businesses by enabling the theft of credentials such as login details and account numbers. The ACSC has observed a shift in cybercriminals' targeting practices and capability. Specifically, they are developing expertise and malware to target Australia and they are increasingly targeting Android smartphones.

Gozi is one of the longest operating credential-harvesting malware campaigns. First discovered in 2007, Gozi's impact on Australian victims has increased. Gozi was originally operated by a closed group of cybercriminals who continually upgraded the malware and added new features. Three members of the group were arrested in 2013 but the malware continues to be operated by other cybercriminal groups. Gozi shows that experienced cybercriminals can become a persistent threat to the financial sector and can be resistant to law enforcement intervention.

Source: ACSC 2017

Government agencies

As more government services move online there is a new imperative to embrace cybersecurity as a core objective of digital transformation. No system connected to the internet can have guaranteed security. However, information security must be integral at all steps in the rollout of online services. The Australian National Audit Office (ANAO) in 2016 found Commonwealth entities were striving to meet the requirements of the Australian Government Information Security Manual (ISM) to reduce the role of cybercrime in identity crime (ANAO 2016). A survey conducted by the Australian Cyber Security Centre (ACSC 2016) found that 70 percent of organisations (private and governmental) displayed a high level of cyber-resilience, although 43 percent of organisations identified cybersecurity threats only after they had manifested as a compromise, indicating there was still room for improvement.

Conclusions

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 rose in the past year, from 8.5 percent of respondents to 13.1 percent. This increase particularly reflects the rise in phishing scams via email and telephone.

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 that the true extent of the problem could be understood. Further research is, however, needed to understand the extent of identity crime, particularly through improved official statistics, data collected in the private sector, 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 to increase. Financial losses also continue to rise, as do the equally harmful non-financial consequences, which include damage to credit ratings, being wrongly accused of crime, and psychological 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 August 2018

Attorney-General's Department (AGD) 2017a. Document Verification Service. https://www.dvs.gov.au

Attorney-General's Department (AGD) 2017b. Victims of Commonwealth identity crime. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime

Attorney-General's Department (AGD) 2016. *Identity crime and misuse in Australia 2016*. Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime

Attorney-General's Department (AGD) 2015. *Identity crime and misuse in Australia 2013–14.* Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/criminal-justice/files/identity-crime-misuse-australia-2013-14.pdf

Attorney-General's Department 2014. *Identity crime and misuse in Australia – Key findings from the National Identity Crime and Misuse Measurement Framework Pilot.* Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-crime-and-misuse-pilot.pdf

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

Australasian Centre for Policing Research 2006. *Standardisation of definitions of identity crime terms: A step towards consistency.* Report series no. 145.3. Canberra: Commonwealth of Australia

Australian Bureau of Statistics (ABS) 2017a. *Crime victimisation, Australia, 2015–16.* ABS cat. no. 4530.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0

Australian Bureau of Statistics 2017b. Customised report. Data provided by National Centre for Crime and Justice Statistics. Melbourne: ABS

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. http://www.abs.gov.au/ausstats/abs@.nsf/mf/3101.0

Australian Bureau of Statistics 2012. *Personal fraud, 2010–11.* ABS cat. no. 4528.0. Canberra: ABS

Australian Bureau of Statistics 2011. *Australian and New Zealand Standard Offence Classification (ANZSOC), 2011.* ABS cat. no. 1234.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/1234.0

Australian Bureau of Statistics 2008. *Personal fraud, 2007.* ABS cat. no. 4528.0. Canberra: ABS

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) 2017. *Australian Communications and Media Authority 2016–17 Annual Report.* https://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/annual-report

Australian Competition and Consumer Commission (ACCC) 2017a. *Targeting scams: Report of the ACCC on scams activity 2016.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

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

Australian Criminal Intelligence Commission (ACIC) 2018. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Cybercrime Online Reporting Network (ACORN) 2018. About the ACORN. https://www.acorn.gov.au/about-acorn

Australian Cyber Security Centre (ACSC) 2017. *Australian Cyber Security Centre threat report 2017.* Canberra: ACSC. https://www.acsc.gov.au/publications.html

Australian Cyber Security Centre 2016. *Australian Cyber Security Centre 2016 cyber security survey.* Canberra: ACSC. https://www.acsc.gov.au/publications.html

