Identity·crime·and·misuse·in·Australia·2016¶

IDENTITY SECURITY

Acknowledgements

The Attorney-General's Department appreciates the assistance of:

- Australian Institute of Criminology (AIC) in undertaking the 2016 AIC Identity Crime and Misuse in Australia online survey, including the ongoing assistance from Penny Jorna and Dr Russell Smith.
- IDCARE in peer reviewing this report and their ongoing support to the victims of identity crime.
- Australian Bureau of Statistics (ABS) in peer reviewing this report.

ISBN 978-1-925290-84-4 Identity crime and misuse in Australia 2016 (Print)
ISBN 978-1-925290-85-1 Identity crime and misuse in Australia 2016 (Online)

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au

Table of Contents

Foreword

I am pleased to release the *Identity Crime and Misuse in Australia 2016* report. This report provides the latest estimates on the prevalence and cost of identity crime, based on data from over 50 different Commonwealth and state and territory agencies, and community surveys conducted by the Australian Institute of Criminology and Australian Bureau of Statistics.

Identity crime continues to be one of the most common crimes affecting our community and is also a key enabler of serious and organised crime. In addition to considerable financial losses, a significant proportion of victims experience adverse impacts on their mental or physical health, reputations and general wellbeing.

The Australian Government is committed to combating identity crime, protecting the identities of Australians from being misused and making it easier for people to transact online safely and with confidence. This is particularly important given the growing nexus between identity crime and cybercrime identified in this report. Our efforts need to continue to adapt to new and emerging technologies, while adapting to changes in criminal methodologies.

Whether by expanding private sector access to the Document Verification Service to make it easier for business to detect fake identity documents, utilising technologies such as biometrics to strengthen identity verification processes used by government agencies, or resourcing Australian Government law enforcement response, the Government will continue to combat the scourge of identity crime.

The Hon Michael Keenan MP

Minister for Justice

Minister Assisting the Prime Minister on Counter-Terrorism

Executive Summary

This is the third in a series of reports that seek to analyse the nature and extent of identity crime and misuse in Australia. These reports compile data from Commonwealth, state and territory agencies, as well as the private sector and other non-government sources. The Attorney-General's Department leads the development of these reports as a key initiative of the National Identity Security Strategy.

Cost of identity crime

The annual cost of identity crime in Australia is $2.2b. This includes the direct and indirect losses incurred by government agencies and individuals; and the cost of identity crimes recorded by police.

Figure 1: Estimated total direct and indirect cost of identity crime in Australia

The costs of preventing and responding to identity crime are estimated to be a further $390m, bringing the total economic impact of identity crime in Australia to approximately $2.6b per year. These figures represent a revised estimate of the cost of identity crime in Australia to $2.2b compared to the estimate of $2b from the 2013–14 report. This is due to better availability of data and is not necessarily an indicator of change over the intervening time.

Prevalence of identity crime

Identity crime continues to be one of the most prevalent crimes in Australia, with recent surveys suggesting that around 4-5% of Australians experience a financial loss from identity crime each year (Figure 2).

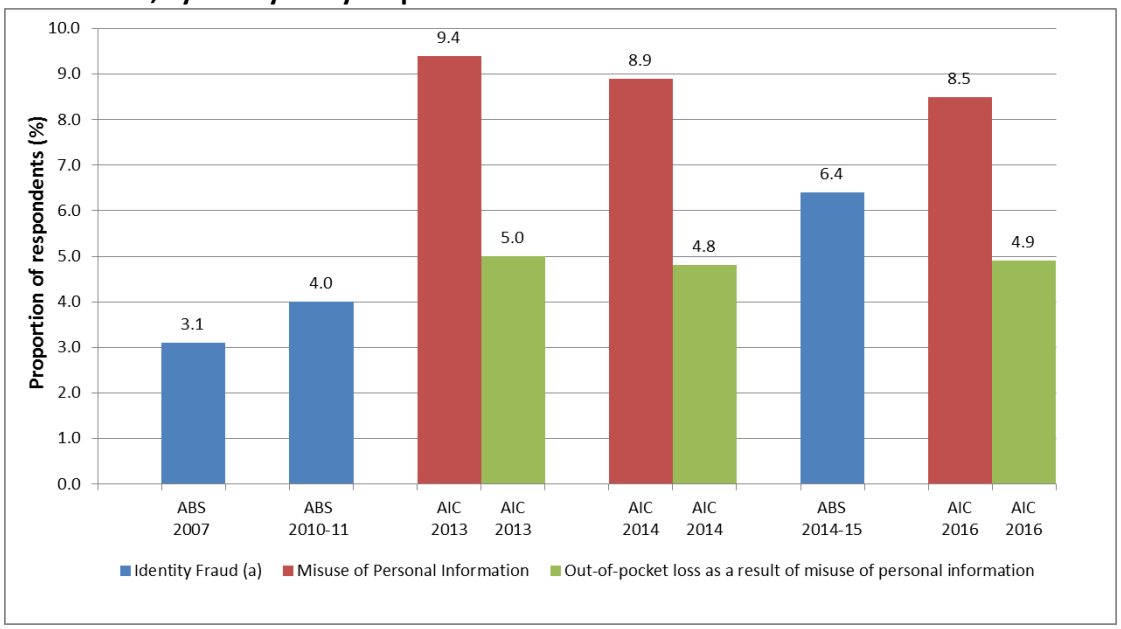
In a 2016 survey, the Australian Institute of Criminology (AIC) found that 8.5% of respondents experienced some form of misuse of their personal information in the previous 12 months, with 4.9% of all respondents incurring out-of-pocket losses as a result of this misuse.

An Australian Bureau of Statistics (ABS) survey found that around 6.4% of the Australian population aged 15 years and over reported being victims of identity fraud[1] in 2014-15. This is greater than the 4% noted in the 2010-11 ABS survey.

This makes identity crime more common than other forms of personal and household theft related crimes (Figure 3). Unsurprisingly, identity crime continues to be of concern to Australians, with 96% of respondents to the AIC surveys perceiving misuse of personal information to be either a 'very serious' or 'somewhat serious' issue.

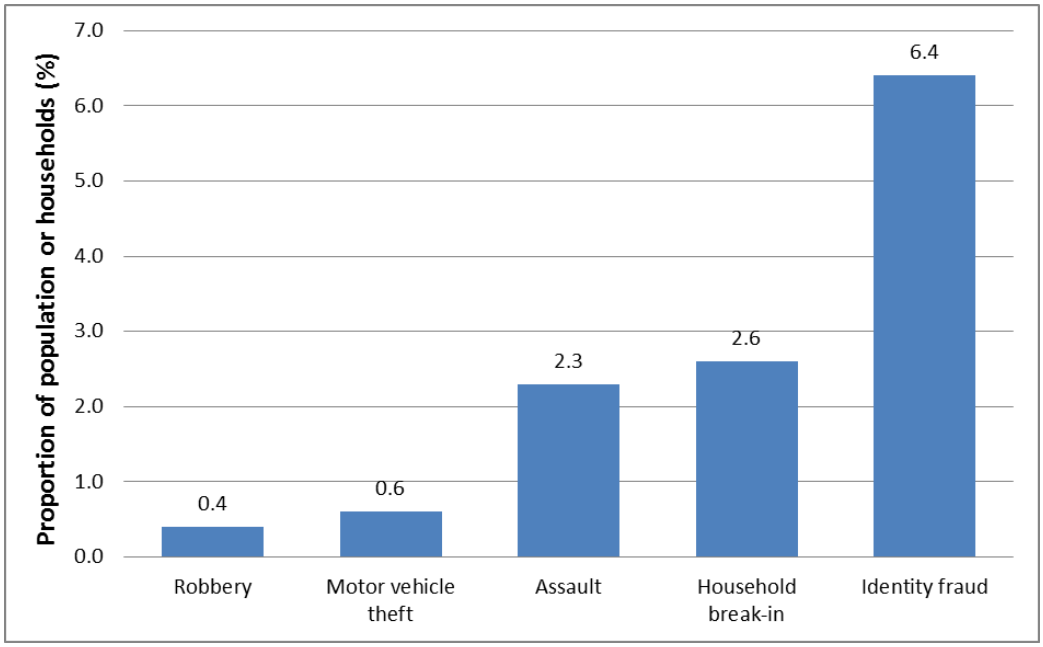
[1] Identity fraud includes both identity theft and card fraud

Figure 2: Proportion of respondents reporting identity crime victimisation or misuse of personal information, by survey and year published



Source: AIC Survey 2013, 2014 and 2016; ABS Personal Fraud Survey 2007, 2010-11 and 2014-15.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.
Note (a): Identity fraud is comprised of identity theft and card fraud. It does not include incidents of scams.

Figure 3: Proportion of individuals or households affected by crimes, by offence type, ABS, 2014-15

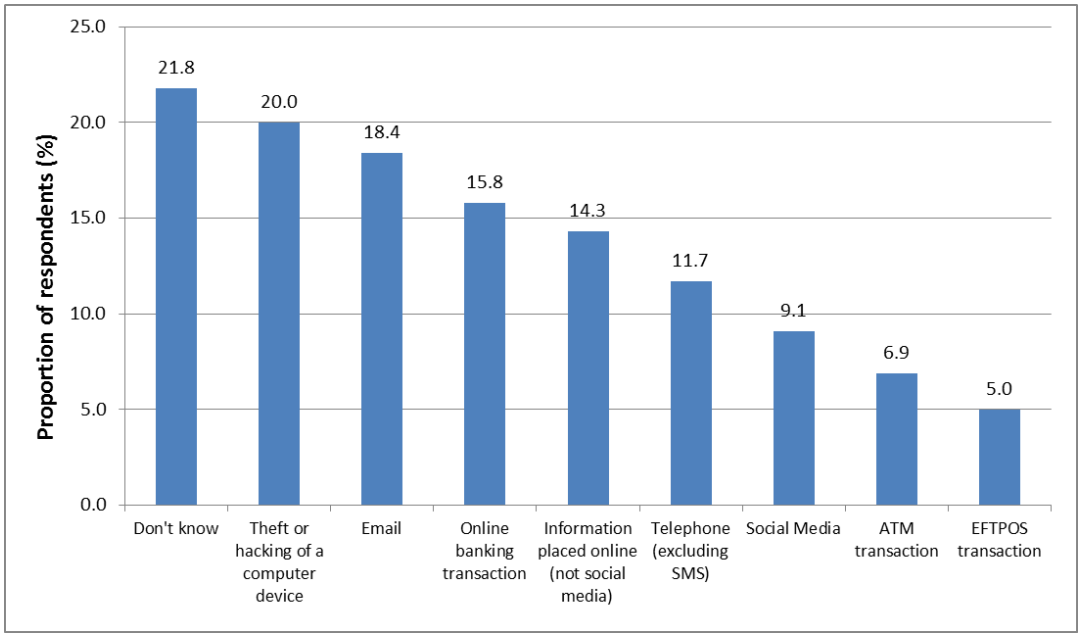


Source: ABS Personal Fraud Survey 2014-15 (ABS 2016a) and ABS 2016b.

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 via online, email, social media or scams or through data breaches. Many victims (22%) do not know how their personal information was obtained.

Figure 4: How personal information was obtained on the most serious occasion, by method, AIC, 2016



Source: AIC Survey 2016.
Note: The AIC Survey is based online survey; so there may be inherent bias in the methodology towards online mediums.

There is a high demand for these forms of stolen or fraudulent identity information in online marketplaces, with personal information and credentials attracting high fees including driver licences (approximately $400) and passports (approximately $5,000).

Anecdotal reports from police agencies highlight that driver licences and Medicare cards continue to be the most likely identity credentials used in identity crime. This is further supported by IDCARE which found driver licences were the most compromised credential amongst clients seeking assistance with recovery from IDCARE .

Furthermore, IDCARE found that where a breach of personal information occurred, 32% of individuals detected further misuse of this information.

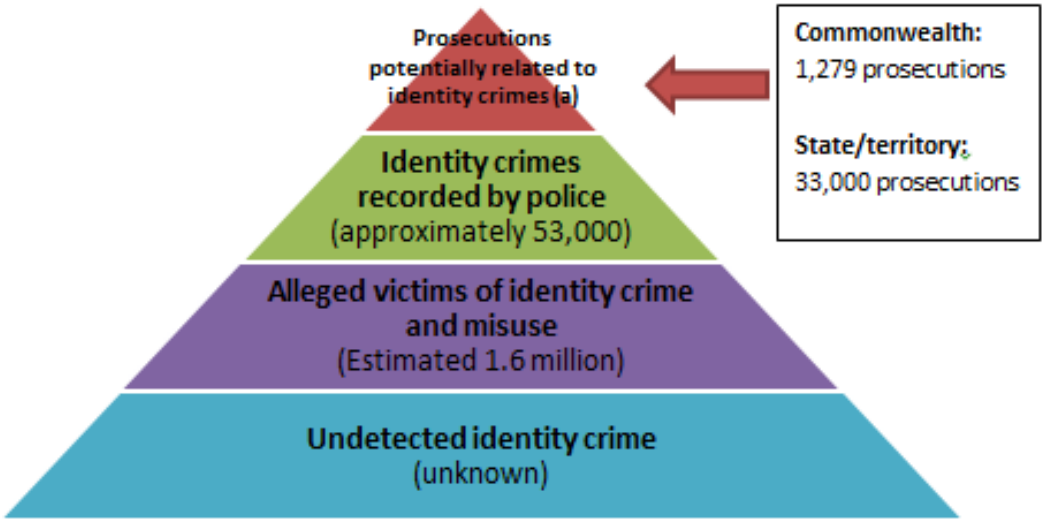
The number of data breaches reported to the Office of the Australian Information Commissioner (OAIC) continues to increase, with 110 data breaches recorded in 2014-15, compared to 71 in 2013-14.

Use of fraudulent identities

IDCARE found that the misuse of identity on average occurs 72 hours after the initial compromise, with the majority of these incidents (87%) first detected by the victim. In the majority of identity theft incidences, the credential information is misused while the physical credential remains with the victim. This highlights the need for document-issuing agencies to cancel and reissue credentials that are reported as lost or stolen with a new document number rather than only replacing the physical document.

Like other types of crime, only a small proportion of identity crime incidents are eventually prosecuted (Figure 5).

Figure 5: Estimated number of identity crimes in 2014-15, compared to those that were prosecuted

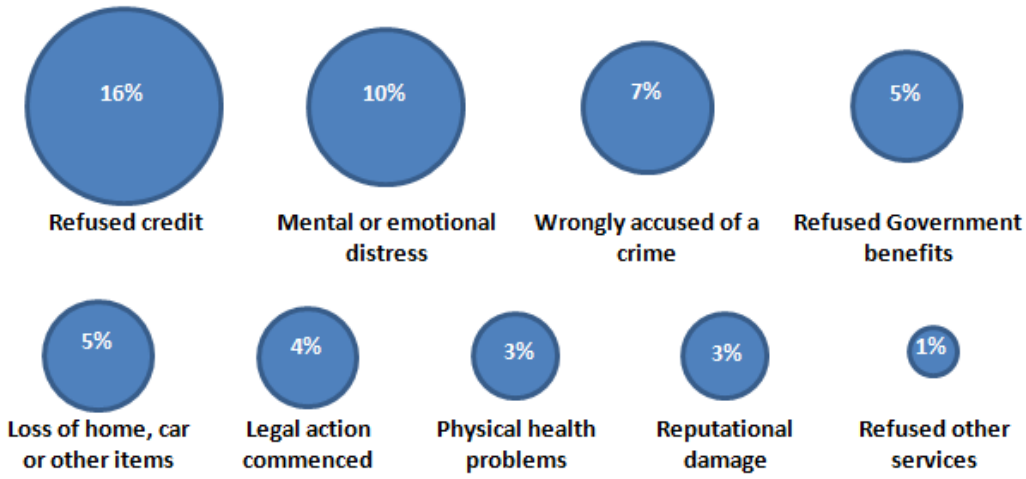


Note (a): Prosecutions that included any component of identity crime, noting that police reported identity crime are incidents where the major offence was identity related.

Impact of identity crime on victims

Most identity crime victims lose relatively small amounts of money (up to $1,000) although in some cases losses can run into the hundreds of thousands of dollars. A significant proportion of victims also experience demands on their time, adverse impacts on their mental or physical health, reputational damage or negative impacts on their general wellbeing.

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



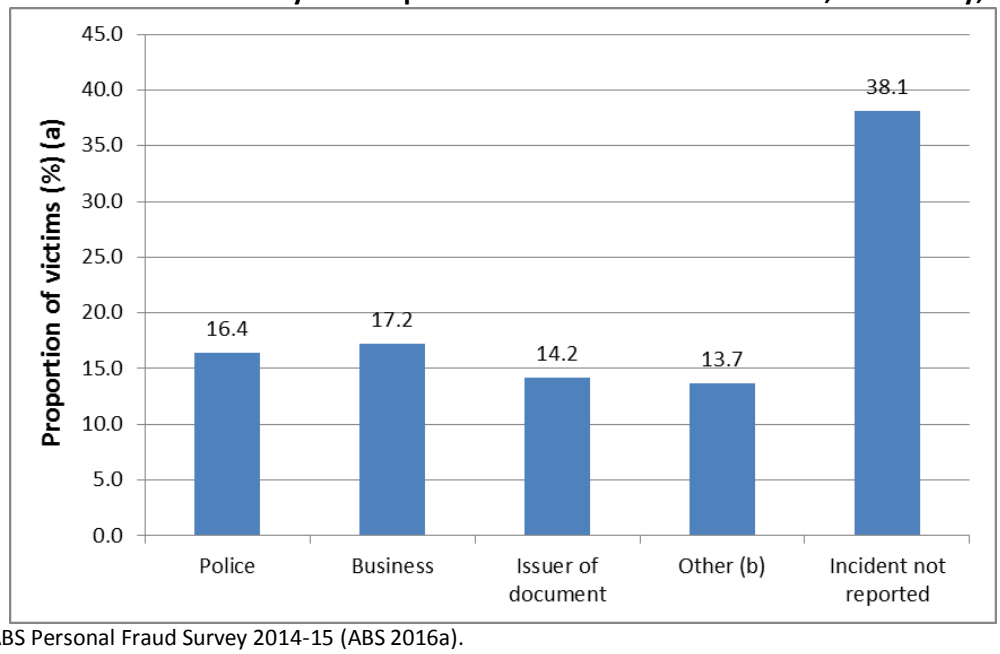
Source: AIC Survey 2016.

Despite this, identity crime continues to be under-reported by victims in Australia. About 38% of respondents in the 2016 ABS Personal Fraud Survey who experienced misuse of their personal information in the previous 12 months did not report the incident, with only 16% reporting it to police.

Reasons for respondents' reluctance to report their victimisation include a lack of immediate awareness that they have been targeted; embarrassment; the fact that they did not lose money

and therefore do not believe there is any need to report the crime; a belief that the police or other authorities will not be able to do anything; and confusion about to which agency they should report the incident. The significant under-reporting may suggest increased community awareness is needed about how and to which organisations victims should report identity crime incidents.

Figure 7: Who victims of identity theft reported the most recent incident to, ABS Survey, 2014-15

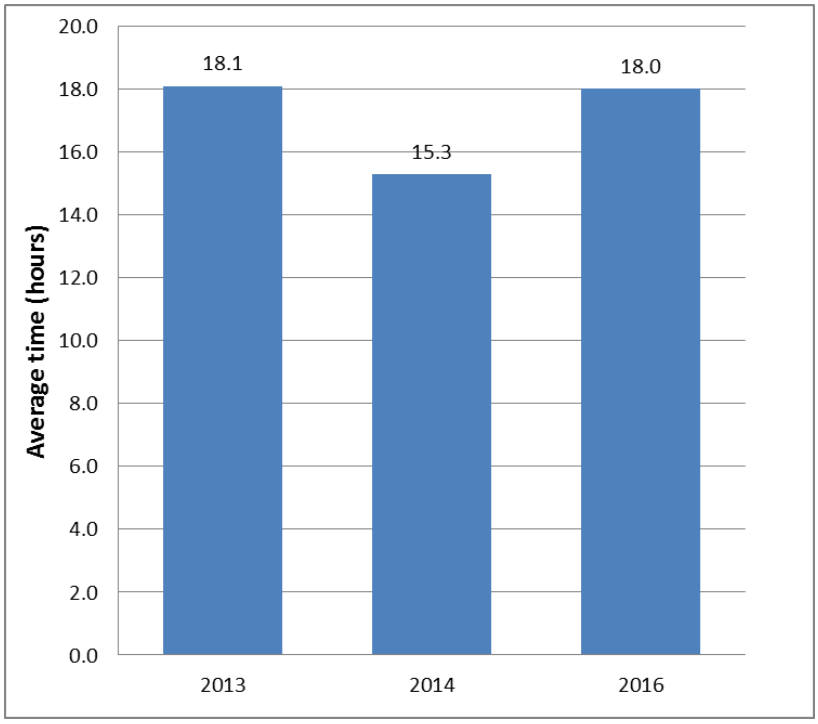


Source: ABS Personal Fraud Survey 2014-15 (ABS 2016a).
Note (a): Incidents may have been reported to more than one authority.
Note (b): Other includes consumer affairs and ombudsman, government agency, bank/financial institution, and other. Data for the percentage of whom reported to consumer affairs or Ombudsman estimate has a relative standard error greater than 50% and is considered too unreliable for general use.

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 18 hours in 2016 (Figure 8), with many unsure of where to report the incident. In the vast majority of cases reported to IDCARE, victims engaged with more than seven organisations, taking 18 hours per incident.

Figure 8: Average time spent by victims dealing with consequences of misuse of personal information, AIC, 2013, 2014 and 2016



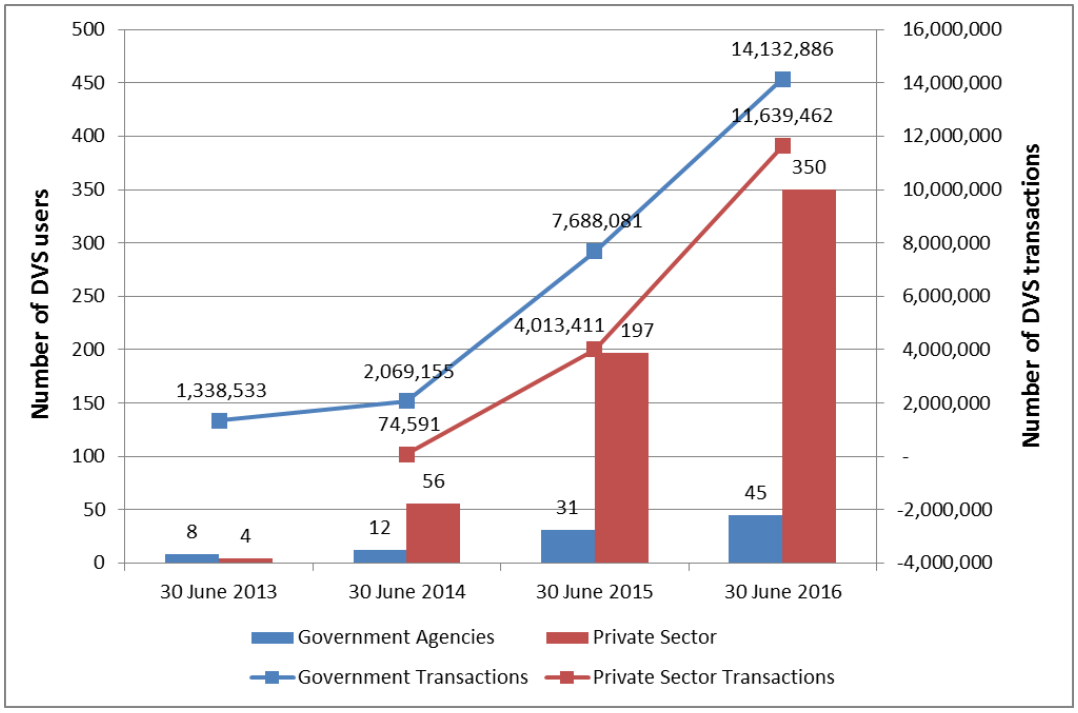
Source: AIC Surveys 2013, 2014 and 2016

AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

Prevention of identity crime

There has been a substantial increase in the number of private sector organisations using the Document Verification Service (DVS), with 350 private sector organisations and only 45 government agencies using the DVS as of 30 June 2016. Even with this increase the majority of government agencies which issue evidence of identity documents are yet to commence using the service to check identity documents. The number of DVS transactions during 2015-16 has also increased considerably in recent years to just less than 26 million.

Figure 9: Number of DVS users and number of transactions by government and private sector, 2013 to 2016



Source: AGD unpublished data.
Note: The DVS was not available to private sector users prior to 30 June 2013.

Conclusion

These reports improve our understanding of the nature and extent of identity crime in Australia. Noting the under-reporting and lack of consistent identity crime statistics, the available data suggests that the rate of identity crime is increasing, and remains one of the most common types of crimes in Australia. The DVS continues to be successful in preventing the use of fake identity documents, providing incentives for criminals to rely on identity takeover or theft. This underscores the need for government, business and the community to continue to work together to respond to this threat.

Introduction

This report represents the most comprehensive attempt to measure the extent and effect of identity crime and misuse in Australia. However, identity crime continues to be difficult to measure due to the lack of comprehensive and consistent identity crime statistics. The true extent of identity crime in Australia is likely to be both underreported and underestimated. Nevertheless, every effort has been made to ensure that the findings of this report are as accurate as possible with the data available.

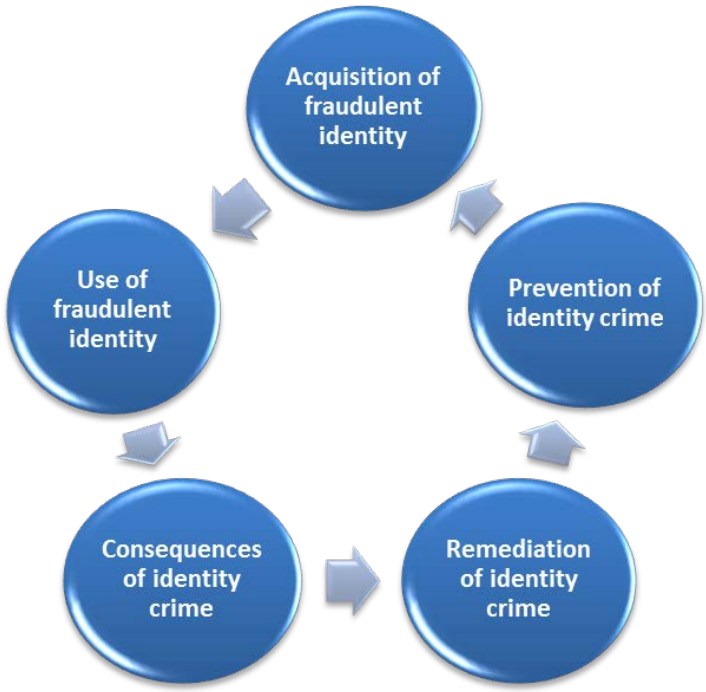
Identity crime covers a wide range of activities and offences where a perpetrator uses personal information, or documents personal information that is fabricated, manipulated, stolen or assumed from another person in order to facilitate or commit crimes.

Fraudulent identities have been used to commit welfare, tax and other fraud against government agencies, gain unauthorised access to sensitive information or facilities, conceal other criminal activities such as drug trafficking, and even to facilitate the commission of terrorist acts.

Methodology

In quantifying identity crime and its broader impacts, this Identity crime and misuse in Australia (ICAMIA) 2016 report publishes findings against a number of key indicators (Figure 10). The Attorney-General's Department (AGD) developed this methodology with assistance from the Australian Institute of Criminology (AIC) (Bricknell & Smith, 2013) and has been used as the basis for the previous ICAMIA reports (AGD 2013, AGD 2014). The methodology is explained in greater detail in Appendix C.

Figure 10: Identity crime conceptual model



Source: Attorney-General's Department.

Throughout this report a number of external surveys have been used which measure experiences of individuals in relation to personal fraud and identity crime and misuse. These include:

- AIC Survey 2016 (Smith & Jorna forthcoming 2017)
- ABS Personal Fraud Survey 2014-15 (ABS 2016a)

Empirical data about identity crime and misuse from IDCARE is used to give further insight into experiences of individuals. IDCARE is a non-profit organisation, supported by the Australian Government, which provides free support services to victims of identity theft and related cybercrimes to help repair the damage to their reputation, credit history and identity.

