



NATIONAL IDENTITY SECURITY STRATEGY

**Identity crime and
misuse in Australia
2013–14**



IDENTITY SECURITY

Acknowledgement

The Attorney-General's Department appreciates the assistance of the Australian Institute of Criminology in preparing the report, including Catherine Emami and Dr Russell G Smith who undertook the analysis and prepared the text for publication.

ISBN: 978-1-925290-16-5

© Commonwealth of Australia 2015

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au).

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

Contents

Foreword	3
Executive Summary	4
Economic impact of identity crime	4
Prevalence of identity crime	4
Acquisition of fraudulent identities	6
Identity crime and the criminal justice system	8
Impacts on victims	10
Remediation of identity crime	12
Prevention of identity crime	12
Data quality and availability	14
Introduction	15
Indicators of identity crime	16
1. Acquisition of fraudulent identities	17
2. Use of fraudulent identities	17
3. Impacts of identity crime	17
4. Remediation of identity crime	18
5. Prevention of identity crime	18
Key findings	19
1. Acquisition of fraudulent identities	19
1.1 Price of fraudulent identity credentials	19
1.2 Number of reported data breaches	20
2. Use of fraudulent identities	23
2.1 Number of identity crime incidents recorded by government agencies	23
2.2 Prosecutions involving identity crime and other related offences	39
2.3 Number of people who self-report being victims of identity crime or misuse	44
2.4 Number of people who perceive identity crime and misuse as a problem	49
2.5 The types of personal information most susceptible to identity theft or misuse	50

3. Impacts of identity crime	51
3.1 Direct cost of identity crime and misuse to government agencies	51
3.2 Direct costs of identity crime and misuse to business	54
3.3 Direct cost to individual victims of identity crime and misuse	58
3.4 Non-financial consequences of identity crime and misuse	61
4. Remediation of identity crime	63
4.1 Average time by victims spent in remediation activity	63
4.2 Number of enquiries to government agencies regarding assistance to recover identity information	66
4.3 Number of applications for victims' certificates	69
5. Prevention of identity crime	70
5.1 Range of identity credentials verifiable using the Document Verification Service (DVS)	70
5.2 Number of government agencies using the DVS	71
5.3 Number of private sector organisations using the DVS	71
5.4 Number of DVS transactions each year	71
5.5 Online security practices—individuals, business and government	72
6. Estimating the economic impact of identity crime to Australia	75
6.1 Calculating the cost of identity crime	75
Conclusions	80
References	81
Appendix A—Graphs of state and territory police data	87
Appendix B—Measurement framework indicators	91
Appendix C—Government agencies involved in this report	94
Appendix D—Definition of key terms	96
Appendix E—Calculating the cost of identity crime	98
Appendix F—Methodology for estimating the cost of identity crime	105

Foreword

The Australian Government is committed to combating identity crime and boosting the safety and security of all Australians. Central to this process is the development of innovative, evidence-based policies and services that enhance our nation's identity infrastructure.

As part of this process, in October last year, the Australian Government released the pilot *Identity Crime and Misuse in Australia* report, one of the most comprehensive attempts by any government worldwide to measure the impact of identity crime. Building on the success of the pilot, I am very pleased to introduce this latest report which provides updated data on identity crime for the 2013–14 financial year.

Identity crime is one of the most prevalent crimes in Australia, affecting hundreds of thousands of Australians each year, and surpassing conventional crime types like assault, motor vehicle theft and robbery. The impacts of these crimes are far-reaching and affect not only individuals, but also businesses and organisations in the public and private sectors. In addition to the considerable financial losses, victims of identity crime can also suffer non-financial impacts on their mental health.

This report represents an important component of the Council of Australian Governments' plan to combat identity crime, as enshrined in the National Identity Security Strategy. This strategy has been instrumental in the development of key improvements to our nation's identity security infrastructure including the development of the Document Verification Service and the National Identity Proofing Guidelines.



A handwritten signature in black ink, appearing to read 'Michael Keenan'.

The Hon Michael Keenan MP
Minister for Justice
Minister Assisting the Prime Minister on Counter-Terrorism

Executive Summary

Economic impact of identity crime

Summary Finding: It is estimated that in 2013–14 the total direct and indirect cost of identity crime in Australia was approximately \$2b (see figure 1 below). This includes the direct and indirect losses incurred by government agencies and individuals; and the cost of identity crimes recorded by police. The costs of preventing and responding to identity crime are estimated to be a further \$350m. In total, it is estimated that the economic impact of identity crime in Australia would be approximately \$2.4b. These estimates adopt a different methodology from that used in the *'National Identity Crime and Misuse Measurement Framework Pilot'* (the Pilot) report published in 2014, and so are not directly comparable as an indicator of change over the intervening time.

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

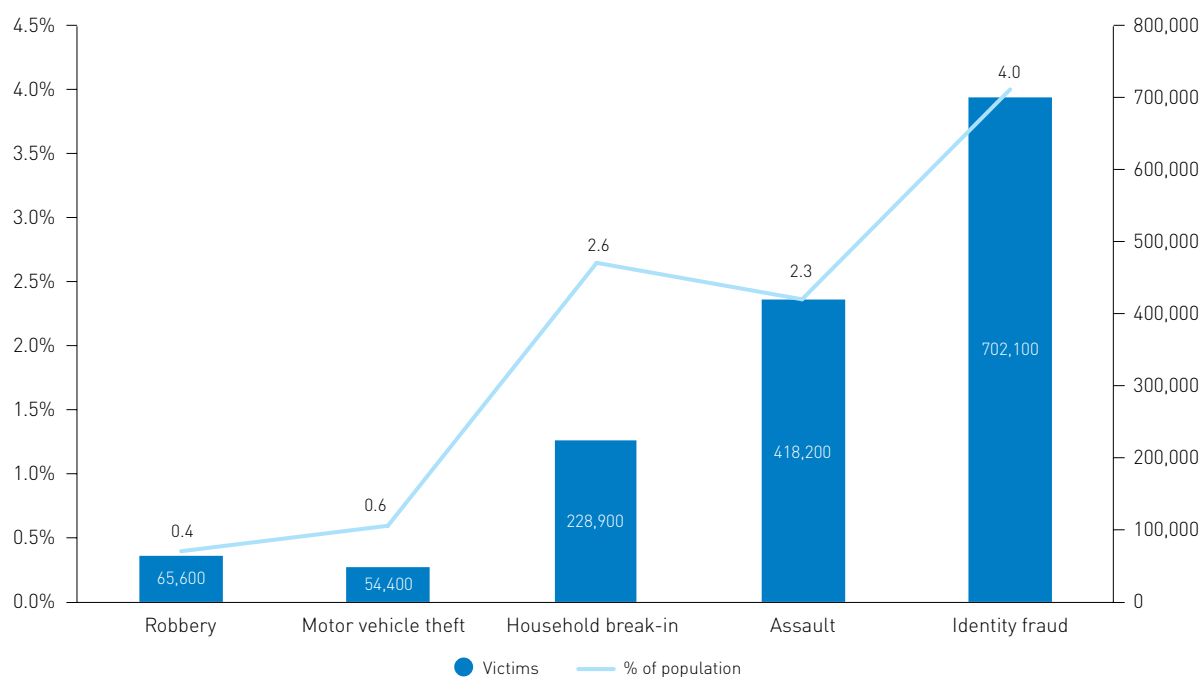


Prevalence of identity crime

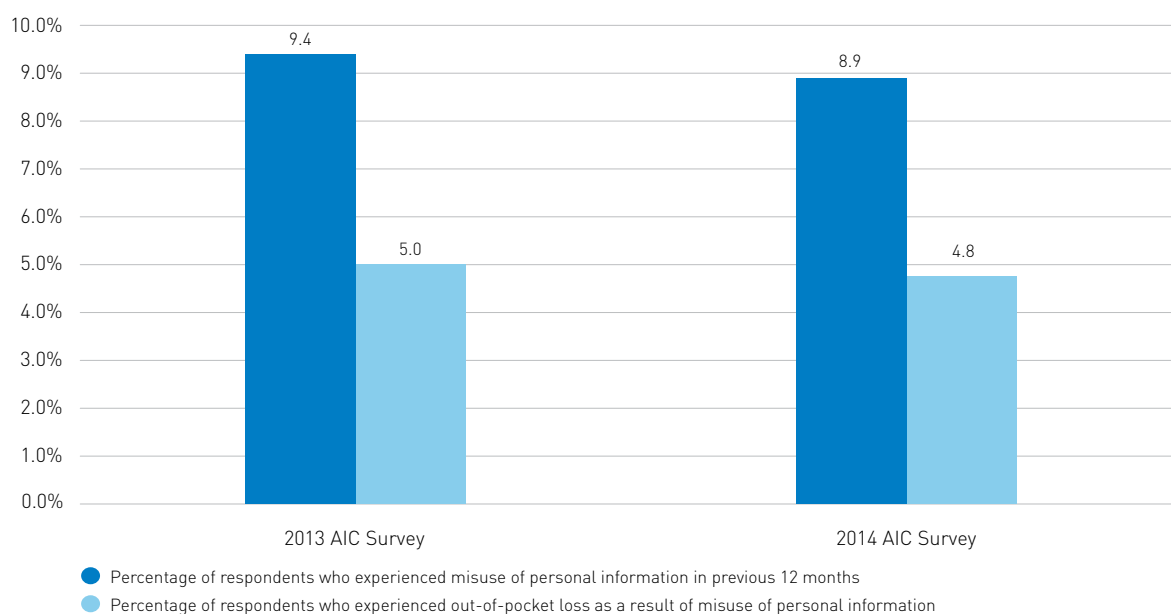
Summary Finding: Identity crime continues to be one of the most prevalent crimes in Australia, with the Australian Bureau of Statistics (ABS) finding that around 4% of the Australian population aged 15 years and over reported being victims of identity fraud or identity theft in 2010–11. By comparison, other personal and theft-related crimes (i.e. assault, robbery, break-ins and motor vehicle theft) each affected only around 0.4 – 2.3% of people and 0.6 – 2.6% of households respectively in 2013–2014 (see Figure 2).

The Australian Institute of Criminology (AIC) found that approximately 9% of all respondents in its 2013 and 2014 Identity Crime and Misuse Surveys (Smith & Hutchings 2014 [2013 AIC Survey] and Smith, Brown & Harris-Hogan forthcoming [2014 AIC Survey]) experienced some form of misuse of their personal information in the previous 12 months, with approximately 5% of all respondents incurring out-of-pocket losses as a result of this misuse (see Figure 3).

Identity crime continues to be of great concern to Australians, with around 96% of respondents to the surveys perceiving misuse of personal information to be a very serious or somewhat serious issue (see Figure 4).

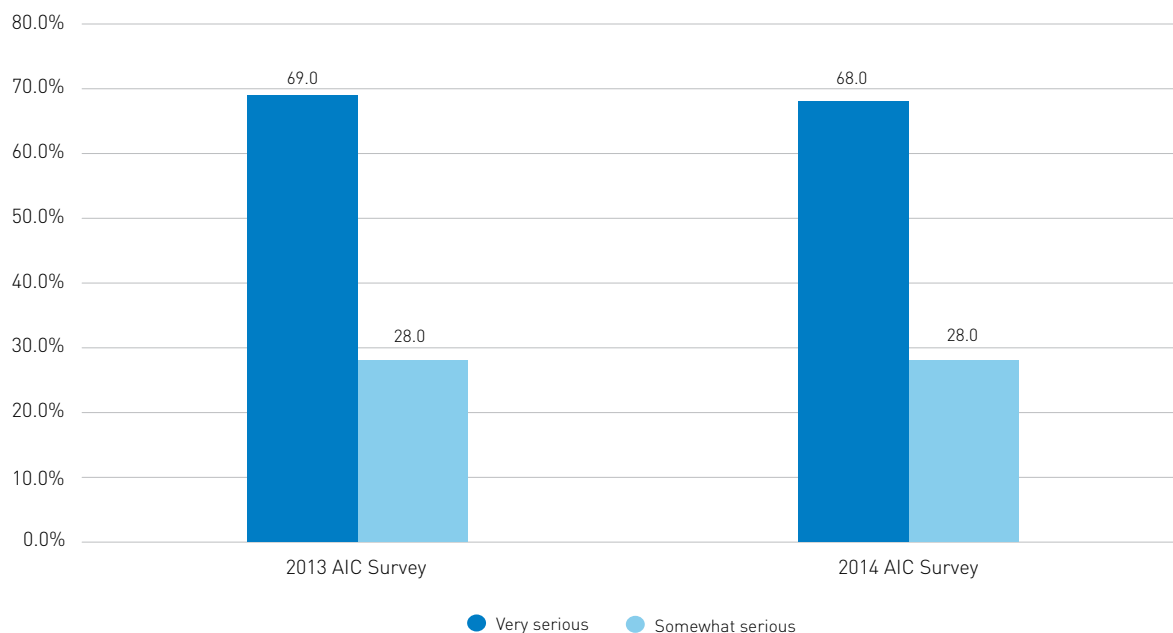
Figure 2: Number of victims and proportion of population, by offence type (n and %)

Source: ABS 2015, and ABS 2012.

Figure 3: Percentage of respondents in 2013 and 2014 AIC Surveys who experienced misuse of personal information and out-of-pocket loss

Source: 2013 and 2014 AIC Surveys (weighted data).

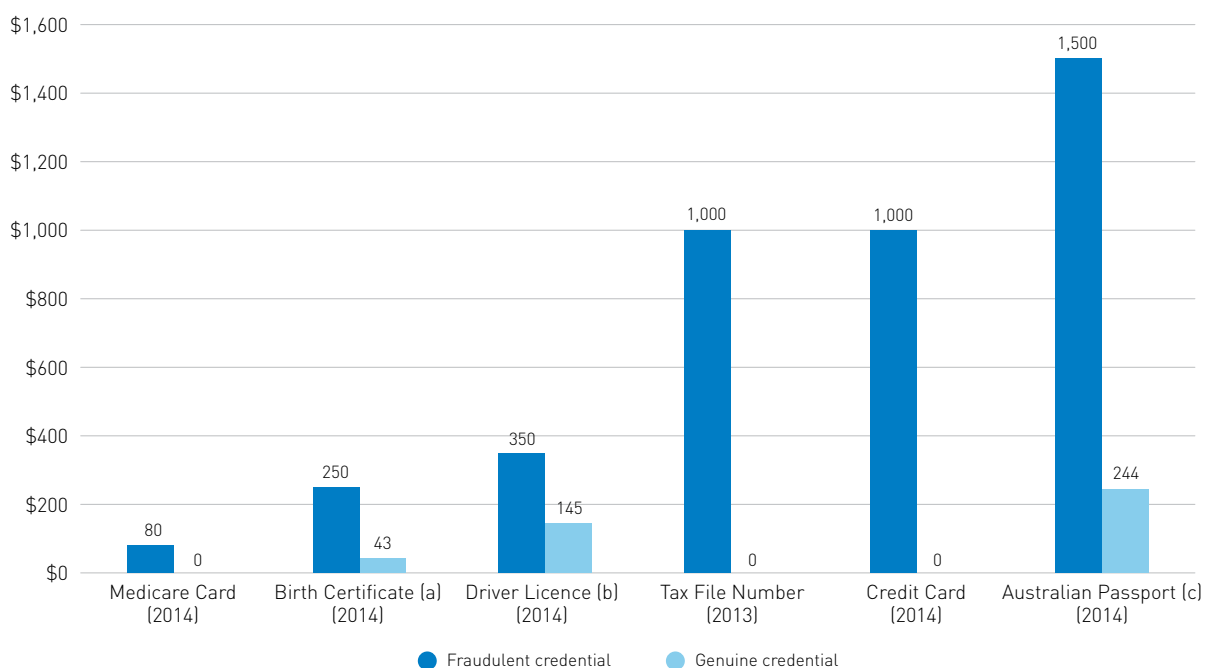
Figure 4: Perceptions of misuse of personal information in AIC Identity Crime surveys



Source: 2013 and 2014 AIC Surveys.

Acquisition of fraudulent identities

Summary Finding: Stolen identity information and fraudulent identity credentials continue to be highly sought after by criminals, including via online marketplaces (e.g. the 'dark-net'). The number of data breaches appears to be increasing, with the number of breaches reported to the Office of the Australian Information Commissioner in 2013–14 being the highest in five years (see Figure 6). The prices of fraudulent Australian identity credentials remain largely unchanged from those disclosed in the Pilot Report (see Figure 5 below). Anecdotal evidence from police and victims suggests that driver licences and Medicare cards continue to be the most likely identity credentials used in the facilitation of identity crime.