Australian Electoral Commission (AEC) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Federal Police (AFP) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian National Audit Office (ANAO) 2016. *Cyber resilience across entities.* Auditor-General's Report no. 37 of 2015–16. https://www.anao.gov.au/work/performance-audit/cyber-resilience

Australian Payments Network 2017. *Australian payments fraud 2017: Jan–Dec 2016 data.* https://www.auspaynet.com.au/resources/fraud-statistics/2016-calendar-year

Australian Securities and Investments Commission (ASIC) 2018. Our role. https://asic.gov.au/about-asic/what-we-do/our-role/

Australian Securities and Investments Commission 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Taxation Office (ATO) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Australian Transaction Reports and Analysis Centre (AUSTRAC) 2017. 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 prepared for the Commonwealth Attorney-General's Department. Canberra: Australian Institute of Criminology

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

Consumer Affairs Victoria 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Coyne A 2016. Australia's biggest data breach sees 1.3m records leaked. *ITNews* 28 Oct. https://www.itnews.com.au/news/australias-biggest-data-breach-sees-13m-records-leaked-440305

Crime Statistics Agency (Victoria) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

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

Department of Foreign Affairs and Trade (DFAT) 2017b. *Annual report 2016–17.* Canberra: DFAT

Department of Foreign Affairs and Trade (DFAT) 2015. DFAT passport fraud, in *Identity crime and misuse in Australia 2016.* Canberra: AGD. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime

Department of Home Affairs 2018. Document verification service. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/document-verification-service

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

Department of Human Services (DHS) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Department of Immigration and Border Protection (DIBP) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Farrell P 2017. The Medicare machine: Patient details of 'any Australian' for sale on darknet. *Guardian Australia,* 4 Jul. https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet

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

IDCARE 2018a. Strategic intelligence assessment: Dark net tradecraft after Operation Bayonet

IDCARE 2018b. Identity & cyber security community aftermath report 2018

IDCARE 2018c. Exploitation of birth certificates by identity criminals

IDCARE 2015. Australia Observations of Identity Compromise and Misuse 2015, in *Identity crime and misuse in Australia 2016.* Canberra: Attorney-General's Department. Available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security/identity-crime

Jorna P & Smith RG 2018a. *Commonwealth fraud investigations 2015–16.* Statistical Report no. 7. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr7-0

Jorna P & Smith RG 2018b. *Fraud against the Commonwealth: Report to Government 2014–15.* Statistical Report no. 3. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/sr/sr3

KPMG 2013. *A survey of fraud, bribery and corruption in Australia and New Zealand 2012.* Melbourne: KPMG

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

Machado L 2017. Within an hour of taking over her phone number, they got into her internet banking. *Daily Telegraph* 18 Jan. https://www.dailytelegraph.com.au/newslocal/rouse-hill-times/within-an-hour-of-taking-over-her-phone-number-they-got-into-her-internet-banking/news-story/32103dfa6997c5d76048a86b9f01041d

Morri M 2017. Identity theft: Ruthless gangs use fake driver-licences and Medicare cards for crime sprees. *Daily Telegraph* 12 Mar. http://www.dailytelegraph.com.au/news/nsw/identity-theft-ruthless-gangs-use-fake-drivers-licences-and-medicare-cards-for-their-crime-sprees/news-story/831a7b814d7b2b4868eab31da044de57

National Fraud Authority (NFA) 2013. *Annual fraud indicator 2013.* London: NFA. https://www.gov.uk/government/publications/annual-fraud-indicator--2

New South Wales Bureau of Crime Statistics and Research (NSW BOCSAR) 2017. NSW Recorded Crime Statistics July 2015 to June 2017: National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

New South Wales Fair Trading 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

New South Wales Police Force (NSWPF) 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

New South Wales Registry of Births, Deaths and Marriages 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Northern Territory Police, Fire and Emergency Services 2017. *Annual report 2016–17.* Darwin: NTPFES. http://www.pfes.nt.gov.au/Publications-and-forms.aspx

Office of the Australian Information Commissioner (OAIC) 2018. *Quarterly statistics report: January 2018 – March 2018.* Canberra: OAIC. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Office of the Australian Information Commissioner 2017a. Notifiable Data Breaches scheme. https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

Office of the Australian Information Commissioner 2017b. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Ponemon Institute 2017. 2016 *Cost of data breach study: Australia.* Ponemon Institute Research Report, IBM Security. Michigan, USA: Ponemon Institute LLC. https://www-03.ibm.com/security/au/en/data-breach/