A total of 51 Commonwealth and state and territory agencies assisted in the preparation of data for this report, an indication of the breadth of identity crime experienced by government agencies.

Data quality and availability

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

- under-reporting by individuals and organisations
- the number of undetected identity thefts
- inter-jurisdictional inconsistencies in legislation, recording, investigation and prosecution resulting in identity crimes being absorbed into broader crime categories such as fraud and agency-specific offences.

The actual number of identity crime offences and their financial and non-financial impacts could be much greater than some of the estimates. To build a more reliable evidence-base, it will be necessary for a range of Commonwealth, state and territory government agencies to invest time and resources into developing the capacity of current databases and recording practices to more accurately capture data on identity crime.

Definition of identity crime

The terminology used to describe identity crime and misuse varies widely between agencies. To ensure consistency within this report and where possible identity crime is used as a generic term to describe activities or offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime.

A detailed list of definitions can be found in Appendix B.

Findings

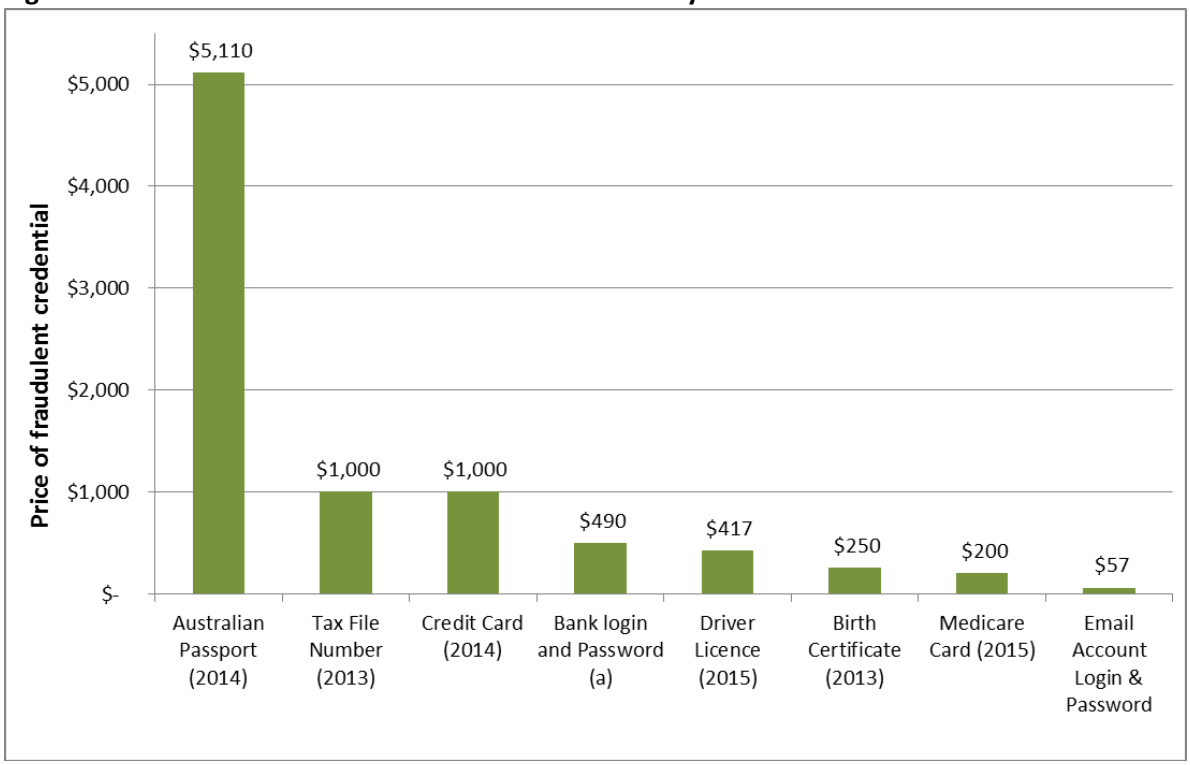
1. Acquisition of fraudulent identities

1.1 The price of fraudulent identity credentials

Key finding: The price of Australian identity credentials in illegal online marketplaces ('the dark net') ranges from $50 to $5,200. The price of these identity documents gives an indication of their availability and the extent to which the credential could be used in identity related crime.

IDCARE, an independent support service for victims of identity crime, has been able to monitor the cost of the most common types of identity documents on the black market (Figure 11). The relatively low prices of fraudulent credentials on the black market serve as an indicator of the availability of that type of credential.

Figure 11: Price of selected Australian fraudulent identity credentials



Note (a): Accounts with balances of up to $100K

Source: Australian Federal Police, Victoria Police, Attorney-General's Department and Department of Foreign Affairs and Trade unpublished data, IDCARE.

Case Study 1: Melbourne crime syndicate using false documents

A Melbourne-based organised crime syndicate operated an Australian student migration and support company. This company was used to enable a credit card shopping fraud scheme. The syndicate recruited foreign nationals with significant gambling debts to assist in fraudulently purchasing high-value portable goods that are easily able to be resold.

The syndicate used false identity documents and fraudulently obtained genuine documents to create false identities for recruits. These documents were used to obtain other legitimate identity documents, which were then used to set up bank accounts and obtain bank loans.

Using the funds from loans to those identities, including other fraudulently obtained credit cards, recruits purchased high-value portable goods which the syndicate resold for cash.

Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment, the other to 12 months.

Source: AUSTRAC unpublished information

1.2 The number of reported data breaches

Key finding: In 2014-15, the Office of the Australian Information Commissioner (OAIC) received a total of 110 Data Breach Notifications (DBNs), an increase from 71 notifications reported in 2013-14. Based on an independent analysis of a sample of these data breaches, the recorded breaches could have resulted in around 2.2 million records being compromised.

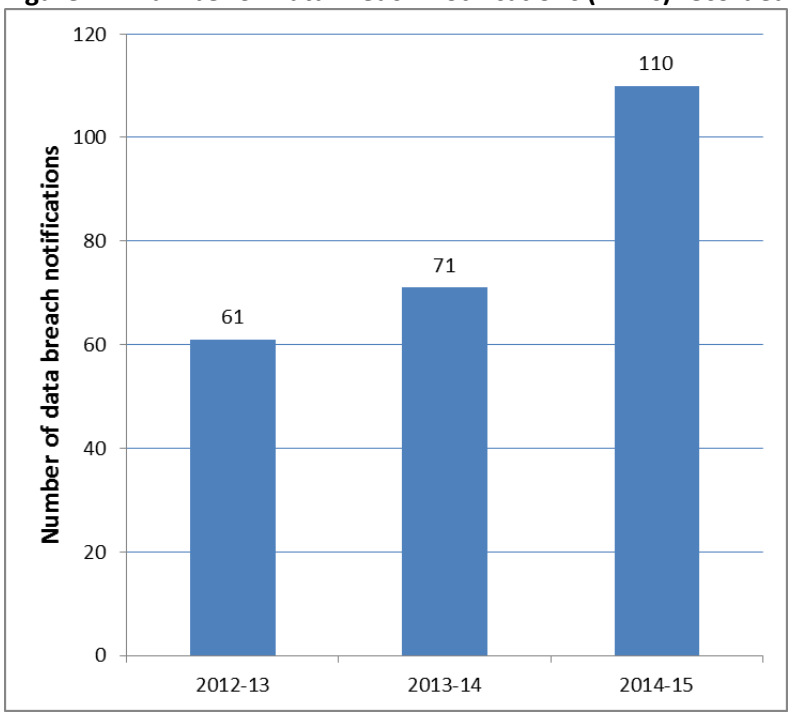
In 2014-15, the OAIC recorded a total of 110 DBNs. This was a 55% increase on the number of data breaches reported to the OAIC in 2013-14. This does not necessarily indicate an increase in the actual number of data breaches in Australia, as organisations may be becoming more likely to report such incidents following the development of new voluntary data breach reporting guidelines in 2012.

The OAIC does not record the number of individual records involved in reported data breaches; and so the number of DBNs, on its own, provides only a limited indication of the scale of these incidents.

Research conducted by the Ponemon Institute in recent years provides further insight into the nature of data breaches experienced by Australian organisations. The 23 Australian data breaches examined by the Ponemon Institute in 2014-15 found that, when compared with 2013-14:

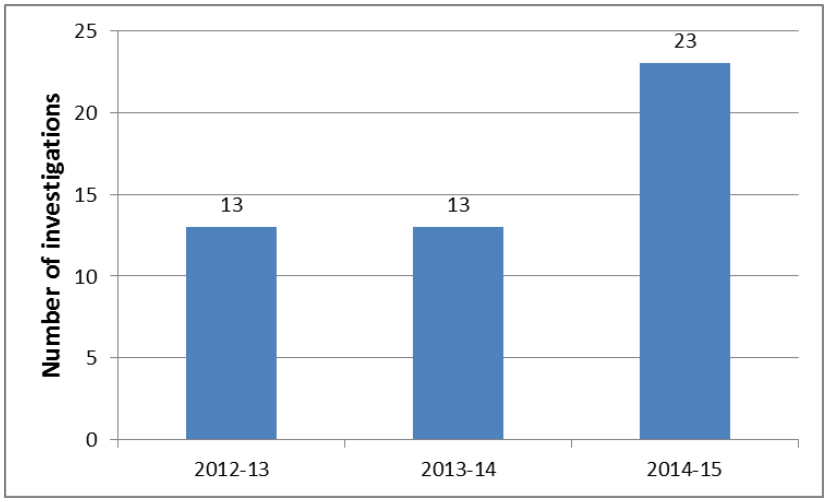
- the average number of records per breach decreased slightly from 20,073 to 19,788;
- the cost of data breaches to organisations remained stable from $145 (2014 calendar year) to $144 (2015 calendar year) per incident; and
- the total cost per incident remained stable at $2.8m.

Figure 12: Number of Data Breach Notifications (DBNs) recorded by the OAIC, 2012-13 to 2014-15



Source: OAIC Annual Reports, 2013 – 2015.
Note (a): The numbers of data breaches illustrated in this figure are not just those data breaches that have been identified by the OAIC as possibly involving identity crime. These are the total number of data breaches recorded by the OAIC in the Annual Reports for the relevant financial years.
Note (b): 110 represents the total number of voluntary DBNs received by the OAIC. The OAIC also received 7 mandatory DBN under s 75 of the Personally Controlled Electronic Health Records Act 2012 (PCEHR Act).

Figure 13: Number of investigations by OAIC involving instances of identity crime, 2012-13 to 2014-15

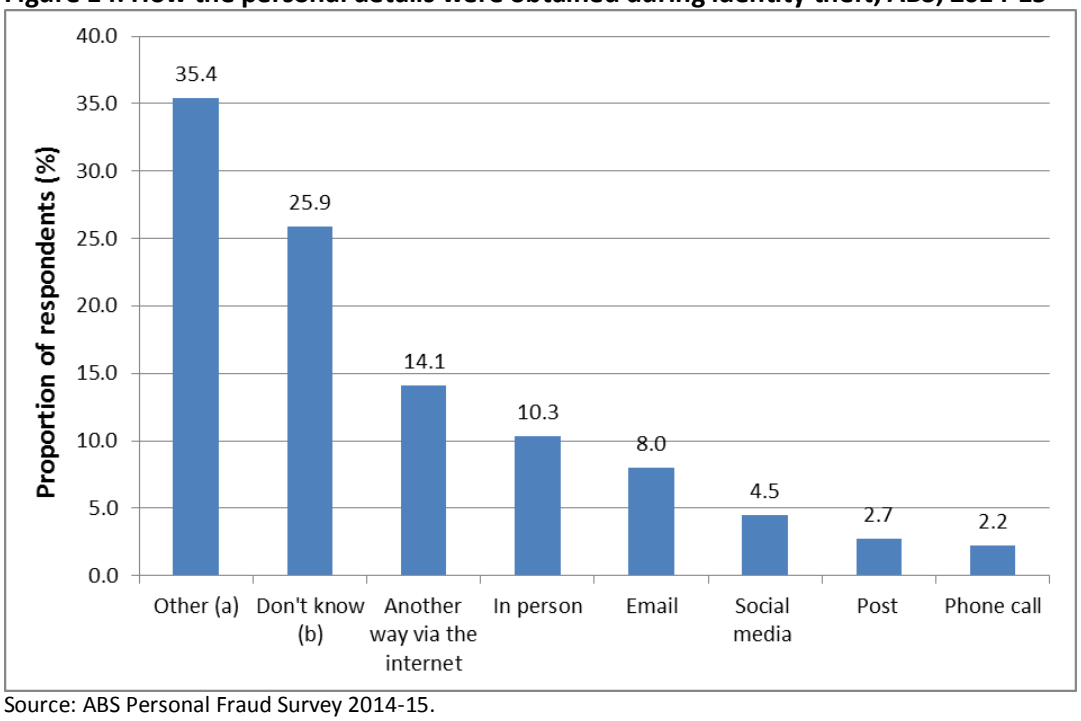


Source: OAIC, unpublished data

1.3 How criminals are gaining access to personal information

Key finding: According to the ABS Personal Fraud survey personal information was obtained via physical means (51%)[2] such as in person or through a phone call, meanwhile 27% of personal information was obtained via the internet. Around one quarter (22-26%) of identity theft victims did not know how their personal information was obtained. Results from the AIC Survey show a similar pattern.

Figure 14: How the personal details were obtained during identity theft, ABS, 2014-15



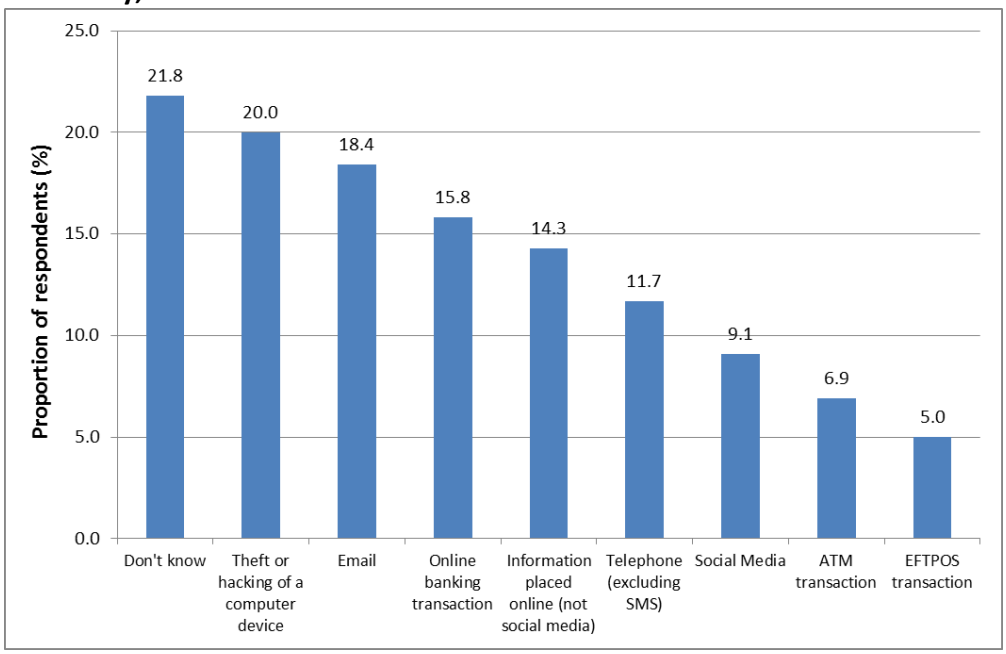
Source: ABS Personal Fraud Survey 2014-15.

Note (a): Other includes lost or stolen item/document, whilst using credit card to make a purchase or withdraw money, text messages and other.

Note (b): Don't know includes victims who experienced the subsequent misuse of their identity, however could not explain how their identity was initially compromised. Estimates for 'post' and 'phone call' have a relative standard error of 25% to 50% and should be used with caution.

[2] Physical includes methods including in person, post, phone call and lost or stolen item/document, whilst using credit card to make a purchase or withdraw money, text messages and other.

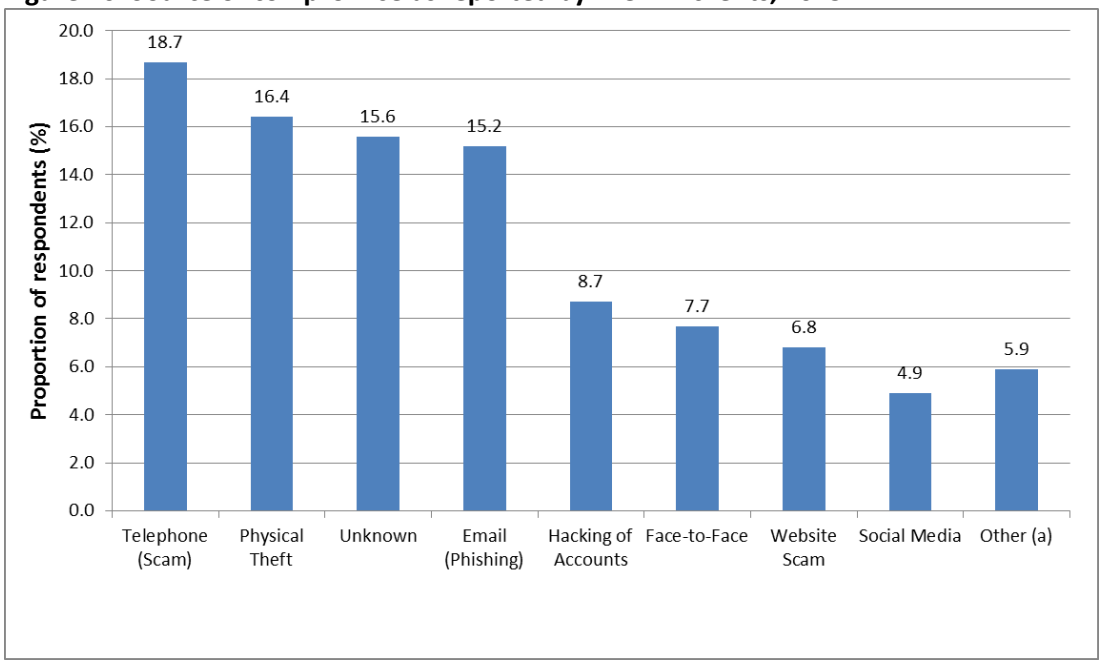
Figure 15: How personal information was obtained on the most serious occasions, by method, AIC Survey, 2016



Source: AIC Survey 2016.
Note: The AIC Survey is an online survey; so there may be inherent bias in the samples towards online media.

IDCARE found that approximately 57% of its clients during 2015 were tricked into directly enabling the compromise[3] of their identifying information. This includes incidents of telephone scams where victims would engage directly with the identity criminal and provide access to their identifying information (Figure 16).

Figure 16: Source of compromise as reported by IDCARE clients, 2015



Source: IDCARE 2016a
Note (a): Other includes loss, job applications, virus and SMS (SMIShing)

[3] Enabled compromise includes telephone (scams), email (phishing), face-to-face, website scam, social media, loss, job applications, virus and SMS (SMIShing).

Further research by IDCARE has found that when identity information was breached, 32% of individuals detected a further misuse of this information. IDCARE also found that in 78% of all instances, the physical credential remained with the victim, while the credential information was misused by the identity thief. More information on the types of personal information most susceptible to identity theft can be found in Section 2.5.

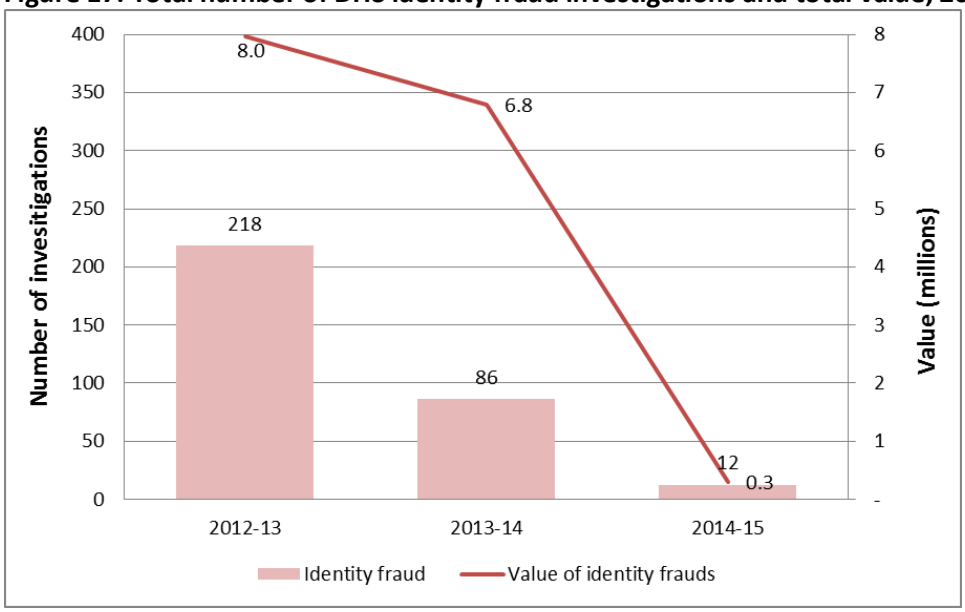
2. Use of fraudulent identities

2.1 The number of identity crime incidents recorded by government agencies

2.1(a) Benefits Fraud

Key finding: There was a reduction in the number of identity fraud-related investigations recorded by the Department of Human Services (DHS) between 2013-14 and 2014-15, with the value of these frauds also decreasing. This is in part attributed to DHS's focus on more complex fraud cases as well as a growing focus on preventative activities. DHS is investing in the development of automated controls to assist in the prevention of identity fraud, and in 2015-16 intercepted and disrupted 56 attempts to redirect payments by assuming a customer's identity.

Figure 17: Total number of DHS identity fraud investigations and total value, 2012-13 to 2014-15



Source: DHS Annual Reports 2013, 2014, 2015 and unpublished data.

The decline in the number of identity fraud related matters relates to the evolving nature of identity fraud in the welfare space. The use of the Document Verification Service (DVS) by DHS has also had a significant impact on reducing the amount of fraud involving fabricated or fictitious identities which was traditionally perpetrated against DHS.

Case Study 2: 70-year-old man claims two pensions

Through data-matching analysis, DHS detected a 70-year-old Queensland man who claimed a second Age Pension and Disability Support Pension using a fabricated identity. Data-matching analysis revealed identity and banking documents in two different names.

Optical surveillance was used as part of the investigation to establish the man's multiple identities. Footage was taken of the man to establish his place of residence. Investigators then took footage of the man at a local establishment and at another time entering a Centrelink office signing documents. This footage helped prove the fabricated identity as he had previously attended a Centrelink office in relation to payments under another name.

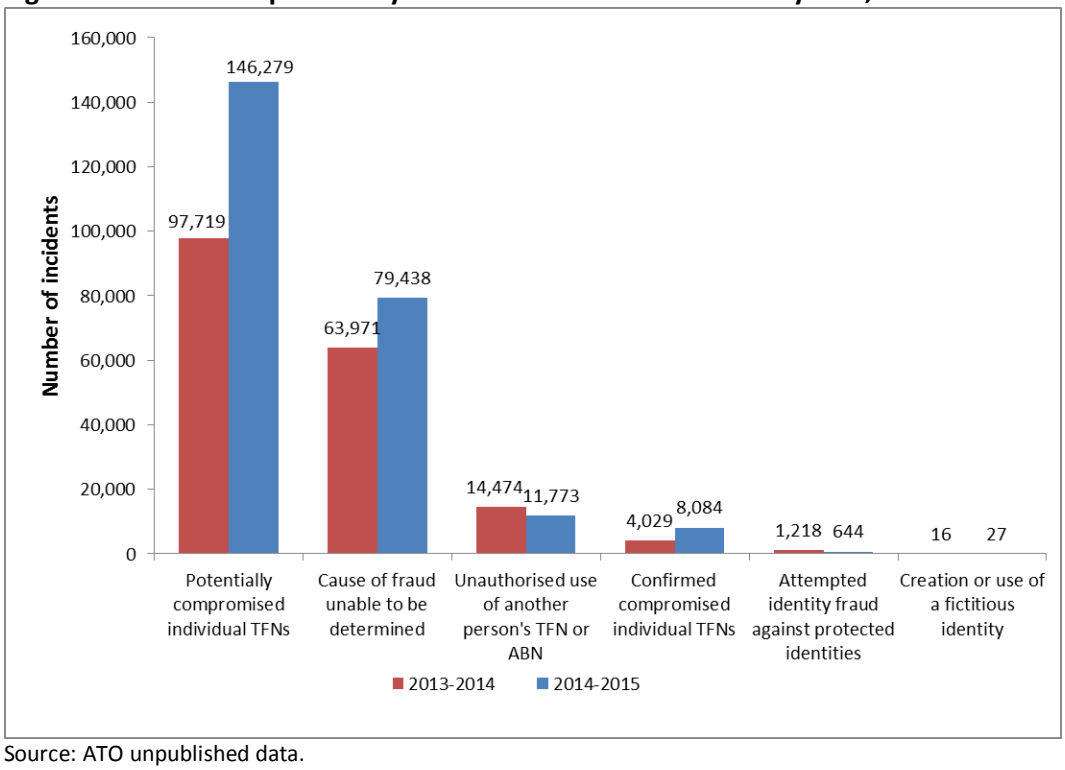
The man pleaded guilty to fraudulently claiming over $199,000. He was sentenced to four years' imprisonment, with a non-parole period of 12 months.

Source: DHS, unpublished report.

2.1(b) Taxation-related identity fraud

Key finding: Between 2013-14 and 2014-15 there was a 49.7 per cent increase in the number of potentially compromised Tax File Numbers (TFNs) identified by the Australian Taxation Office (ATO); and a 18.7 per cent decrease in the number of fraud incidents involving unauthorised use of another person's TFNs and ABNs. This may suggest an increase in fraud, but may also be attributable to improvements in the fraud detection and prevention practices of the ATO and other government agencies.

Figure 18: Number of potentially fraudulent incidents detected by ATO, 2012-13 to 2014-15

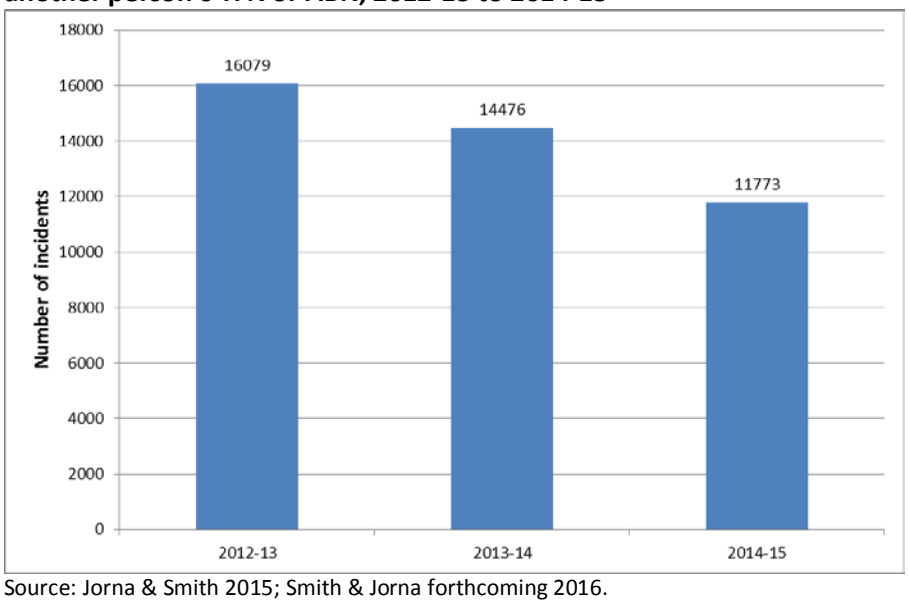


Source: ATO unpublished data.

The Australian Institute of Criminology's *Fraud against the Commonwealth* annual census have also found a substantial number of fraud incidents involving the unauthorised use of another person's

TFN or ABN across Commonwealth government agencies, although these have declined over recent years.