Figure 5: Price of fraudulent and genuine Australian identity credentials

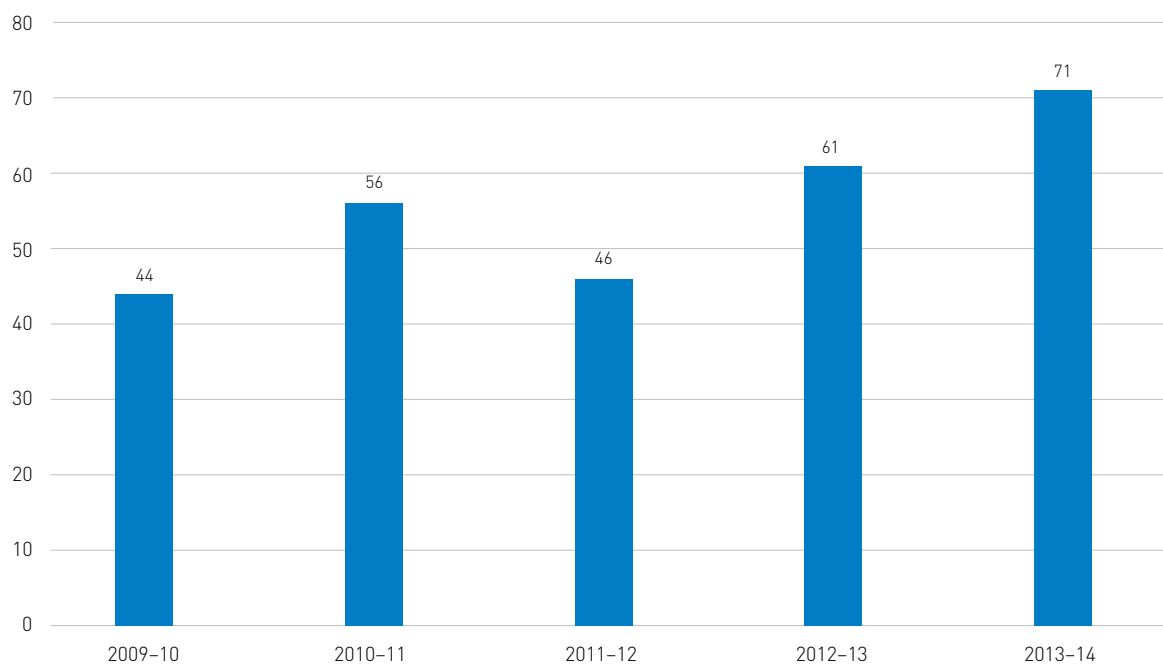
a. Based on fees for a standard birth certificate accessed from state and territory Offices of Births, Deaths and Marriages websites on 3 December 2014: \$42 (ACT); \$51 (NSW); \$30.20 (Vic); \$42 (QLD); \$44 (WA); \$43 (NT); \$46 (SA); \$45.88 (Tas).

b. Based on fees for a 5 year licence renewal accessed from State and Territory Motor Vehicle Registry websites on 3 Dec 2014: \$167.10 (ACT); \$170 (NSW); \$154 (QLD); \$128.70 (WA); \$217 (SA); \$91 (NT); \$106.20 (Tas). The cost of a licence renewal in Victoria for 10 years is \$253.60. This figure was halved to reach a figure for five years (\$126.80). The average was then calculated.

c. Cost to have a genuine passport altered by a professional document forger. A legitimately issued passport with fraudulent information retails for between \$20,000 and \$30,000 on the black market.

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

Figure 6: Total number of data breaches recorded by the OAIC (2009–10 to 2013–14)



Source: Office of the Australian Information Commissioner Annual Reports, 2011, 2012, 2013 & 2014.

Note: 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.

Identity crime and the criminal justice system

Summary Finding: Police agencies recorded a total of 126,305 fraud and deception offences in 2013–14. Up to 40%—or just over 50,000 of these offences—involved identity crime. This is higher than the 30,000 identity crimes estimated in the Pilot Report; the difference in figures being due to the availability of more complete fraud offence data for the 2013–14 report (see Figure 7).

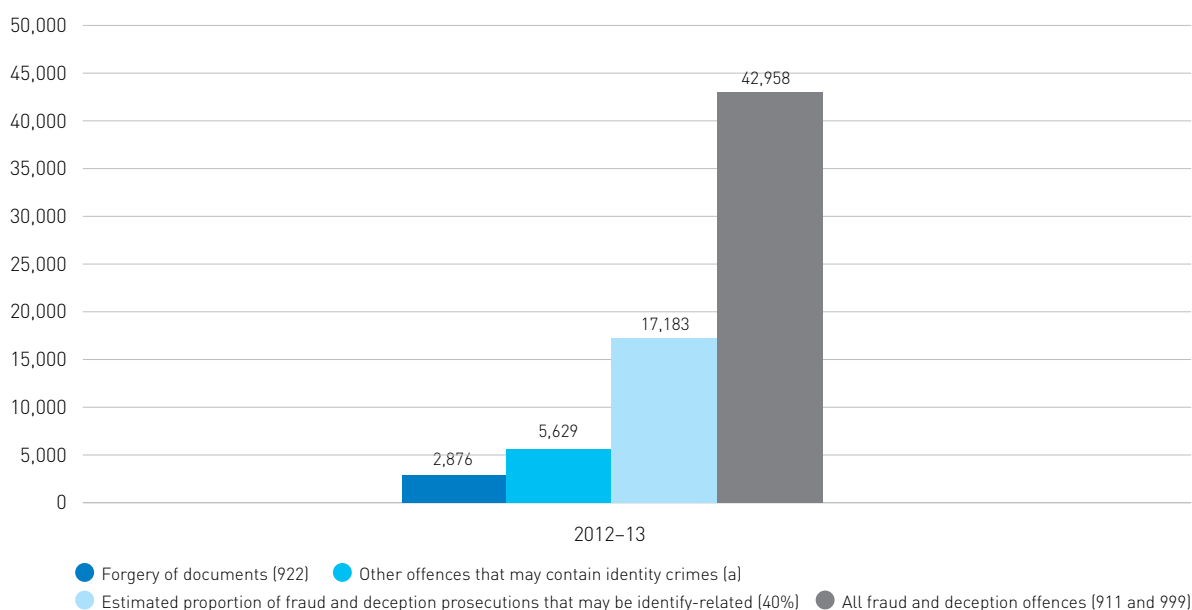
There were almost 26,000 offences proved in state and territory courts in 2012–13 that may have been related to identity crimes. This figure is based on the assumption that of the approximately 43,000 fraud and deception offences proven in state and territory courts in 2012–13, around 17,000 offences, or 40%, were possibly enabled by the use of stolen or fabricated identities. In addition, there were also approximately 9,000 ‘core’ identity crime offences (such as forgery, making false representations and possessing equipment to manufacture fraudulent credentials) proven in 2012–13 (see Figure 8).

Figure 7: Number of police-recorded fraud and deception offences compared with the estimated number that involved identity crime, 2013–14



Source: BOCSAR 2014; WA Police 2014; Dept. Police and Emergency Management 2014 TAS; SA Police 2014; Vic Police 2014; NT Police, Fire and Emergency Services 2014; Unpublished data from ACT Policing and QLD Police.

Figure 8: Estimated number of offences proved in state/territory courts which may have been related to identity crime



Source: Based on ABS Customised Report Data 2014, 2015.

(a) = Includes offences coded under the following ANZSOC codes: 829, 831, 923, 931, 932, 933, 991, 1111, 1542, 1543, 1559, 1612, and 1694

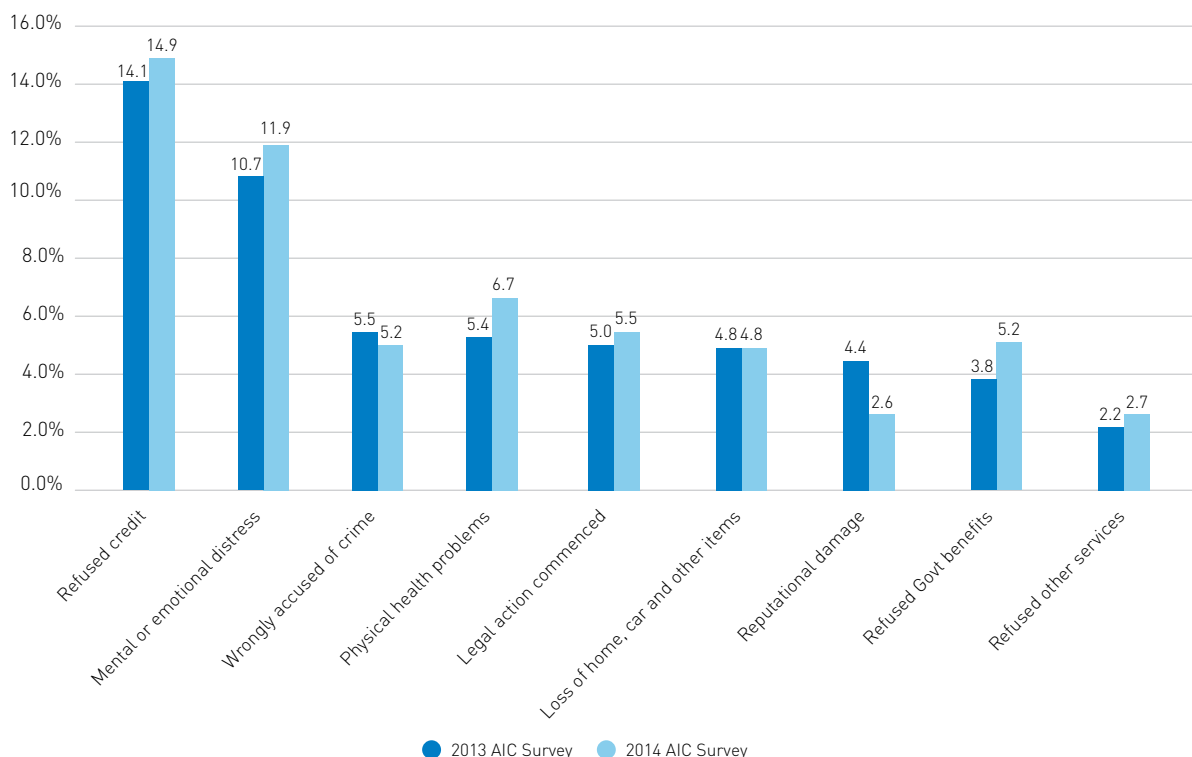
Impacts on victims

Summary Finding: It continues to be the case that most identity crime victims lose relatively small amounts of money (up to \$1,000), although in some cases losses can run to hundreds of thousands of dollars. A significant proportion of victims also experience demands on their time, or other adverse impacts on their mental or physical health, reputations or general wellbeing (see Figure 9).

Identity crime continues to be under-reported by victims in Australia. Just over 10% of respondents in the 2014 Survey who experienced misuse of their personal information in the previous 12 months did not report their victimisation to anyone. If victims did tell someone, almost half of the respondents indicated that they reported their victimisation to friends or family members (see Figure 10).

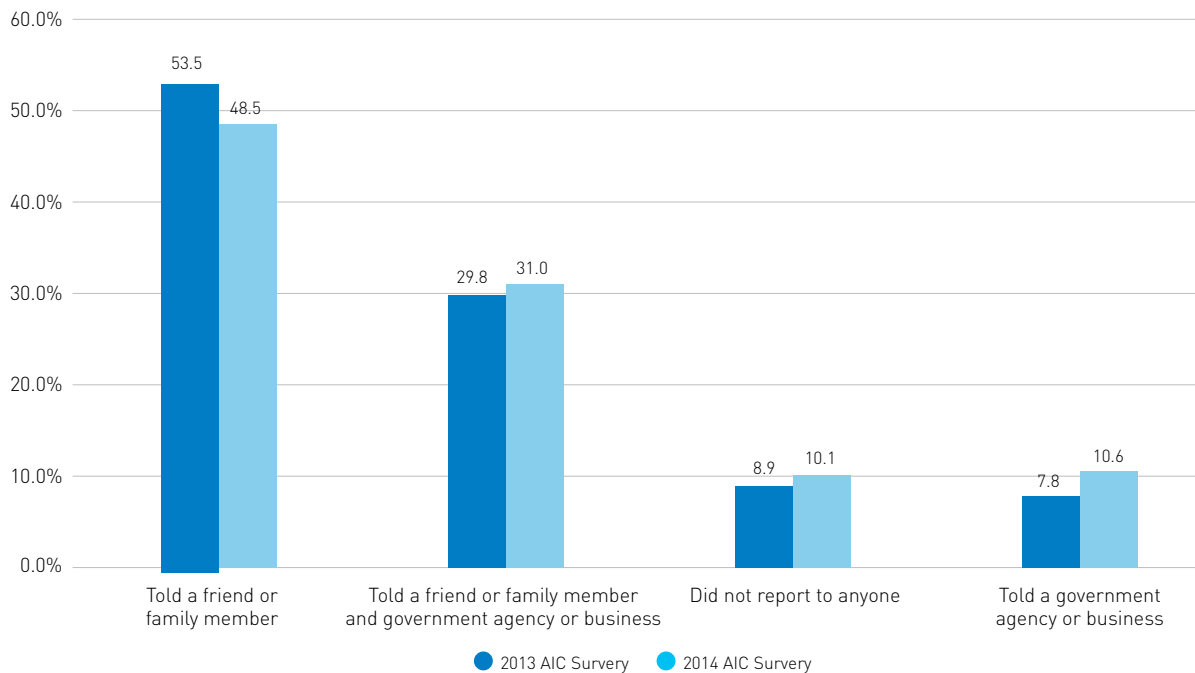
Reasons for respondents' reluctance to report their victimisation include a lack of immediate awareness that they have been the victim of a crime; embarrassment; the fact that they did not lose money and therefore do not believe there is any need to report the crime; a belief that the police or other authorities will not be able to do anything, and confusion regarding the agency to which they should report the incident (see Figure 11).

Figure 9: Consequences experienced as a result of personal information being misused in the previous 12 months



Source: 2013 and 2014 AIC Surveys.

Figure 10: Reporting misuse of personal information: AIC Surveys



Source: 2013 and 2014 AIC Surveys.

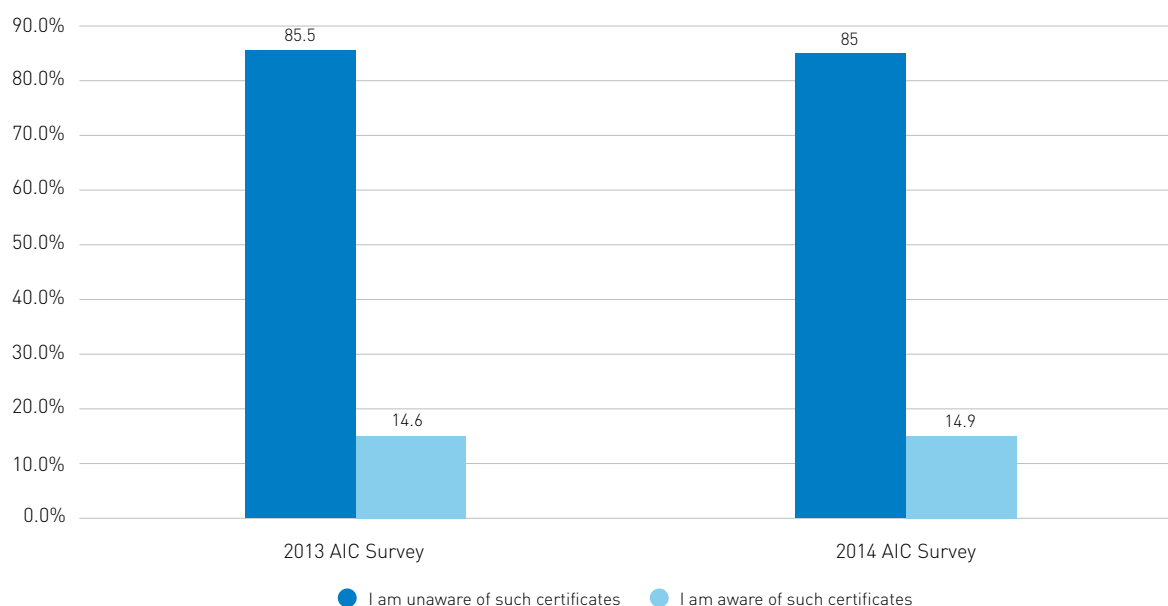
Figure 11: Reasons why people do not report misuse of personal information



Remediation of identity crime

Summary Finding: Identity crime victims' certificates continued to be under-utilised by victims of identity crime, with no certificates being issued at the Commonwealth level in 2013–14, and no specific data available with respect to the number of certificates issued at the state and territory levels during this period. In 2013 and 2014, approximately 15% of respondents in the Survey indicated they were even aware that victims' certificates exist (see Figure 12).

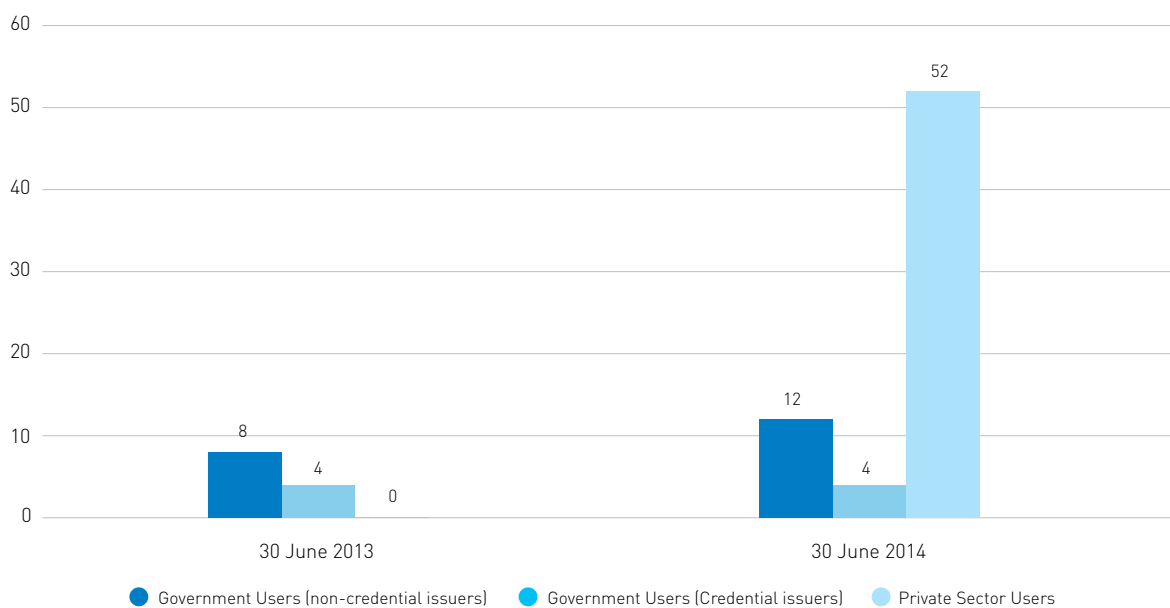
Figure 12: Respondents' awareness of victims' certificates



Source: 2013 and 2014 AIC Surveys.