PricewaterhouseCoopers (PwC) 2018. *The economic impacts of potential illegal phoenix activity.* Report prepared for the Australian Taxation Office, Fair Work Ombudsman and Australian Securities and Investments Commission. https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/The-economic-impact-of-potential-illegal-phoenix-activity-report

Queensland Office of Fair Trading 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Queensland Police Service (QPS) 2018. *Region and district crime statistics 1 July 2012 to 30 June 2017.* https://www.police.qld.gov.au/rti/published/about/crime+statistics.htm

Robertson A 2017. Tax: Be careful with that big return, it could be a costly scam. ABC News 11 Aug. http://www.abc.net.au/news/2017-08-11/new-cyber-scams-worry-ato/8795520

Smith RG 2018. *Estimating the cost to Australian businesses of identity crime and misuse*. Research Report no. 15. Canberra: Australian Institute of Criminology

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 & 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

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

Smith RG, Jorna P, Fuller G & Sweeney J 2014. *Counting the costs of crime in Australia: A 2011 estimate.* Research and public policy series no. 129. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/rpp/rpp129

South Australia Office of Crime Statistics and Research (SA OCSAR) 2017. Office of Crime Statistics Police Database (Police Apprehension Reports). National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

South Australia Police 2018. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Symantec 2017. *Internet security threat report (ISTR)* vol 22. California: Symantec Worldwide

Tasmanian Department of Police, Fire and Emergency Management (DPFEM) 2017. *Annual report 2016–17.* http://www.police.tas.gov.au/historical-corporate-documents/annualreport20162017

Tasmanian Registry of Births, Deaths and Marriages 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Veda 2016. *2016 cybercrime and fraud report.* https://www.equifax.com.au/idmatrix/resources/news-and-articles/vedas-2016-cybercrime-fraud-report

Vedelago C & Houston C 2016. Fake identities: Buying counterfeit Medicare cards, no questions asked. *Sydney Morning Herald* 10 Jun. http://www.smh.com.au/national/buying-counterfeit-medicare-cards-no-questions-asked-20160610-gpgj1v.html

Verizon 2017. *2017 Data breach investigations report 10th edition.* https://www.verizonenterprise.com/verizon-insights-lab/dbir/

VicRoads 2017. *Annual report 2016–17*. Melbourne: VicRoads. https://www.vicroads.vic.gov.au/about-vicroads/corporate-responsibility/vicroads-annual-report

Victoria Police 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

Wakatama G 2017. Woman fights to reclaim identity after ID theft. ABC News 4 Jul. http://www.abc.net.au/news/2017-07-04/id-theft-like-a-bad-movie/8672400

Western Australia Police Force 2018. Crime Statistics. https://www.police.wa.gov.au/Crime/CrimeStatistics#/

Western Australia Registry of Births, Deaths and Marriages 2017. National Identity Crime and Misuse in Australia 2017 Report: Data Request. Unpublished data

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
1.2 Number of reported data breaches	Acts as a proxy measure of organisational cyber security 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

Table A1: Measurement indicators of identity crime and misuse and data sources

Indicator	Description	Data source
Use of fraudulent identities		
This component covers activities associated with the different uses to which fraudulent identity information may be put; or 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 DIBP ACCC Registries of births, deaths & marriages Consumer protection agencies Police (state & territory) Privacy commissioners Road & traffic authorities
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
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

Table A1: Measurement indicators of identity crime and misuse and data sources

Indicator	Description	Data source
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 DIBP 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 Symantec KPMG
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
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 the broader activities such as support services for victims, and the time they spend recovering their identity.		
4.1 Average time by victims spent in remediation activity (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 courts)	Assesses the application rate for Victims' certificates in each Australian jurisdiction.	Home Affairs ABS CDPP

Table A1: Measurement indicators of identity crime and misuse and data sources

Indicator	Description	Data source
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 CERT Australia Australian Cyber Security Centre ANAO ACMA AIC Ponemon Verizon
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

Cybersecurity incident: an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it. A compromise is an incident where the security of a system or its information was successfully harmed. (ANAO 2016)

Data breach: an incident in which information was 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. (2007 Intergovernmental agreement to a National Identity Security Strategy: 2)

Identity fabrication: the creation of a fictitious identity. (Adapted from Australasian Centre for Policing Research 2006: 15)

Identity fraud: gaining money, goods, services or other benefits or avoiding obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity. (2007 Intergovernmental agreement to a National Identity Security Strategy; Australasian Centre for Policing Research 2006: 15)

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,

(k) an ABN.