Figure 19: Number of external Commonwealth fraud incidents involving unauthorised use of another person's TFN or ABN, 2012-13 to 2014-15



Source: Jorna & Smith 2015; Smith & Jorna forthcoming 2016.

Case Study 3: Creation of fraudulent identities

Between February 2013 and June 2014, an employee of a Perth-based accountancy firm set up a complicated regime using five different bank accounts and five fictitious agencies to access the dormant balances of 20 different agencies, mostly the firm's clients and ex-clients. The offender lodged false Business Activity Statements and redirected the refunds into his own bank accounts.

In the course of the offender's employment, he had access to the ATO internet portal with the ability to electronically change relevant details of the firm's clients (tax payers) such as postal address and banking details.

The offender obtained $339,856 and used the money to fund a lavish lifestyle including gambling, drugs and high-end shopping sprees.

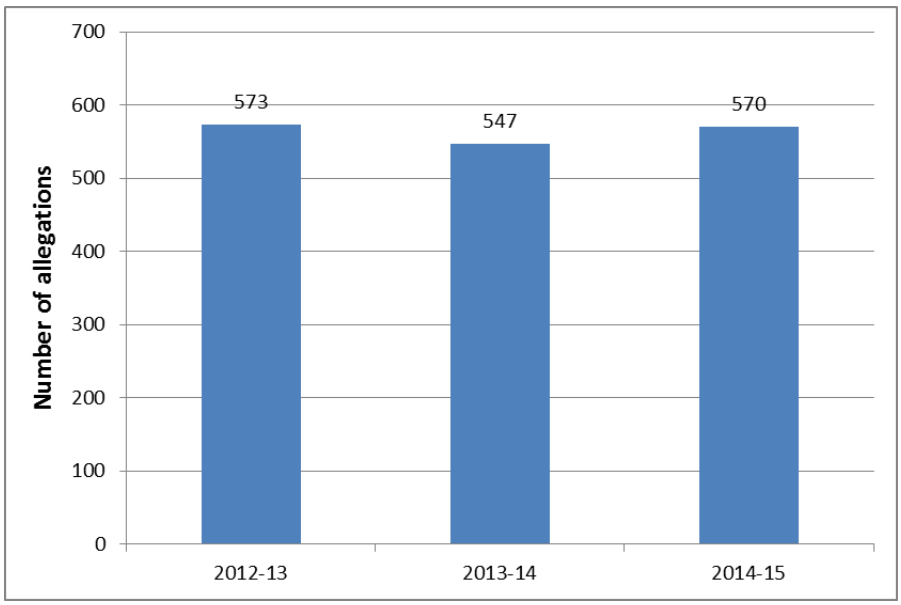
The offender was convicted and sentenced in relation to 46 counts of dishonestly obtaining a financial advantage and one count of dishonestly influencing a public official. The offender was sentenced to four years and six months imprisonment with a non-parole period of three years.

Source: The Commonwealth Director of Public Prosecutions, Case Report 2014-15 https://www.cdpp.gov.au/case-reports/jason-gilby

2.1(c) Immigration, customs and transport security related identity fraud

Key finding: The Department of Immigration and Border Protection (DIBP) recorded 570 allegations of possible immigration visa-related identity fraud in 2014-15. This has remained stable over the last three years.

Figure 20: Number of allegations of possible immigration visa-related identity fraud, 2012-13 to 2014-15



Source: DIBP unpublished data, AGD 2014b.

In 2014-15 there were 68 incidents of fraud regarding false declarations recorded by the then Australian Customs and Border Protection Service (ACBPS), now Australian Border Force. There was also one importation of 'Tier 2' prohibited goods detected in the form of blank credit cards, which can be used to manufacture fraudulent identity credentials. This is a decrease from 158 allegations in 2013-14 of identity crime and four importations of 'Tier 2' prohibited goods.

These figures are only approximate as systems do not categorise and record the results of goods and personal searches in a way that enables alleged incidents of 'identity crime' to be identified easily.

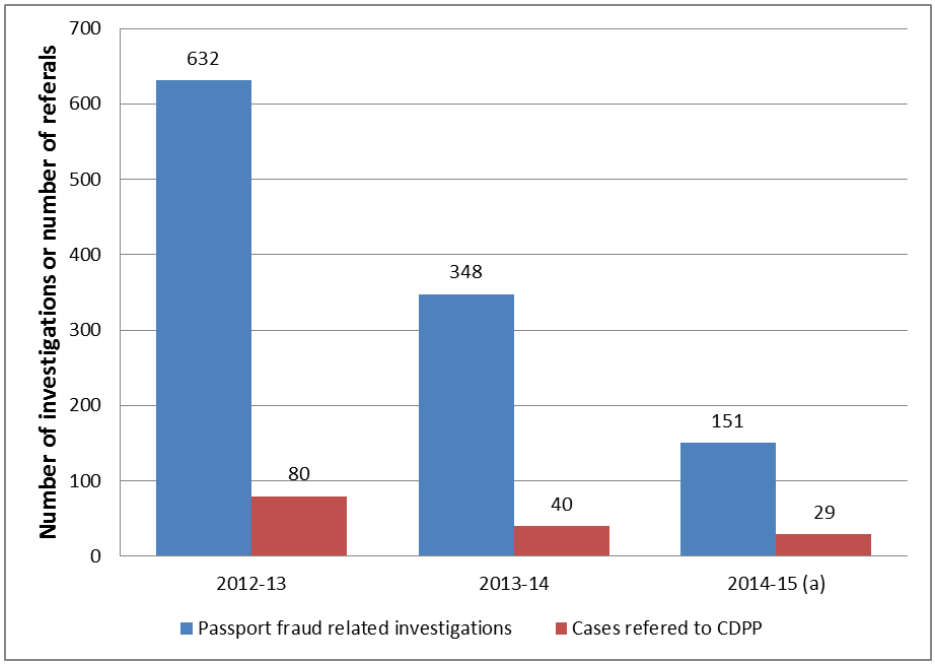
In 2014-15, the Office of Transport Security (OTS) in the Department of Infrastructure and Regional Development, recorded 50 incidents of fraud involving aviation and maritime security identity cards. Of these 12 were detected as identity crime incidents.

2.1(d) Passport identity fraud

Key finding: Between 2013-14 and 2014-15 the number of passport-related identity fraud incidents detected and investigated by the Department of Foreign Affairs and Trade (DFAT) declined, while the number of lost and stolen passports has remained stable during this period.

DFAT began 151 investigations during 2014-15 into allegations of passport fraud including identity fraud, application fraud and improper use or possession of Australian passports. DFAT referred 29 matters to the CDPP (Figure 21). Of the 151 investigations into allegations of passport fraud, 23 of these were found to involve identity crime (Figure 22), a decrease over recent years.

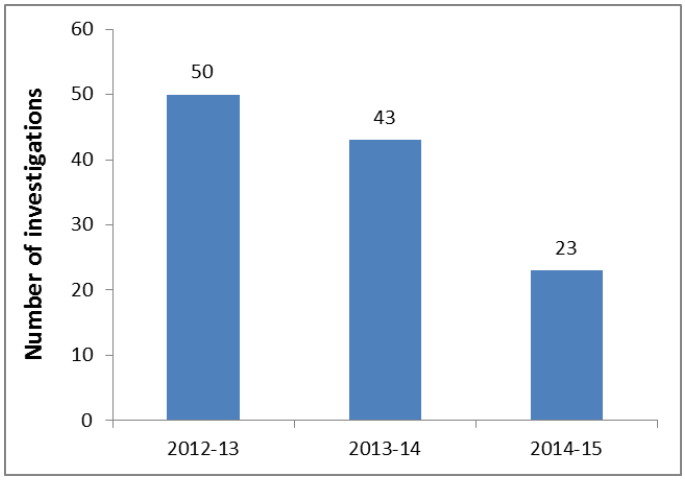
Figure 21: Number of DFAT passport fraud investigations and referrals to CDPP, 2012-13 to 2014-15



Source: DFAT Annual Reports, 2013, 2014, 2015.

Note (a): DFAT has changed the way it records passport fraud investigations in recent years. Instances of minor non-identity-related passport fraud are now resolved by administration action and no longer recorded as investigations. This allows investigators to focus on more serious identity-related passport fraud investigations.

Figure 22: Number of DFAT passport fraud investigations related to identity crime, 2012-13 to 2014-15



Source: DFAT Annual Reports, 2013, 2014, 2015 and DFAT unpublished data.

A breakdown of these 23 investigations is presented below.

Table 1: Breakdown of identity crime related investigations by DFAT, 2014-15

Reason for investigation	Number of investigations (a)
Fraudulently obtained genuine passports	18
Imposters	1
Physical alteration	4
Total	**23**

Source: DFAT unpublished data
Note (a): The above cases were detected by DFAT in 2014-15. However, it should be noted that the date of detection may be different compared to the date when the offence was committed.

Case Study 4: Lodgement of a fraudulent passport application

A person had been on bail in New South Wales for serious drug offences since September 2012 and was due to appear in court in December 2014. In November 2014, the person lodged a passport application in the identity of an associate, who had never previously held an Australian travel document. Facial recognition checks identified that the applicant's passport photo matched a passport issued in November 2009.

The Australian Passport Office identified that the passport issued in November 2009 had been surrendered to the court in September 2012 as part of his bail conditions. It is assumed that he was seeking to obtain a passport in a false identity to evade prosecution.

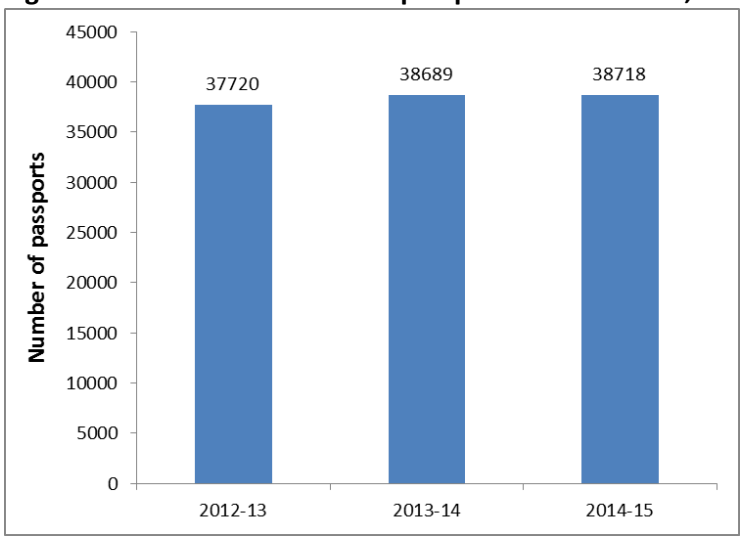
He was sentenced in July 2015 for a range of offences. For the passport-related offences, he was sentenced to 15 months imprisonment.

Source: Department of Foreign Affairs and Trade, unpublished.

2.1(e) Lost and stolen passports

In 2014-15, the number of Australian passports reported as lost or stolen remained stable, representing only a small fraction of the total number of passports in circulation. These numbers only consider the number of physical documents lost or stolen; it does not capture the number of compromises to the information of these credentials which could be higher.

Figure 23: Number of Australian passports lost or stolen, DFAT, 2012-13 to 2014-15



Source: DFAT Annual Reports, 2012-13, 2013-14, 2014-15.
Note: Cancelled passports cannot be verified via the DVS.

2.1(f) Identity fraud detected by Registries of Births, Deaths and Marriages (RBDMs)

Key finding: The number of registry certificates reported as lost, stolen or fraudulent in Victoria was considerably higher than any other jurisdiction that provided data. This can be attributed to differences in the RBDMs' data collection methods.

The various types of certificates issued by RBDMs are an important source of personal information that can be exploited by criminals seeking to commit identity crime. While each of the eight states and territory RBDMs were asked to provide data for this report, the extent to which data could be provided varied considerably between jurisdictions and may be due to the way that jurisdictions collect, record and subsequently report this information.

As can be seen in Table 2, the Victorian RBDM recorded a considerably larger number of lost or stolen certificates than the other RBDMs that provided data. The Victorian RBDM's data were collated based on the responses of applicants on the certificate application form, where applicants are required to provide a reason for why they are applying for a certificate. The Victorian RBDM advised that it does not keep data on how many, if any, allegations of stolen or fraudulent certificates were referred to the police by the applicant.

Table 2: Crime and misuse associated with certificates issued by RBDMs in 2014-15

RBDM Name	Lost	Lost/Stolen	Unauthorised change	Fraudulent	Referred to police
ACT	N/A	N/A	N/A	N/A	N/A
NSW	2	4	20	9	5
NT	2	0	0	2	15
Qld	N/A	N/A	0	0	0
SA	0	0	0	1	N/A
Tasmania	N/A	N/A	0	1	0
Vic	9632	192	0	0	0
WA	N/A	N/A	1	3	1

Source: Unpublished data from ACT, NSW, NT, Queensland, SA, Tasmania, Victoria and WA RBDM.
Note: N/A represents data is not available for the jurisdiction.

2.1(g) Driver licence fraud

Key finding: The relatively small number of identity crime incidents involving driver licences that were reported by road agencies appears to be at odds with other data on the use of driver licences in identity crime.

Nationally, there were 328 reported cases of suspected identity crime incidents detected by three reporting road agencies. The limited numbers of identity crime incidents reported by these agencies may relate to identity incidents that become apparent when the licences are first applied for or issued, as opposed to the later theft or use of driver licences which had initially been legally obtained. It should be noted that this figure does not include the number of licences recorded as lost or stolen.

This is in contrast to IDCARE which has found driver licences to be the most targeted source of personal information, with 22.2% of clients reporting them as being compromised.

Case Study 5: Real estate fraud

In December 2012, a property manager of a Mandurah real estate agent was contacted by a man claiming to be the owner of a house managed by the agency. He requested property documents, which were provided, and his contact details changed.

A month later, the agency received a request to sell the property. The agent then received a sales agreement containing false signatures, copies of two fraudulent passports of the two owners and forged documents purporting to be from the Australian High Commission in Pretoria confirming the owners' identity.

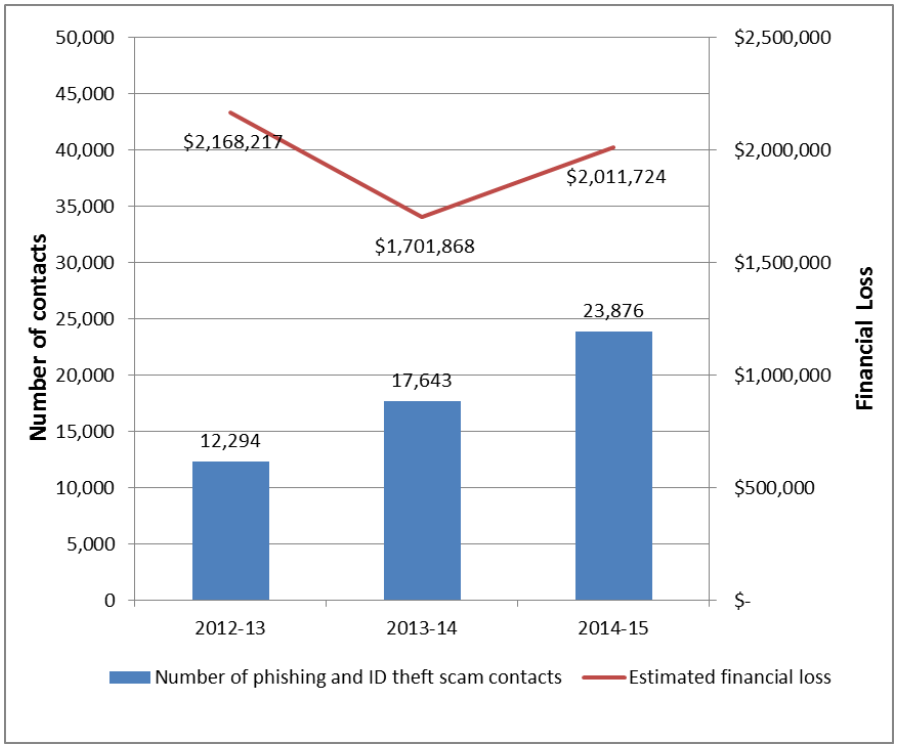
Staff at the real estate agent became suspicious and contacted the WA Police. The agents pretended to go ahead with the sale to try to identify the offenders. With the help of South African and Nigerian Police, the offender was convicted in 2014 of conspiracy to defraud, attempt to obtain money by false pretences and forgery and jailed for 1 year.

Source: Yahoo News, 27 December 2014. https://au.news.yahoo.com/thewest/wa/a/25860969/nigerian-jailed-for-wa-property-scam/

2.1(h) Consumer identity fraud

Key finding: Between 2013-14 and 2014-15 the number of phishing and identity theft incidents recorded by Scamwatch increased by 35.3%, and the reported losses increased by 18.2% to just over $2m.

Figure 24: Number of phishing and identity theft scam contacts recorded by ACCC and their associated financial costs, 2012-13 to 2014-15



Source: ACCC unpublished data.

2.1(i) Identity fraud incidents recorded by police and ACORN

Key finding: Police agencies recorded 133,921 fraud and deception offences in 2014-15. This is up 6% from the 126,305 incidents reported in 2013-14. It is estimated up to 54,000 of these fraud and deception incidents involved a component of identity crime.

The nature of identity offences differs between Australian jurisdictions. Most states including 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 business/investigative needs. A summary of the information available in each jurisdiction is presented in Appendix F.

Case Study 6: Identity crime offences

An offender employed in the service department of a South Australian car dealership made a number of loan applications using false documents containing the personal particulars from various customers who had their cars serviced at the dealership. A significant amount of money was obtained fraudulently by the offender using the false information involving financial institutions and over 16 victims. The offender stated that the offending was in part due to a gambling addiction.

The offender received a sentence of nine years imprisonment with a non-parole period of five years and six months. Certificates for the victims of identity theft under s54 of the *Criminal Law (Sentencing) Act 1988* were issued.

Source: South Australia Police

Australian Cybercrime Online Reporting Network (ACORN)
Launched in November 2014, the Australian Cybercrime Online Reporting Network (ACORN) provides a mechanism for members of the public to report a variety of cybercrimes, including identity crimes. These reports are then referred to the most appropriate law enforcement agency for consideration and possible investigation.

Between 1 July 2015 and 30 June 2016 there were a total of 4,761 identity crime reports submitted to the ACORN, based on reports received under the sub category of Online identity theft. Of the victims who reported financial losses, there was a total loss of $364.5m.

The reports made to ACORN by victims showed that the most common accounts compromised were email (43.7%), bank (39.8%), social media (22.4%) and PayPal (8.9%).

Case Study 7: Identity theft through event tickets
In its first year of operation, information sent to ACORN revealed a scam involving the sale of music and festival tickets. The offender either listed tickets to sell or contacted victims advertising the need to purchase tickets through websites such as Gumtree. Contact was made primarily through SMS or email. The offender provided a copy of a driver's licence (stolen from a previous victim) and requested the victim provide a copy of their driver licence or passport to confirm their identity. Once the details of the transaction were confirmed, the offender requested the victim transfer the funds to a designated bank account to finalise the sale. No tickets were sent to the victim after which all contact ceased.

The identity details provided by the victim as part of the scam were then used by the offender to activate new mobile carriage services or bank accounts in the victim's name and provided to future victims as 'assurance'. A victim's identity was used several times before being discarded and a new identity assumed.

Source: Australian Crime Commission unpublished report.

2.1(j) Other

Australian Securities & Investments Commission (ASIC)
ASIC received a total of 8,185 general reports of misconduct regarding activities or persons regulated by ASIC during 2014-15. Of these 58 reports involved identity crime or misuse.

Australian Transaction Reports and Analysis Centre (AUSTRAC)
AUSTRAC is the anti-money laundering and counter-terrorism financing (AML/CTF) regulator. In 2014-15, 1,959 Suspicious Matter Reports (SMRs) were received from industry with the reason for suspicion being 'false name/identity or documents'; of these 170 were assessed by AUSTRAC as involving the suspected use of a false identity or false names in connection with regulated financial transactions. This is a small decrease from the 188 assessments in 2013-14.

Australia Post
Australia Post also collects data on suspicious mail theft. During 2014-15, 226 allegations or suspicions of mail theft during the course of postal handling were referred to the Australia Post Security Group, for investigation and analysis. From the 226 referrals, there were 181 incidents where an actual mail theft offence was detected and established to at least a high degree of probability. In addition, there were 16 reported cases of identity crime (victims in these cases were advised to report the matter to the police). Of these 15 were fraudulent mail redirection (11 online and 4 retail Post shops) and 1 case involved credit card misuse.

2.2 The number of prosecutions involving identity crime and other related offences

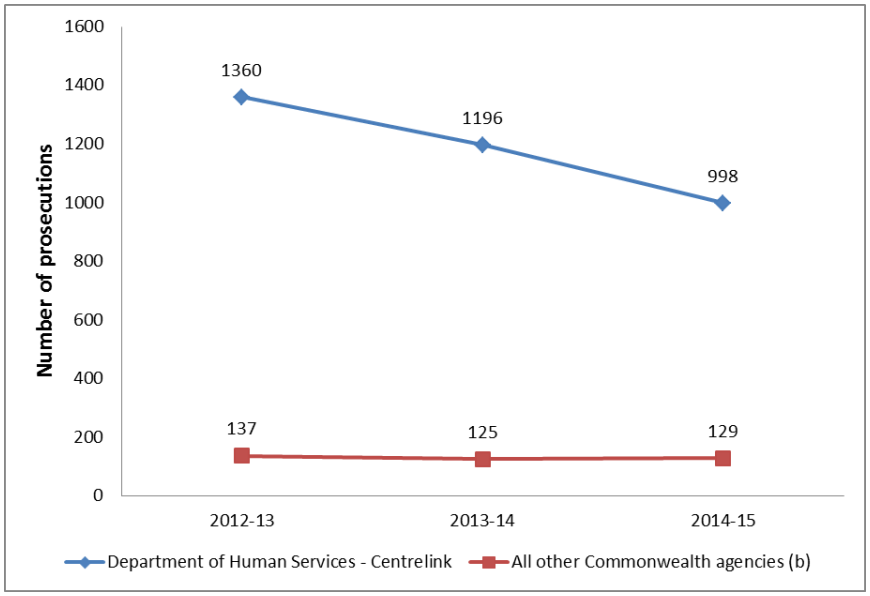
2.2(a) Commonwealth prosecutions

Key finding: There continues to be a decline in the number of identity crime prosecutions by the CDPP, which fell by around ten per cent between 2013-14 and 2014-15.

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 *Trademarks Act 1995 (Cth)*. These are explained in greater detail in Appendix G.

For offences regarding fraudulent conduct (Division 133-137 *Criminal Code Act 1995*) there were 1,127 prosecutions by the CDPP in 2014-15, most of which (998) were referred by DHS.

Figure 25: Number of CDPP prosecutions for fraudulent conduct (a), by referring agency, 2012-13 to 2014-15



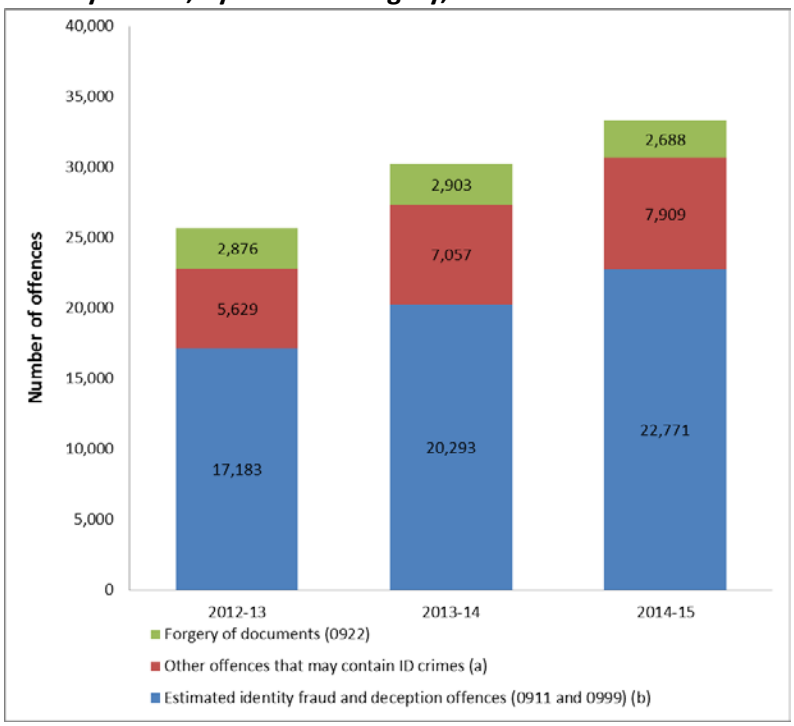
Source: CDPP, unpublished data.
Note (a): Fraudulent conducts refers to prosecutions under Division 133-137 *Criminal Code Act 1995*.
Note (b): Excludes State and Territory Police referrals and International Police (retired) categories.

2.2(b) State and territory identity crime prosecutions

Key finding: There were approximately 33,000 offences proven in state and territory courts in 2014-15 which may have related to identity crime, representing a 10% increase from the 30,000 offences proven in 2013-14.

A wide range of legislation is used in jurisdictions for prosecuting identity crimes. Therefore, quantifying the true number of identity crimes proved in state and territory courts requires a count of the identity crime offences such as forgery and impersonation, combined with an estimation of the proportion of other fraud offences that were identity-crime related.

Figure 26: Number of offences proved in all state and territory courts that may have involved identity crimes, by offence category, 2012-13 to 2014-15



Source: ABS 2016c.
Note (a): Includes offences coded under the following ANZSOC codes: 0829, 0831, 0923, 0931, 0932, 0933, 0991, 1111, 1542, 1543, 1559, 1612, and 1694.
Note (b): Estimated identity fraud and deception offences are based on 40 per cent of fraud offences in categories 0911 and 0999.

The ABS criminal courts data provided for this report includes a count of defendants proven guilty for an offence under a number of Australian and New Zealand Standard Offence Classification (ANZSOC) codes.[4] These particular ANZSOC codes include offences that may or may not involve identity crime. As such, these data should be used with caution when being interpreted within the context of this report.

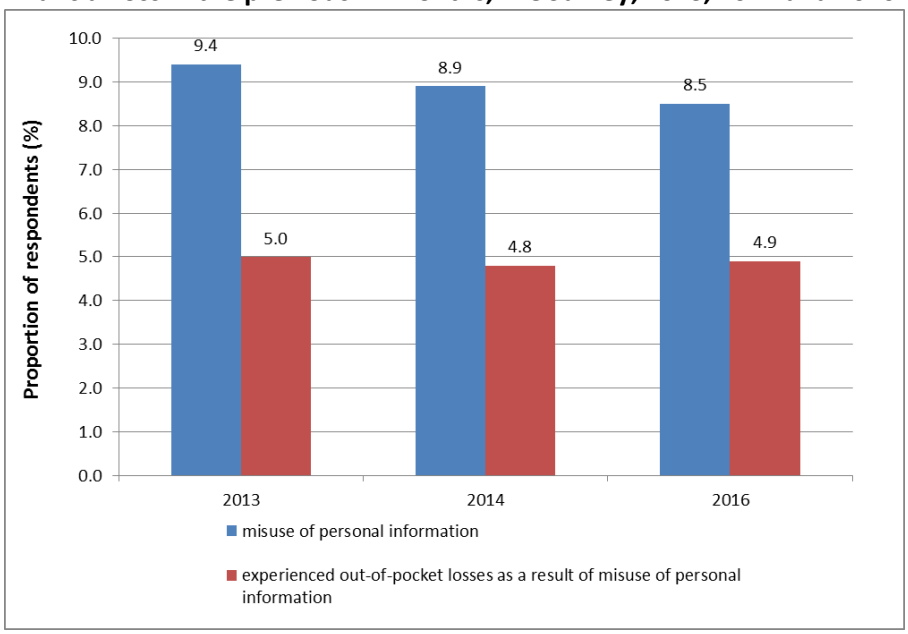
[4] ANZSOC codes provide a uniform national statistical framework for classifying criminal behaviour in the production and analysis of crime and justice statistics (ABS 2011).