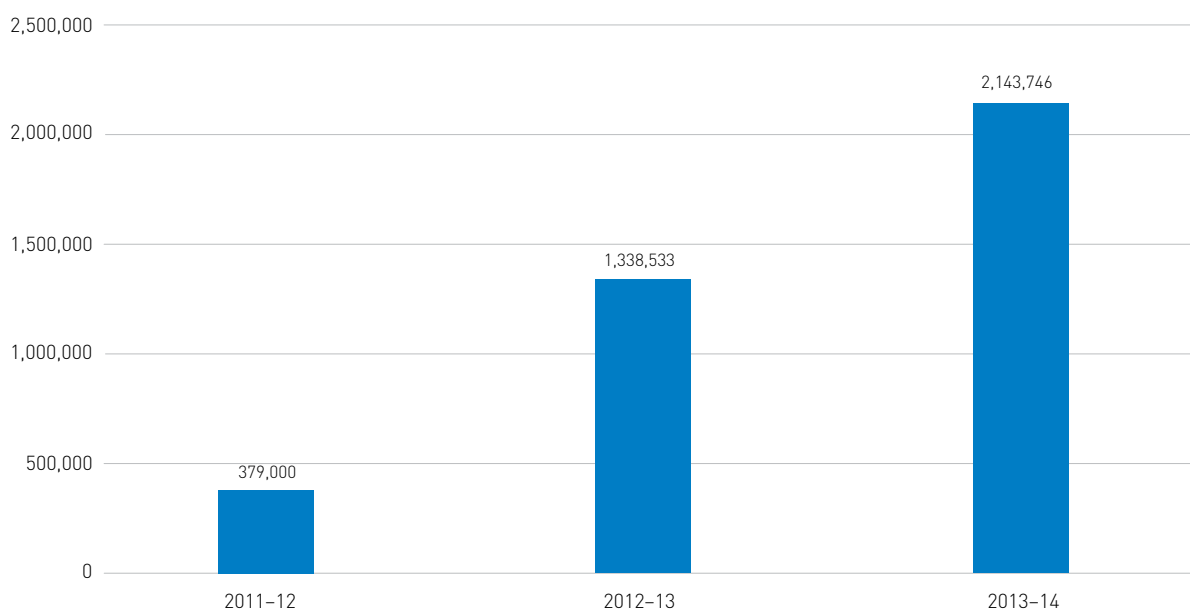
Prevention of identity crime

Summary Finding: There has been a substantial increase in the number of organisations using the Document Verification Service (DVS), particularly since certain private sector organisations were provided with access to the service in early 2014. As of 30 June 2014 there were 16 government agencies and 52 private sector organisations using the DVS (see Figure 13). During 2013–14 there were a total of 2,143,746 DVS transactions conducted—an increase of 60% from 2012–13, and 465% from 2011–12 (see Figure 14). Notwithstanding this, there are still a significant number of government agencies—many of which issue proof of identity documents—yet to commence using the service.

Figure 13: Number of DVS users in 2013 and 2014 by government and private sector

Source: AGD unpublished data.

Note: the DVS was not available to private sector users at 30 June 2013.

Figure 14: Number of DVS transactions, by year (2011–12 to 2013–14)

Source: AGD unpublished data.



Data quality and availability

Summary Finding: Gaining a precise understanding of the prevalence and impact of identity crime in Australia remains problematic due to the level of under reporting by victims at the individual and organisational level. There are also inter-jurisdictional inconsistencies in legislation, recording, investigation and prosecution which often results in identity crimes being absorbed into broader crime categories such as fraud offences. Consequently, the actual number of identity crime offences and their financial and other impacts may well be greater than some of the estimates.

Introduction

This report provides a comprehensive review of identity crime and misuse in Australia, based on information provided by relevant government agencies at the Commonwealth and state and territory level, business organisations, and the results of surveys of members of the public. It is clear that misuse of personal information for criminal purposes is an enduring problem in Australia, as well as in other developed nations, with substantial harms caused to the economy and individuals each year.

Misuse of personal information for criminal purposes is an enduring problem in Australia with substantial harms caused to the economy and individuals each year.

Identity crime is a generic term that describes a range of activities in which evidence of identity and other personal information is fabricated, manipulated, stolen or assumed, in order to facilitate the commission of a crime. Identity crime is rarely an end in itself, but is an important element in a wide range of criminal activities. These include credit card, superannuation and other financial frauds against individuals; welfare, tax and other fraud against government agencies; money laundering and financing of terrorism; gaining unauthorised access to sensitive information or facilities for unlawful purposes; and concealing other activities such as drug trafficking or the production and distribution of child exploitation material. Misuse of identity has also been present in connection with the commission of terrorist acts.

The national identity security infrastructure employed in Australia is built around a range of documents, cards and other credentials issued by a number of government, commercial and other non-government organisations. While the primary purpose of these credentials is not to serve as evidence of a person's identity, they have become increasingly used in this way throughout the community. Within this system, over 20 government agencies manage more than 50m 'core' identity credentials such as passports, birth certificates, visas, citizenship certificates, driver licences and Medicare cards. In addition, a comparable number of credentials are issued by private sector and other non-government organisations.

Unfortunately, misuse of these credentials for criminal purposes is an ongoing concern for governments. Detecting and preventing the fraudulent use of personal information in the current network of identity management systems presents significant challenges for the range of service delivery, regulatory and law enforcement agencies involved.

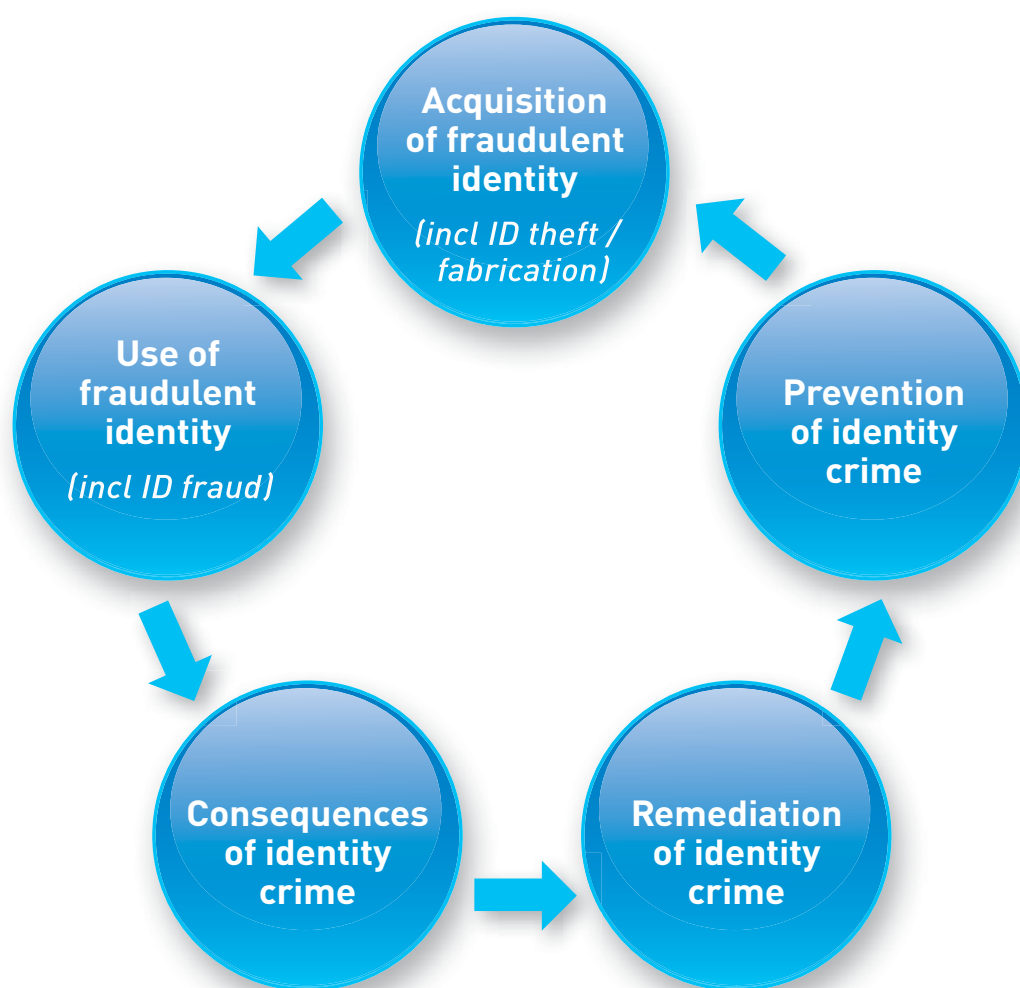
This report presents evidence of identity misuse gathered from as many reliable sources as possible. Monitoring a crime problem such as identity crime raises many conceptual and methodological issues, as data are collected and categorised in widely varying ways by different government agencies and private sector bodies. Nonetheless, an attempt has been made to compile the available information in as systematic and uniform a way as possible, while making clear where differences in definitions and categories are present.

Detecting and measuring identity crime in such a diverse, dynamic system presents significant challenges for the service delivery, regulatory and law enforcement agencies involved.

Indicators of identity crime

In order to gather all the relevant information, a number of individual measurement indicators were developed. These fall into five categories, illustrated in the Identity Crime Conceptual Model in Figure 15 below.

Figure 15: Identity Crime Conceptual Model



Source: Attorney-General's Department.

1. 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.

Two indicators were developed to measure this component of identity crime:

- Indicator 1.1—the price of fraudulent identity credentials
- Indicator 1.2—the number of reported data breaches.

While it would be desirable to measure the incidence of criminal activity specifically related to the manufacture or theft of credentials (as opposed to use of these), it is not feasible to extract this information from within currently available data sources. Most cases of identity crime which come to the attention of authorities involve both the fraudulent acquisition and use of identity information, but do not distinguish between these for reporting purposes.

2. 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 (ie real) identities in connection with financial, taxation, immigration and identity fraud.

There are five indicators which seek to measure this component of identity crime:

- Indicator 2.1—the number of identity crime and misuse incidents recorded by government agencies
- Indicator 2.2—the number of prosecutions for identity crime and other related offences
- Indicator 2.3—the number of people who self-report being victims of identity crime or misuse
- Indicator 2.4—the number of people who perceive identity crime and misuse as a problem
- Indicator 2.5—the types of personal information that may be more susceptible to identity theft or misuse.

3. 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.

There are four indicators aligned to this component:

- Indicator 3.1—direct costs of identity crime and misuse to government agencies
- Indicator 3.2—direct costs of identity crime and misuse to business
- Indicator 3.3—direct cost to individual victims of identity crime and misuse
- Indicator 3.4—non-financial consequences of identity crime and misuse.

4. Remediation of identity crime

This component covers the broader activities such as support services for victims, and the time they spend recovering their identity.

There are three indicators that endeavour to measure this component:

- Indicator 4.1—the average time spent by victims in remediation activity (i.e. recovering their identity)
- Indicator 4.2—the number of enquiries to government agencies regarding assistance to recover identity information
- Indicator 4.3—the number of applications for Victims' Certificates (issued by the courts).

5. 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.

There are six indicators designed to measure identity crime prevention activities in this component:

Use of the DVS

- Indicator 5.1—the number of identity credentials verifiable via the DVS
- Indicator 5.2—the number of government agencies using the DVS
- Indicator 5.3—the number of private sector organisations using the DVS
- Indicator 5.4—the number of DVS transactions each year.

Online security

- Indicator 5.5—the proportion of individuals, business and government that adopt robust online security practices to protect personal information.

Prevention costs

- Indicator 5.6—the costs incurred by individuals, business and government to protect personal information and to prevent the commission of identity crime (this forms part of the overall estimate of the cost of identity crime, above).

Key findings

1. Acquisition of fraudulent identities

Case Study 1

In February 2014, Western Australia police charged two people with a number of offences after discovering that they had allegedly stolen other people's mail and used the credit cards and cheques contained therein to assume the identities of the intended recipients.

The offenders allegedly then used fraudulent identities to facilitate the commission of a number of fraud offences around Perth including the withdrawal of money from bank and other financial institution accounts, purchasing debit cards, opening new bank accounts, hiring cars, and renting hotel rooms.

Western Australia police charged the offenders with 18 counts of stealing, 12 counts of fraud, eight counts of mail theft, two counts of vehicle theft, two counts of unlawful damage and 10 counts of possession of identification material with intent to commit an offence.

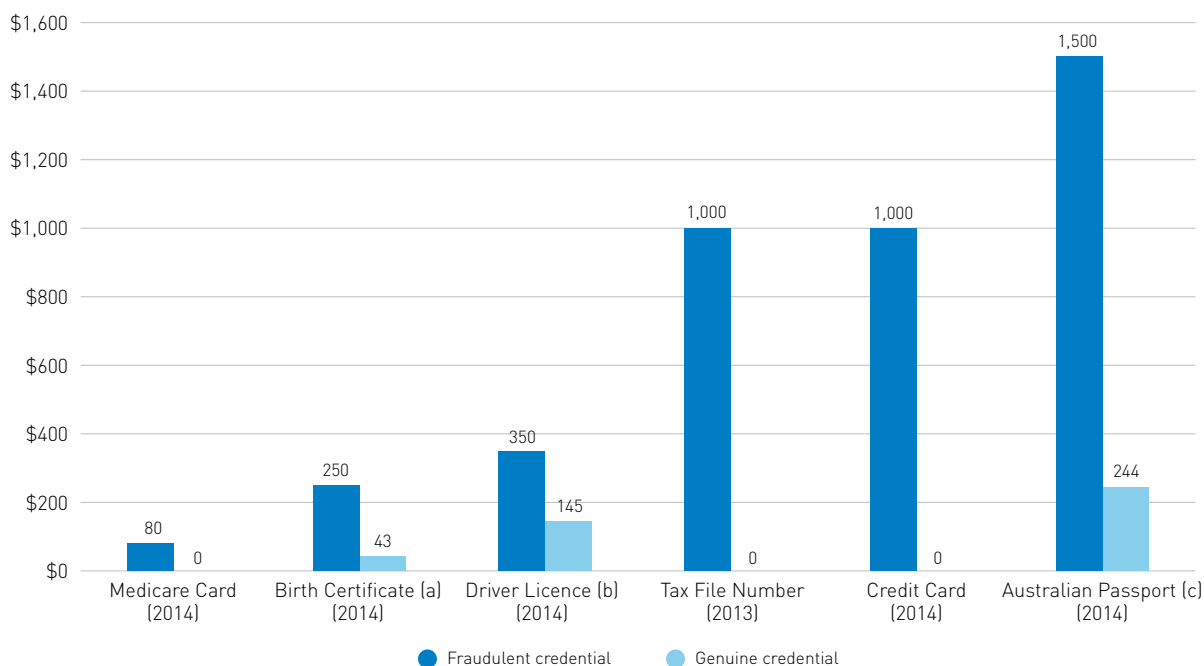
Source: Perth Now, 17 February 2014, <http://www.perthnow.com.au/news/western-australia/warning-to-lock-mailboxes-as-couple-charged-with-identity-theft/story-fnhocxo3-1226829682159?nk=d13823177566f81571d716ecdd93386e>

1.1 Price of fraudulent identity credentials

Key finding: There is a high demand for stolen or fraudulent identity information in online marketplaces ('the dark net'). The prices of fraudulent Australian identity credentials remain largely unchanged from the prices disclosed in the Pilot Report. Medicare cards continue to be one of the least expensive fraudulent credentials to obtain at a price of \$80, with passports being the most expensive at \$1,500. This can be as high as \$20,000-\$30,000 if the passport is obtained through legitimate processes but using fraudulent details, as opposed to having original passport details altered.

The price of fraudulent identity documents serves as an indicator of the availability of that type of fraudulent credential on the black market, and the extent to which the credentials are used in identity-related crime. Information from police intelligence holdings indicates that the cost of fraudulent identity credentials remains similar to those identified in the Pilot Report (see Figure 16).

Figure 16: Price of fraudulent and genuine Australian identity credentials



a. Based on fees for a standard birth certificate accessed from State and Territory Offices of Births, Deaths and Marriages websites on 3 December 2014: \$42 (ACT); \$51 (NSW); \$30.20 (Vic); \$42 (QLD); \$44 (WA); \$43 (NT); \$46 (SA); \$45.88 (Tas).

b. Based on fees for a 5 year licence renewal accessed from State and Territory Motor Vehicle Registry websites on 3 Dec 2014: \$167.10 (ACT); \$170 (NSW); \$154 (QLD); \$128.70 (WA); \$217 (SA); \$91 (NT); \$106.20 (Tas). The cost of a licence renewal in Victoria for 10 years is \$253.60. This figure was halved to reach a figure for five years (\$126.80). The average was then calculated.

c. Cost to have a genuine passport altered by a professional document forger. A legitimately issued passport with fraudulent information retails for between \$20,000 and \$30,000 on the black market.

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

1.2 Number of reported data breaches

Key finding: In 2013–14, the Office of the Australian Information Commissioner (OAIC) received a total of 71 data breach notifications, the highest number reported in five years. It must be emphasised that this figure relates to *total* data breaches, and does not reflect the number of data breaches that were identified by the OAIC as possibly involving identity crime. The increase in the numbers of data breaches reported to the OAIC could at least partly be attributed to the OAIC's introduction of voluntary data breach notification guidelines in 2012. However, in the absence of a compulsory requirement to report data breaches, it is reasonable to assume that the actual number of data breaches that take place in Australia each year is actually higher than the figures recorded by the OAIC.

In 2013–14, the OAIC received 71 data breach notifications (DBNs) including privacy complaints and contact with individuals or entities through the Enquiries line. This was a 16% increase on the number of data breaches reported to the OAIC in 2011–12, but does not necessarily indicate an increase in the *actual* number of data breaches in Australia. Rather, organisations may be becoming more likely to report such incidents to the OAIC following the development of new voluntary data breach reporting guidelines in 2012. However, it is reasonable to assume that data breaches reported to the OAIC are only a subset of the total number of incidents that occur.

Key finding: The OAIC identified 69 data breach notifications and 13 Commissioner-Initiated Investigations as possibly involving instances of identity crime or identity theft in 2013–14.

In 2013–14, the OAIC recorded a total of 71 data breach notifications and identified 69 as possibly involving instances of identity crime or identity theft. The remaining 2 DBNs were ruled out as not involving identity crime or identity theft. The OAIC also identified 13 Commissioner-Initiated Investigations (previously called Own Motion Investigations) as possibly involving identity crime in 2013–14.

In 2012–13, the OAIC handled 61 matters that may have involved identity crime or identity theft. Of those matters, 2 were specifically categorised as voluntary data breach reports, and the remaining 59 instances were brought to the OAIC’s attention as a result of privacy complaints, privacy Own Motion Investigations, and contact with individuals or entities through the Enquiries line.