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

Identity manipulation: altering one or more elements of identity (eg name, date of birth, address). (Adapted from Australian Centre for Policing Research 2006: 15)

Identity misuse: using personal information for purposes extraneous to the original transaction—such as renting it to a vendor of related products, or mining it to create a consumer profile or direct marketing list. (Ludington 2006: 146)

Identity takeover: assuming parts or all of the identity of another person with their consent. (Adapted from advice provided by the AFP/NSW Police Force Identity Security Strike Team)

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)

Impersonation: the act of pretending to be another person, or acting in that other person's capacity as a public official; the person does so knowing it to be in circumstances when the official is likely to be on duty; the person does so with the intent to deceive. (Adapted from the *Criminal Code Act 1995* (Cth))

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	No
Australian Bureau of Statistics	Yes
Australian Competition and Consumer Commission	Yes
Australian Communications and Media Authority	No
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 Immigration and Border Protection	Yes
Department of Industry, Innovation and Science	Yes (advised no identity fraud)
Department of Infrastructure 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	No (data not collected)
Vic	Victoria Police	Yes
	Births, Deaths and Marriages Victoria	No (data not collected)
	Roads Corporations Victoria (VicRoads)	No
	Consumer Affairs Victoria	Yes
Qld	Queensland Police Service	No
	Registry of Births, Deaths and Marriages (Department of Justice and Attorney-General)	No
	Office of Fair Trading	Yes
	Department of Transport and Main Roads	Yes
WA	Western Australia Police Force	No
	Department of Transport	Yes
	Registry of Births, Deaths and Marriages	Yes
	Department of Commerce—Consumer Protection	No
SA	South Australia Police	No
	SA Office of Crime Statistics and Research	Yes
	SA Births, Deaths and Marriages Registration Office	No
	Department of Transport and Infrastructure	No
	South Australia Office of Consumer and Business Services	No
Tas	Tasmania Police	No (data included in annual report)
	Consumer Affairs and Fair Trading	No
	Department of Justice—Births, Deaths and Marriages	Yes
	Department of State Growth (Transport)	Yes
ACT	ACT Policing (AFP)	Yes
	Office of Regulatory Services	No
	Transport Canberra and City Services	No
	ACT Births, Deaths and Marriages	No

Table C2: State/territory government agencies asked to provide data		
State or territory	**Agency name**	**Provided data**
NT	NT Police Force	No (crime statistics published)
	NT Department of Transport	No
	NT Registry of Births, Deaths and Marriages	No
	NT Consumer Affairs	No

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 recorded 34 matters involving identity crime in 2015–16 and 2016–17. Of these, 20 matters were reported in the 2015–16 financial year, and 14 matters in 2016–17. 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

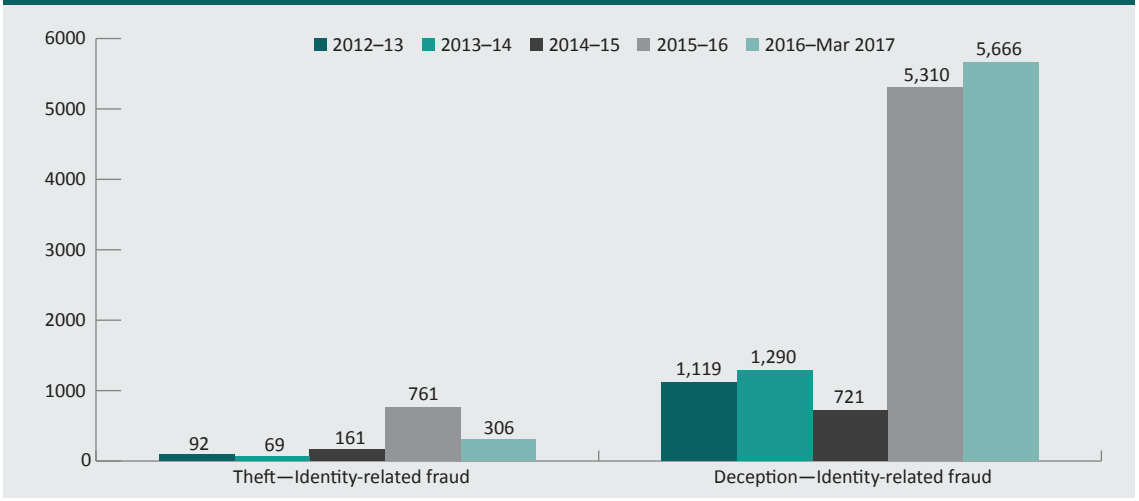
Data from the NSW Police Force indicate that over 30 percent of fraud cases involved identity crime and misuse. The NSW Police Force noted that the way in which police record identity crime and misuse incidents has changed in recent years and comparisons with earlier years were not available.