2.3 The number of people who self-report being victims of identity crime or misuse

2.3(a) Number of people experiencing identity crime

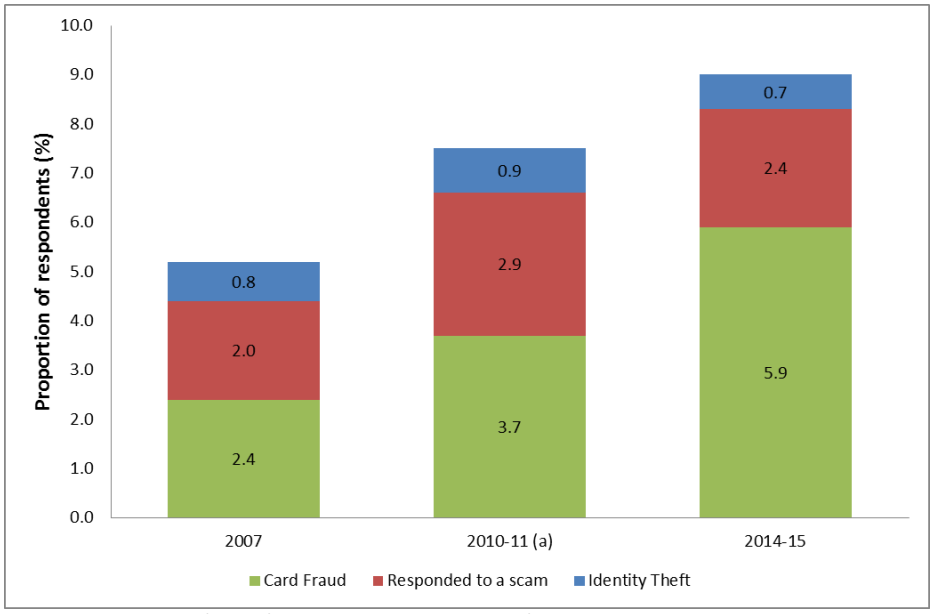
Key findings: The number of people who experience identity crime or misuse each year appears to be relatively steady, with between 6 and 8% of AIC and ABS survey respondents experiencing identity crime in the previous 12 months and 5% of respondents reporting out-pocket losses. The proportion of Australians who report being a victim of identity crime is considerably higher than other personal and theft-related offences – making it one of the most common crimes in Australia.

Figure 27: Proportion of respondents who experienced misuse of personal information and financial loss in the previous 12 months, AIC Survey, 2013, 2014 and 2016



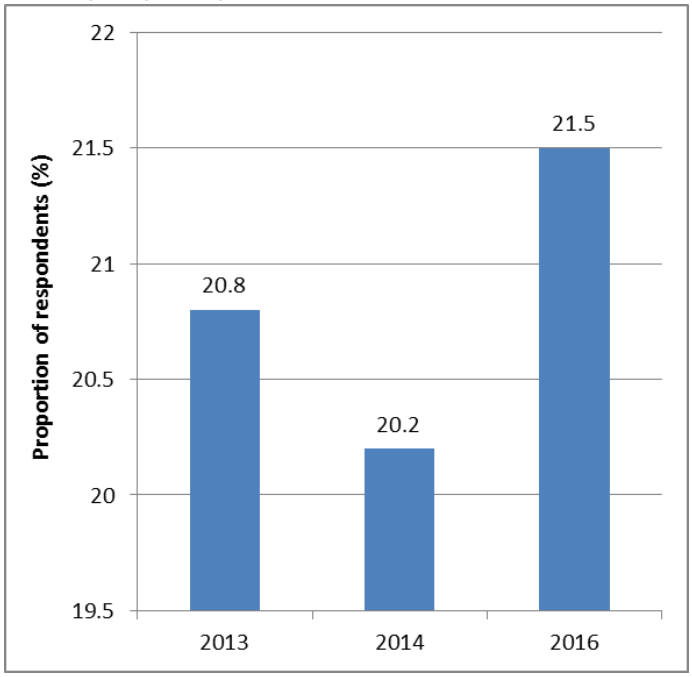
Source: AIC Surveys 2013, 2014 and 2016
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

Figure 28: Proportion of respondents reporting personal fraud victimisation, ABS, 2007, 2010-11 and 2014-15



Source: ABS Personal Fraud Survey 2007, 2010-11 and 2007.
Note (a): 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.

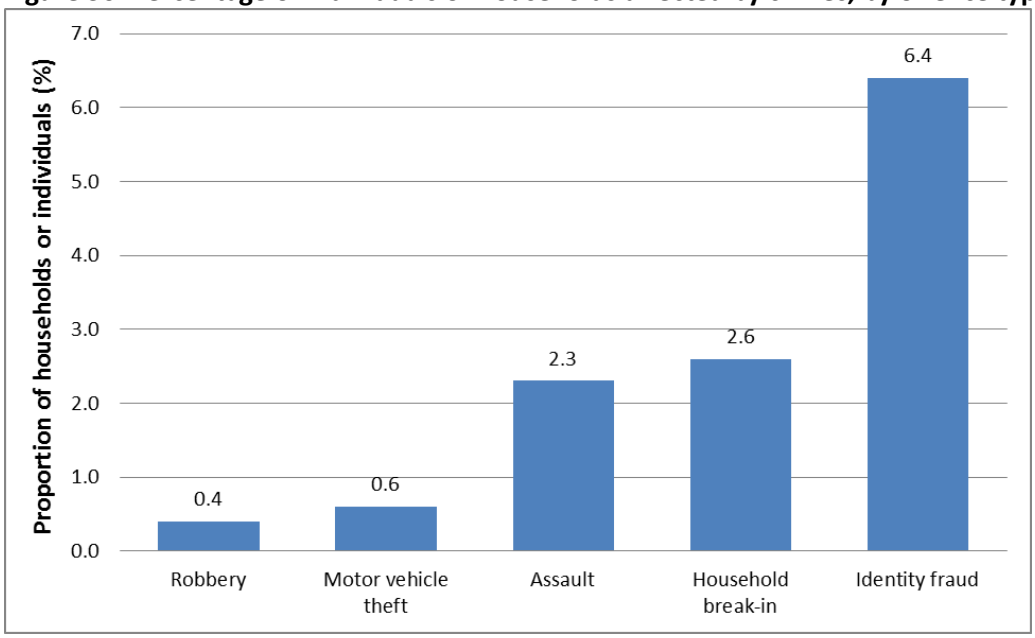
Figure 29: Proportion of respondents reported having ever been a victim of identity crime and misuse, AIC, 2013, 2014 and 2016



Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

Identity crime appears to be one of the most prevalent crimes in Australia when compared with the victimisation rates for other common 'personal and theft-related' crimes such as robbery, motor vehicle theft and assaults (Figure 30).

Figure 30: Percentage of individuals or households affected by crimes, by offence type



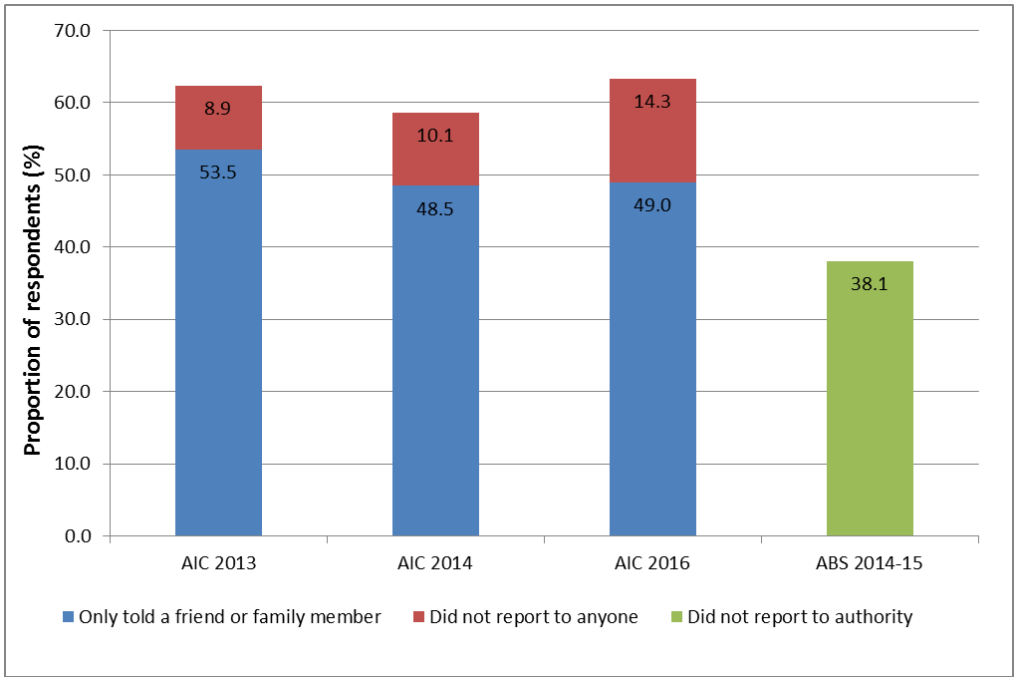
Sources: ABS Personal Fraud Survey 2014-15 (ABS 2016a) and ABS 2016b.

2.3(b) Reporting of identity crimes to authorities

Key finding: Identity crime is greatly underreported by victims (up to 60% do not report the incident officially). The most common reason for not reporting incidents is the belief that the police (or any other authority) would not be able to do anything to assist (33%). Under-reporting continues to be a problem that contributes to the difficulty in determining the true extent of identity crime.

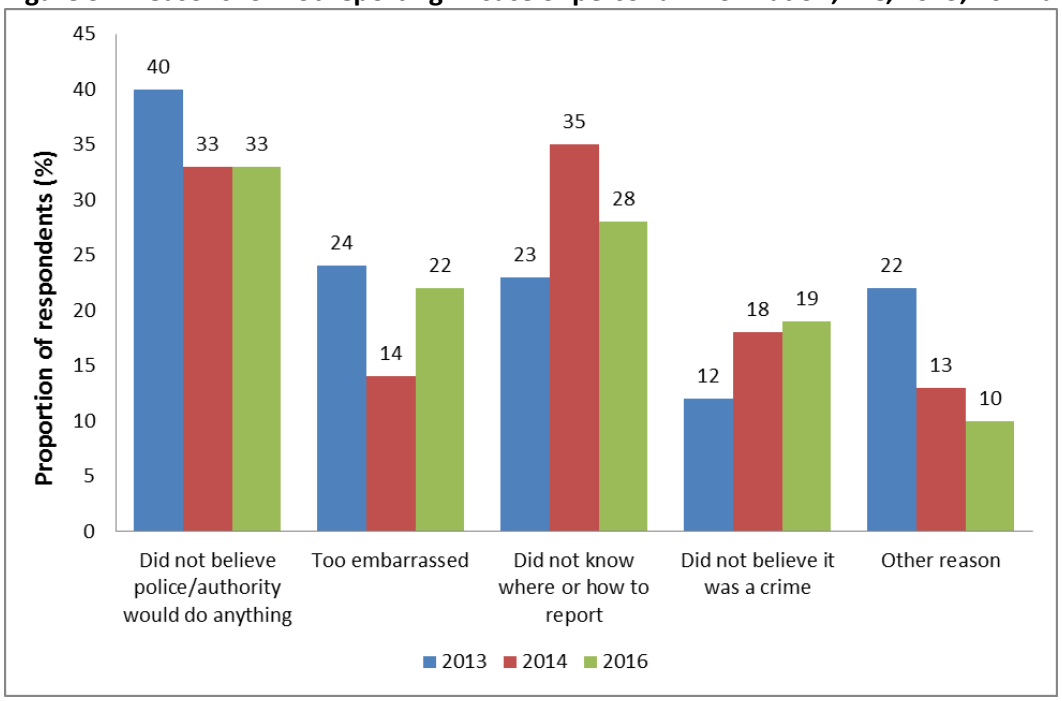
Survey research by the ABS and AIC have found high proportions of identity crime victims failing to report their experiences officially, although credit card companies are invariably notified where payment card misuse takes place, in order for charge-backs to be processed. Despite the advent of ACORN as a centralised online reporting portal, many victims remain unclear about how and where to report identity crime.

Figure 31: Number of respondents who did not report identity theft incident to the authorities, by survey and year



Source: AIC Surveys 2013, 2014 and 2016; ABS Personal Fraud Surveys 2014-15. AIC and ABS data are not directly comparable due to differences in sampling frames used.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

Figure 32: Reasons for not reporting misuse of personal information, AIC, 2013, 2014 and 2016



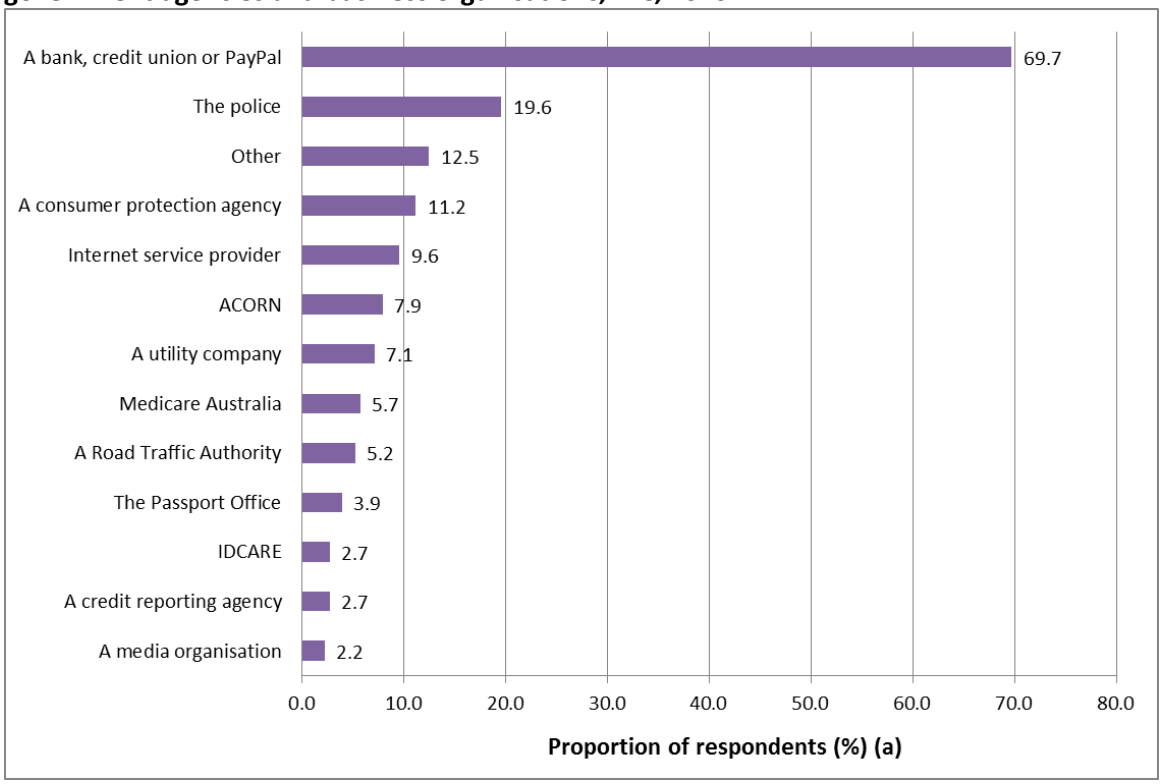
Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

IDCARE has also noted a decline in the reporting rate to law enforcement by victims of identity theft who engaged with them. In 2015, only 3.4% of clients had reported their identity compromise or misuse to law enforcement prior to engaging with IDCARE support services. Respondents to the 2016 AIC survey were also asked to specify which government agency or business organisation to whom they had reported the incident (Figure 33).

These results indicate that:

- further work is required to increase community awareness about the fact that misuse of an individual's personal information is a crime and;
- the community could benefit from education about the organisations to which they should be reporting identity crime.

Figure 33: Percentage of respondents, who reported identity crime incidents to particular government agencies and business organisations, AIC, 2016

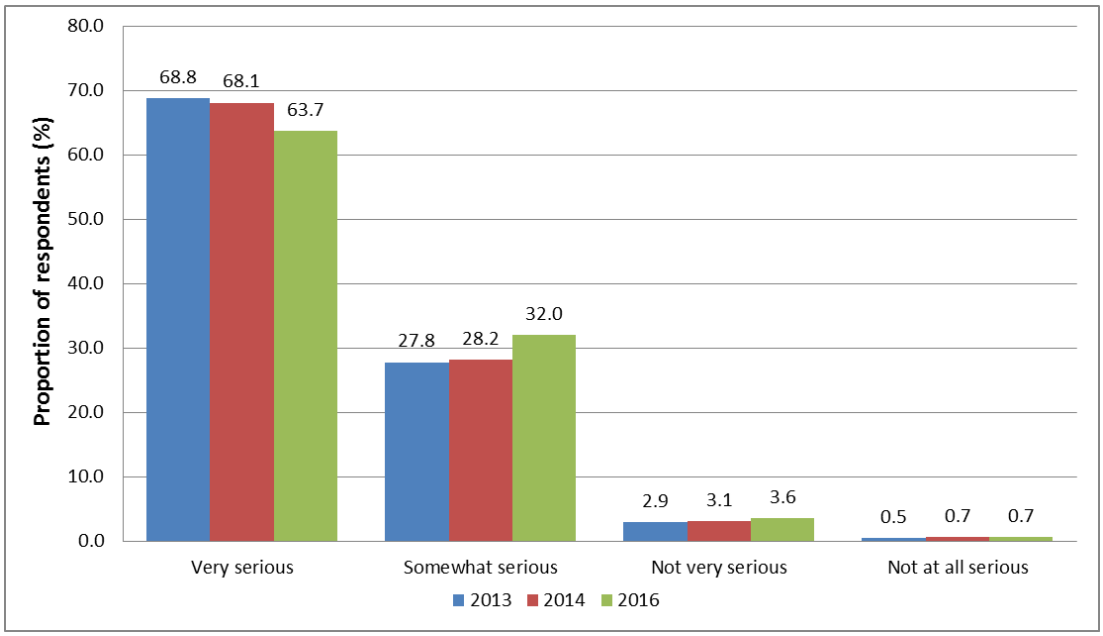


Source: AIC Survey 2016.
Note (a): Respondents could select multiple organisations therefore percentages do not total 100.

2.4 The number of people who perceive identity crime and misuse as a problem

Key finding: Identity crime continues to be of great concern to Australians, with 97% of respondents in the 2016 AIC Survey claiming that misuse of personal information was a very serious or somewhat serious issue.

Figure 34: Percentage of level of concern about identity crime and misuse, AIC, 2013, 2014 and 2016



Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

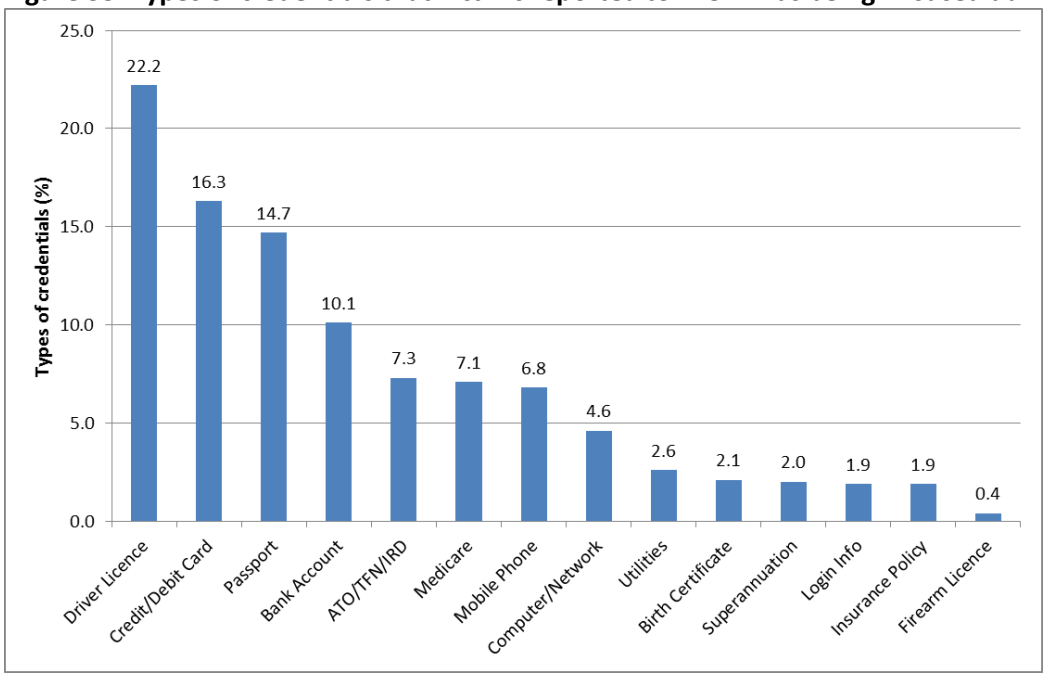
2.5 The types of personal information most susceptible to identity theft or misuse

Key finding: Driver licences, credit/debit cards and passports are the most commonly misused identity credentials, whilst credit/debit card information, a person's name, and bank account information are the most commonly misused personal identifying information.

2.5(a) Credentials susceptible to identity theft or misuse

IDCARE found driver licences were the most targeted identity credential, followed by credit or debit card details, passports, and bank account details (IDCARE 2016). IDCARE classifies the compromise of driver licences and passport information as being a 'high risk event' for individuals due to their frequent use in the community as an identity document and the increased chances of success for criminals when using the information on the credential. (IDCARE 2016).

Figure 35: Types of credentials that victims reported to IDCARE as being misused during 2015

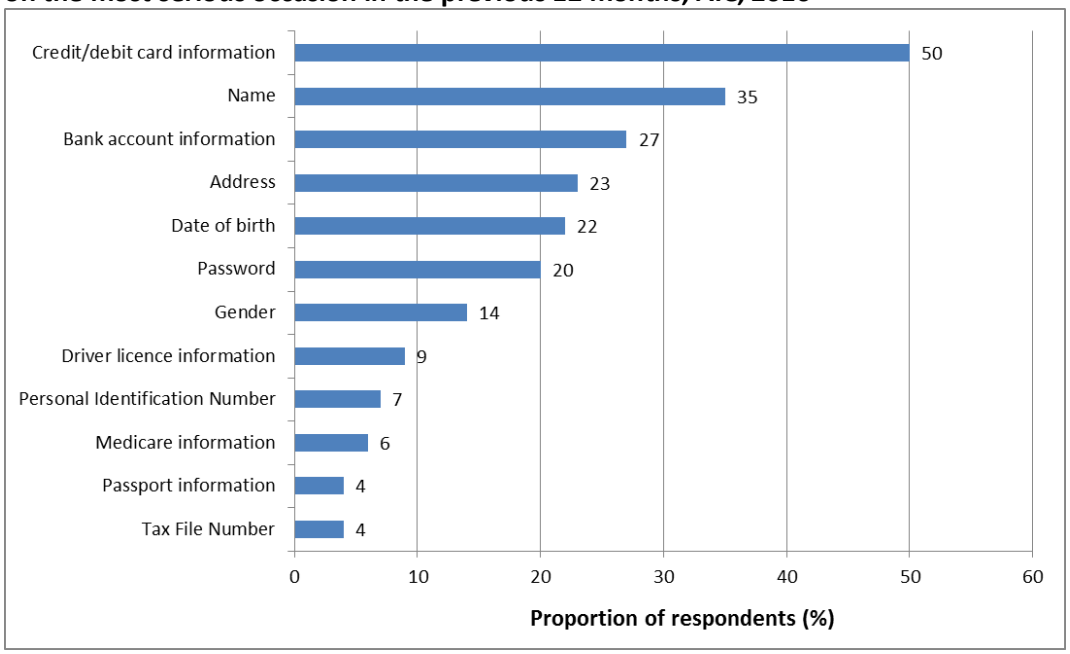


Source: IDCARE 2016.

2.5(b) Personal identifiable information susceptible to identity theft or misuse

IDCARE also found that in 78% of instances of identity theft or misuse, the physical credential remained in the possession of the victim. This indicates that the personal identifiable information that appears on the credential is being sourced by means other than the theft of the credential itself. Figure 36 shows the most common types of personal identifiable information susceptible to misuse in the AICs 2016 survey.

Figure 36: Types of personal identifiable information that respondents reported as being misused on the most serious occasion in the previous 12 months, AIC, 2016



Source: AIC Survey 2016.

Case Study 8: Counterfeit licences

In March 2014, the joint AFP-NSW Police Identity Security Strike Team (ISST) detected a parcel from China containing 5,000 counterfeit NSW Driver Licences' holograms.

Search warrants were executed on premises and a number of items were seized including computer equipment, printers, card cutters, thousands of blank cards, holograms for licences and credit cards, electronic card templates, card readers, and fraudulent identity documents in various states of manufacture from both Australia and overseas. A number of offenders were charged in relation to the matter. The offence of dealing with identification information carries a penalty of up to 10 years imprisonment, while participating in a criminal group carries a penalty of up to 15 years imprisonment.

Source: New South Wales Police Force 2015, 'Joint agency investigation shuts down fraudulent identity manufacturing operation', media release, 26 February 2015.

3. Impact of identity crime

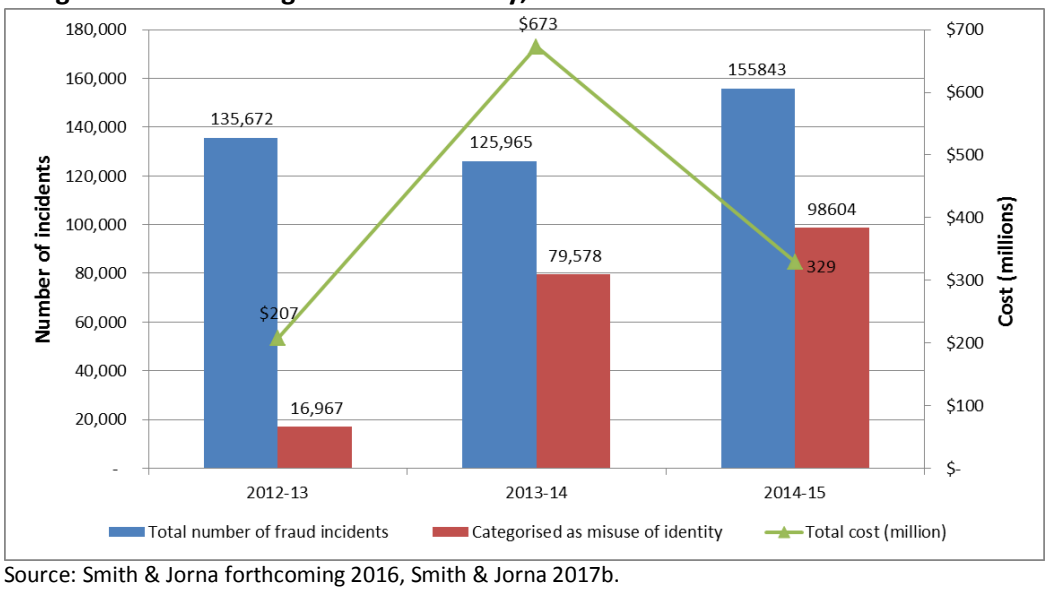
3.1 Direct cost of identity crime and misuse to government agencies

Key finding: There were almost 100,000 incidents of identity fraud recorded by Commonwealth agencies in 2014-15.

In 2014-15, 154 Commonwealth agencies participated in the Fraud against the Commonwealth census. Of these, 65 reported a total of 155,843 incidents of internal and external fraud; this included 98,604 incidents that were classified as involving 'misuse of identity'. The estimated value of fraud losses in 2014-15 was $328.9m.[5] Details regarding the methodology used to calculate this estimate can be found in Section 6.

[5] The census asked about alleged/suspected or proved fraud incidents therefore the total cost is just an estimate of loss at that point in time.

Figure 37: Number of fraud incidents reported by Commonwealth agencies and those that were categorised as involving misuse of identity, 2012-13 to 2014-15



Source: Smith & Jorna forthcoming 2016, Smith & Jorna 2017b.