The differences between the numbers of matters identified by the OAIC as possibly involving identity crime or identity theft in 2013–14 and 2012–13 can be explained by the fact that the OAIC changed the way that it collated its data for the 2013–14 report. In 2012–13, the OAIC focussed purely on National Privacy Principle (NPP) 4 and Information Privacy Principle (IPP) 4, as the most relevant to identity crime. However, for its data in 2013–14, the OAIC looked at a broader range of Australian Privacy Principles, IPPs and NPPs under which identity crime incidents may fall.

Accordingly, the identity crime related data provided by the OAIC for the Pilot Report and this report are not directly comparable. It should also be noted that the OAIC does not specifically collect data on ID crime; but rather, for the purposes of this report, searches for identity crime terminology in the complaints it receives under each APP or credit-related provision.

Key finding: Based on an independent analysis of a sample of data breaches that occurred in 2013–14, the 71 DBNs recorded by the OAIC could have resulted in over 1.4m records being compromised, and cost the organisations involved over \$205m.

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

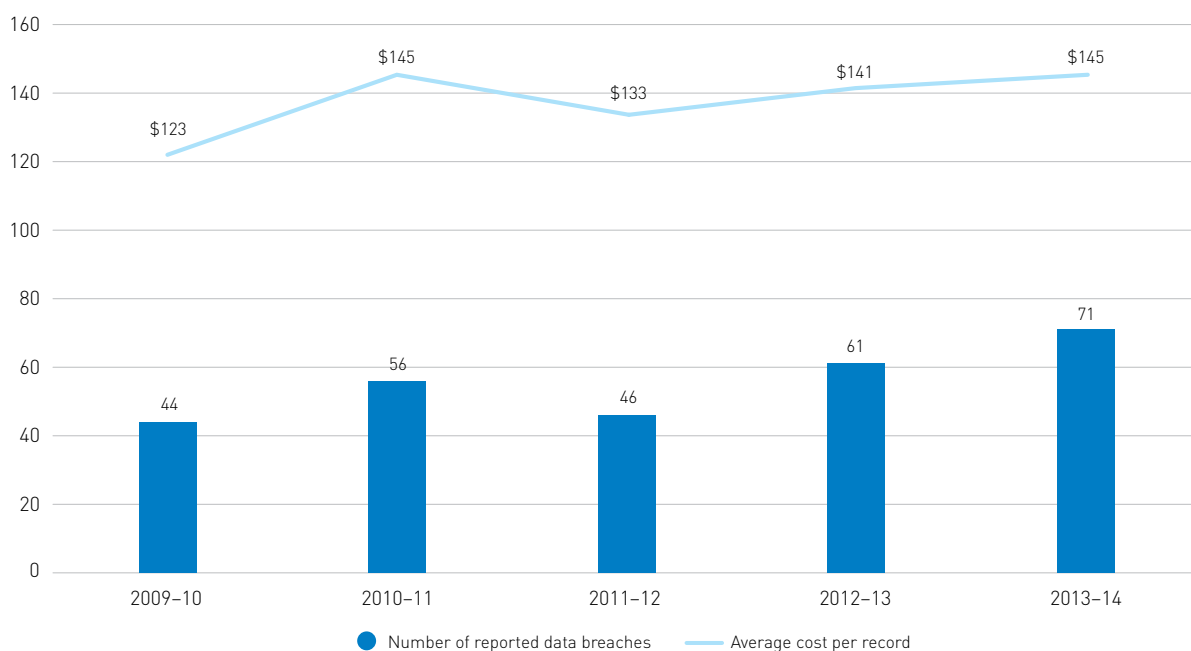
Research conducted by the Ponemon Institute over recent years provides some insight into the nature of data breaches experienced by Australian organisations. The 22 Australian data breaches examined by the Ponemon Institute in 2013–14 found that, when compared with 2012–13, these incidents involved increases in each of:

- the average number of records per incident (20,073)
- the average cost per record (\$145), and
- the total cost per incident (\$2.8m).

A comparison of the Ponemon Institute figures between 2009–10 and 2013–14 is illustrated in Figure 17 below.

Applying these figures to the 71 data breaches recorded by the OAIC in 2013–14, these incidents could have resulted in over 1.4m records being compromised and cost the organisations involved over \$205m.

Figure 17: Total number of data breaches recorded by the OAIC and the average cost per lost or stolen record, by year (2009–10 to 2013–14)



Source: Office of the Australian Information Commissioner Annual Reports, 2011, 2012, 2013 & 2014; Ponemon Institute 2012, 2013 & 2014.

Note: The numbers of data breaches illustrated in this figure represent the total numbers of data breaches recorded by the OAIC in its Annual Reports for the relevant financial years. They are not the numbers of data breaches that have been identified by the OAIC as possibly involving identity crime.

2. Use of fraudulent identities

Fraudulent identities can be used to facilitate a diverse range of illicit activities, from enabling an underage individual to gain access to an age-restricted venue, to more serious criminal activities such as drug trafficking, financial fraud, and terrorism. Whilst these crimes differ in terms of their levels of seriousness, they all rely on the use of fraudulent identities to deceive others and subsequently avoid detection (AFP 2014).

2.1 Number of identity crime incidents recorded by government agencies

Key finding: Identity crime is being experienced by agencies at both the Commonwealth and state/territory levels.

A total of 58 Commonwealth and state and territory agencies were invited to provide data for this report. Of these, 35 agencies were able to do so, including:

Commonwealth agencies

- Australian Federal Police
- Australian Securities and Investments Commission
- Australian Taxation Office
- Australian Transaction Reports and Analysis Centre
- Department of Defence
- 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 (n=4)
- Registries of Births, Deaths and Marriages (n=3)
- roads and traffic authorities (n=3)

Whilst the data report provides an incomplete picture of the total identity crime experienced by government agencies, it does give an indication of the breadth of portfolios impacted by identity crime.

Benefits Fraud

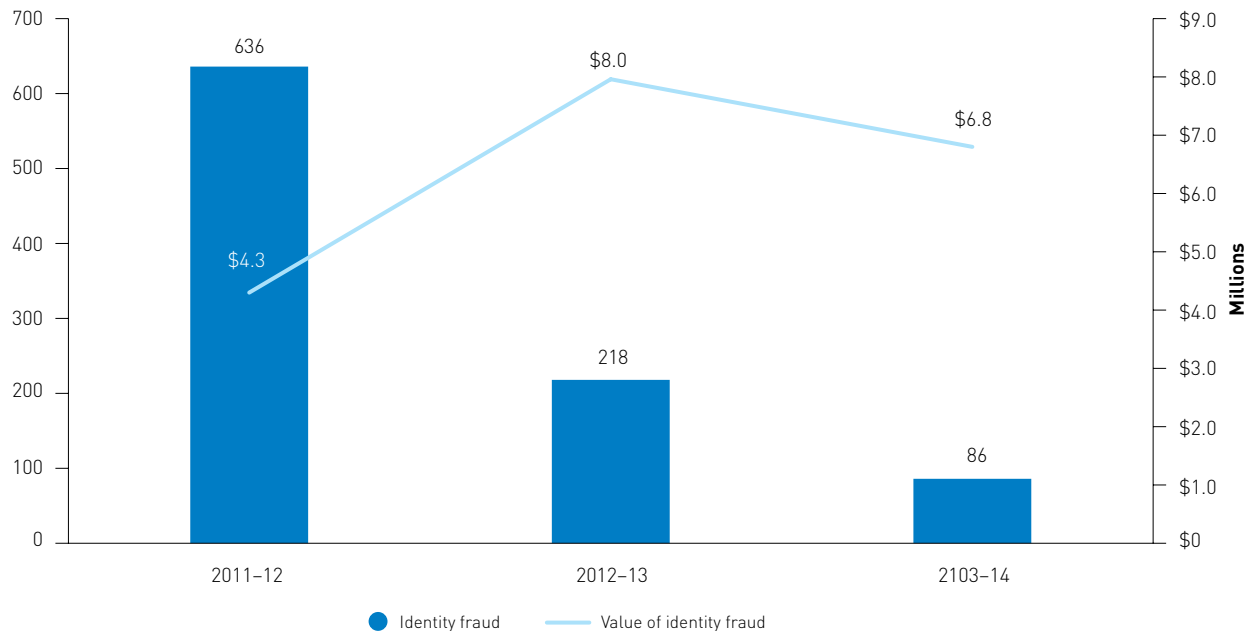
Key finding: There was an almost 60% reduction in the number of identity fraud-related investigations recorded by the Department of Human Services (DHS) between 2012–13 and 2013–14, with the value of these frauds decreasing by 15%. This may in part be attributed to DHS' focus on more complex fraud cases as well as a growing focus on preventative activities.

Fraudulent identities are often used to attempt to obtain benefits or payments from government agencies. Coinciding with the increasing use of technology by government agencies, and the focus on providing members of the public with the convenience of updating personal information and accessing government services quickly and easily on the Internet, a large proportion of revenue and benefits fraud is now committed online (Commonwealth Director of Public Prosecutions (CDPP) 2014).

The majority of data provided by DHS relates to Centrelink payments. There was a 60% decrease in the number of identity fraud investigations conducted by DHS in 2013–14 compared with 2012–13, continuing the substantial decline in the number of these investigations since 2011–12 (see Figure 18 below).

While DHS data also show decline in previous years, these are not directly comparable to more recent years' statistics. Following changes to recording practices made around 2011–12, DHS now records only those suspected frauds that are formally investigated or prosecuted.

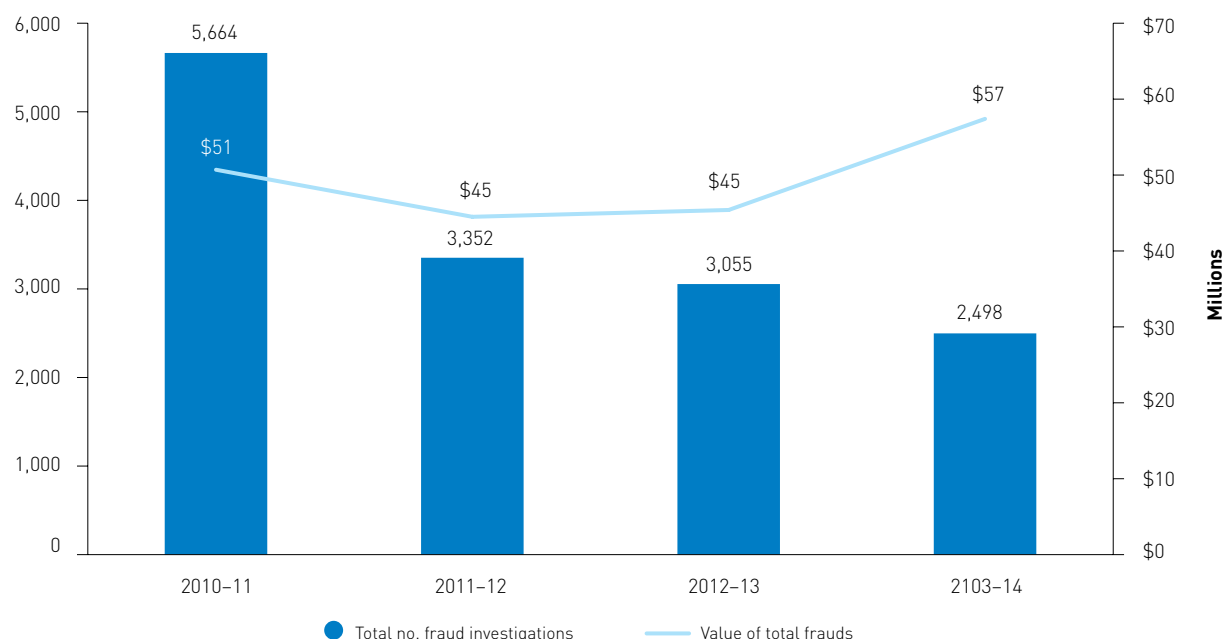
Figure 18: Total number of DHS identity fraud investigations and total value, by year, 2011–12 to 2013–14



Source: DHS Annual Reports 2011, 2012, 2013 and unpublished data.

There has also been a decline in the number of frauds reported by DHS (Centrelink) over recent years, with the total number of fraud investigations conducted reducing by 18% between 2012–13 and 2013–14, continuing the declining trend in the number of fraud investigations since 2010. While the total number of fraud investigations decreased in 2013–14, the total value of the frauds detected increased over 2012–13 and 2013–14 (see Figure 19).

Figure 19: Total number of DHS (Centrelink) fraud investigations and total value, by year, 2010–11 to 2013–14



Source: DHS unpublished data.

It should be noted that these figures do not relate to the number of investigations conducted in any of the years, but rather to the investigations finalised in those years. An investigation is finalised when a criminal prosecution is finalised; or the matter is closed and dealt with administratively, a process which takes less time.

Thus, the decline in the number of fraud investigations does not necessarily reflect diminished investigative effort (or a reduction in the number of fraud incidents), but rather may be an illustration of the length of time involved in taking more complex fraud investigations to resolution through the courts.

An increase in government funding to DHS was used to enhance specialised fraud investigation teams within the department. This has provided DHS with greater capacity to detect frauds sooner and before substantial debts can be accumulated. In addition, the agency's decision to focus on the most serious cases of non-compliance—eg those involving criminal intent—rather than on people who simply make mistakes—is likely to have contributed to a decline in the number of fraud investigations, and consequently, the number of matters prosecuted by the CDPP.

DHS expects to see a continuing decrease in the number of its fraud investigations—both general and identity-related fraud—as the agency's focus shifts increasingly to prevention. Significant investment in new technology will play a major role in reducing program leakage through fraud, with an anticipated ability to report on the number of confirmed preventions.

Case Study 2: 80 year old woman claims two pensions for 17 years

The defendant was 80 years old, and for 17 years claimed the Aged Pension using both her real name and a false name. As proof of identity to establish the false name, the offender used an extract from a birth entry that had been altered to show a different surname. Over the 17 years that she received the fraudulent pension payments, the offender obtained \$221,248.47 to which she was not entitled. In February 2013, she pleaded guilty to one count of defrauding the Commonwealth and one count of obtaining financial advantage by deception. She was sentenced to 4 years imprisonment with a non-parole period of 6 months.

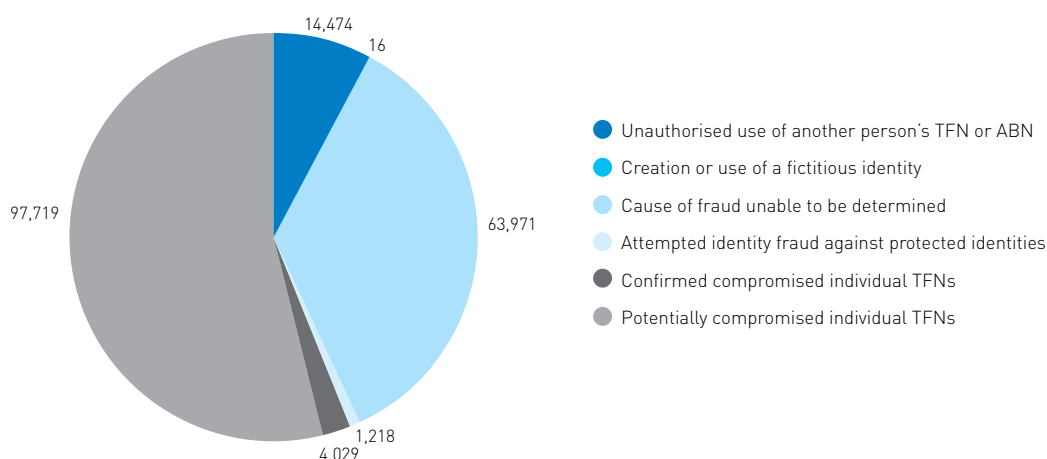
Source: The Commonwealth Director of Public Prosecutions, Case Report 2012–13. <http://www.cdpp.gov.au/case-reports/daphne-josephine-bargh-aka-smith/>

Taxation-related identity fraud

Key finding: Between 2012–13 and 2013–14 there was a 108% increase in the number of potentially compromised Tax File Numbers (TFNs) identified by the Australian Taxation Office, and a 10% decrease in the number of external fraud incidents detected by other organisations, which involved the unauthorised use of another person's TFN or Australian Business Number (ABN). While the increase in the number of potentially compromised TFNs may indicate an increase in fraud, it may also be attributable to improvements in the fraud detection practices of the ATO and other government agencies.

The ATO has greatly improved the way in which it manages and addresses identity crime and refund fraud in recent years, resulting in the detection of a considerable number of fraudulent and potentially fraudulent incidents (see Figure 20 below). This has been achieved by placing a greater emphasis on better protecting the ATO's business practices, enhancing its detection processes, improving its response to incidents, and further developing inter-government and community relationships (ATO 2014:60).

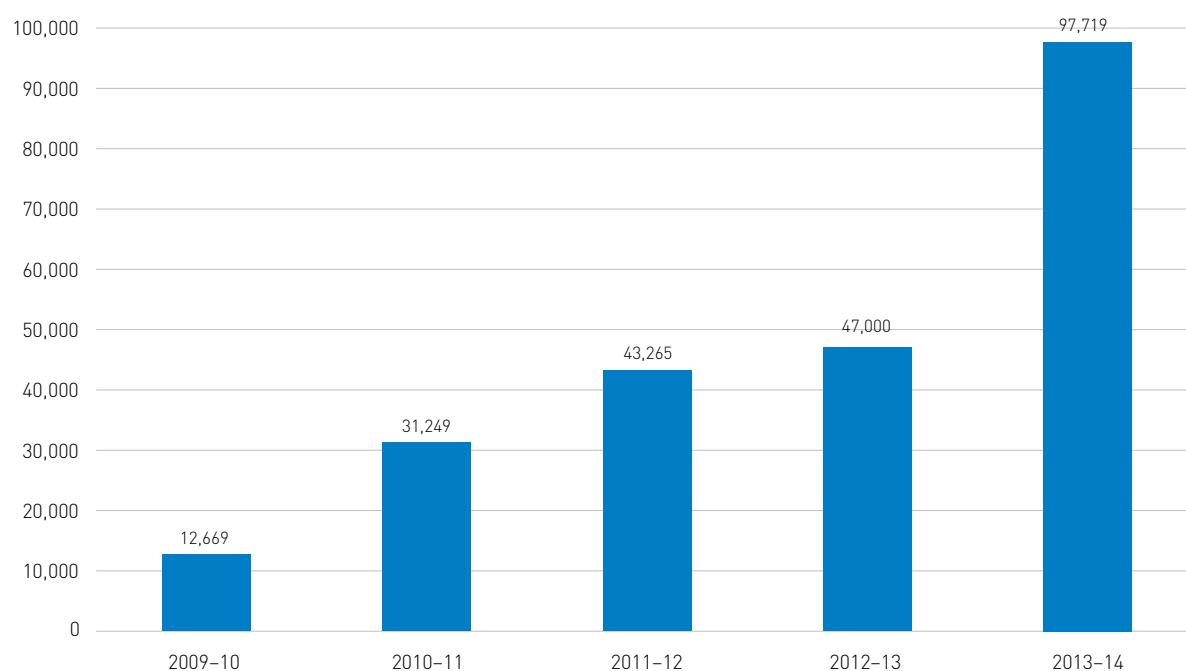
Figure 20: Number of fraudulent and potentially fraudulent incidents detected by ATO in 2013–14



Source: ATO unpublished data.