However, the NSW Bureau of Crime Statistics (BOCSAR) supplied data. According to the NSW BOCSAR, 47,934 cases of fraud were reported in New South Wales during 2016–17 (NSW BOCSAR 2017), compared with 51,137 reported cases in 2015 (AGD 2016).

Victoria Police

There were 34,605 fraud (deception) offences recorded by Victoria Police in the calendar year 2016, a decrease from the 36,988 recorded for the 2015 calendar year (Table D1). 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, 2012–13 to 2016–17 (n)

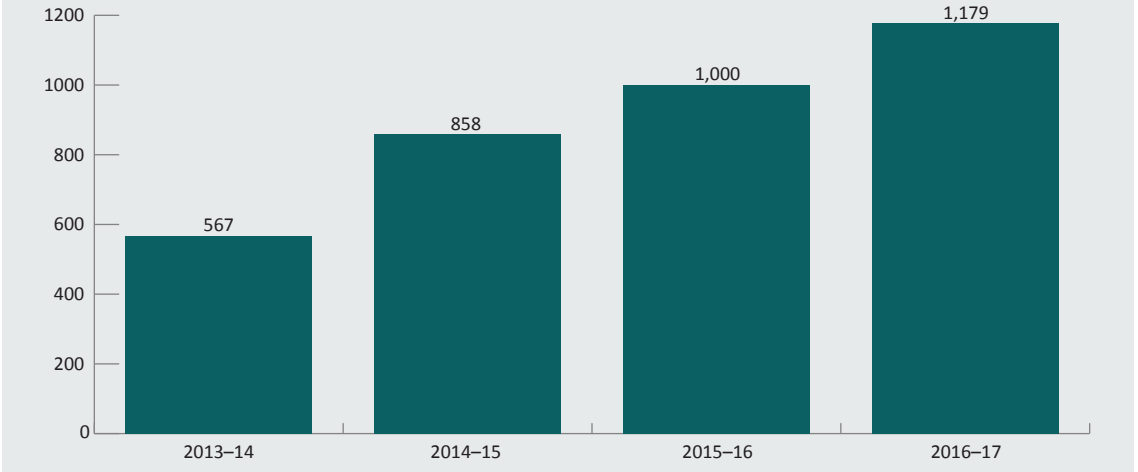


Source: Crime Statistics Agency 2017 (unpublished data)

Queensland Police Service

In total, there were 27,258 fraud offences reported to the Queensland Police Service in 2016–17. Of those offences, 1,179 involved identity fraud, while 13,203 involved credit card fraud and 454 fraud by computer. These last two types could also involve an element of misuse of personal information.

Figure D2: Identity fraud offences in Queensland, 2013–14 to 2016–17 (n)



Source: QPS 2018

Western Australia Police Force

The Western Australia Police Force did not provide data about the number of identity crime investigations or losses experienced by victims but does publish information on fraud offences which allows for comparisons with other jurisdictions. There were 16,154 reported cases of fraud in 2016–17, a decrease from the 22,212 cases reported in 2015–16 (WA Police Force 2018). A description of what a fraud offence may include is provided below.

This offence category includes the following offences:

- offences involving a dishonest act or omission carried out with the intention of deceiving for the purpose of obtaining a benefit, or avoiding some detriment/advantage
- forging or uttering records with intent to defraud, counterfeiting currency, or possessing equipment to forge or counterfeit. Includes all attempts;
- the use of deception or impersonation with the intent of dishonestly obtaining property, services or other benefits, or to avoid detriment/disadvantage, through the use of unlawfully obtained credit/debit card information; and

fraud not elsewhere classified. Prior to June 2017 this offence type included credit card fraud (WA Police 2018: np).