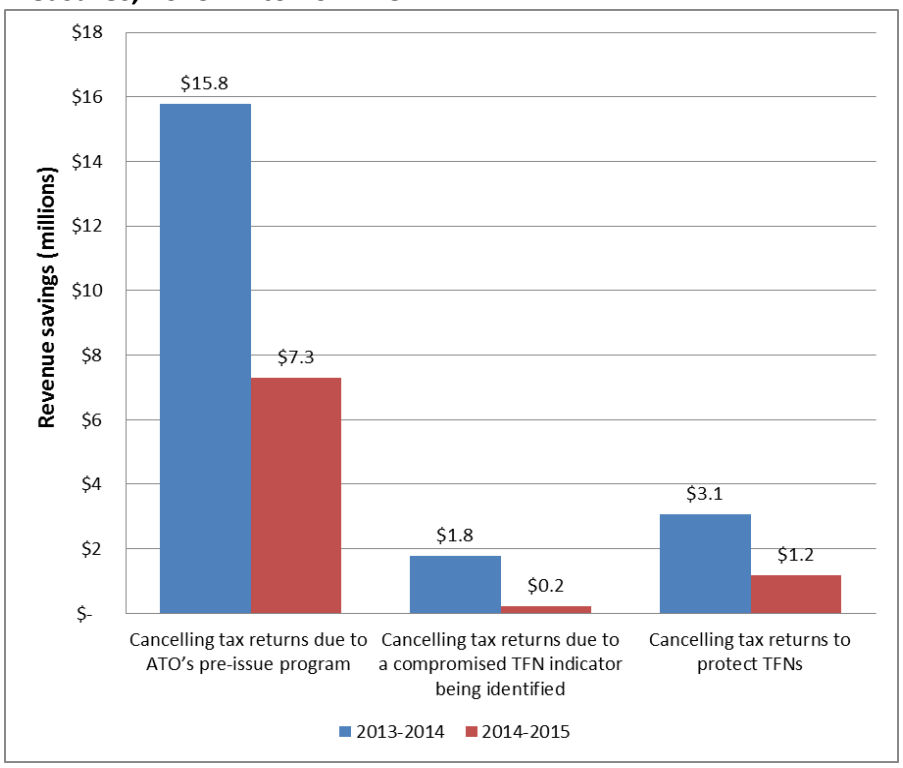
3.1(a) Costs to individual agencies

In addition to the results of the annual Commonwealth Fraud census, separate statistics were also sought from selected Commonwealth agencies that were willing to disclose their information publicly.

Australian Taxation Office (ATO)

The costs associated with detected identity crime incidents can be substantial. In 2014-15, the ATO saved $8.7m in protected revenue as a result of identity fraud protective measures (Figure 38) that disrupt attempts to claim returns using stolen identities. Although considerably less than the $20.7m savings in 2013-14, the total remains an indication of the extent of identity misuse that the ATO has dealt with.

Figure 38: Protected revenue savings as a result of ATO identity fraud protective measures, 2013-14 to 2014-15



Source: ATO unpublished data.
The pre-issue activity involves the ATO taking action to correct errors or to verify the details and amounts reported in an income tax return before a notice of assessment (and any associated refund) issues to the taxpayer. (Inspector-General of Taxation 2013).

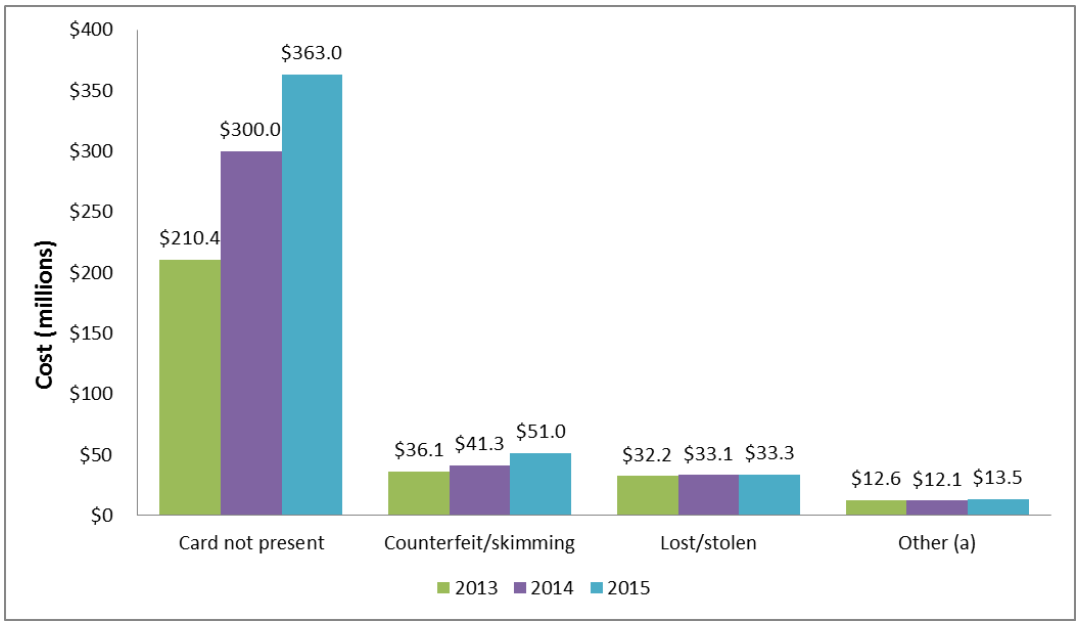
3.2 Direct costs of identity crime and misuse to business

Key finding: The value of frauds involving Australian-issued payment cards continues to rise, costing Australian businesses over $400m in 2014-15 an increase from $304m in 2013-14.

3.2(a) Identity fraud involving transaction payment systems

In 2014-15, there were a total of 6.9b transactions involving Australian-issued payment cards. Of these transactions, 1.9m (0.03%) were deemed to be fraudulent, with a total value of approximately $406m (APCA 2015). The majority of these are card-not-present fraud, where account information is used without the authority of the cardholder where no physical card is involved, via the phone or internet.

Figure 39: Costs associated with Australian-issued payment card fraud, by reason, APCA, 2013-15



Source: APCA 2016.
Note (a): Other includes never received and fraudulent application.

Case Study 9: Conspiracy to steal credit card details

In August 2014, a man was found guilty of four offences relating to conspiring with others to steal credit card details and use false identification.

The court found that he had entered Australia on a false Canadian passport in 2011 and then organised for the importation of an EFTPOS terminal from Canada and for a co-conspirator with technical expertise to be flown to Australia. The EFTPOS terminal was then modified to record credit card details, including the holder's name and PIN number without the transaction being sent to financial institutions.

The offender intended for the EFTPOS terminal to be installed in a grocery store in Western Sydney offering to pay the store owner for 1,000 skimmed cards during a week-long operation. It had also been organised for a young Indian national to be employed in the store that could be blamed for the skimmings and organised people in Malaysia and Singapore to withdraw the money from skimmed accounts.

The offender was sentenced to a minimum of 8 years and 3 months imprisonment.

Source: SBS, 25 September 2014, http://www.sbs.com.au/news/article/2014/09/25/skimming-mastermind-gets-11-years

3.2(b) Identity fraud against Australian businesses

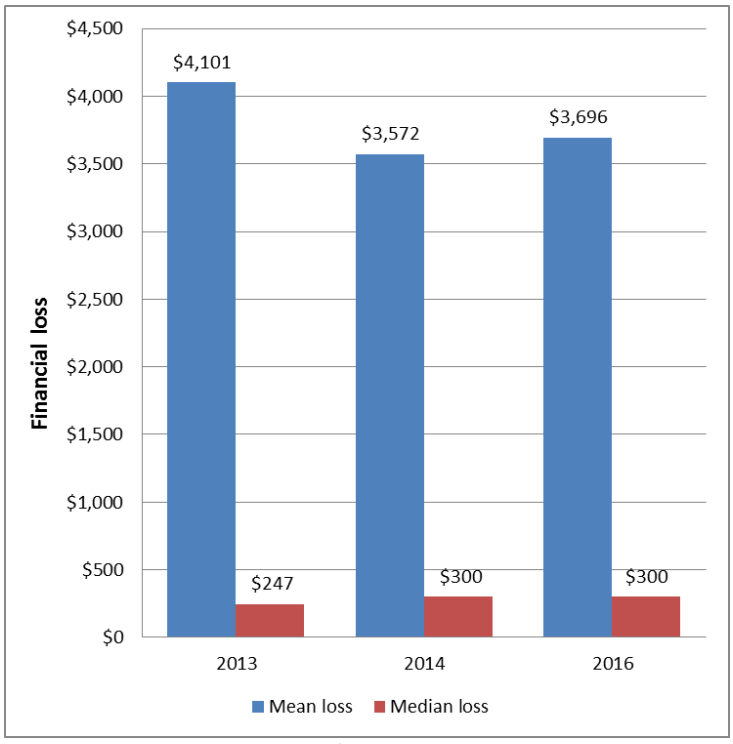
Surveys of Australian businesses have been carried out by large consultancy firms such as KPMG and PricewaterhouseCoopers (PwC) in the past, in an effort to understand how widespread fraud is within the Australian business community (KPMG 2013; PwC 2014). Unfortunately, these reports have not been reproduced in 2015, however findings from these reports can be found in previous ICAMIA reports.

3.3 Direct cost of identity crime to individuals victims

Key finding: The direct cost of identity crime and misuse to individual victims in Australia each year is approximately $657m, a 51% increase from $435m in 2013-14. The cost to individual victims varies considerably. While most lose relatively small amounts, in some cases losses can run to millions of dollars.

Details of the methodology used to calculate the total cost of identity crime to victims can be found in Section 6. The 2016 AIC survey found that victims experienced out-of-pocket losses ranging between $1 and $500,000. The average losses have remained relatively stable over the last three surveys.

Figure 40: Mean and median out-of-pocket financial losses suffered by victims of identity crime and misuse



Source: AIC Survey 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

The mean losses suffered by victims can vary greatly between organisations which collect data. Community surveys reporting mean losses of approximately $3000 which is much smaller than IDCARE which has a mean value of over $27,000 (Table 3). IDCARE found that the majority of clients report more complex incidents of identity misuse which may explain the difference.

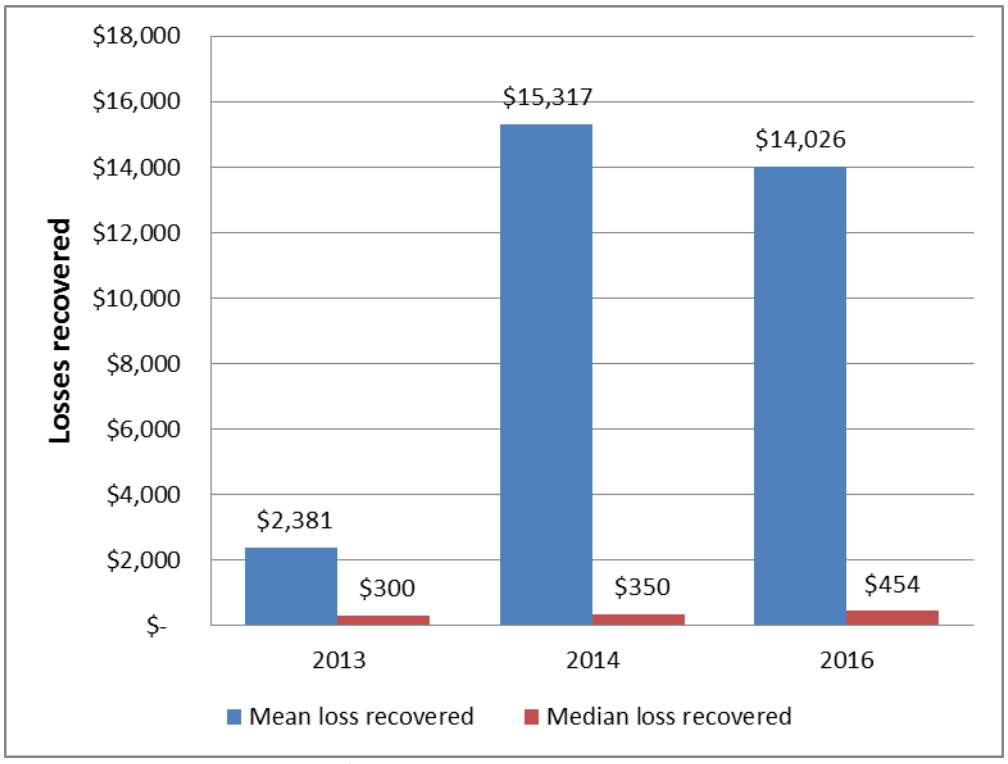
Table 3: Mean and median losses suffered by victims of identity crime and misuse, by survey

Source	Mean loss	Median loss
IDCARE (a)	$27,267	$1,100
AIC Survey 2016	$3,696	$300
ABS Personal Fraud Survey 2014-15 (b)	$2,700	$400

Note (a): IDCARE deals specifically with victims who require assistance and support often involving cases with large losses, unlike ABS and AIC surveys that canvass populations more generally.
Note (b): Value includes losses to all personal fraud (card fraud, ID theft and people responding to scams). Estimates for identity theft and people responding to scams have a relative standard error of 25% to 50% and should be used with caution.

Some victims seek reimbursement of the financial losses they incur as a result of misuse of their personal information. The average recovered loss in 2014 and 2016 is considerably higher than that recorded in the 2013 AIC Survey due to one-off amounts that are considerably larger than in 2013.

Figure 41: Mean and median recovered losses experienced by victims, AIC Survey, 2013, 2014 and 2016



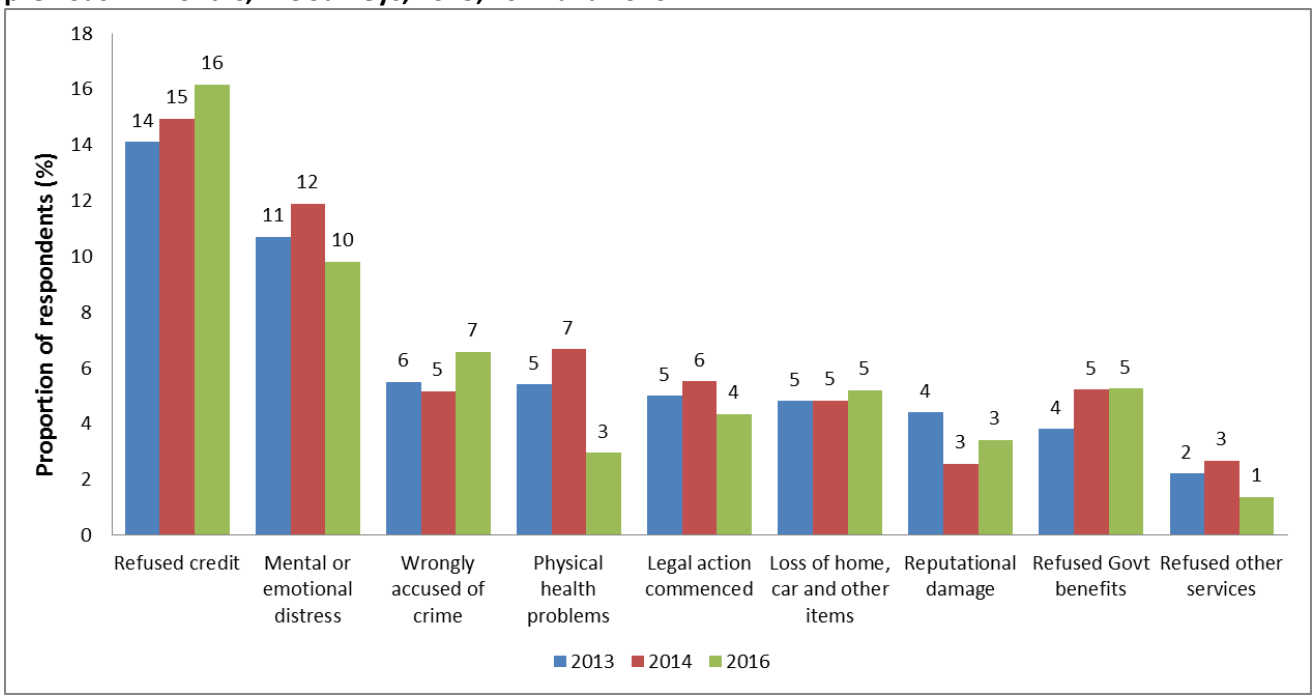
Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

3.4 Non-financial consequences of identity crime and misuse.

Key finding: Aside from financial losses, the three most prevalent consequences that victims have reported were being refused credit, experiencing mental or emotional distress and being wrongfully accused of a crime.

The most recent AIC survey in 2016 found that there had been an increase in the percentage of victims who reported having been refused credit and wrongly accused of a crime as a consequence of misuse of personal information in the preceding 12 months (Figure 42). Most other consequences were reported by fewer victims in 2016 than in previous survey years.

Figure 42: Consequences experienced as a result of personal information being misused in the previous 12 months, AIC Surveys, 2013, 2014 and 2016



Source: AIC Survey 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

4. Remediation of identity crime

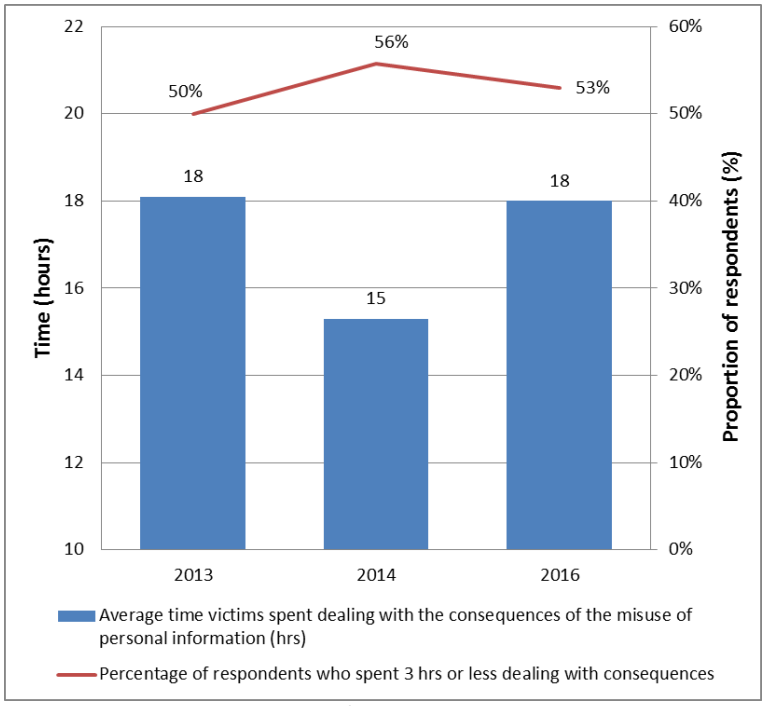
The amount of time it takes for a victim to deal with the impact and consequences of identity crime varies depending on the extent that their identity has been misused. In cases that involved one fraudulent application or transaction, victims only incurred minimal inconvenience and financial impost. In more serious cases, such as those involving a complete takeover of the victim's identity, it took some victims over 200 hours to obtain new credentials and sort out the consequences of the crime (IDCARE 2015).

4.1 The average time spent by victims recovering their identity

Key finding: The process of restoring identity and reputation within the community is often complex, harmful and uncertain. The average time victims spend dealing with the consequences of identity crime is around 18-19 hours; an increase from the 15 hours found in the 2014 AIC Survey.

The ABS has found the large amount of time victims spend dealing with the misuse of personal information reflects the potential complexity of having to restore a compromised identity. This includes not only financial losses (that can run into the hundreds of thousands of dollars), but non-financial harms such as loss of reputation, which can affect personal relationships, patterns of work and sleep and even lead to mental and physical health problems.

Figure 43: Time spent by victims dealing with consequences of misuse of personal information, 2013, 2014 and 2016



Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.

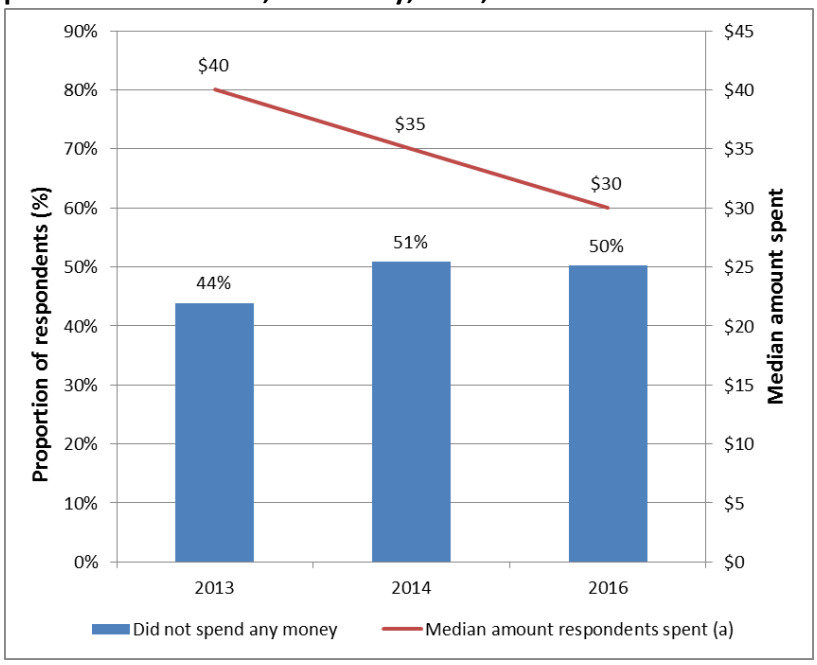
In 2015, victims who contacted IDCARE experienced the compromise of at least two credentials. This required victims to engage with, on average, over seven organisation taking clients 19 hours to respond to each event. This finding is consistent with the average time taken by respondents to the AICs surveys (18 hours in 2013 and 2016). The results of the nationally representative ABS survey for 2014-15 show that dealing with the consequences of identity theft takes considerably longer than dealing with the consequences of card fraud (Figure 44).

Figure 44: Amount of time spent by victims dealing with consequences of misuse of personal information, ABS Survey, 2014-15

Source: ABS Personal Fraud Surveys 2014-15.

In addition, the AIC Surveys also collected data on how much money those victims had spent dealing with the consequences of the misuse (Figure 45). The 2016 survey found that half of the respondents did not spend anything, while the median amount spent was $30. This does not include the cost of time taken to deal with the consequences.

Figure 45: Amount of money spent by victims dealing with the consequences of misuse of personal information, AIC Survey, 2013, 2014 and 2016



Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.
Note (a): This Figure presents the median amount that respondents spent (not including those who spent $0) on dealing with the consequences of misuse of personal information.

4.2 The number of enquiries to government agencies regarding assistance to recover identity information

Key finding: Reporting of identity crime to state and territory agencies appears to be very low, compared to IDCARE which engaged with over 15,000 victims.

4.2(a) Enquiries to IDCARE

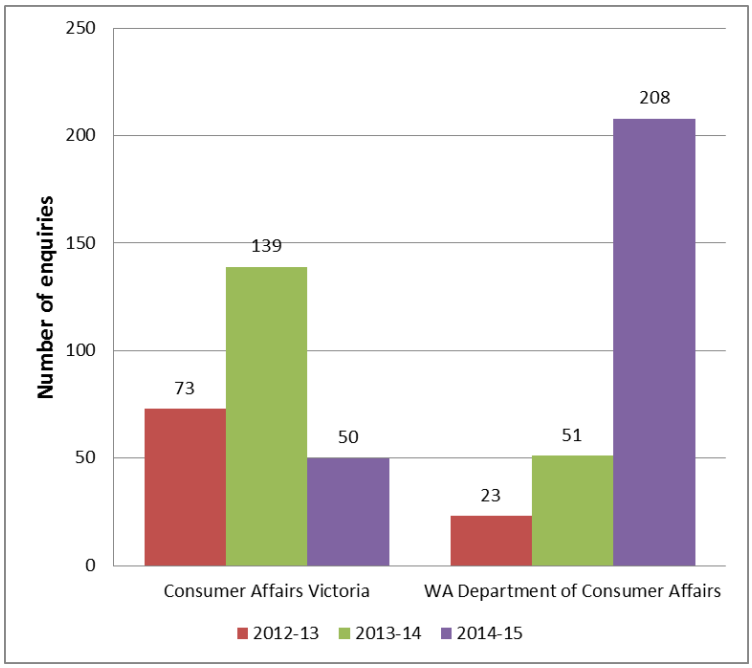
During 2015, a total of 15,592 clients engaged with IDCARE, a quarter of whom engaged with IDCARE on multiple occasions. Furthermore IDCARE provided 39,904 individual response plans during 2015, which gave clients personalised plans on how to mitigate the future misuse of their identifying information. (IDCARE 2016).

4.2(b) Consumer Affairs Agencies

The 2016 AIC survey found that 11.2% of respondents who had their identities compromised, reported it to a consumer protection agency (e.g. Scamwatch, Consumer Affairs or Office of Fair Trading), while the 2016 ABS found that of the number identity theft victims who reported the incident to a consumer affairs agency or ombudsman was much lower. There may be a lack of awareness of the role of these agencies which is supported by numbers provided by agencies.

Consumer Affairs agencies from Victoria and Western Australia were able to provide data regarding the numbers of identity crime enquiries received in 2014-15 (Figure 46). When compared to the number of identity crime victims each year, the number of identity crime enquiries reported to state and territory consumer affairs agencies appears to be very low, possibly due to the definition of 'identity crime' employed.

Figure 46: Number of enquiries received in relation to identity crime, by agency, 2012-13 to 2014-15



Source: Consumer Affairs Victoria and Western Australian Department of Consumer Affairs.

NSW Fair Trading could only identify three identity-related complaints in 2014-15. Meanwhile Consumer Affairs and Fair Trading Tasmania could only provide data on scams, of which there were 215 enquiries and five complaints.

Case Study 10: False identification to enrol in diploma courses

A consumer contacted NSW Fair Trading to complain that their identity documents and personal information were being used by a VET training organisation to enrol them in multiple diploma level college courses under the VET-HELP loan scheme without their consent. At the time of the complaint the total value of the fraudulent enrolments was $20,000.

NSW Fair Trading contacted the training organisation about the complaint and redress was offered to the complainant.

Source: NSW Fair Trading unpublished information

4.2(c) Commonwealth Attorney-General's Department (AGD)

During 2014-15, AGD received 83 enquiries relating to the theft or misuse of personal information relating to the reasons for contact listed in Table 4.

Table 4: Reason for contacting AGD

Issue/Reason for contact	Number of enquiries
Lost/stolen documents (a)	15
Scams	17
Identity fraud	6
Identity theft	14
Unsafe disclosure of personal information	3
Cyber-security	3
Organisation privacy practices (b)	7
Other (not elsewhere classified)	18
TOTAL	**83**

Source: Attorney-General's Department, unpublished data.
Note (a): Includes instances where personal information and documents have been stolen in electronic formats.
Note (b): Includes businesses and government agencies seeking guidance in relation to best practices for collecting, using and disclosing personal information.

4.2(d) Office of the Australian Information Commissioner (OAIC)

The OAIC received a total of 8,739 enquiries that were related to the Australian Privacy Principles (APP) 2014-15, this included 2,302 enquiries relating to APP6 which deals with the use or disclosure of personal information (Table 5).

Table 5: Number of enquiries related to the APPs received by the OAIC, 2014-15

Issue	Number of enquiries possibly involving identity related issues	Complaints	Investigations
APP 1 - open and transparent management of personal information	217	16	0
APP 2 - anonymity and pseudonymity	16	6	0
APP 3 - collection of solicited personal information	1484	161	0
APP 4 - dealing with unsolicited personal information	21	1	0
APP 5 - notification of the collection of personal information	820	38	0
APP 6 - use or disclosure of personal information	2302	454	3
APP 7 - direct marketing	402	110	4
APP 8 - cross-border disclosure of personal information	125	1	0
APP 9 - adoption, use or disclosure of government related identifiers	12	1	0
APP 10 - quality of personal information	151	129	0
APP 11 - security of personal information	1421	197	0
APP 12 - access to personal	1655	359	0

Issue	Number of enquiries possibly involving identity related issues	Complaints	Investigations
information			
APP 13 - correction of personal information	113	17	0
Total	**8739**	**1490**	**7**

Source: OAIC unpublished data.

Case Study 11: Breach of personal information
During a routine traffic stop in June 2015, NSW Police searched a vehicle and discovered documents which did not match the occupants or driver of the vehicle. The documents were linked to customers of Citibank who had reported funds missing from their accounts.