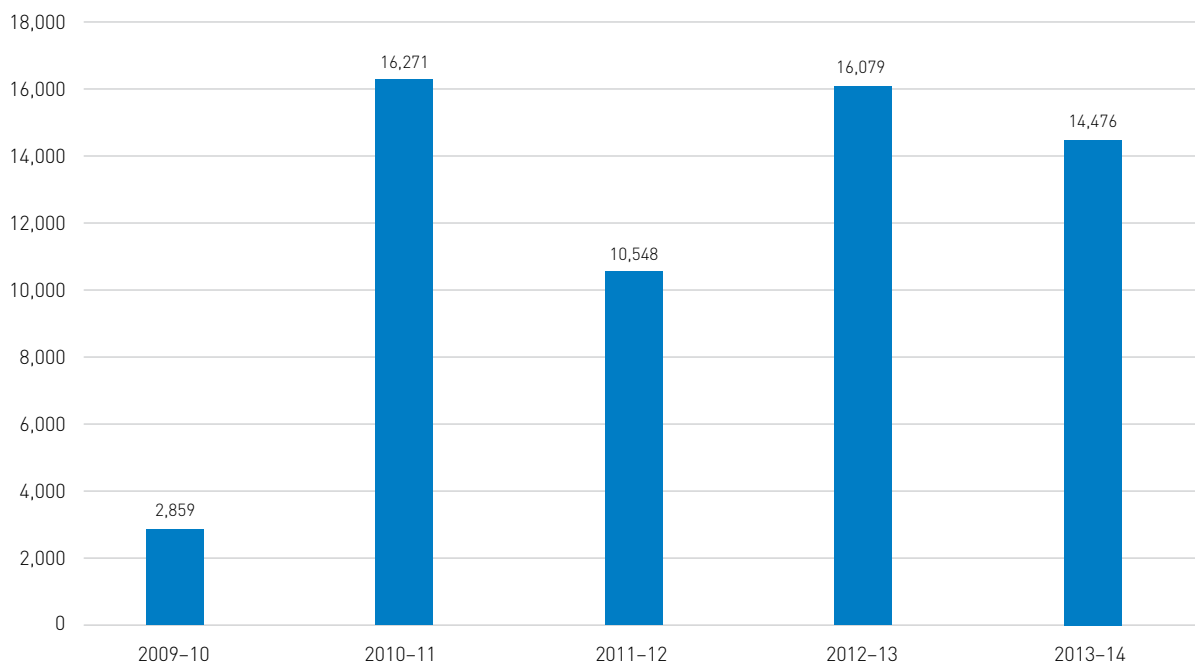
The number of TFNs that the ATO has identified as being potentially compromised has increased each year since 2009-2010, as illustrated in Figure 21 below. While the ATO's enhanced fraud detection processes may be responsible for these increased rates of detection, these figures appear to be consistent with a broader trend across Commonwealth agencies regarding unauthorised use of another person's TFN or ABN. Indeed, the AIC's *Fraud against the Commonwealth Annual Reports to Government* have also reported a substantial increase in the number of external fraud incidents involving the unauthorised use of another person's TFN or ABN across Commonwealth government agencies since 2009-2010 (see Figure 22). One reason for this increase may be the increased availability of this information online as individuals seek to complete their tax returns via the Internet, or the fact that some people save completed drafts of forms such as tax returns on unsecured home computers.

Figure 21: Number of potentially compromised individual TFNs identified by ATO



Source: Australian Taxation Office Annual Reports and unpublished data.

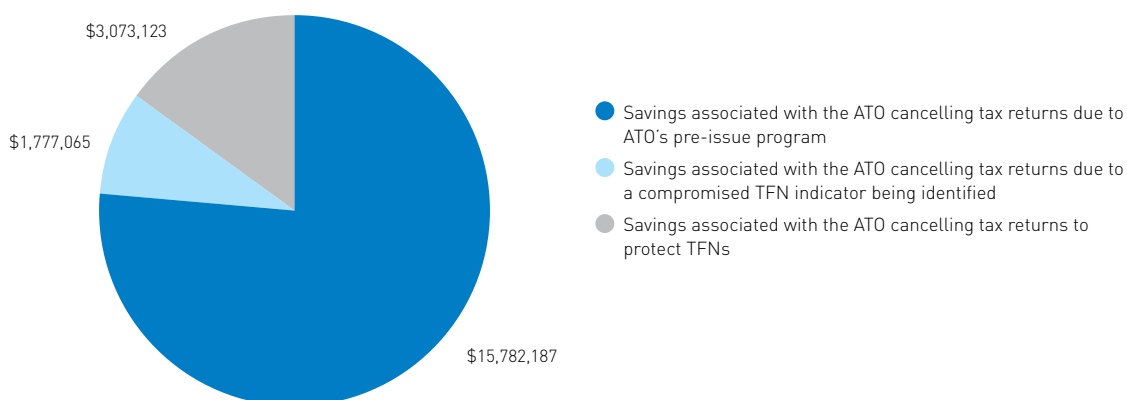
Figure 22: Number of external Commonwealth fraud incidents involving unauthorised use of another person's TFN or ABN



Source: Lindley J, Jorna P & Smith RG 2010; Jorna P & Smith R G forthcoming.

The costs associated with detected identity fraud incidents can be substantial. In 2013-14, the ATO saved approximately \$20m in protected revenue as a result of identity fraud protective measures (see Figure 23). Similar data for previous years was not obtainable prior to this report being published, so a comparison of how these savings may have changed over time could not be undertaken.

Figure 23: Protected revenue savings as a result of ATO identity fraud protective measures 2013-14



Source: ATO unpublished data.

Case Study 3:

Between 2004 and 2005, a registered tax agent who was an accountant and senior partner in an accounting firm, logged into the ATO Tax Agent Portal and electronically lodged 131 false Business Activity Statements (BAS) relating to 22 entities, many of whom were clients of the accounting firm where she worked. The BAS contained false information in relation to GST and Pay As You Go (PAYG) refunds. As a result of the defendant's conduct, the ATO generated \$1,820,939 in refunds which were then paid into accounts that the defendant controlled.

The defendant pleaded guilty to dishonestly obtaining a financial advantage by deception pursuant to section 134.2(1) of the *Criminal Code* (Cth), and in June 2013, was sentenced to 4 years imprisonment with a non-parole period of 2 years.

Source: The Commonwealth Director of Public Prosecutions, Case Report 2012–13. <http://www.cdpp.gov.au/case-reports/loukia-bariamis/>

Immigration-related identity fraud

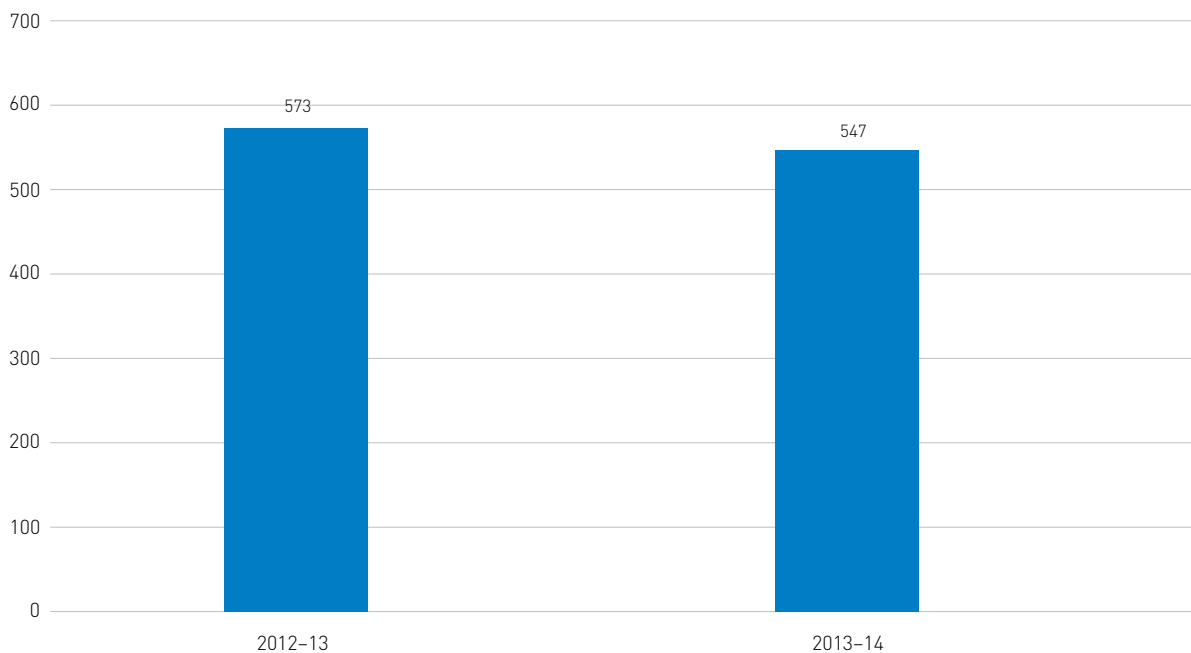
Key finding: The Department of Immigration and Border Protection (DIBP) recorded 547 allegations of possible immigration visa-related identity fraud in 2013–14, which is approximately 5% fewer than the number identified in 2012–13.

The Department of Immigration and Border Protection (DIBP) recorded 547 allegations of possible immigration visa-related identity fraud in 2013–14, which is around 5% less than the 573 potential visa-related identity frauds identified by the Department in 2012–13 (see Figure 24).

A number of policy initiatives have been implemented by the DIBP in an effort to better detect, and deal with, individuals who seek to use false or misleading information in an effort to obtain a visa. For instance, in March 2014, the *Migration Regulations 1994* were amended so that the Immigration Minister can now refuse to issue a visa in cases where he or she is not satisfied of the identity of the applicant. In 2013–14 there were nine cases of possible identity misuse under review, and four cases of this nature which were finalised.

The DIBP estimated that in 2013–14 the average cost of investigating and prosecuting detected identity crime incidents involving visa and migration offences was \$24,000 per incident.

Figure 24: Allegations of possible immigration visa-related identity fraud, 2012–13 and 2013–14



Source: DIBP unpublished data, AGD 2014b.

Case Study 4:

A 30 year old individual, who had initially entered Australia in 2002 under one identity, submitted a Protection Visa application that was subsequently refused. The individual left the country following this refusal. In October 2005, the same individual re-entered Australia as a dependent on his spouse's Student Visa. While this individual was in Australia, another person (related to the individual) submitted a Tourist Visa invited by an individual that was found to be the same name that the individual had previously used while entering Australia.

The individual was charged in connection with entering Australia on two separate identities. The individual received a conviction and was ordered to pay \$3,750 in court costs.

Source: Department of Immigration and Border Protection, unpublished.

Customs identity fraud

Key finding: In 2013–14, the Australian Customs and Border Protection Services (ACBPS) recorded approximately 158 allegations of identity crime, and referred 12 allegations of identity crime to the police. It detected four importations of 'Tier 2' prohibited goods in the form of blank credit cards.

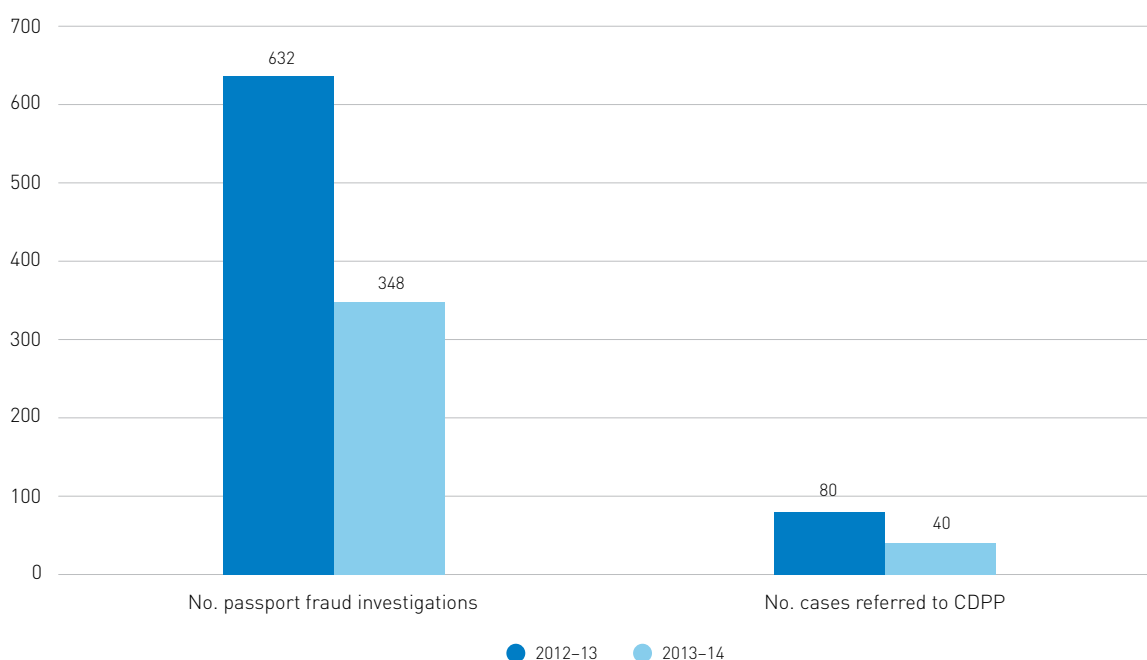
The ACBPS recorded 158 allegations of identity crime in 2013–14 and referred 12 allegations of identity crime to the police. It must be emphasised that these figures are only approximate as ACBPS does not categorise and record the results of goods and personal searches in a way that enables alleged incidents of 'identity crime' to be identified easily.

Passport identity fraud

Key finding: Between 2012–13 and 2013–14 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 increased slightly during this period.

DFAT recorded approximately 50% fewer investigations into allegations of passport fraud in 2013–14 compared with 2012–13 (see figure 25). This reduction may be explained by recent changes to the way that DFAT records passport fraud investigations. Specifically, instances of minor, non-identity-related passport fraud are no longer recorded as investigations.

Figure 25: Number of DFAT passport fraud investigations and referrals to CDPP



Source: DFAT Annual Reports, 2013, 2014.

Note: The 632 and 348 figures relate to investigations into allegations of passport fraud involving identity or application fraud or the improper use or possession of an Australian passport. They do not represent the number of purely identity crime related investigations conducted by DFAT.

There was a similar reduction in the number of passport fraud-related cases referred to the CDP for prosecution. Of the 40 cases referred to the CDP in 2013–14, 25 resulted in a conviction. These cases involved identity fraud, application fraud and improper use or possession of Australian passports (DFAT 2014:207).

Data provided by DFAT regarding the total number of investigations carried out in 2013–14 which were found to explicitly involve identity crime, indicated that fraudulently-obtained genuine passports were the most common type of identity-related passport fraud committed during 2013–14. The next most common type of passport fraud was the use of another person’s passport by imposters (ie individuals using a passport that has been issued in another person’s name, date of birth, and photo), passports which had been physically altered, and the electronic alteration or creation of an electronic copy of a passport biographic page. These data should not be confused with the data illustrated in Figure 25, which captures a broader range of investigations involving identity or application fraud or the improper use or possession of an Australian passport.

There were fewer identity frauds against passports detected by DFAT in 2013–14 compared with previous years (see Table 1). It must be noted that the fact that there has been a reduction in the number of detections by DFAT does not necessarily mean that the total numbers of incidents themselves are declining. It should also be noted that the year in which the passport fraud is detected is often not the year in which the passport fraud was first committed.

Table 1: Identity-related passport frauds, by year of fraud detection, 2010–11 to 2013–14

	2010–11	2011–12	2012–13	2013–14
Identity fraud against passport	128	113	50	43

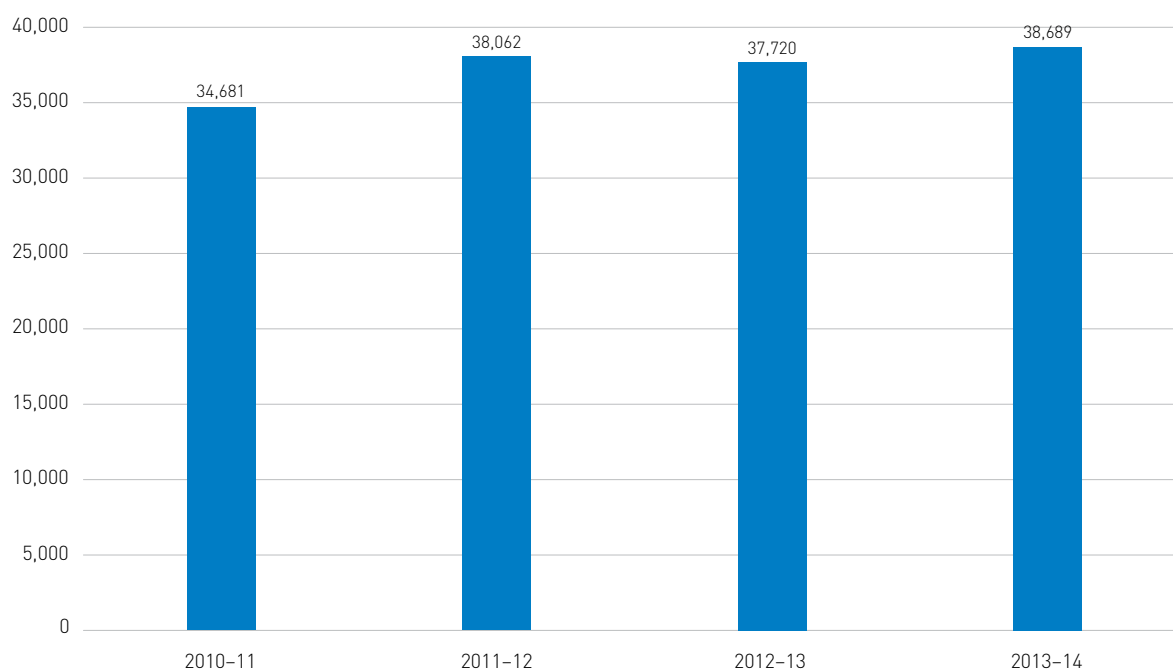
Source: DFAT—Australian Passport Office unpublished data.