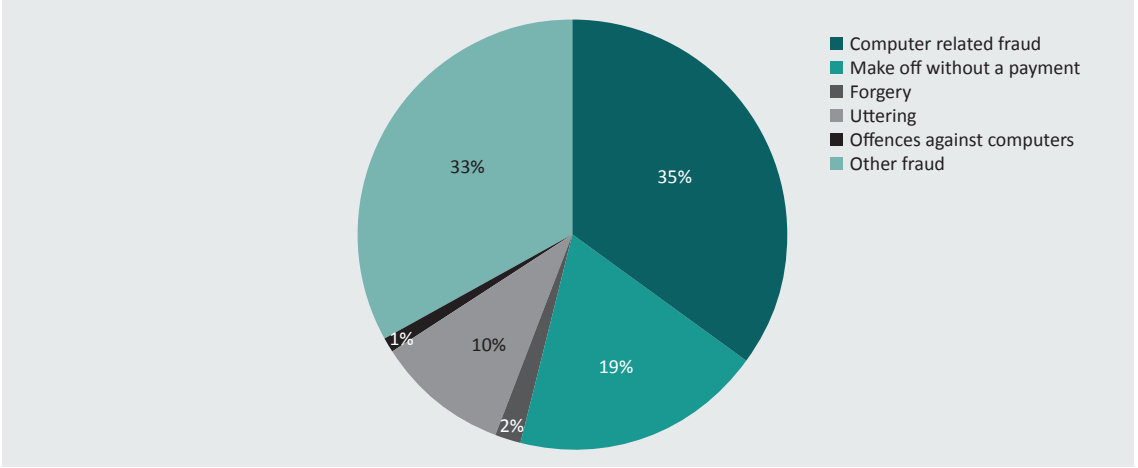
South Australia Police

During 2015–16, there were 2,909 fraud offences recorded by SA Police, and in 2016–17 the number decreased to 2,753. Of these recorded fraud offences, 560 cases in 2015–16 and 462 cases in 2016–17 either involved identity offences or could have potentially involved identity offences.

Tasmania Police

Tasmania Police do not capture specific data on identity crime. However, they do publish information on fraud and similar offences. In 2016–17, there were 825 fraud and similar offences recorded, an increase of 10 percent on the 750 offences recorded in 2015–16. The distribution of fraud and similar offences in 2016–17 is provided in Figure D3.

Figure D3: Distribution of all fraud and similar offences in Tasmania, 2016–17 (%)

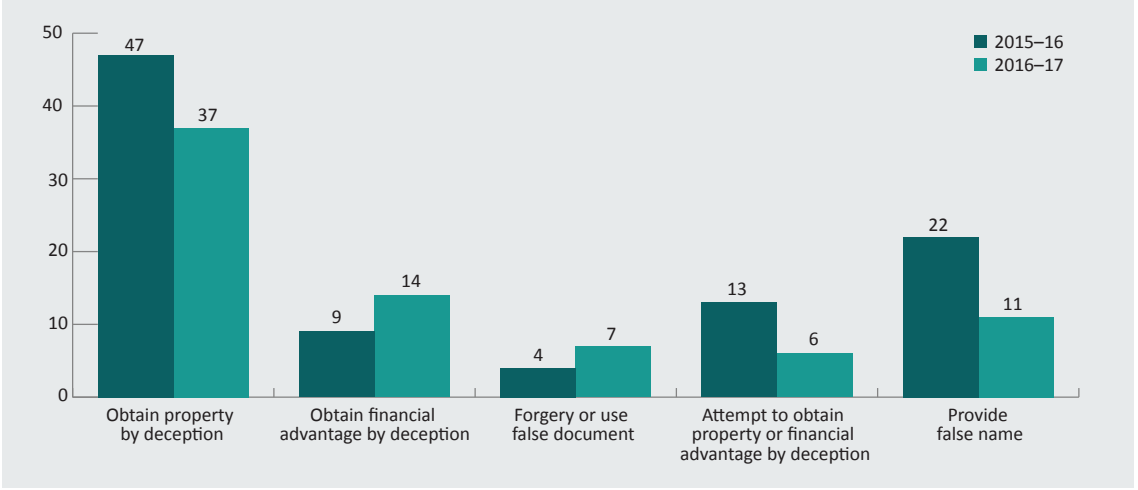


Note: 'Uttering' is the action of knowingly using a forged document with the intent to defraud
Source: Tasmanian DPFEM 2017

Australian Capital Territory Policing

The ACT 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 2015–16 was 553, and the total number of fraud offences in the ACT for 2016–17 was 668. Of the offences committed, the most frequently cited apprehensions recorded by ACT Policing were obtaining property by deception, providing a false name, and obtaining financial advantage by deception (see Figure D4).