Police were able to trace the leak back to a Filipino call centre used by Citibank. The breach of personal information affected up to 30 customers at a cost of more than $1m. It was linked to a call centre worker who had been selling customers' personal information to a crime syndicate in Sydney.

On 2 July 2015, NSW Police arrested four men in Sydney who had allegedly used the personal information to obtain credit cards and bank loans.

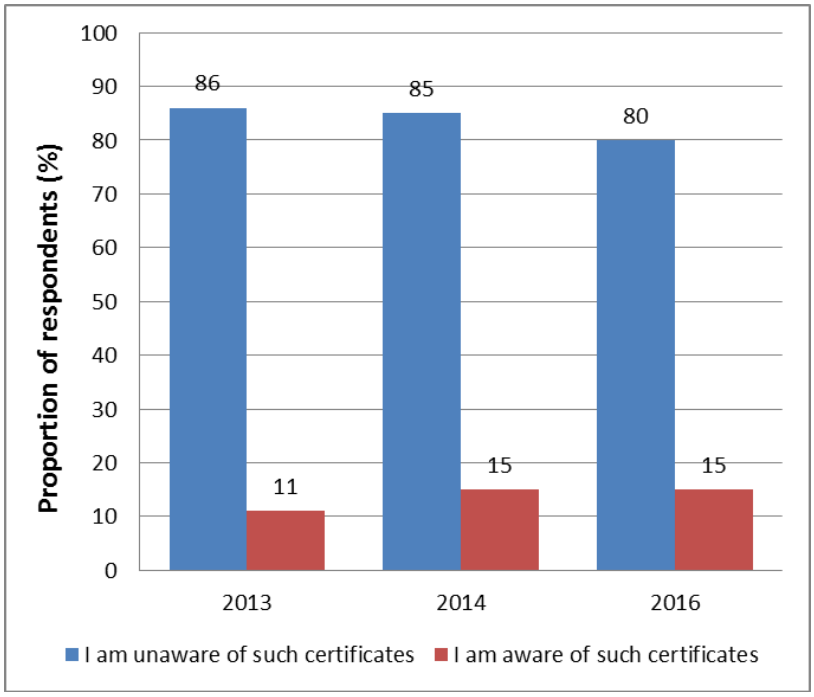
Source: http://www.dailytelegraph.com.au/news/alleged-identity-crime-and-fraud-from-citibank-call-centre-sydney-police-arrest-four/story-fni0cx4q-1227425412865

4.3 The number of applications for Victims' Certificates

Key finding: 'Victims of Identity Crime' Certificates continue to be under-utilised, with a very small number of certificates being issued at the Commonwealth level in 2014-15.

The low uptake rate of these certificates has been partially attributed to the fact that in a number of jurisdictions, legislative requirements predicate the issuing of Victims' Certificates upon conviction of the offender. This is problematic given only a very small number of identity crime offenders are actually convicted (IDCARE 2014a).

Figure 47: Proportion of respondents who are aware of Victims' Certificates, AIC Survey, 2013, 2014 and 2016



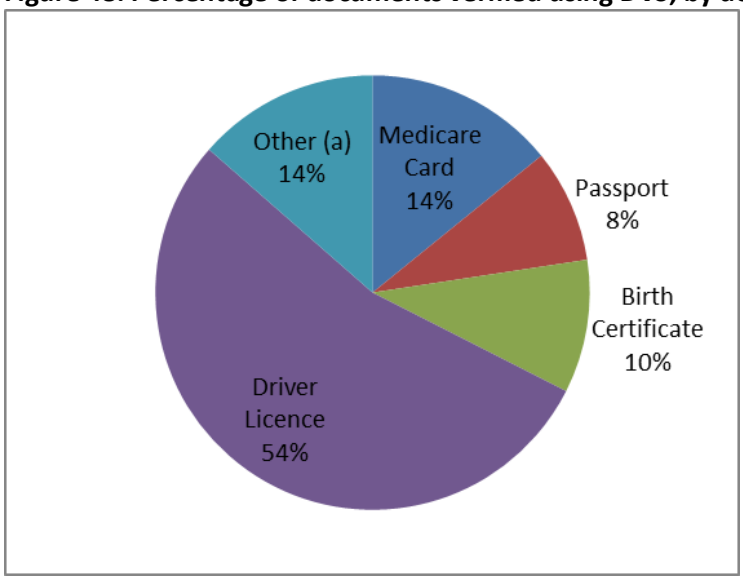
Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex. Due to rounding percentages may not total 100.

5. Prevention of identity crime

5.1 The range of identity credentials verifiable using the DVS

Key finding: The DVS can be used to verify information on the majority of government-issued identity credentials that are relied upon as evidence of identity. This includes four credentials that have been identified through this report as being amongst the most at risk of misuse (ie Medicare cards, driver licences, birth certificates and passports).

Figure 48: Percentage of documents verified using DVS, by document type, during June 2016



Source: DVS unpublished data
Note (a): Other includes Marriage Certificates, Citizenship Certificate, Change of Name Certificates, ImmiCard and Registration of Descent Certificate.

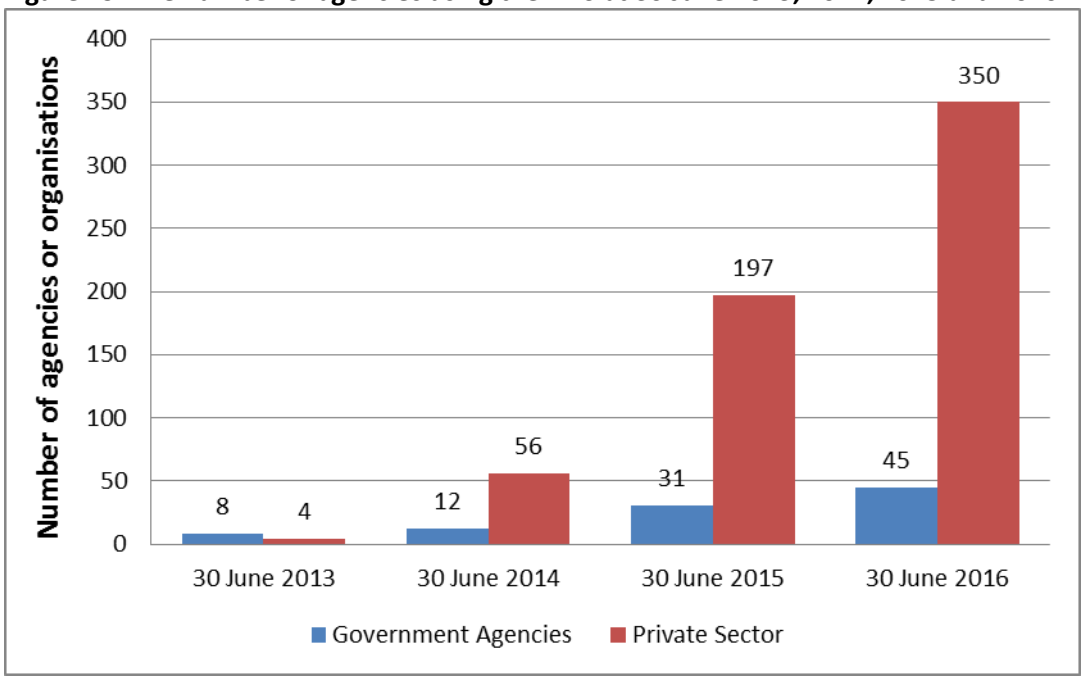
5.2 The number of government agencies using the DVS

Key finding: At 30 June 2016, 45 government agencies were using the DVS, compared to 31 at 30 June 2015. Only one of the eight road authorities and four of the eight RBDMs were using the DVS as of June 2016. While the use of the DVS by government agencies has increased between 2015 and 2016 the rate of uptake is considered small compared to that of the private sector.

5.3 The number of private sector organisations using the DVS

Key findings: The number of organisations in the private sector using the DVS continues to increase with 350 organisations using DVS in 2015-16.

Figure 49: The number of agencies using the DVS at 30 June 2013, 2014, 2015 and 2016

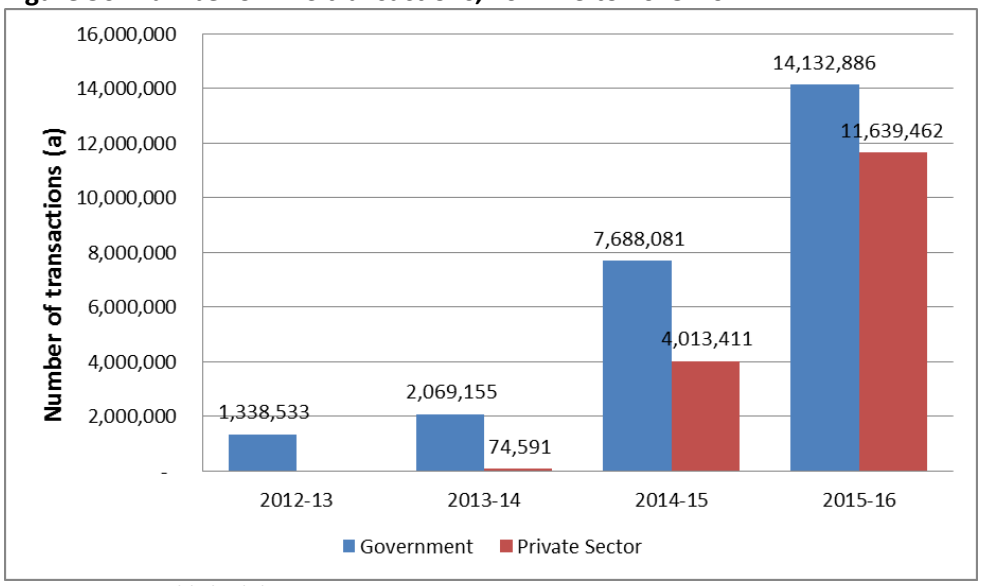


Source: DVS unpublished data.
Note: Private sector access to DVS has only been available since 2014.

5.4 The number of DVS transactions each year

Key findings: Document verifications using the DVS have increased from 11.7m transactions in 2014-15 to 25.8m transactions in 2015-16 - an increase of over 120%. This significant increase can be attributed to the increase in private sector users and larger government agencies becoming users of DVS.

Figure 50: Number of DVS transactions, 2012-13 to 2015-16



Source: DVS unpublished data.
Note (a): These figures include repeat transactions, for example where data entry errors occur. Some validation attempts can involve numerous transactions.

5.5 Online security practices of individuals, businesses and government agencies

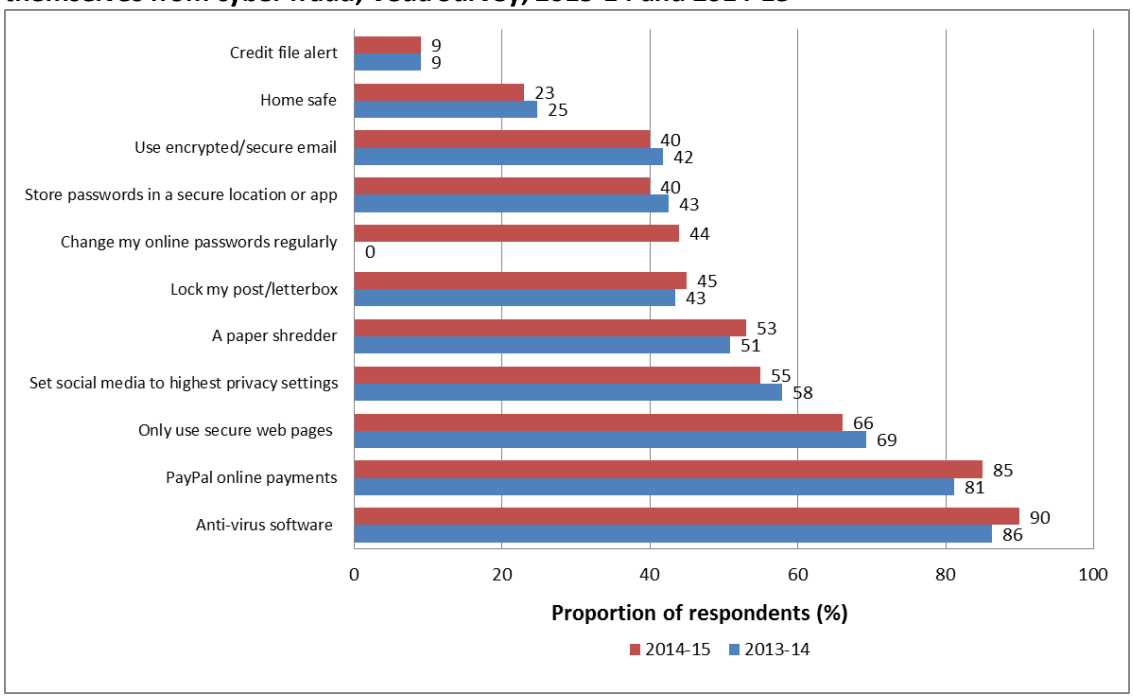
Key Finding: Despite the increased reliance on technology, the percentage of Australians who install or implement IT security measures has remained stable with a decline in the percentage of those who modify their behaviour to protect their identity once misuse has occurred.

Reports from IDCARE have shown that in 2015, 29.5% of initial identity compromise occurred online (principally through phishing) while 79% of further identity misuse occurred online. A range of sources across government and the private sector produce data on Australians' online security practices, providing a rich source of information relating to the use of preventive measures for online identity crime, some of which are outlined below.

5.5(a) Individuals

Society's reliance on information technology and the internet in particular, means that there is a significant market of potential victims for cyber-criminals to target. Veda, a national credit reference organisation, produces reports on insights into consumers' views and concerns about identity theft and other cybercrime. Veda found that while most respondents were concerned about identity theft, not as many were taking proactive measures to protect themselves against it online.

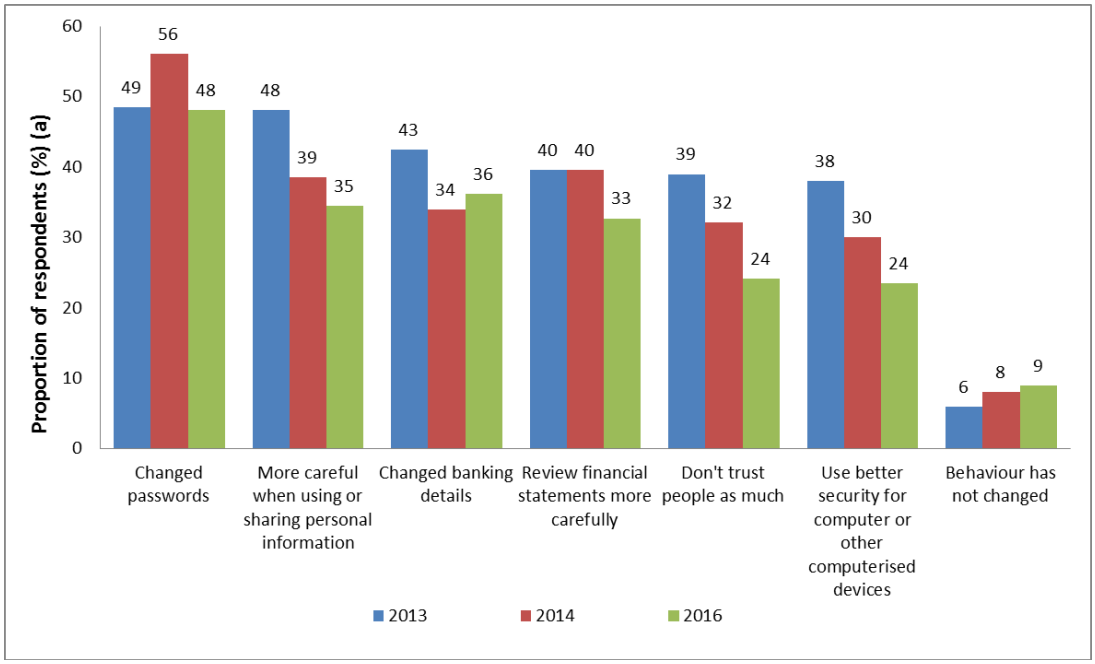
Figure 51: Proportion of respondents whom implemented security measures to protect themselves from cyber fraud, Veda Survey, 2013-14 and 2014-15



Source: Veda 2015.

The AICs Identity crime and misuse surveys have further reported on the ways in which individuals change their behaviour following the misuse of their personal information (Figure 52). The most common behavioural changes involve changing passwords, exercising greater care when reviewing financial statements, and taking greater care when using or sharing personal information.

Figure 52: Proportion of victim's who changed their behaviour following the misuse of personal information, 2013, 2014 and 2016

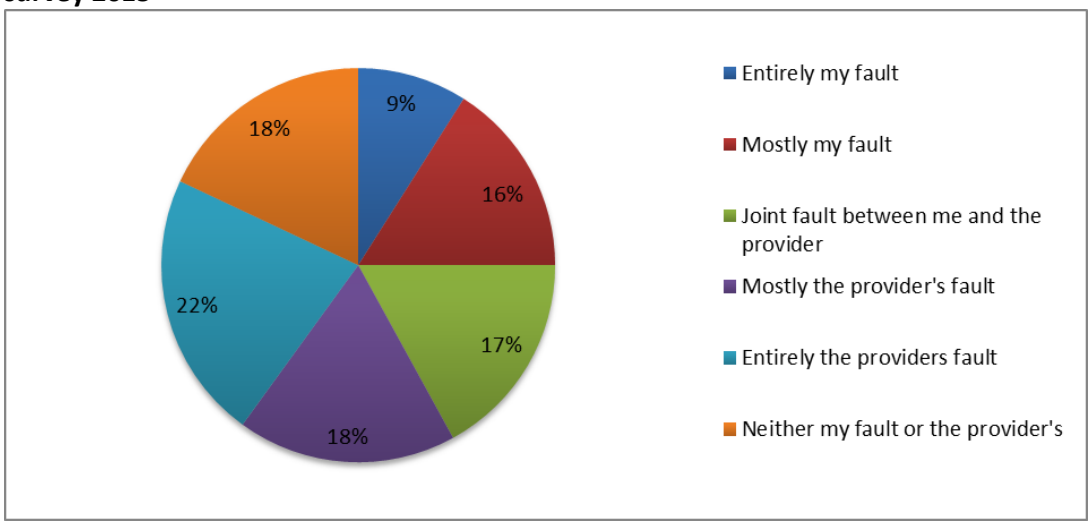


Source: AIC Surveys 2013, 2014 and 2016.
AIC weighted data: 2013 and 2014 data were weighted by location and 2016 data were weighted by age/sex.
Note: Respondents were able to select more than one response for this survey question therefore percentages will not total 100.

5.5(b) Business

A recent study by Telstra (Telstra 2015) on the importance of the security of personal information found less than 50% of respondents were happy with the security methods of their financial institution, with 40% of victims of identity theft blaming the financial institution (Figure 53).

Figure 53: Fault for identity theft according to victims of identity theft according to a Telstra survey 2015



Source: Telstra 2015.

The Computer Emergency Response Team (CERT) Australia is the national organisation that works with major Australian businesses to provide cyber security advice and support for critical infrastructure and other systems of national interest.

In 2015 the CERT Australia responded to 14,401 cyber security incidents affecting Australia businesses, 310 of which involved systems of national interest, critical infrastructure and government.

According to the *2015 Cyber Security Survey: Major Australian Businesses* (ACSC 2015a) 50% of respondents experienced at least one cyber incident in the past year, with 8% of respondents unsure if they had (or had not) experienced a cyber-incident.

All respondents reported using anti-virus software and all but one respondent reported using network-based firewalls. It was also found that 77% of respondents had cyber security incident response plans in place with 37% of respondents regularly reviewing them. Small and medium-sized businesses often do not have the same capacity as larger organisations to deal with cybercrime incidents and may not be reflected in the CERT survey. Accordingly, they are often a relatively easy target for cybercriminals (Verizon 2016).

Case Study 12: GameOver Zeus malware

Gameover Zeus is an advanced type of malware that was designed to steal banking information and other credentials from an infected computer. The malware first appeared in September 2011 and was spread through spam e-mail or phishing messages.

The infected computer (unknown to its owner) would become part of a global network of compromised computers known as a botnet. Once the program had captured banking credentials from infected computers, the credentials were then used to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals.

According to the FBI, the virus infected between 500,000 and a million computers in 12 countries (including Australia) with losses estimated to be more than $100m.

Source: ACSC 2015 Threat Report and https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/

5.5(c) Government agencies

Government agencies have taken positive steps to address the threats posed by cybercrime. The security of government Information and Communications Technology (ICT) systems has been the subject of a number of audits at both the Commonwealth and state levels. The most recent of which was in 2015 when the Australian National Audit Office (ANAO) conducted an audit entitled *Cyber Resilience* (ANAO 2016).

Of the four agencies that were audited, two achieved compliance of the mandatory strategies in the Australian Government Information Security Manual (ISM). The non-compliant agencies had initiatives underway to achieve compliance, but they did not provide a timeframe when compliance would be achieved across their enterprise ICT systems.

6. Estimating the economic impact of identity crime to Australia

Key findings: The annual direct and indirect cost of identity crime in Australia is approximately $2.2b. If the costs associated with preventing and responding to identity crime by government, business and individuals are included ($390m), the estimated total economic impact of identity crime in Australia is approximately $2.6b per year.

6.1 Calculating the cost of identity crime

Cost of crime estimates generally relate to direct and indirect financial effects of crime, while economic impact includes other economic consequences such as preventing and responding to crime by government agencies, business and individuals. Sometimes the terms 'cost' and 'economic impact' are used interchangeably.

The present methodology for estimating the cost of identity crime is consistent with that used in 2013-14. These estimates are derived from the methodology used to calculate the costs of crime in the AIC's *Counting the costs of crime in Australia: A 2011 estimate* (Smith, Jorna, Sweeney & Fuller 2014).

The methodology used to calculate the economic impact of identity crime can be separated into three components as illustrated in Figure 54. Further detail regarding the methodology, and data used in the calculation process, are presented in Appendices H and I.

Figure 54: Components of identity crime costing

Step 1: Calculating the direct cost of identity crime for each fraud category

The direct costs of identity crime for each fraud category were determined using the formula in Figure 55.

Figure 55: Formula for direct costs of identity crime

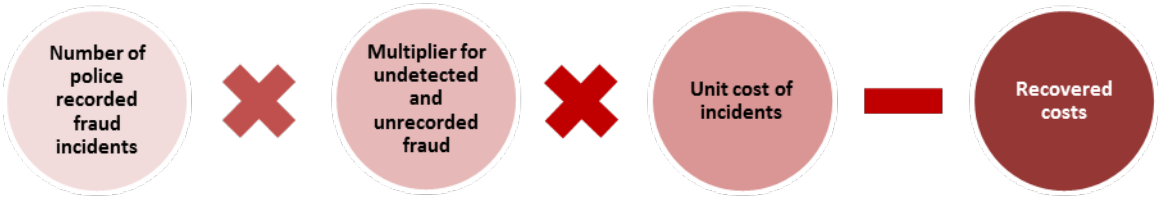


Table 6 below presents the data for each element of this formula. These figures have been rounded to the nearest whole number. Further details regarding the methodology, and data used in the calculation process are contained in Appendices H and I.

Table 6: Data for calculating direct cost of identity crime

Fraud category	Incidents	Multiplier	Cost per incident	Recovered costs	Total direct cost (a)
Commonwealth fraud (b)	155,843	1.15	$2,111	$24,465,519	$353,866,740
Personal fraud	1,641,376	N/A (c)	$400	N/A	$656,550,506
Serious fraud	300	2.2	$1,500,000	N/A	$990,000,000
Police recorded fraud (d)	79,097	4.0	$4,412 per unrecorded fraud; $27,981 per recorded fraud	N/A	$3,260,141,049

Note (a): numbers rounded to the nearest whole number
Note (b): Commonwealth fraud refers to fraud against the Commonwealth
Note (c): Multiplier is inapplicable because incident numbers are derived from a victimisation survey.
Note (d): The number of incidents recorded by police does not include 77 incidents of Commonwealth fraud, 660 incidents of serious fraud and 54,142 incidents of personal fraud that were removed to avoid double counting.

Step 2: Calculating the indirect costs of identity crime for each fraud category

Indirect losses refer to costs such as the time spent by victims dealing with any consequences of the identity crime, as well as emotional costs associated with the victimisation.

In the absence of relevant Australian research on indirect losses, reliance has been placed on the work of Harrell (2015) in the United States[6], who found that 5% of all identity theft victims reported indirect losses as a result of their most recent incident of identity theft. Victims reported a mean indirect loss of US$261 (AU$365) and a median loss of US$30 (AU$42).

For each of the four categories of fraud examined in this report, the median or mean was used, where appropriate, as the value to determine the amount that indirect losses contributed to the cost of each fraud category.

The median was used to calculate the indirect costs attributable to identity crime for fraud against the Commonwealth and personal fraud, due to the fact that smaller amounts of money are usually involved in both these types of fraud. The mean was used in the calculations for serious and police-recorded fraud, owing to the fact that these categories of fraud usually involve larger amounts per incident.

The indirect costs of identity crime for Commonwealth fraud and personal fraud were determined using the formula in Figure 56.

Figure 56: Formula for indirect costs of Commonwealth and personal identity crime

[6] Ideally data from Australia would be used; however this information is not available. It should be noted that the United States has a different identity ecosystem compared to Australia.

The indirect costs of identity crime for serious and police recorded frauds were determined using the formula in Figure 57.

Figure 57: Formula for indirect costs of serious and police recorded identity crime

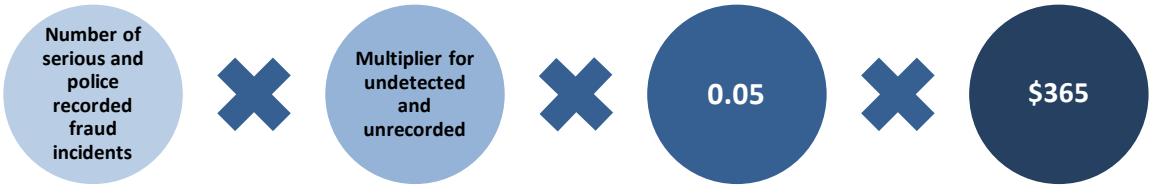


Table 7 presents data for each element of these formulae. These figures have been rounded to the nearest whole number. Further details regarding the methodology, and data used in the calculation process are contained in Appendices F and G.

Table 7: Data for calculating indirect cost of identity crime

Fraud category	Incidents (after multiplier applied)	# incidents considering only 5% had indirect loss	Total indirect cost
Commonwealth fraud	179,219	8,961	$376,362
Personal fraud	1,641,376	82,069	$3,446,890
Serious fraud	660	33	$12,045
Police recorded fraud	316,388	15,819	$5,774,081

Note (a): Numbers rounded to nearest whole number

Step 3: Calculating total identity crime cost for each fraud category

The total identity crime costs for each fraud category were determined using the formula in Figure 58 below.

Figure 58: Formula for calculating the total cost of identity crime

Table 8 below presents the data for each element of this formula. The estimated cost of identity crime in Australia was approximately $2b for 2013-14. Further details regarding the methodology, and data used in the calculation process are contained in Appendices E and F.

Table 8: Data for calculating total cost of identity crime

Fraud category	Direct cost	Indirect cost	% Identity Crime	Identity Crime Cost
Commonwealth fraud	$353,866,740	$376,362	25.1	$88,915,019
Personal fraud	$656,550,506	$3,446,890	100	$659,997,396
Serious fraud	$990,000,000	$12,045	15	$148,501,807
Police recorded fraud	$3,260,141,049	$4,505,195	40	$1,306,366,052
TOTAL				**$2,203,780,274**

Calculating the costs of responding to and preventing identity crime

The estimated costs associated with preventing and responding to identity crime by government, business and individuals were determined by estimating the percentage of their annual recurrent expenditure attributable to crime-related functions and activities, and then estimating the percentage of their crime-related costs that can be attributed to identity crime and misuse.

An attempt was made to assess costs for as many Commonwealth and state and territory agencies as possible. The agencies considered, and the costing details of the percentage of identity-related crime costs incurred by the agencies and organisations, are presented in Appendix H and I.

The total estimated cost of prevention and response activities was approximately $390 million.