Lost and stolen passports

Lost and stolen passports are a valuable source of personal information for criminals. Given how valuable this type of identity credential is on the black market, and the possibility that it will be used in the facilitation of more serious criminal activities, DFAT has procedures in place to deal with lost and stolen passports quickly.

In 2013–14, some 38,689 Australian passports were reported as lost or stolen—a relatively small increase over the figures for the last few years (see Figure 26). As a percentage of passports issued in the year, the rate of passports reported lost or stolen remains stable. According to DFAT’s 2013–14 Annual Report, this is consistent with the annual rate of increase since the 2005 introduction of fees for lost and stolen passports.

Figure 26: Number of passports lost and stolen, by year, 2010–11 to 2013–14



Source: DFAT Annual Reports, 2013–14, 2012–13, 2011–12.

Identity fraud detected by Registries of Births, Deaths and Marriages (RBDM)

Key finding: The number of registry certificates reported as lost, stolen or fraudulent in Victoria was significantly higher than the other two jurisdictions that were able to provide data. This can be attributed to differences in the RBDMs' data collection methods, which are explained in greater detail below.

Registries of Births, Deaths and Marriages (RBDMs) play a critical role in establishing the identities of persons born in Australia, recording registered changes of name, registering marriages and other significant relationships which can also lead to a person changing their name, and registering a person's death. 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 state and territory RBDMs was asked to provide data for this report, only three were able to do so (New South Wales, South Australia and Victoria) (see Table 2).

Table 2: Crime and misuse associated with certificates issued by RBDMs in 2013–14

RBDM Name	Lost	Stolen	Unauthorised change	Fraudulent	Referred to police
NSW RBDM					
Birth Certificate	10	26	24	0	12
Death Certificate	0	0	0	0	0
Marriage Certificate	1	2	0	0	2
Change of name	0	2	0	0	1
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
VIC RBDM					
Birth Certificate	6660	121	4	5	0
Death Certificate	237	2	0	0	0
Marriage Certificate	1050	23	0	0	0
Change of name	7	0	0	0	0

Source: Unpublished data from NSW, SA and Victoria RBDMs.

As can be seen in Table 2, the Victorian RBDM recorded a considerably larger number of lost or stolen certificates than the other two RBDMs that provided data. This was due to differences in the ways that the RBDMs collected their data for this report. 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. Further, the Registry does not refer allegations by applicants of stolen certificates to police.

The NSW RBDM's data differed from that of the Victorian RBDM because it was based on the numbers of lost, stolen and fraudulent certificates that have been referred to the NSW RBDM's Identity Security Division, or identified through the NSW RBDM's certificate validation service, CertValid.

It is difficult to determine whether the small number of stolen or fraudulent certificates recorded by these three RBDMs is representative of the number recorded in other states and territories. However, the price of fraudulent birth certificates on the black market would appear to suggest that these documents are more widely available than figures otherwise indicate.

One of the reasons that could be attributed to this is a lack of information-sharing between the organisations which detect suspected fraudulent certificates, and the RBDMs which issued those certificates. It is possible that agencies which identify suspected fraudulent certificates do not think to inform the relevant RBDM of their suspicions. Fraudulent certificates could also be more easily detected by increasing the number of organisations, across both the public and private sectors, which routinely verify information on birth certificates with the issuing RBDM through systems such as the DVS and CertValid—including the RBDMs themselves.

Driver licence fraud

Key finding: A number of the road transport and licensing agencies which provided data for this report indicated that they had identified a small number of identity crime incidents involving driver licences during 2013–14. 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. Indeed, the independent iDcare support service for victims of identity crime has found driver licences to be the most targeted source of personal information associated with identity crime.

Driver licences are the most commonly issued photographic credential relied upon as evidence of an individual's identity. Accordingly, they are considered a valuable source of information for criminals seeking to steal a person's identity or fabricate a new identity—particularly as they contain a photograph of the holder.

While each of the eight state and territory road agencies was asked to provide data for this report, only two were able to do so (Queensland and Western Australia).

The Queensland Department of Transport and Main Roads (QLD DTMR) identified a number of identity fraud incidents in relation to driver licences during the reporting period, each of which was referred to police. The QLD DTMR requested that further details of these data remain confidential.

The Western Australia Department of Transport (WA DoT) detected 30 suspected identity fraud incidents involving WA driver licences in 2013–14. Sixteen of these incidents were referred to police. In terms of the direct staffing costs associated with the facial recognition process alone, the estimated cost to WA DoT for dealing with these incidents was around \$275,000. The information provided above suggests that there may be only a relatively small number of cases of identity-related fraud detected by road agencies nationally, particularly when compared with the total number of driver licences in Australia.

This may indicate that road agencies need to improve processes for receiving and recording suspected cases of identity crime involving driver licences that are detected by other organisations which rely on these credentials as evidence of a person's identity.

Case Study 5:

In late 2013 a casual employee of the Queensland Department of Transport and Main Roads (DTMR) allegedly used her knowledge of the issuing processes to override internal control mechanisms and issue more than 60 genuine driver licences with false details, in return for cash payments of up to \$1,000 per licence.

Following an investigation by the Crime and Corruption Commission (CCC), a 30 year old man and 25 year old woman were identified as allegedly organising cash payments from their friends and associates to the DTMR employee who then fraudulently issued 57 new licences or licence upgrades between November 2012 and December 2013.

The CCC said all the licences issued were in people's real names. However, their licence categories were upgraded to allow them to drive vehicles including trucks and boats. The CCC alleged that each of the fraudulent deals was worth between \$150 and \$1,500.

The woman faces corruption charges that carry a maximum term of imprisonment of seven years.

Forty-two people who allegedly received the illegal licences have already been charged.

Sources: <http://www.news.com.au/national/fake-queensland-drivers-licences-being-investigated-by-crime-commission-amid-terror-identity-fears/story-fncynjr2-1227065858086> and <http://www.ccc.qld.gov.au/news-and-media/ccc-media-releases/ccc-makes-official-corruption-and-fraud-arrests-in-driver-licence-investigation-2014-18.12.2014>.

<http://www.smh.com.au/queensland/former-queensland-transport-worker-allegedly-ran-fake-licence-scam-20150218-13i1ej.html>

Conveyancing identity fraud

Legal practitioners, conveyancers and mortgage lenders are expected to take reasonable steps to verify the identities of the parties involved in conveyancing transactions. Notwithstanding this, in recent years, there have been cases where properties have been sold by criminals using fraudulent identity documents. There have also been cases of mortgage brokers using fraudulent documents to obtain loans for their clients for amounts that those clients would not ordinarily be approved to borrow.

It is unclear how many incidents of conveyancing-related identity fraud take place each year, as little quantitative data exist. However, when it does occur, there can be serious ramifications for both the unsuspecting buyer, who may unknowingly purchase the property from the offenders, as well as the person who legally owns the property.

Case Study 6:

A Canberra property owner living in South Africa discovered that her home had been sold by overseas identity fraudsters when she called her property manager to ask why rental payments were no longer being made.

ACT Policing and the Office of Regulatory Services are currently investigating the series of exchanges between the overseas identity fraudsters and a Canberra real estate agent which led to the property being sold and funds disbursed to South Africa.

The new property owners were not aware that they had bought the property from international scammers, but would likely be entitled to keep the house as the title had been legally transferred and they were now the registered proprietors.

It is unlikely that the original property owner will be able to get the house back, but may be able to claim damages.

Source: The Canberra Times, 23 & 24 July 2014.

<http://www.canberratimes.com.au/act-news/police-probe-macgregor-property-scam-20140723-zvers.html>

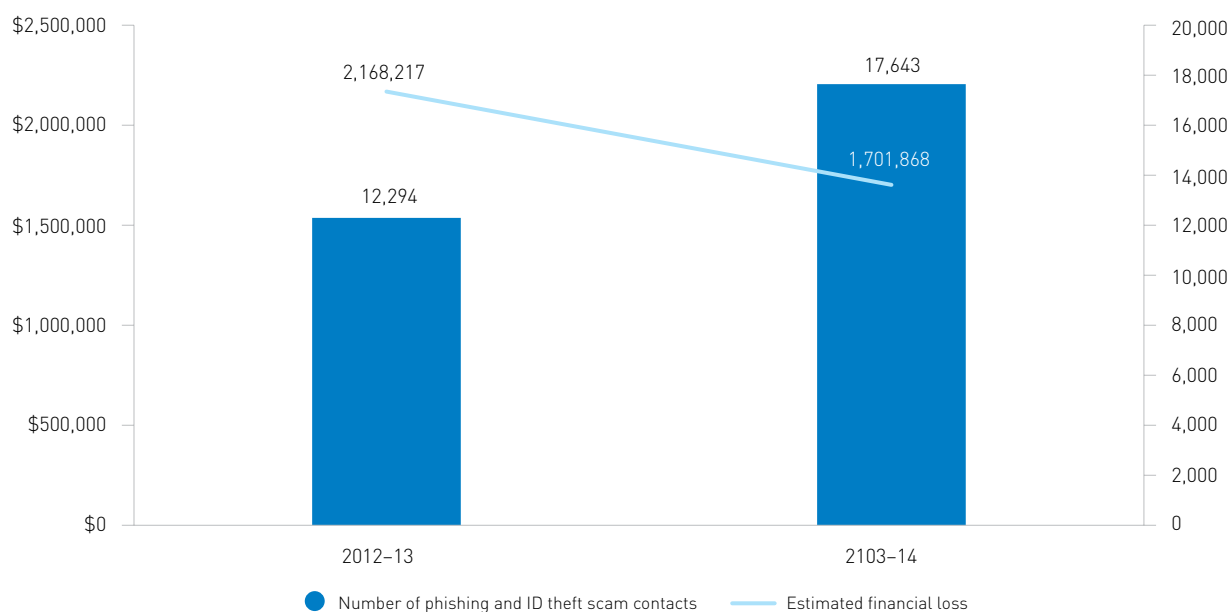
<http://www.canberratimes.com.au/act-news/new-owners-didnt-know-they-bought-a-house-sold-by-scammer-20140723-zw1p9.html>

Consumer identity fraud

Key finding: Between 2012–13 and 2013–14 the number of phishing and identity theft incidents recorded by the Australian Competition and Consumer Commission (ACCC) increased by 44%, while the reported losses decreased by 22% to just over \$ 1.7m.

In 2013–14, the Australian Competition and Consumer Commission (ACCC) received 12,294 phishing and identity theft related contacts, with estimated reported losses amounting to just over \$1.7m (see Figure 27). This is a 44% increase on the number of phishing and identity theft incidents reported to the ACCC in 2012–13. Interestingly however, the value of the estimated reported losses associated with phishing and identity theft actually decreased by 22% in 2013–14, down from just over \$2.1m in 2012–13. The ACCC has suggested that this decrease may be attributed to a greater focus by offenders on obtaining personal information from victims, which could then be used to facilitate other, more serious criminal activities [ACCC 2014: 12].

Figure 27: Number of phishing and identity theft contacts recorded by ACCC, 2012–13 & 2013–14



Source: ACCC unpublished data.

Identity fraud incidents detected by police

Key finding: Police agencies recorded 126,305 fraud and deception offences in 2013–14. Up to 40%, or just over 50,000 of these offences, involved identity crime. This is higher than the 30,000 identity crimes that were estimated to have been detected by police agencies in the Pilot Report. The difference in figures is due to the availability of more complete fraud and deception offence data for the 2013–14 report.

In the Pilot Report, only Queensland Police provided data regarding the number of identity crime offences they had dealt with in the preceding 12 months. For this report, the Australian Federal Police (AFP), West Australia Police, Victoria Police, Queensland Police and ACT Policing provided data. Figures illustrating the state and territory police data can be found in Appendix A.

The nature of identity offences differs between Australian jurisdictions. Some states such as Queensland, South Australia, New South Wales, Western Australia and Victoria, have introduced specific identity crime provisions into their criminal statutes. Other jurisdictions, such as the Australian Capital Territory (ACT) and Tasmania, appear to continue to rely on more general deception and dishonesty offences to capture identity crimes, thus making inter-jurisdictional comparisons difficult.

The manner in which identity-related offences are reported also differs between jurisdictions. Police data systems record crimes using the Australian Bureau of Statistics (ABS) standard offence classification codes, known as the *Australian and New Zealand Standard Offence Classification (ANZSOC) 2011* (ABS, 2011), whereby specific codes apply to crimes such as fraud, deception and forgery.

However, there are no codes for identity-related crimes, which mean identity crimes are often recorded under more general crime categories like fraud. Accordingly, and as noted in the Pilot Report, it was not possible to identify the exact number of fraud and deception offences recorded by all police agencies that were identity crimes.

Notwithstanding these difficulties, the actual number of fraud and deception offences recorded by each of the state and territory police agencies in 2013–14 was obtained, with the total number of offences amounting to 126,305 (BOCSAR 2014; WA Police 2014; Dept. Police and Emergency Management 2014; SA Police 2014; Vic Police 2014; NT Police, Fire and Emergency Services 2014; unpublished data from ACT Policing and QLD Police). This is more than double the estimated figure for national fraud offences (58,851 frauds) used in the Pilot Report.

For the purposes of this report, it has been estimated that up to 40% of police-recorded fraud and deception offences involve identity crime. This estimate is based on discussions with experts in this area, and recent observations by the United Kingdom's Credit Industry Fraud Avoidance Service (CIFAS) which found that 41% of all frauds recorded by CIFAS in 2014 involved instances of identity fraud (CIFAS 2015).

Accordingly, if it is assumed that up to 40% of the national fraud and deception offence figure outlined above (126,305 offences) involved identity crime, it is possible that there were just over 50,000 identity crimes detected by police in Australia in 2013–14. This is higher than the 30,000 identity crimes that were estimated to have been detected by state and territory police agencies in the Pilot Report. This difference can be attributed to the availability of more complete fraud offence data for the 2013–14 report. It should also be noted that this estimate may not capture all the identity crimes committed in Australia each year, given that false and stolen identities can be used to facilitate a number of criminal activities apart from fraud.

Australian Cybercrime Online Reporting Network (ACORN)

Police and other relevant agencies also now receive reports of identity crime via the Australian Cybercrime Online Reporting Network (ACORN). Launched in November 2014, the 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. Data from the ACORN may provide useful insights into the types of identity crimes being experienced by the Australian public in future versions of this report.

2.2 Prosecutions involving identity crime and other related offences

Commonwealth prosecutions

Key finding: There continued to be a decline in the number of identity crime prosecutions by the CDPP, which fell by around 10% between 2012–13 and 2013–14. However, this does not necessarily indicate a reduction in the number of offences, as it also reflects changes in the ways that agencies manage less complex cases.

There are several Commonwealth statutes that contain provisions relating to identity crime and fraud, upon which the CDPP can rely for prosecuting criminals who offend in this way. 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)*.

The total number of identity crime prosecutions conducted by the CDPP fell by around 10% between 2012–13 and 2013–14 (see Table 3). As noted earlier, one factor in the reduction in such prosecutions is the decision by some agencies such as DHS (Centrelink) to focus on referring only the most serious prosecution matters.

The fraudulent conduct offences under Divisions 133–137 of the Criminal Code were the most common identity-related offences prosecuted by the CDPP in 2013–14, with approximately 94% of Commonwealth defendants prosecuted for identity or fraud related offences in 2013–14 charged under these Criminal Code provisions. This is consistent with prosecution data provided by the CDPP for the Pilot Report.

Table 3: Total number of defendants prosecuted by the CDPP by Act and Year (2010–11—2013–14)

Offence	2010–11	2011–12	2012–13	2013–14
Divisions 370, 372, 375 <i>Criminal Code</i> —Identity Crime	0	0	1	3
Divisions 133–137 <i>Criminal Code</i> —Fraudulent Conduct	3215	1796	1458	1313
Divisions 144–145 <i>Criminal Code</i> —Forgery	31	19	24	19
Division 480 <i>Criminal Code</i> —Financial information offences	12	10	9	3
Section 234 <i>Migration Act 1958</i> —False documents	17	16	29	10
<i>AMLCTF Act 2006</i> sections 135–138	3	4	2	7
Section 24, <i>Financial Transactions Report Act 1988</i> —Opening account etc in false name	10	7	9	3
Part XII <i>Customs Act 1901</i> —Penal provisions (s.233BAB)	16	7	13	38
Part 14 <i>Trademarks Act 1995</i> —ss.146–148	8	10	9	4
Total	3312	1869	1554	1400

Note: 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 and 1397 unique defendants prosecuted in 2010–11, 2011–12, 2012–13 and 2013–14 respectively.

Source—CDPP unpublished data.

Note: Data as at 10 December 2014.