Figure D4: Identity-related apprehensions in the ACT, 2015–16 and 2016–17 (n)

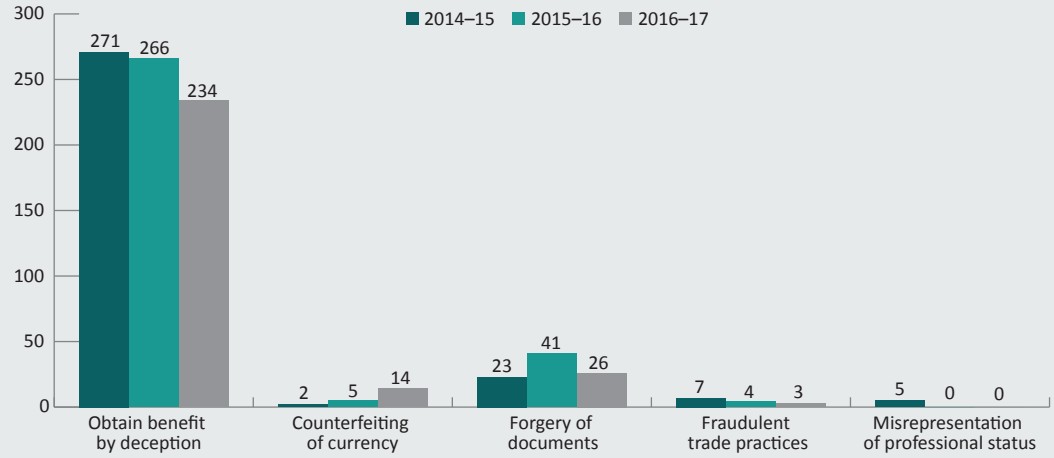


Source: ACT Policing 2017 (unpublished data)

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 277 reported cases of fraud in 2016–17, a 12 percent decrease from the 316 reported cases in 2015–16 (NTPFES 2017). The distribution of fraud offences for 2014–15 to 2016–17 is presented in Figure D5.

Figure D5: Fraud, deception and related offences in the Northern Territory, 2014–15 to 2016–17 (n)



Source: NTPFES 2017

Summary

Table D1 presents summary statistics of the number of fraud offences recorded by police jurisdictions between 2014–15 and 2016–17 (and identity fraud offences where available). Over these three years the number of reported fraud offences decreased by three percent.

Table D1: Fraud and identity fraud offences reported to state and territory police, 2014–15 to 2016–17 (n)

State or territory	Type	2014–15	2015–16	2016–17
NSW	Fraud	51,137	51,935	47,934
	ID fraud			15,639 (33%)
Vic[a]	Fraud	36,668	36,988	34,605
	ID fraud	882	6,071	5,972 (17%)
Qld	Fraud	23,382	22,054	27,258
	ID fraud	858	1,000	1,179 (4%)
WA		19,290	22,212	16,154
SA	Fraud	2,757	2,909	2,753
	ID fraud		560	462 (17%)
Tas		646	750	825
ACT	Fraud	1,195	553	668
	ID fraud		26	18 (3%)
NT[b]	Fraud	317	316	277
	ID fraud		41	26 (9%)
Total	Fraud	133,967	137,717	130,474

a: Victorian Crime Statistics Agency collects data on calendar years, not financial years

b: NT identity crime component includes 'forgery of documents'

Note: Numbers in parentheses are percentage of all fraud offences in each jurisdiction that were identity-related offences. Definitions of identity-related offences differ between jurisdictions

Source: NSW BOCSAR 2017; Tas DPFEM 2017; NTPFES 2017; Crime Statistics Agency (Vic) 2017; QPS 2018; SA Police 2018; SA OCSAR 2017 (unpublished data); AFP 2017 (unpublished data); WAPF 2018

Penny Jorna 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.

AIC reports

Statistical Report

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

aic.gov.au