Total estimated cost of identity crime

Finally, the total economic impact of identity crime on the economy in Australia was calculated in accordance with the formula in Figure 59. This includes direct and indirect costs as well as the costs of prevention and response activities.

Figure 59: Formula for calculating the total economic impact of identity crime

The total cost of identity crime as a proportion of the different categories of fraud outlined above is estimated to be approximately $2.2b. These figures include direct and indirect costs, but do not include prevention and response costs. If the estimated cost of preventing identity crime of $390m is added to this total, it is estimated that the economic impact of identity crime in Australia would be approximately $2.6b.

Comparison with previous years' estimates

The overall annual economic impact of identity crime and misuse has increased from $2b to $2.2b. In addition, the individual components of the calculation have changed considerably.

The cost of Commonwealth Fraud has increased from $28.5m in 2012-13 to $89m in 2014-15. This increase is due to both an increase in the number of fraud incidents that fall into the category of misuse in identity from 12.5% to 25.1% of overall frauds and a large increase in the average cost of each incident from $1,526 to $2,111 per incident.

The cost for personal fraud has increased from $435m to $660m. This increase is due to an increase of victimisation from 7.7% used in the 2013-14 report to 8.5% used in this report. In particular there was an increase in the victimisation rate between the 2010-11 ABS Personal Fraud Survey (6.7%) and 2014-15 ABS Personal Fraud Survey (8.5%).

The cost of serious fraud remains largely the same as the previous report. The data used in this calculation are the same as in the previous reports, so is consistent with previous year's calculations. Noting the slight decrease in overall serious fraud value is due to the decrease in associated indirect costs.

The cost of police recorded fraud decreased from $1.4b to $1.3b. There are a greater number of reports being made to police 133,921 in 2014-15 compared to 126,457 in 2013-14. The overall value of police recorded fraud has decreased as more personal fraud is being detected and the value of which is removed from this estimate to avoid double counting.

Conclusions

As highlighted in this report, identity crime continues to be one of the most prevalent crimes in Australia. To respond effectively to identity crime, governments need evidence-based policies and programs.

This and previous reports seek to add to this evidence-base by presenting a comprehensive range of quantitative and qualitative information on the nature and extent of identity crime and misuse. A substantial number of government agencies provided valuable data for inclusion in this report. This is to be commended, as it is only through the sharing of information and analysis that the extent of identity crime in Australia can be better understood. Surveys conducted by agencies such as the AIC and ABS provide critical information of the widespread nature of identity crime.

This 2016 report also contains new insights into the experience of victims through input from IDCARE. This unique perspective allows greater understanding of both the financial and emotional impacts of identity crimes on victims, which provides for the development of better policy decisions and more effective use of resources to combat the problem.

Addressing the concerns and challenges raised in this report requires a collaborative and sustained effort by government agencies and private sector organisations continuing to work together to develop more effective policy and operational responses to minimise the harm of identity crimes to the Australian community.

This report emphasises the importance of both comprehensive and accurate data to understand the real impacts (both financial and non-financial) of identity crime. Findings of the report also suggest a need to raise awareness in the Australian community about the importance of reporting incidents of identity misuse. This can be achieved through greater support from government agencies and private sector organisations. In addition, the report highlights the need for further investigation about the needs of those individuals impacted by identity crime.

While it is clear that identity crime has significant widespread impacts, a lack of comprehensive data makes it difficult to fully quantify the extent of identity crime and associated costs. As a result, identity crime is likely to be both underreported and its impacts underestimated.

References

All URLs are current at 1 October 2016.

Australian Cyber Security Centre (ASCS) 2015a. *2015 ASCS Cyber Security Survey: Major Australian Businesses.* Canberra. https://www.cert.gov.au/system/files/614/691/2015-ACSC-Cyber-Security-Survey-Major-Australian-Businesses.pdf

Australian Cyber Security Centre (ASCS) 2015b. *The Australian Cyber Security Centre Threat Report 2015. Canberra*. :https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf

Association of Certified Fraud Examiners (ACFE) 2016. *Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study.* http://www.acfe.com/rttn2016.aspx

Attorney-General's Department 2016a. *Cyber Emergency Response Team (CERT) website*. Canberra: http://www.ag.gov.au/RightsAndProtections/CERT/Pages/default.aspx

Attorney-General's Department 2016b. *Document Verification Service website*. Canberra: http://www.dvs.gov.au/Pages/default.aspx

Attorney-General's Department 2016c. *Protective Security Policy Framework website*. Canberra: http://www.protectivesecurity.gov.au/Pages/default.aspx

Attorney-General's Department 2016d. *Victims of Commonwealth Identity Crime*. Canberra: http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/VictimsofCommonwealthidentitycrime.aspx

Attorney-General's Department 2015. *Identity crime and misuse in Australia 2013-14*. Canberra: https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-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: http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Trends-in-Identity-Crime.aspx

Attorney-General's Department 2012b. *National Identity Security Strategy 2012,* Canberra: http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/National%20Identity%20Security%20Strategy%202012.PDF

Australian Bureau of Statistics 2016a. *Personal Fraud, 2014-2015*, ABS Cat. No. 4528.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4530.0~2012-13~Main%20Features~Victims%20of%20personal%20crime~4 (ABS 2016a)

Australian Bureau of Statistics 2016b. *Crime Victimisation, Australia, 2014-15,* ABS Cat No.4530.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0 (ABS 2016b)

Australian Bureau of Statistics 2016c. *Criminal Courts, Australia, 2014-15,* ABS Cat No.4513.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/mf/4513.0 (ABS 2016c)

Australian Bureau of Statistics 2015. *Australian Demographic Statistics, June 2015*, ABS Cat. No. 3101.0, Canberra: http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/6CBA90A25BAC951DCA257F7F001CC559?opendocument

Australian Bureau of Statistics 2012. *Personal Fraud, 2010-2011*, ABS Cat. No. 4528.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/4530.0~2012-13~Main%20Features~Victims%20of%20personal%20crime~4

Australian Bureau of Statistics 2011. *Australian and New Zealand Standard Offence Classification (ANZSOC), 2011*, ABS Cat. No. 1234.0, Canberra: http://www.abs.gov.au/AUSSTATS/abs@.nsf/ProductsbyCatalogue/E6838CDEE01D34CBCA25722E0017B26B

Australian Bureau of Statistics 2008. *Personal Fraud, 2007*, ABS Cat. No. 4528.0, Canberra: http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/226E9A7C56865433CA2579E40012097D?opendocument

Australian Communications and Media Authority (ACMA) 2011. *Digital Australians—Expectations about media content in a converging media environment.* http://www.acma.gov.au/~/media/Research%20and%20Reporting/Information/pdf/Digital%20Australians%20Expectations%20about%20media%20content%20in%20a%20converging%20media%20environment.PDF

Australian Competition and Consumer Commission (ACCC) 2016. *Targeting Scams – Report of the ACCC on scams activity 2015*. Canberra: https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scam%20activity%202015.pdf

Australian Competition and Consumer Commission (ACCC) 2015. *Targeting Scams – Snapshot 2014*. Canberra: http://www.accc.gov.au/system/files/Targeting-scams-2014-infographic.pdf

Australian Crime Commission 2015. *Organised Crime in Australia 2015*, Canberra: https://crimecommission.gov.au/sites/default/files/FINAL-ACC-OCA2015-180515.pdf

Australian Cybercrime Online Reporting Network (ACORN) 2016. *Australian Cybercrime Online Reporting Network website.* http://www.acorn.gov.au/

Australian Federal Police (AFP) 2014. *Platypus Magazine*. Jan-June 2014. https://www.afp.gov.au/sites/default/files/PDF/Platypus/platypus115.pdf

Australian National Audit Office (ANAO) 2016. *Cyber Resilience Across Entities.* https://www.anao.gov.au/sites/g/files/net1336/f/ANAO_Report_2015-2016_37.pdf

Australian National Audit Office (ANAO) 2014. *Cyber Attack: Securing Agencies' ICT Systems*. Audit Report No. 50 - 2013-14. Canberra: https://www.anao.gov.au/sites/g/files/net1336/f/AuditReport_2013-2014_50.pdf

Australian Payments Clearing Association (APCA) 2016. *Australian Payments Fraud Details and Data*. http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf

Australian Payments Clearing Association (APCA) 2015. *Payment Fraud Statistics – Summary of Results* http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2015.pdf

Australian Signals Directorate (ASD) 2016. *2016 Australian Government Information Security Manual – Controls.* Canberra: http://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf

Australian Taxation Office (ATO) 2015. *Annual Report 2014-15*. Canberra: https://annualreport.ato.gov.au/sites/g/files/net376/f/AR_14-15_Vol1_n0995_js34758_w.pdf

Australian Taxation Office (ATO) 2009-2014. *Annual Reports*. Canberra: https://www.ato.gov.au/About-ATO/Access,-accountability-and-reporting/Reporting-to-parliament/Annual-report/

Bricknell, S and Smith, R. G., 2013, *Developing a monitoring framework for identity crime and misuse,* (AIC Report) Australian Institute of Criminology, Canberra.

Centre for the Protection of National Infrastructure 2013. *CPNI Insider Data Collection Study – Report of Main Findings*, United Kingdom. https://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider_data_collection_study.pdf

Commonwealth Director of Public Prosecutions 2015. *Annual Report 2014/15*. Canberra: https://www.cdpp.gov.au/2014-15-annual-report-html-0

Credit Industry Fraud Avoidance Service (CIFAS) 2015. *Fraudscape UK fraud trends*, United Kingdom, http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20-%20Fraudscape%20main%20report%20for%20website.pdf

Cross C, Smith RG & Richards K 2014. Challenges of responding to online fraud victimisation in Australia. *Trends & Issues in Crime and Criminal Justice*, no.474. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/461-480/tandi474.html

Department of Foreign Affairs and Trade (DFAT) 2015. *Annual Report 2014-2015.* Canberra: http://dfat.gov.au/about-us/publications/corporate/annual-reports/annual-report-2014-2015/dfat-annual-report-2014-15.pdf

Department of Foreign Affairs and Trade (DFAT) 2011-2014. *Annual Reports.* Canberra: http://dfat.gov.au/about-us/publications/corporate/annual-reports/pages/annual-reports.aspx

Department of Human Services (DHS) 2015. *Annual Report 2014-15*, Canberra: https://www.humanservices.gov.au/corporate/annual-reports/annual-report-2014-15

Department of Human Services (DHS) 2008-2014. *Annual Reports*, Canberra: http://www.humanservices.gov.au/corporate/publications-and-resources/annual-report/

Department of Police and Emergency Management (DPEM) 2015. 2014-2015 *Crime Statistics Supplement*. http://www.police.tas.gov.au/about-us/corporate-documents/crime-statistics-supplement/

Harrell E 2015. *Victims of Identity Theft, 2014*. Bureau of Justice Statistics, Office of Justice Programs, US Department of Justice. http://www.bjs.gov/content/pub/pdf/vit14.pdf

IDCARE 2016a. *Australia Observations of Identity Compromise and Misuse 2015*.

IDCARE 2016b. *Australian Compromised Credentials Study Final Report 2016*.

IDCARE 2016c. *Submission to the Serious Data Breach Notification*.

IDCARE 2014. *IDCARE Quarterly Report 1 October 2014 - 31 December 2014*.

IDCARE 2014a. *Submission to Parliamentary Joint Committee on Law Enforcement's Inquiry into Financial Related Crime*.

Inspector-General of Taxation 2013. Review into the Australian Taxation Office's compliance approach to individual taxpayers – income tax refund integrity program, http://igt.gov.au/files/2014/11/income-tax-refund-integrity-program.pdf

Jorna P & Smith RG 2015. *Fraud against the Commonwealth Report to Government 2010-11 to 2012-13*. Monitoring Reports 24, Australian Institute of Criminology: Canberra.

KPMG 2013. *A survey of fraud, bribery and corruption in Australia and New Zealand 2012*. http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/fraud-bribery-corruption-survey-2012.aspx

Lindley J, Jorna P & Smith RG 2010. *Fraud against the Commonwealth 2009-10 Annual Report to Government.* AIC Monitoring Reports 18, Australian Institute of Criminology: Canberra. http://www.aic.gov.au/media_library/publications/mr/18/mr18.pdf

Mayhew P 2003. Counting the Costs of Crime in Australia: Technical Report. *Australian Institute of Criminology Technical and Background Paper Series*, no. 4. Canberra: Australian Institute of Criminology.

Macdonald W, Fitzgerald J, 2014. *Understanding fraud: The nature of fraud offences recorded by NSW Police*. NSW Bureau of Crime Statistics and Research (BOSCAR). http://www.bocsar.nsw.gov.au/Documents/CJB/cjb180.pdf

Northern Territory Police, Fire and Emergency Services 2015. *Annual Report 2014-15.* Darwin: http://www.pfes.nt.gov.au/Publications-and-forms.aspx

NSW Bureau of Crime Statistics and Research (BOCSAR) 2015. NSW Recorded Crime Statistics 2015. http://www.bocsar.nsw.gov.au/Documents/RCS-Quarterly/NSW_Recorded_Crime_June_2015.pdf

Office of the Australian Information Commissioner 2015. *OAIC Annual Report – 2014-15*, Canberra: https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201415/

Office of the Australian Information Commissioner 2010-2014. *OAIC Annual Reports*, Canberra: https://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/

Office of the Australian Information Commissioner (OAIC) 2013. *Community attitudes to privacy survey: Research report 2013*. Canberra: http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013#_Toc368300726

Ponemon Institute 2016. *2016 Cost of Data Breach Study: Australia,* http://www-03.ibm.com/security/au/data-breach/index.html

Ponemon Institute 2013. 2012 Cost of Data Breach Study: Global Analysis. http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

Ponemon Institute 2012. 2011 Cost of Data Breach Study: Australia. http://www.ponemon.org/library/2011-cost-of-data-breach-australia

PricewaterhouseCoopers (PWC) 2014. *Global Economic Crime Survey: The Australian Story*. file://aicfs/downloads/catherine.emami/Downloads/global-economic-crime-survey-2014%20(3).pdf

Reserve Bank of Australia (RBA) 2015, *Inflation Calculator*, http://www.rba.gov.au/calculator/annualDecimal.html

Rollings K 2008. Counting the Costs of Crime in Australia: A 2005 update. *Research and Policy Series*, no.91. Canberra: Australian Institute of Criminology.

Smith RG & Jorna P forthcoming 2016. *Fraud against the Commonwealth Report to Government 2014. Statistical Report No 1*. Australian Institute of Criminology: Canberra

Smith RG & Jorna P forthcoming 2017a. *Identity crime and misuse in Australia: Results of the 2016 online survey*. Australian Institute of Criminology: Canberra.

Smith RG & Jorna P forthcoming 2017b. *Fraud against the Commonwealth Report to Government 2015*. Australian Institute of Criminology: Canberra

Smith RG, Brown R, & Harris-Hogan S 2015. *Identity crime and misuse in Australia: Results of the 2014 online survey*. Australian Institute of Criminology: Canberra. http://www.aic.gov.au/publications/current%20series/rpp/121-140/rpp130.html

Smith R G & Hutchings A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey*. Research & Public Policy Series, Australian Institute of Criminology: Canberra. http://www.aic.gov.au/media_library/publications/rpp/128/rpp128.pdf

Smith RG, Jorna P, Sweeney J & Fuller G 2014. *Counting the costs of crime in Australia – A 2011 estimate*. Research and Public Policy Series, Australian Institute of Criminology: Canberra.

South Australia Police 2015a. *Annual Report 2014-15.* Adelaide https://www.police.sa.gov.au/__data/assets/pdf_file/0005/244517/SAPOL-annual-report-2014-2015.pdf

South Australia Police 2015b. *General Offence Descriptions.*

https://www.police.sa.gov.au/__data/assets/pdf_file/0007/39688/Crime-stats-criminal_offence_descriptions.pdf

Tasmanian Department of Police and Emergency Management (DPEM) 2015. *2014-15 Crime Statistics Supplement.* http://www.police.tas.gov.au.s3.amazonaws.com/wp-content/uploads/2013/10/2014-15-Crime-Statistics-Supplement.pdf

Telstra 2015. Mobile Identity: The Fusion of Financial Services, Mobility and Identity. https://www.telstraglobal.com/images/mobile-identity/mobile-identity-whitepaper.pdf

Veda 2015. *2015 Cybercrime and Fraud Report*. https://www.veda.com.au/insights/cybercrime-and-fraud-report

Verizon 2016. 2016 *Data Breach Investigations Report*. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

WA Police 2015. *Western Australia Police Service Monthly Verified 2014-15 Crime Statistics*. https://www.police.wa.gov.au/~/media/Files/Police/Crime/Monthly-crime-figures/Internet-Web-201415-All.pdf?la=en

Appendix A – Measurement framework indicators

Table A1 –Measurement indicators of identity crime and misuse and data sources		
Indicators	**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.	Data from law enforcement, government agencies and IDCARE on the cost to illicitly acquire the most common identity credentials such as: • driver licences • Australian passport • Medicare card • birth certificate.
1.2 The number of reported data breaches	Acts as a proxy measure of organisational cyber security arrangements for protecting personal information.	Privacy (information) Commissioners. IDCARE
1.3 The source of the data breach	Gives an idea how criminals are gaining access to personal information.	ACORN ABS IDCARE
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 (i.e. real) identities in connection with financial, taxation, immigration and identity fraud.		
2.1 The 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 governments administrative and law enforcement datasets.	AFP ATO DFAT DHS (Centrelink) DIBP ACCC Births, Death & Marriages Consumer Affairs / Protection Police (state & territory) Privacy Commissioners Road & Traffic Authorities
2.2 The number of prosecutions involving 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	AIC survey ABS surveys AGD surveys

Table A1 –Measurement indicators of identity crime and misuse and data sources		
Indicators	**Description**	**Data source**
	consumer surveys.	
2.4 Number of people who perceive identity crime and misuse as a problem	Estimate the number and proportion of people who perceive identity crime and misuse as a problem based on data collected from attitudinal surveys.	ABS AGD AIC survey IDCARE
2.4 The types of personal information most susceptible to identity theft or misuse	Estimates the types of personal information and identity credentials that may be more vulnerable to theft or misuse, based on data collected from attitudinal surveys.	ABS AGD AIC survey
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 DHS DIBP ACCC Births, Death & Marriages Consumer Affairs / Protection 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.	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 AGD AIC survey IDCARE
3.4 Number of identity crime victims experiencing non-financial consequences	Seeks to quantify the non-monetary harm caused by identity crime victimisation.	AIC survey Academic literature IDCARE
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 (i.e. recovering their identity)	Estimates the time victims (broadly individual, business and government victims)	ACCC ABS AGD

Table A1 –Measurement indicators of identity crime and misuse and data sources		
Indicators	**Description**	**Data source**
	spend trying to resolve the issue of having their identity stolen or misused.	AIC survey IDCARE Police (state & territory) Consumer Affairs / Protection
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 State Consumer Affairs agencies
4.3 Number of applications for Victims' Certificates (issued by the courts)	Assesses the application rate for Victims' Certificates in each applicable Australian jurisdiction.	AGD AIC survey
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 (DVS), 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	AGD (DVS)
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	AGD (DVS)
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	AGD (DVS)
5.4 Number of DVS transactions each year	The number of validation transactions through the DVS each year	AGD (DVS)
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.	AGD (CERT) ASD ANAO ACMA Veda

Appendix B – Definition of key terms

Card Not Present Fraud: *the use of account information (including pseudo account information without the physical card being involved) via the phone, mail, internet etc. without the authority of the cardholder. This also includes fraud where a card should normally be present (eg in a retail transaction) but a merchant has chosen to accept the transaction based on a card number only and it turns out to be a fraudulent transaction. http://www.apca.com.au/payment-statistics/fraud-statistics/2014-calendar-year?SchemeCredit,DebitandChargeCardFraud*

Cyber Security 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 that resulted in confirmed disclosure of information to an unauthorised party*

External fraud incidents: *Any incident of suspected fraud allegedly committed against an entity by a person other than an employee (including contracted employees) of the entity.*

Forgery: *the act of producing a false document with the intention of using it to dishonestly induce 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 Division 135 of the *Criminal Code Act 1995* Cth; Commonwealth Fraud Control Framework 2014)

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 crime.*
(2007 Intergovernmental agreement to a National Identity Security Strategy; 2)

Identity fabrication: *the creation of a fictitious identity.*
(Adapted from Australian 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; Australian 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) 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.

(*Criminal Code Act 1995* Cth, Part 9.5, Division 301.1)

Identity manipulation: *altering one or more elements of identity (e.g. 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, S, 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 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, whether the person is living or deceased.* (Australian 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 money or otherwise obtain a financial benefit by deceptive means.* (ABS 2016a)

Appendix C - Methodology

Australian Institute of Criminology (AIC) Identity Crime Survey

The AIC developed a community survey of individual's experiences of identity crime and misuse, for both the preceding 12 months and over their lifetime. Three online questionaries were conducted comprising 23 main questions.

Table C1: AIC Identity Crime Surveys conducted, year and number of respondents

Year	Analysed Responses	Sample Quota	Weighting	Reference
September 2013	4,995	Survey distributed based on age (15 and over) and gender	Based on national state and territory place of residence	Smith & Hutchings 2014
May 2014	5,000	Survey distributed based on age (15 and over) and gender	Based on national state and territory place of residence	Smith, Brown & Harris-Hogan 2015
May 2016	9,956	Larger sample used, with no sample quotas (included respondents aged 15-94 years)	Based on age and gender.	Smith & Jorna forthcoming 2017

Source: AIC Surveys 2013, 2014 and 2016.

In 2016, unlike previous years, a larger sample size was used so state and territory quotas were not employed. Instead the final results were weighted to reflect the distribution of the Australian population in terms of age and gender (either male or female only) based on census data from the Australian Bureau of Statistics. The results of these surveys are not statistically representative of the entire Australian population, but only a reflection of the experiences of those surveyed.

Australian Bureau of Statistics (ABS) 2014-15 Personal Fraud Survey

In 2014-15 the ABS conducted a survey of 27,341 Australian households[7] 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 a member aged 15 years and over from each household.

The Personal Fraud Survey collected information from individuals about their experience of selected personal fraud in the 12 months prior to interview (except for identity theft where persons were asked if they had ever been a victim of identity theft and then data were collected about experiences in the five years and 12 months prior to interview), and whether they incurred any financial loss.

[7] These 27,341 represent those who fully responded to the survey

IDCARE observations of identity compromise and misuse

IDCARE is a non-profit organisation, supported by the Australian Government, which provides free support services to victims of identity theft to help with repairing the damage to their reputation, credit history and identity.

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

(1) From individual clients that access their National Case Management Centre via either hotline, web-form, or email;
(2) From organisational partners that work with IDCARE to respond to detected data breaches;
(3) From independent testing by IDCARE of organisational response measures from non-partners that gather critical insights on what individuals may experience when having to respond to the compromise of their identifying information; and
(4) From IDCARE's National Identity Lab that proactively monitors illicit marketplaces online that buy and sell compromised identifying information.

Commonwealth and state/territory agency input

Data was provided by 51 agencies including:

Commonwealth agencies

- Australian Bureau of Statistics
- Australian Competition and Consumer Commission (Scamwatch)
- Australian Federal Police
- Australian Institute of Criminology
- Australian Securities and Investments Commission
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Department of Foreign Affairs and Trade
- Department of Human Services
- Department of Immigration and Border Protection
- Office of the Australian Information Commissioner

State and Territory agencies

- Police agencies
- Registries of Births, Deaths and Marriages (RBDMs)
- Roads and traffic authorities (RTAs)

The data provided in the report gives an indication of the breadth of identity crime experienced by government agencies.

Appendix D – Government agencies involved in this report

Table D1 - Australian Government agencies involved in the Identity crime and misuse in Australia Report 2014-15
Attorney-General's Department
Australian Bureau of Statistics
Australian Competition and Consumer Commission
Australian Crime Commission
Australian Federal Police
Australian Institute of Criminology
Australian Securities and Investments Commission
Australian Taxation Office
Australian Transaction Reports and Analysis Centre (AUSTRAC)
Commonwealth Director of Public Prosecutions
CrimTrac
Department of Defence
Department of Foreign Affairs and Trade - Australian Passport Office
Department of Human Services
Department of Immigration and Border Protection
Department of Industry, Innovation, Science, Research and Tertiary Education
Department of Infrastructure and Regional Development
Office of the Australian Information Commissioner

Table D2 - State/territory government agencies involved in the Identity crime and misuse in Australia Report 2014-15	
NSW	NSW Police Force NSW Registry of Births, Deaths and Marriages NSW Fair Trading
VIC	Victoria Police Births, Deaths and Marriages Victoria Roads Corporation Victoria – VicRoads Consumer Affairs Victoria
QLD	Queensland Police Service Registry of Births, Deaths and Marriages (Department of Justice and Attorney-General) Office of Fair Trading Department of Transport and Main Roads
SA	South Australia Police Births, Deaths and Marriages Registration Office
WA	Western Australia Police Registry of Births, Deaths and Marriages Department of Commerce – Consumer Protection Department of Transport
ACT	ACT Policing ACT Registry of Births, Deaths & Marriages Office of Regulatory Services
Tas	Tasmania Police Tasmanian Births, Deaths and Marriages Department of Justice
NT	Northern Territory Police Force Northern Territory Registry of Births, Deaths and Marriages Department of Transport

Appendix E – Registries of Birth, Deaths and Marriages data

Table E1: Crime and misuse associated with certificates issued by RBDMs in 2014-15

RBDM Name	Lost	Lost/Stolen	Unauthorised change	Fraudulent	Referred to police
NSW RBDM					
Birth Certificate	2	4	20	8	2
Death Certificate	0	0	0	0	0
Marriage Certificate	0	0	0	0	2
Change of name	0	0	0	1	1
Vic RBDM					
Birth Certificate	8332	159	0	0	0
Death Certificate	219	7	0	0	0
Marriage Certificate	1071	26	0	0	0
Change of name	10	0	0	0	0
Qld RBDM					
Birth Certificate	NA	NA	0	0	0
Death Certificate	NA	NA	0	0	0
Marriage Certificate	NA	NA	0	0	0
Change of name	NA	NA	0	0	0
WA RBDM					
Birth Certificate	NA	NA	1	0	1
Death Certificate	NA	NA	0	3	0
Marriage Certificate	NA	NA	0	0	0
Change of name	NA	NA	0	0	0
SA RBDM					
Birth Certificate	0	0	0	1	NA
Death Certificate	NA	NA	NA	NA	NA
Marriage Certificate	NA	NA	NA	NA	NA
Change of name	NA	NA	NA	NA	NA
TAS RBDM					
Birth Certificate	NA	NA	0	1	0
Death Certificate	NA	NA	0	0	0
Marriage Certificate	NA	NA	0	0	0
Change of name	NA	NA	0	0	0
NT RBDM					
Birth Certificate	2	0	0	2	0
Death Certificate	0	0	0	0	0
Marriage Certificate	0	0	0	0	0
Change of name	0	0	0	0	15

Source: Unpublished data from NSW, Victoria, Queensland, WA, SA, Tasmania and NT RBDMs.

Appendix F – Police data

Requests were sent to all state and territory police agencies to obtain data on the number of recorded identity crime incidents and related offences (eg fraud, forgery and impersonation).