Note: Fraudulent Conduct—Division 133-137 *Criminal Code Act 1995*

- Div. 134—Obtaining property or a financial advantage by deception
- Div. 135—Other offences involving fraudulent conduct
- Div. 136—False or misleading statements in applications
- Div. 137—False or misleading information or documents

There were only three prosecutions using the identity crime offences in Divisions 370, 372 and 375 of the Criminal Code in 2013–14. Whilst this is two more than the number of offences prosecuted under these provisions in 2012–13, these are still some of the identity-related offences least used by the CDPP.

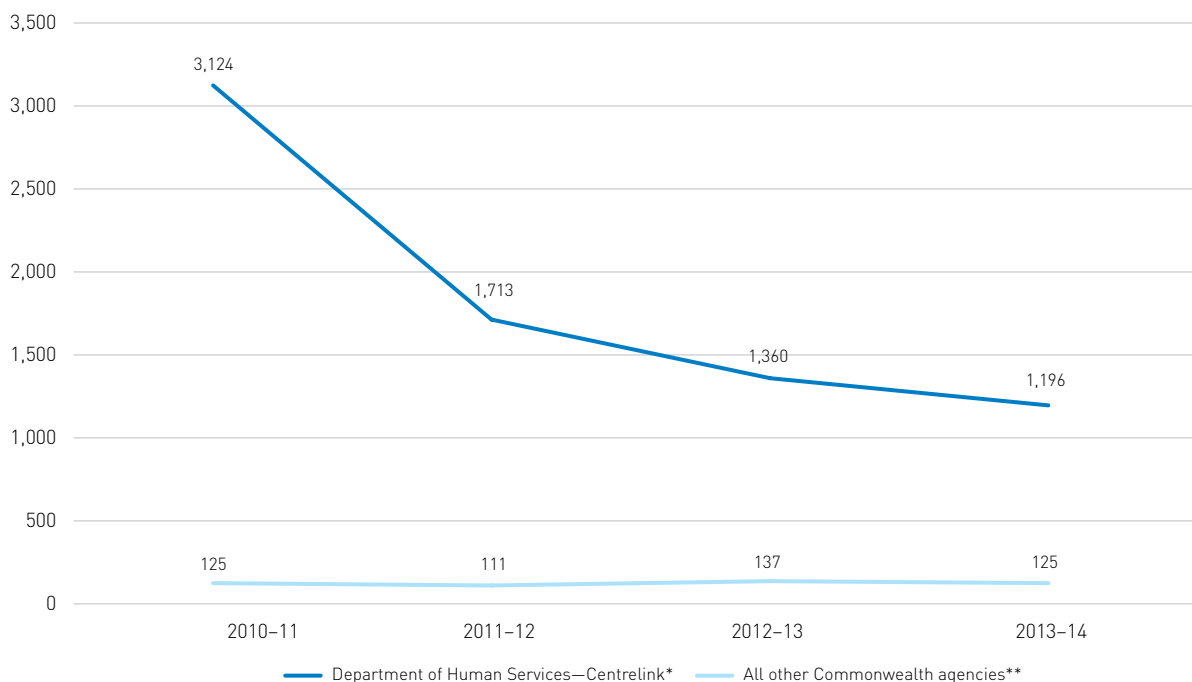
The lack of prosecutions under these provisions may be attributed to a number of factors. First, prosecutors may prefer to prosecute offenders for the more serious crimes that their identity offences facilitate. Data obtained from Australian law enforcement agencies would tend to support this idea, with many identity criminals being prosecuted for offences which are enabled through the use of a stolen or fraudulent identity, rather than for the offences of actually possessing or using the stolen identity information in the first place. Other reasons that may explain the small number of prosecutions under these provisions could be difficulties in actually apprehending identity criminals, and then proving the necessary elements of the identity crime offences to the standard of proof necessary to result in the defendant being found guilty.

The CDPP is able to prosecute offenders after receiving referrals from Commonwealth agencies or the AFP. Since 2010–11, DHS (Centrelink) has consistently referred the highest number of fraudulent conduct offences to the CDPP for prosecution (see Figure 27). This trend continued in 2013–14, with DHS (Centrelink) cases still representing over 90% of all referrals for Commonwealth prosecutions for fraudulent conduct.

The number of matters referred to the CDPP by DHS (Centrelink) has substantially decreased since 2010–11. Whilst it is possible that the decline is due to a decrease in the number of frauds being carried out, it may be attributed to the decision by DHS (Centrelink) to focus on only referring the most serious cases of non-compliance, such as those involving criminal intent, rather than cases involving inadvertent error (DHS 2014).

There were only 125 referrals for fraudulent conduct made by all other Commonwealth agencies in 2013–14. This is broadly consistent with CDPP data since 2010–11, with the total number of referrals for fraudulent conduct by all Commonwealth agencies remaining relatively stable over the last four years (see Figure 28).

Figure 28: Total number of CDDP prosecutions for fraudulent conduct, by referring agency, 2010–11 to 2013–14



Source: * CDDP unpublished data.

** Unpublished data from CDDP (excludes State and Territory Police referrals and International Police (retired) categories)

State and territory identity crime prosecutions

Key finding: There were almost 26,000 offences proven in state and territory courts in 2012–13 which may have been related to identity crimes. These were comprised of approximately 17,000 offences which were possibly enabled by the use of stolen or fabricated identities, and approximately 9,000 ‘core’ identity crime offences such as forgery, making false representations and possessing equipment to manufacture fraudulent credentials.

Based on customised data provided by the Australian Bureau of Statistics (ABS), it is estimated that there were almost 26,000 forgery and fraud and deception offences proven in state and territory courts in 2012–13, which may have been related to identity crimes. This is slightly higher than the 22,000 offences estimated in 2011–12 (AGD 2014b: 40).

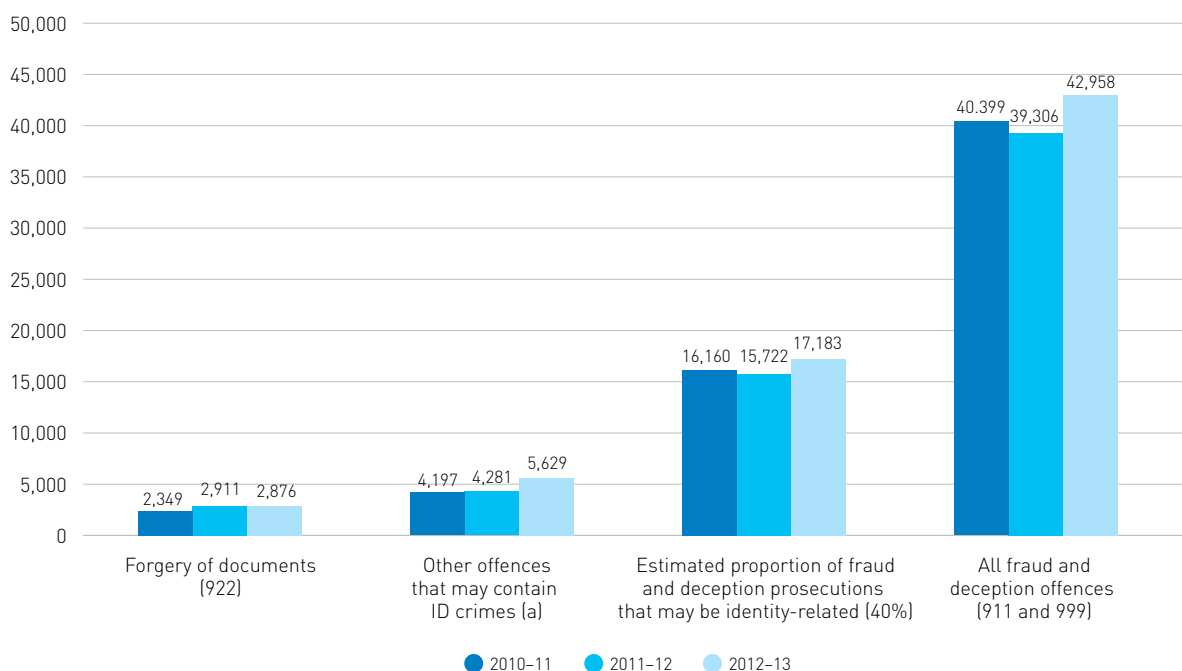
Figures for 2012–13 have been used, as ABS data for 2013–14 was unavailable. It must be emphasised that the data provided by the ABS do not represent a count of ‘identity crime’ offences per se. Rather, they are offences with specific combinations of legislation and offence codes which may be more likely to be related to identity crimes. Nor do these figures include the numbers of fraud offences reported to police. They are simply the number of ANZSOC fraud offences finalised by the courts.

As noted in the Pilot Report, quantifying the true number of identity crimes proven in state and territory courts requires a count of the 'core' identity crime offences such as forgery and impersonation, combined with an estimation of the number of identity-related fraud and deception offences.

While the methodology used in this report to obtain the estimated number of state and territory court proven identity crime-related offences is the same as that used in the Pilot Report, the estimated percentage of fraud offences that are identity related has been increased to 40% for this report, compared with 37.5% in the Pilot Report. This is based on information from the United Kingdom's CIFAS, which indicated that 41% of all frauds recorded in the UK in 2014 were identity related (CIFAS 2015). It is also consistent with the estimate used in this report in relation to the number of police-recorded fraud offences that may have been identity-related.

Based on the data illustrated in Figure 29 below, it is estimated that of the approximately 43,000 fraud and deception offences proven in state and territory courts in 2012–13, around 17,000 offences, or 40%, were possibly enabled by the use of stolen or fabricated identities. In addition, there were also approximately 9,000 'core' identity crime offences such as forgery and making false representations and possessing equipment to manufacture fraudulent credentials, proven in 2012–13.

Figure 29: Number of offences proven in all state and territory courts that may have involved identity crimes, by offence category and year 2010–11 to 2012–13



Source: Based on ABS Customised Report Data 2014, 2015.

[a] = Includes offences coded under the following ANZSOC codes: 829, 831, 923, 931, 932, 933, 991, 1111, 1542, 1543, 1559, 1612, and 1694

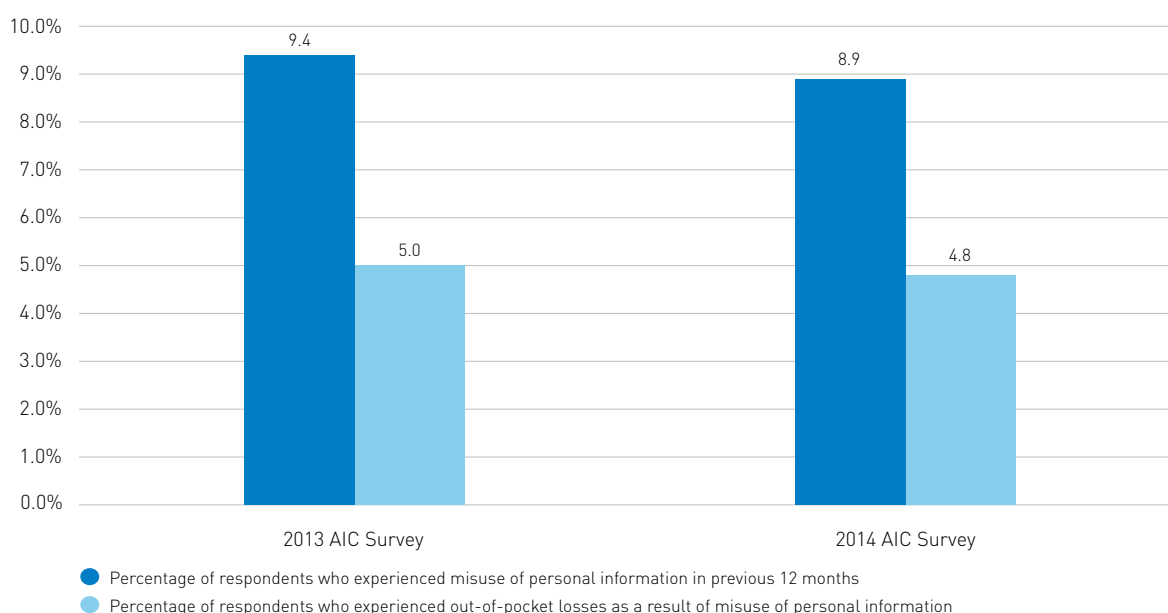
2.3 Number of people who self-report being victims of identity crime or misuse

Key finding: Identity crime continues to be one of the most prevalent crimes in Australia. The AIC's 2013 and 2014 Identity Crime and Misuse Surveys conducted for this report found that around 9% of all respondents experienced some form of misuse of their personal information in the previous 12 months, with around 5% of all respondents incurring out-of-pocket losses as a result of this misuse.

A 5,000 person online community survey conducted by the AIC for this report found that identity crime continues to be experienced by many Australians. Of those people surveyed, 8.9% reported experiencing identity crime or misuse in the previous 12 months. This is slightly less than the corresponding 9.4% figure in the survey conducted for the previous report. This difference is not statistically significant.

The 2014 Survey also found that 4.8% of all respondents reported incurring out-of-pocket losses as a result of misuse of their personal information, compared with 5% of all respondents in the 2013 Survey (see Figure 30 below).

Figure 30: Percentage of respondents in 2013 and 2014 AIC Surveys who experienced misuse of personal information and out-of-pocket losses

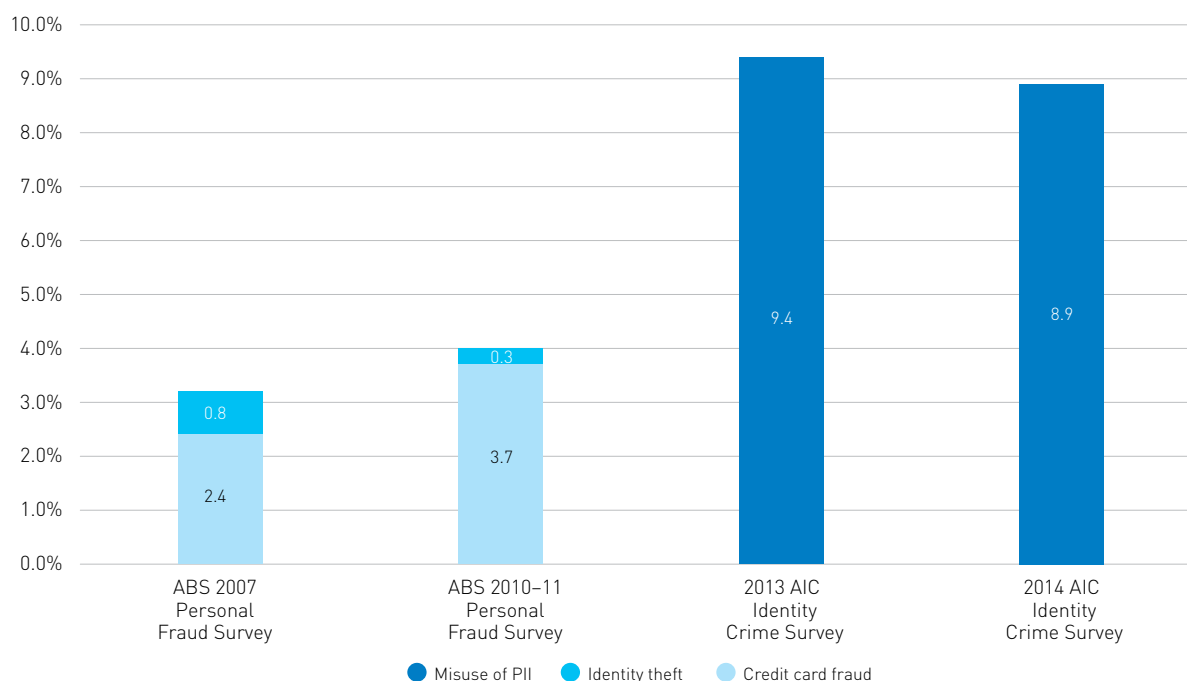


Source: 2013 and 2014 AIC Surveys.

The prevalence findings from the Surveys are higher than the percentage of people who reported experiencing identity crime in the ABS' 2007 and 2010-11 Personal Fraud Surveys which found that identity crime impacts around 4% of people each year (see Figure 31 below).

The AIC's findings regarding the numbers of people who experienced out-of-pocket losses also differed from those obtained by the ABS' 2010-11 Personal Fraud Survey, where approximately 27% of all victims of identity theft in the previous five years had incurred financial losses.

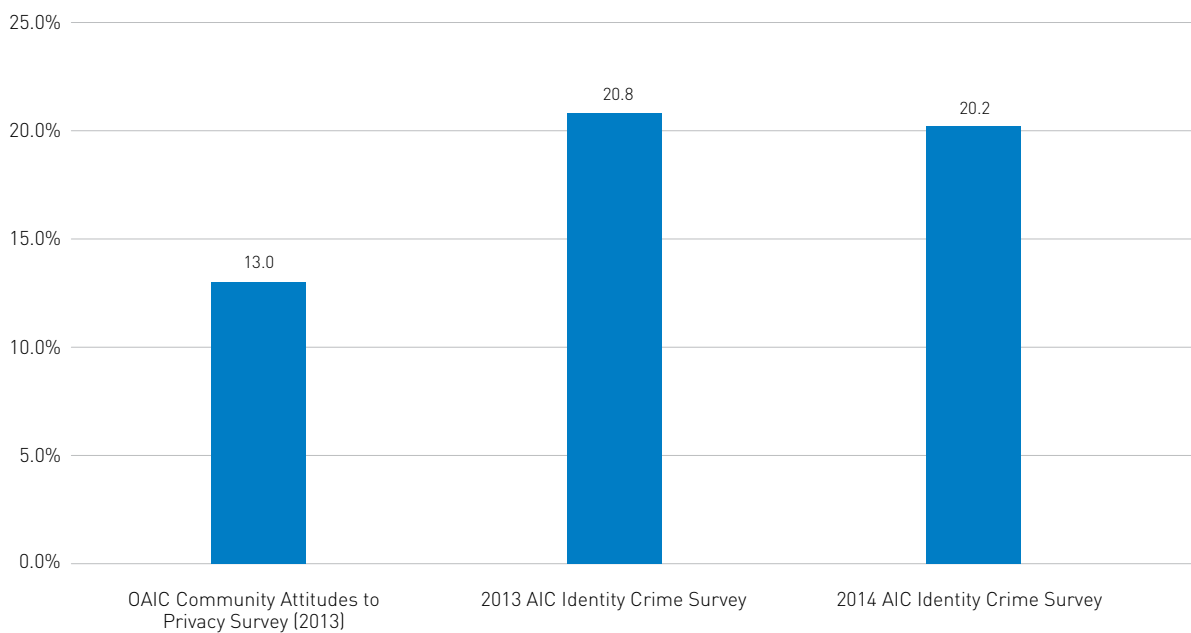
Figure 31: Proportion of respondents reporting identity crime victimisation or misuse of personal information, by survey and year



Source: 2013 and 2014 AIC Surveys.