Australian Federal Police

The Australian Federal Police (AFP) recorded 17 incidents involving identity crime in 2014-15. Of these:

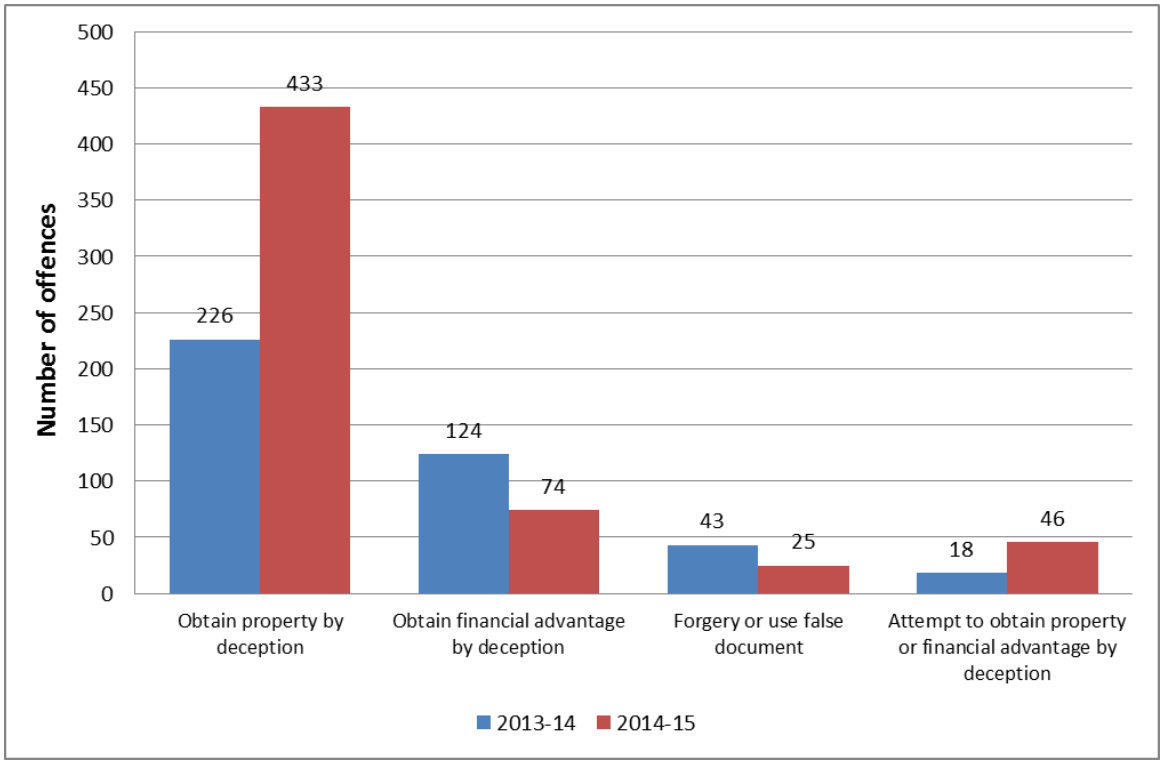
- 2 incidents related to fraud offences;
- 11 incidents explicitly related to identity crime;
- 1 incident related to a federal parolee
- 1 related to a domestic law enforcement agency request;
- 1 related to drug trafficking , and
- 1 related to domestic terrorism.

These 17 incidents do not represent all the offences investigated by the AFP during 2014-15 which might have involved identity crime. It is not mandatory to record that a crime contains an element of identity crime, and accordingly, it is likely that there were additional cases involving identity crime which were not identified as such.

Australian Capital Territory

The ACT does not have legislation specifically relating to identity crime, so police may record offences under more general deception and dishonesty offences. It is therefore difficult to compare the ACT's data with other jurisdictions. The total number of fraud offences in the ACT in 2014-15 was 728. Of the offences committed, obtaining property by deception and obtaining financial advantage by deception were the most common (Figure F1).

Figure F1: Number of identity-related fraud offences in the ACT, 2013-14 and 2014-15



Source: ACT Policing, unpublished data.

Western Australia

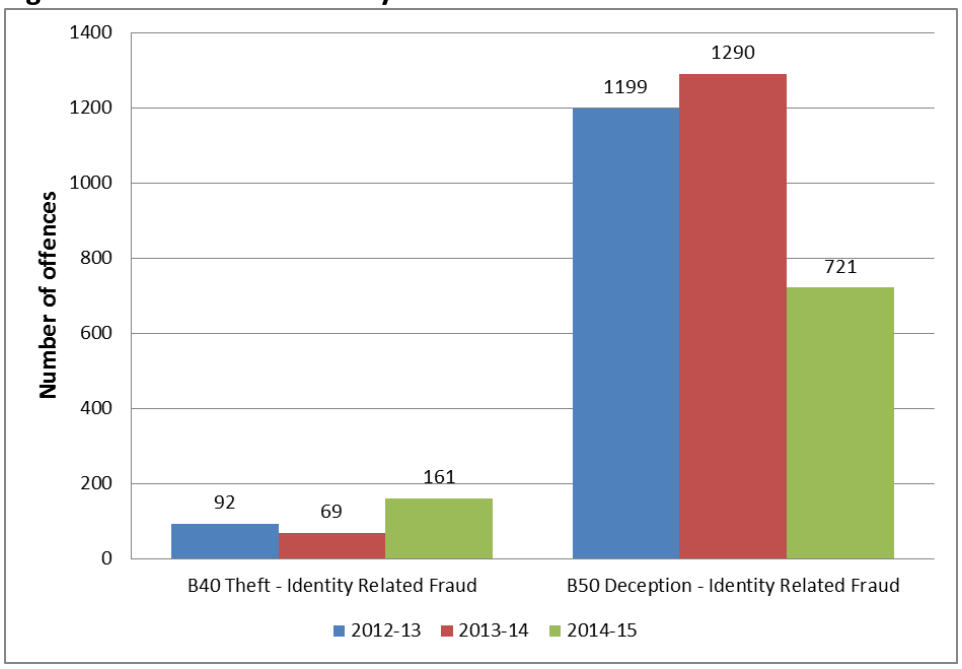
There were 340 identity crime investigations carried out by Western Australia Police (WAPOL) in 2014-15, up from 197 in the year 2013-14. WAPOL estimated that victims lost a total of $1,361,098, or approximately $4,003 per offence. Each identity crime investigation took approximately 23 days to complete.

WA also publishes information on fraud offences which provide a useful comparison with other jurisdictions. (There were 19,253 reported cases of fraud in 2014-15, a decrease from 22,737 offences in 2013-14. (WA Police 2015)

Victoria

There were a total of 35,243 fraud incidents recorded by Victorian Police in 2014-15, of which 882 were identity related. These can be characterised as either as B40 theft and B50 deception offences (Figure 67).

Figure F2: Number of identity-related fraud offences in Victoria

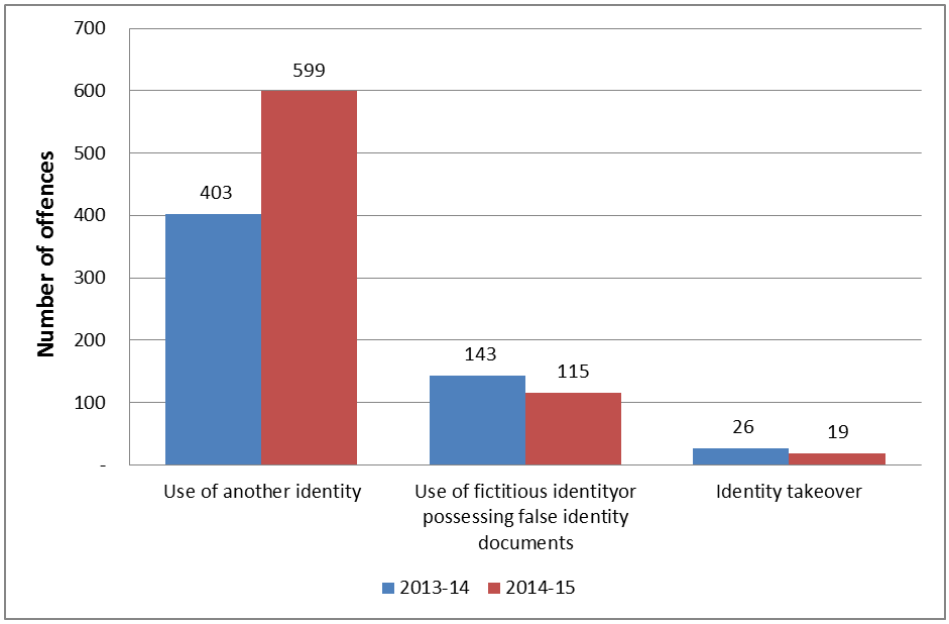


Source: Crime Statistics Agency 2015, unpublished.

Queensland

In total during 2014-15 there were 23,382 recorded fraud offences in Queensland. Of these there were a total of 733 identity-related offences recorded, up from 572 in the year 2013-14 (Figure F3). These offences related to possessing false identity documents, use of another identity, use of a fictitious identity, and identity takeover.

Figure F3: Number of identity related fraud offences recorded by the Queensland Police Service, 2013-14 and 2014-15

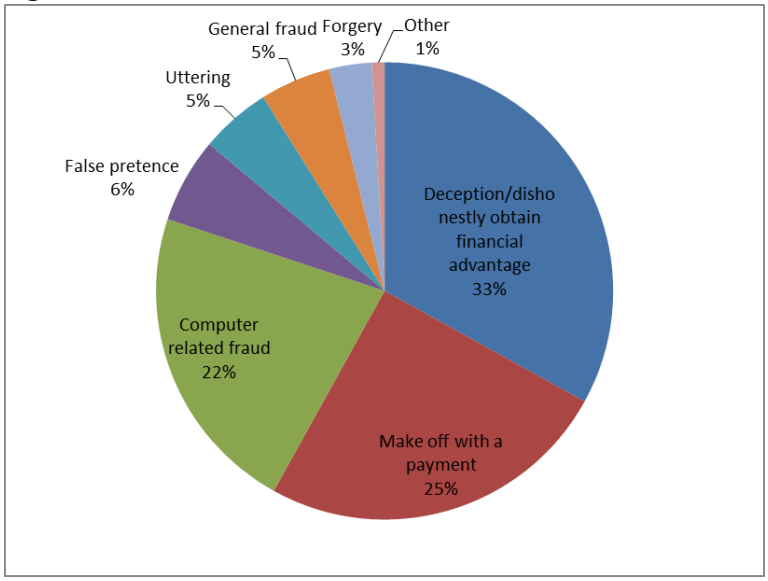


Source: Queensland Police, unpublished data.

Tasmania

Tasmania police do not capture specific data on identity crime. However they do publish information on fraud and similar offenses (DPEM 2015). There were 646 Fraud and Similar Offences recorded in 2014-15, an increase from the 533 offences in 2013-14. The distribution for Fraud and Similar Offences in 2014-15 is detailed in Figure F4.

Figure F4: Distribution of all fraud and similar offences in Tasmania during 2014-15



Source: DPEM 2015.

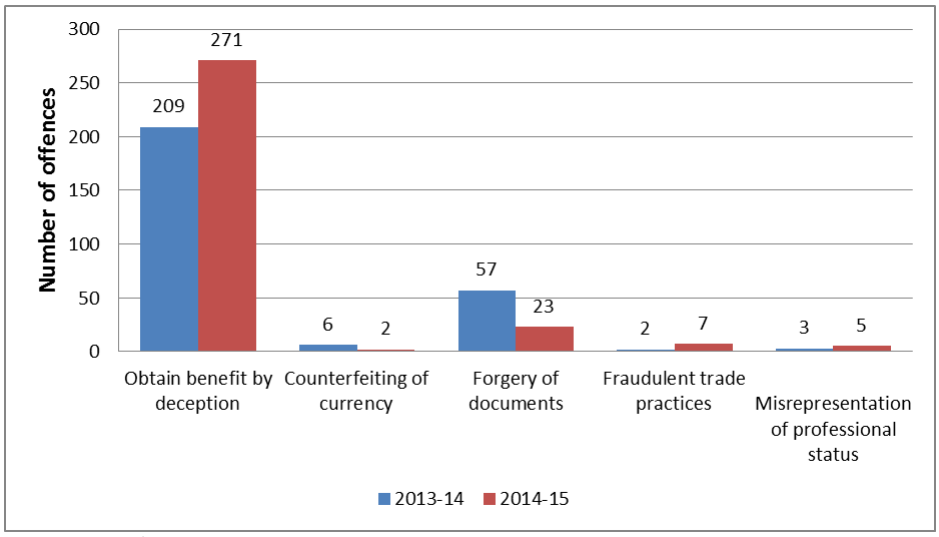
South Australia (SA)
During 2014-15 there were 2,757 cases of fraud recorded by SA police (SA Police 2015a). These included:

- 2,297 offences to obtain benefit by deception ie fraud offenses, identity fraud, pass valueless cheque and credit card scams and;
- 460 offences of other fraud ie forgery, counterfeiting, embezzlement, misappropriation or stealing by a public servant or a person in a position of trust (SA Police 2015b).

New South Wales (NSW)
There were 51,137 reported cases of fraud in NSW during 2015 compared to 49,120 in 2014 (NSW BOSCAR 2015). A study of 1,000 narrative descriptions of fraud incidents reported to or detected by NSW Police between 2008 and 2013 found that the most common types of fraud reported to police were card fraud (35% of incidents), fuel drive-offs (30%), identity theft (5%), embezzlement (4%) and cheque fraud (3%) (Macdonald and Fitzgerald 2014

Northern Territory (NT)
NT does not currently classify data in a manner that enables reporting on identity crime. However, NT does publish information on fraud offences which provide a useful comparison with other jurisdictions. There were 308 reported cases of fraud in 2014-15 compared to 277 in 2013-14. (NT Police 2015)

Figure F5: Number of fraud, deception and related offences in the Northern Territory, 2013-14 to 2014-15



Source: NT Police 2015.

Comparison with previous years

Table F1: Number of fraud offences reported to state and territory police 2012-13 to 2014-15

	2012-13	2013-14	2014-15
Vic (b)	27687	32724	35243 (882)
Qld	19513	17767	23382 (733)
SA	2415	2701	2757
WA	19619	22737	19253 (340)
Tas	581	533	646
NT	254	277	308
ACT	439	598	1195
	2013	**2014**	**2015**
NSW(a)	50270	49120	51137
Total	***120778***	***126457***	***133921***

Note (a): NSW numbers all from calendar year

Note (b): 2014-15 Victoria reporting changed to calendar year

Note (c): Number in brackets represent the number of frauds that could be identified as being classified as an identity crime.

Appendix G – Commonwealth prosecutions by the CDPP

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 identity crime itself. 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 Trademarks Act 1995 (Cth).

Offenders who commit identity-related offences against Australian Government agencies may be prosecuted by the Commonwealth Director of Public Prosecutions (CDPP). The CDPP provided a suite of prosecution statistics relating to identity crime offences under the Criminal Code (Cth) and is presented in Figure 23 and Table G1.

Table G1: Total number of defendants prosecuted by the CDPP by Act and Year (2012-13 – 2014-15)[8]

Offence	2012-13	2013-14	2014-15
Divisions 370, 372, 375 *Criminal Code* - Identity Crime	1	3	6
Divisions 133-137 *Criminal Code* - Fraudulent Conduct	1458	1313	1127
Divisions 144-145 *Criminal Code* - Forgery	24	19	28
Division 480 *Criminal Code* - Financial information offences	9	3	5
Section 234 *Migration Act 1958* - False documents	29	10	7
AMLCTF Act 2006 sections 135-138	2	7	2
Section 24, *Financial Transactions Report Act 1988* - Opening account etc in false name	9	3	2
Part XII *Customs Act 1901* - Penal provisions (s.233BAB)	13	38	57
Part 14 *Trademarks Act 1995* - ss.146-148	9	4	3
TOTAL	**1554**	**1400**	**1279**

Source: CDPP unpublished data as of 19 October 2015

[8] These are the total number of prosecutions on indictment plus summary prosecutions. A defendant may have more than one offence prosecuted under more than one Act and section, and is therefore counted more than once where this occurs. The data in this table represents 3289, 1854, 1535,1397 and 1237 unique defendants prosecuted in 2010-11, 2011-12, 2012-13, 2013-14 and 2014-15 respectively.

Appendix H – Methodology for estimating the cost of identity crime

Several attempts have been made in the past to estimate the cost and economic impact of identity crime in Australia, these include attempts by AGD, where it was estimated that identity crime in Australia cost the Australian economy $1.6b (2014) and $2b (2015)

The present methodology is consistent with the 2013-14 estimates of the cost of identity allowing for direct comparisons to be made. These estimates are derived from the methodology used to calculate the costs of crime in the AIC's *Counting the costs of crime in Australia: A 2011 estimate* ('Counting the costs of crime report') (Smith, Jorna, Sweeney & Fuller 2014).

These estimates rely on data from previous reports that have sought to quantify the cost of crime in Australia (Smith, Jorna, Sweeney & Fuller 2014) and the cost of fraud committed against Commonwealth agencies (Jorna & Smith forthcoming 2016). Personal fraud victimisation survey data (ABS 2016) as well as officially recorded police statistics about fraud have also been relied upon.

Cost of identity crime against Commonwealth agencies

In 2014-15, Commonwealth agencies reported a total of 155,843[9] internal and external incidents of fraud worth $328,959,277 (Smith & Jorna forthcoming 2017b). This equates to approximately $2,111 per incident. A multiplier of 1.15 was applied (Smith, Jorna, Sweeney & Fuller 2014) to account for the frauds that were undetected or unreported. This revises the estimate to **179,219** incidents of fraud with an estimated loss of $378,332,259.

According to Smith & Jorna & Smith (forthcoming, 2017b) a total of $24,465,519 in recovered funds and reparations was recouped by Commonwealth agencies in 2013-14. Deducting this from the total leaves a net total loss of **$353,866,740**.

In the United States, Harrell (2015) found that **5%** of all identity theft victims in their study reported indirect losses as a result of their most recent incident of identity theft. Victims reported an average indirect loss of US$261 and a median loss of US$30 (this was a large decreases from the 2012 mean loss of $4,168 and median of $30 respectively). For the purposes of this category of fraud, the median was used as the value to determine the amount that indirect losses contribute to the cost of each fraud incident. The median was selected due to the fact that frauds against the Commonwealth do not always involve large amounts of money. Assuming an exchange rate of US$30 to AUD$42, a total of $376,362 (5% of 179,219 incidents) in indirect costs needs to be added to the net total loss of $353,866,740. Accordingly, Commonwealth agencies incurred **$354,242,150** in indirect and direct fraud losses.

In 2014-15, there were 98,604 internal and external incidents of fraud that involved 'misuse of identity'. This was considerably higher than the 17,001 internal and external misuse of identity incidents recorded by Commonwealth agencies in 2012-13. It was noted that one entity changed the way they had previously recorded/categorised external fraud which was responsible for 79,438 of the identity related incidents. If data from this entity is excluded, there were 19,166 internal and

[9] This is based on the 154 Commonwealth entities who participated in the Fraud against the Commonwealth census, 65 of whom reported incidents of internal and external fraud.

external misuse of identity incidents recorded, which represents **25.1%** of fraud incidents (76,405 when the outlier is removed) reported.

If it is assumed that identity crime represents 25.1% of all incidents of fraud experienced by Commonwealth agencies, identity crime as a proportion of all Commonwealth fraud would cost approximately **$88.9m** ($88,915,019).

Cost of identity crime against individuals

For the purposes of the identity crime estimate for this report, and in an effort to keep the figures as consistent as possible, ABS demographic data for June 2015 was used to determine the percentage of Australia's population who would have been aged over 15 years in 2015. 81.2% of Australia's population of 23,781,169 was aged 15 years and over at June 2015 (ABS 2015). This equates to **19,310,309** people.

The 2014-15 ABS survey found that **8.5%** of people aged 15 years and over had experienced at least one incident of personal fraud (including identity theft, card fraud and scams) in the 12 months prior. The AIC also found that 8.5% of respondents had experienced misuse of personal information in the previous 12 months. Assuming that 8.5% of people aged over 15 years experienced personal fraud, there would have been **1,641,376** victims of personal fraud in 2014-15.

The 2014-15 ABS survey found that over three quarters of victims (78%)[10] of personal fraud, or 1.2 million people, had lost money as a result of the fraud. This equated to an average loss of $2,700 per victim, and a median loss of $400. Given the mean is very high and most victims of personal fraud suffer only small monetary losses, it was decided that it would be more accurate to use the median figure of **$400** to calculate the direct cost of personal fraud. Accordingly, the total direct cost of personal fraud to individuals in Australia in 2014-15 was **$656,550,506**.

If, as in the case of fraud against Commonwealth agencies, it is assumed that 5% of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell 2015), and victims had a median indirect loss of AUD$42, a total of $3,446,890 in indirect costs needs to be added to the net total loss of $656,550,506. Accordingly, individual victims of personal fraud incurred **$659,997,396** in indirect and direct losses.

Cost of identity crime as a proportion of serious frauds

Serious frauds make up a small proportion of the total incidents of fraud committed in Australia each year. However, they often result in substantial losses to the victims or companies targeted.

In 2012, KPMG surveyed 281 organisations in Australia and New Zealand and found that the participating organisations had experienced 194,454 incidents of fraud in the two years prior to the survey, worth a total of $372.7m. There were 20 incidents of fraud that involved losses of over $1m (KPMG 2013). Only 46% of the major incidents of fraud were reported to police (KPMG 2013). It should be noted that in 2014 no report was produced due to lack of contribution from organisations.

For the purposes of this report, it is assumed that 300 incidents of fraud would have involved losses of $1.5m each, using the calculation of Smith et al. (2014). This results in total losses of $450m. If these 300 cases are inflated using a multiplier of 2.2 to acknowledge the number of serious fraud

[10] This is based on an estimate 1,592,400 people experiencing personal fraud during 2014-15, 1,238,200 of which incurred a financial loss, prior to reimbursement.

incidents that were not reported to police, there would have been a total of 660 reported and unreported serious fraud incidents worth $990m.

If, as noted above, it is assumed that 5% of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell 2015), and victims had an average loss of US$261(AUD$365), a total of $12,045 in indirect costs needs to be added to the total loss of $990m. The mean is used in this case as opposed to the median value due to the assumption that frauds reported to police will usually be of a greater value, and that there are usually significant losses involved in serious fraud cases. Accordingly, the value of serious fraud is $990,012,045 in indirect and direct losses.

If it is assumed that a minimum of 15% of serious fraud incidents involve identity crime, it is estimated that the cost of identity crime as a proportion of serious fraud would be **$148,501,807**.

Cost of identity crime as a proportion of police-recorded fraud

In 2014-15, there were **133,921** fraud and dishonesty offences recorded by police throughout Australia (BOCSAR 2015; WA Police 2015; Dept. Police and Emergency Management 2015; SA Police 2015; Vic Police 2015; NT Police, Fire and Emergency Services 2015; Unpublished data from ACT Policing and QLD Police). Added to this are 55 referrals from Commonwealth agencies that were accepted by the AFP in 2013-14 (Smith & Jorna forthcoming 2016). The financial loss associated with these 55 cases alone was $471,134,682 or $8,566,085 per matter (Smith & Jorna forthcoming 2016). Accordingly, it is estimated that there were a total of **133,996** recorded fraud offences in Australia in 2014-15.

From these 133,996 fraud offences the following deductions need to be made:

- 77 incidents of fraud against the Commonwealth were referred to state and territory police by federal agencies,
- 660 serious fraud incidents estimated above.
- 54,142 incidents of personal fraud that were recorded by police (3.4% of 1,592,400 victims of personal fraud as reported by the ABS)

This brings the total estimated number of officially recorded fraud incidents to **79,097**.

It has been estimated that recorded frauds only represent 25% of the total number of incidents of fraud that actually occur (Mayhew, 2003). Accordingly, we need to inflate the estimate of 79,079 by a multiplier of 4 in order to determine the total number of recorded and unrecorded frauds. This results in a total of **316,388** recorded and unrecorded fraud offences. Deducting the 79,097 recorded fraud offences from the total 316,596 fraud incidents, yields **237,291 unrecorded** fraud offences.

Several studies have attempted to estimate the unit cost per incident of fraud based on the assumption that frauds of lower monetary value are less likely to be reported than frauds that are worth a larger amount of money (Mayhew 2003; Smith et al. 2014; Rollings 2008). The unit cost estimates for recorded frauds have ranged from $9,900 in 2001 (Mayhew, 2003) to $21,500 in 2005 (Rollings, 2008). The unit cost estimates for unrecorded fraud ranged from $1,590 in 2001 (Mayhew, 2003) to $3,390 in 2005 (Rollings, 2008).

Using the Reserve Bank of Australia's inflation calculator (RBA 2015), the unit cost for recorded and unrecorded fraud incidents in 2014-15 would have been **$27,981**, and **$4,412** respectively. This is consistent with data provided by IDCARE who found that the average value of the misuse event

experienced by clients was $27,267 during 2015 where the majority of clients report more complex incidents of identity misuse.

Applying these figures to the estimated 79,079 recorded and 237,291 unrecorded frauds yield totals of $2,213,213,157 for recorded frauds and $1,047,927,892 for unrecorded frauds. This gives a total of **$3,260,141,049**.

If, as noted above, it is assumed that five per cent of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell 2015), and victims had an average loss of US$261 (AUD$365), a total of **$5,774,081** in indirect costs needs to be added to the total loss of $3,260,141,049. The mean is used in this case as opposed to the median value due to the significant losses involved in many of these fraud cases. Accordingly, the total value of police recorded and unrecorded incidents of fraud is **$3,265,915,130**.

It has been estimated that up to 40% of police-recorded fraud and deception offences involve identity crime (CIFAS 2015), then it is estimated that the cost of identity crime as a proportion of police recorded and unrecorded fraud is $1.306b (**$1,306,366,052**).

Costs to agencies of preventing and responding to identity crime

It is estimated that the costs associated with preventing and responding to identity crime by government, business and individuals are $387,576,224 (or approximately $390m). This figure was calculated based on the methodology used in the '*Counting the Costs of Crime in Australia*' report (Smith, Jorna, Sweeney & Fuller 2014).

Prevention costs were calculated for Commonwealth and state/territory government services and included police, prosecutions, courts, corrections and other government services which assist victims or contribute to the prevention of crime. An estimate of the proportion of expenditure spent on identity crime matters for agencies such as the state/territory Registries of births, deaths and marriages; consumer affairs, and road traffic authorities were also included.

Annual recurrent expenditure figures were obtained from the 2014-15 Budget allocations for each agency or the agencies' 2014-15 annual reports. An estimate of the proportion of annual recurrent expenditure that was spent on crime-related issues was then calculated. Percentages were then estimated for identity crime as a proportion of the total cost of crime to the different agencies. A table of the figures that were used to calculate the estimated costs of preventing identity crime can be found in Appendix G.

Appendix I – Calculating the cost of identity crime

Table I1: Total direct and indirect costs of identity crime in Australia

Fraud category	Reference period	Fraud Incidents	Cost per incident	Total cost	Multipliers	Indirect costs	Incidents after multipliers applied	Total cost (after multipliers applied and including indirect costs)	% Identity Crime	Applying % Identity crime to total (b)
Commonwealth fraud	2014-15	155,843	$2,111	$328,959,277	1.15	$376,362	179,219	$378,311,309 (a)	25.1%	$88,915,019
Identity Crime against Individuals (based on National Victimisation Surveys)	2014-15	1,641,376	$400	$656,550,506	NA	$3,446,890	1,641,376	$659,997,396	100%	$659,997,396
Serious fraud	2011	300	$1,500,000	$450,000,000	2.2	$12,045	660	$990,012,045	15%	$148,501,807
Police recorded fraud (excl. above categories)	2014-15	79,097	$27,981 per recorded fraud; $4,412 per unrecorded fraud	$2,213,213,157 in recorded fraud costs; $1,047,927,892 in unrecorded fraud costs (total = $3,260,141,049)	4	$5,774,081	316,388 (79,097 recorded; 237,291 unrecorded)	$3,265,915,130	40%	$1,306,366,052
TOTAL										**$2,203,780,274**

Source: Derived from Smith, Jorna, Sweeney & Fuller 2014.
Note (a): $24,465,519 must be deducted from this total to account for costs that were recovered.
Note (b): numbers rounded to nearest whole number.

Table I2: Total estimated costs of preventing and responding to identity crime in Australia

Jurisdiction	Estimated crime cost $	Estimated identity crime cost $
Commonwealth	$5,185,746,500	$185,254,825
New South Wales	$3,860,191,000	$61,008,455
Victoria	$2,550,768,000	$41,803,340
Queensland	$2,308,879,500	$36,982,319
South Australia	$836,961,000	$13,774,543
Western Australia	$1,508,642,000	$23,115,410
Tasmania	$216,753,400	$3,573,255
Northern Territory	$462,907,600	$6,245,173
Australian Capital Territory	$203,758,900	$2,990,227
All states and territories (a)	$877,056,850	$12,828,678
Total	**$18,011,664,750**	**$387,576,224**

Sources: Derived from Smith, Jorna, Sweeney & Fuller 2014:64-75.

Note (a): This figure includes legal aid, BDM, road traffic authorities and consumer affair agencies which weren't included in the individual jurisdictions.