The 2014 AIC Survey also found that 20.2% of respondents had experienced misuse of their identity at some time in the past (compared with 20.7% in the previous survey). These results are higher than the 13% of respondents in the OAIC survey in 2013 who identified as having ever fallen victim to identity fraud or theft (see Figure 32).

Figure 32: Proportion of survey respondents reporting having ever been a victim of identity theft or misuse, by survey

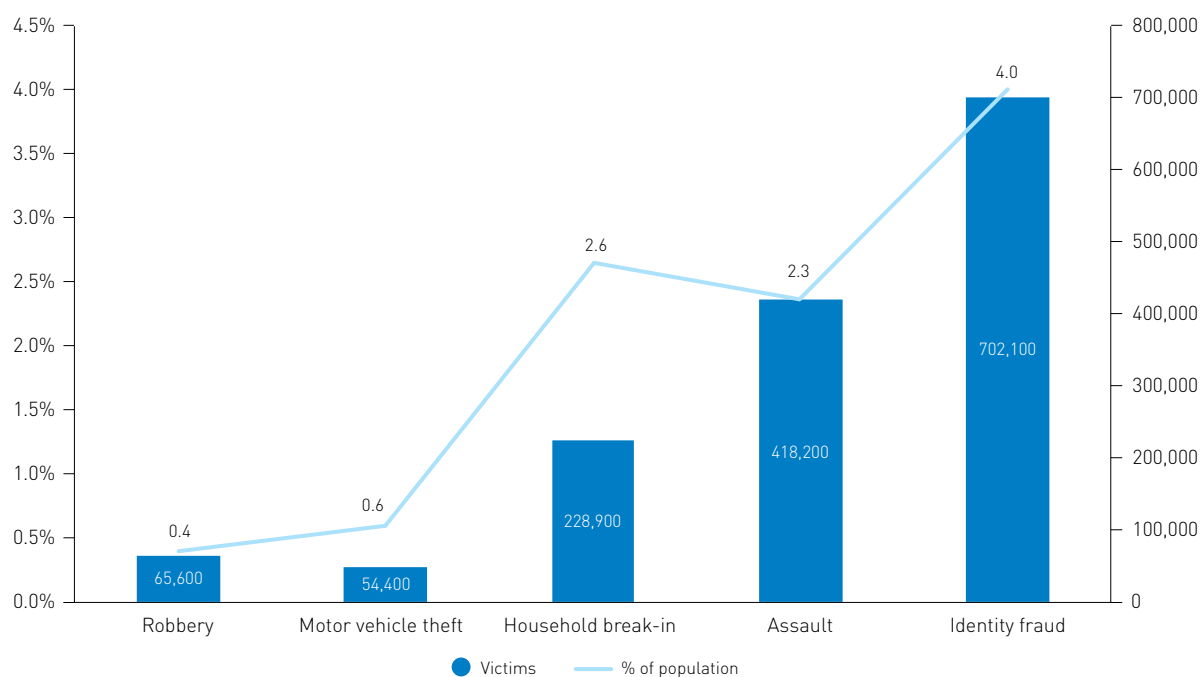


Source: 2013 and 2014 AIC Surveys.

Identity crime victimisation compared with other personal and theft-related crimes

According to data from the ABS' Crime Victimisation Survey in 2015, identity-related crime appears to be one of the most prevalent crimes in Australia when compared with the victimisation rates for other conventional 'personal and theft-related' crimes such as robbery, motor vehicle theft and assaults (see Figure 33).

Figure 33: Number of victims and proportion of population or household, by offence type (n and %)



Sources: ABS 2015, and ABS 2012.

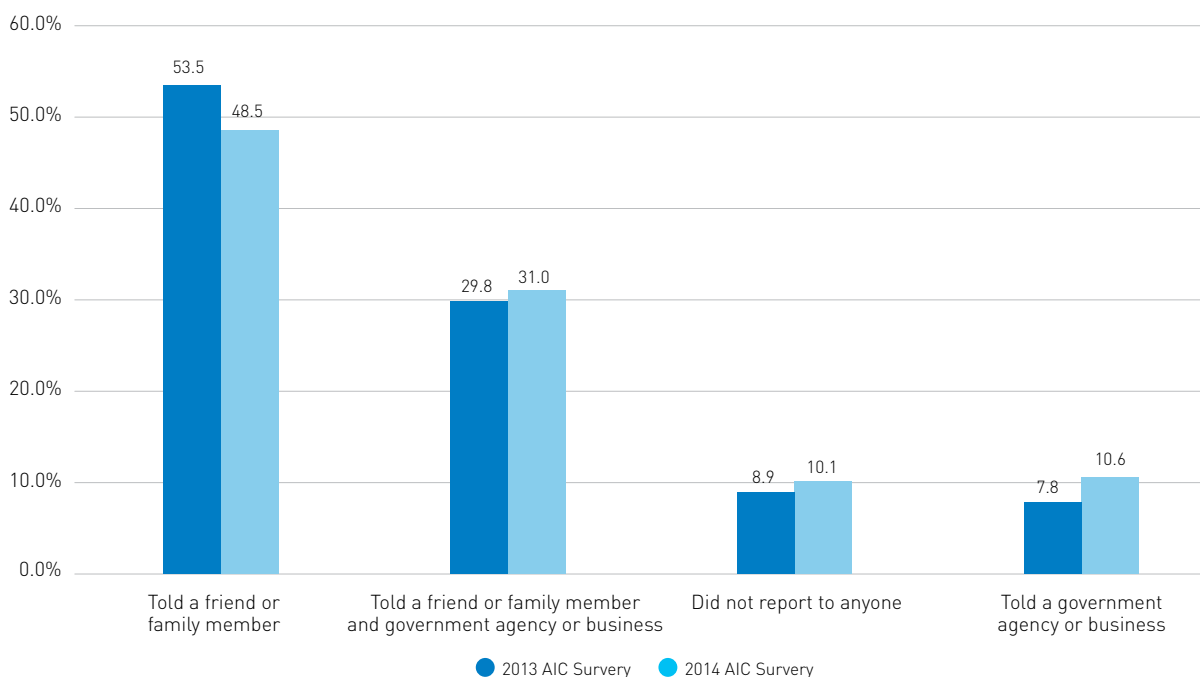
Key finding: A significant proportion of identity crime continues to go unreported by victims. Both the AIC's 2013 and 2014 surveys indicated that around half of victims tell a friend or family member, but that around 10% do not report the incident at all. Of those respondents in the 2014 AIC survey who reported experiencing misuse of their personal information in the previous 12 months, 59% did not report the incident to a business or government agency. This is a decrease from the results of the 2013 AIC Identity Crime and Misuse survey where approximately 63% of victims did not report the incident to these organisations.

Under-reporting continues to be a problem that contributes to the difficulty in determining the true extent of identity crime in Australia. Around 10% of AIC 2013 and 2014 Survey respondents who experienced misuse of their personal information in the previous 12 months indicated that they did not report their victimisation to anyone; almost half of the respondent victims who did tell someone, told friends or family members.

Of those respondents in the 2014 AIC survey who reported experiencing misuse of their personal information in the previous 12 months, 59% did not report the incident to a business or government agency. While this figure remains high, it is a decrease from the results of the 2013 Survey where approximately 63% of victims did not report the incident to these organisations (see Figure 34). It is possible that the increase in reporting may be due to greater awareness in the community about government initiatives such as the ACCC's SCAMwatch website.

The number of respondents in the 2013 and 2014 AIC Surveys who indicated that they reported the misuse of their personal information to a government agency or business is considerably lower than the reporting figures for credit card fraud and identity theft in the ABS' 2010–11 Personal Fraud Survey. That survey found that approximately 50% of credit card fraud victims and 66% of identity theft victims reported the incident to an agency, be this the police, some type of business, or an Ombudsman or consumer affairs agency (ABS 2012).

Figure 34: Reporting experience of identity crime and misuse, by type of report (%)



Source: 2013 and 2014 AIC Surveys.

Note: The categories of 'telling a government agency or business', and 'telling family/friends and government agency or business' are separate. Accordingly, the responses for these categories have not been double-counted.

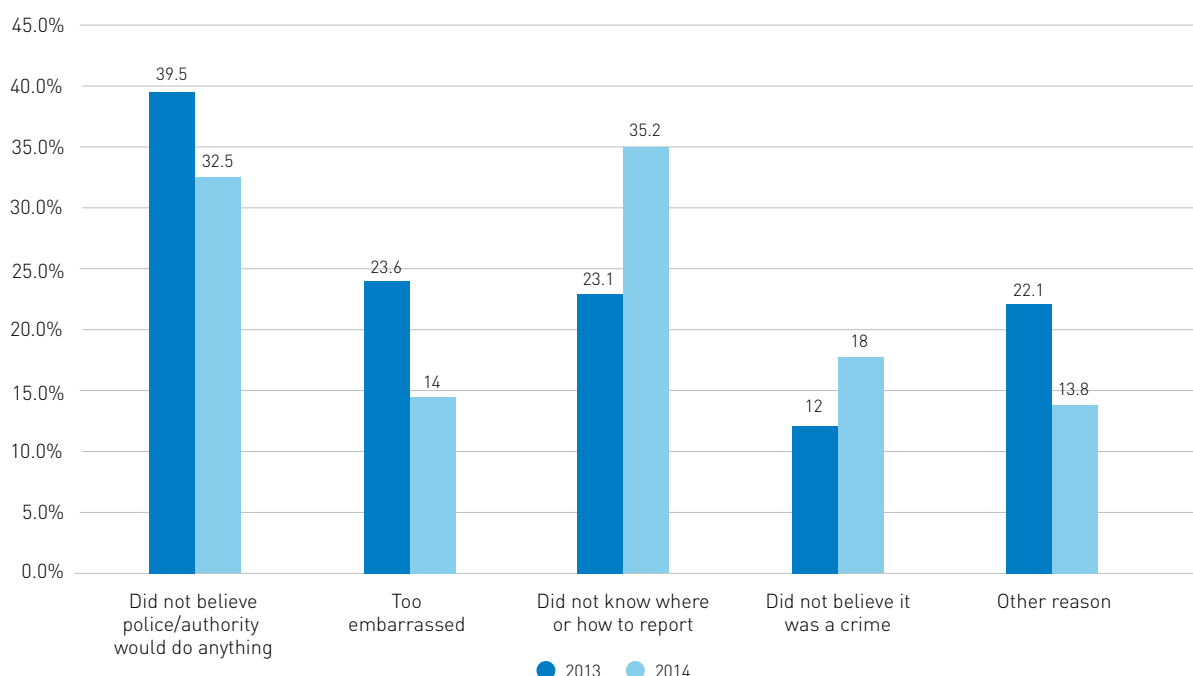
Participants in the 2014 AIC Survey who experienced misuse of their personal information but had not reported this to anyone were asked why they had chosen not to report the incident. A comparison of the responses to the 2013 and 2014 AIC Surveys are illustrated in Figure 35.

Interestingly, there was an increase in the number of respondents who claimed that the reason they did not report the incident was due to the fact they did not know where or how to report it (approximately 35% in 2014 compared with approximately 23% in 2013); or that they did not report because they did not believe it was a crime (18% in 2014 compared with 12% in 2013).

These results indicate that:

- further work is required to increase community awareness around the fact that misuse of an individual's personal information is in fact a crime, and
- greater emphasis should also be placed on educating the community about the organisations to which they should be reporting identity crime.

Figure 35: Reasons for not reporting misuse of personal information, 2013 and 2014 AIC surveys



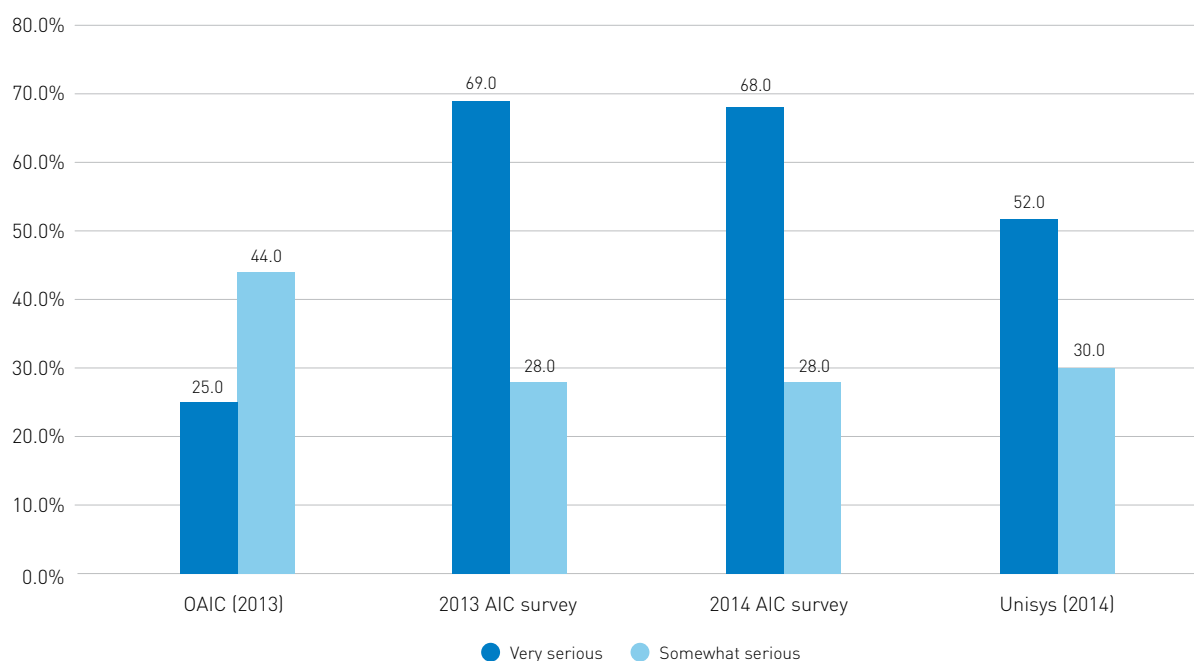
Source: 2013 and 2014 AIC Surveys.

2.4 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 96% of respondents in the 2014 AIC Survey claiming that misuse of personal information was a very serious or somewhat serious issue. These results are almost identical to those obtained in the 2013 AIC Survey in the Pilot Report, where 96.6% of respondents indicated that they felt this way.

Almost identical results across 2012–13 and 2013–14 AIC Surveys indicating the level of public concern regarding misuse of personal information, viewed in comparison with similar recent surveys, suggest that identity crime is of continuing concern to Australians (see Figure 36).

Figure 36: Perceptions of misuse of personal information, by survey



Source: 2013 and 2014 AIC Surveys.

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

Key finding: Certain types of identity credentials are more likely to be targeted for the purposes of identity theft or misuse than others, with credit card information being the type most commonly misused, followed by a person's name, bank account information, address and date of birth. Driver licences and Medicare cards have also been found to be frequently targeted by identity criminals.

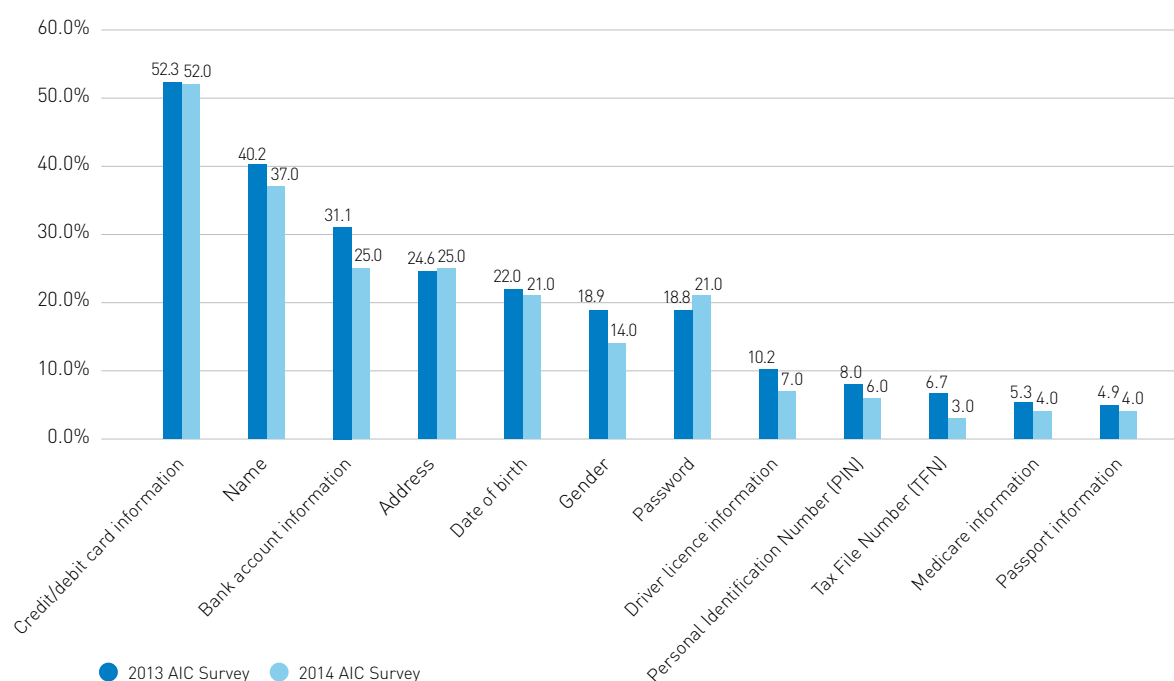
Certain types of Personal Identifying Information (PII) are more susceptible to identity theft or misuse than others. In its 2013 and 2014 surveys about identity crime and misuse, the AIC asked respondents about the types of personal information that they believed had been misused in the most serious incident of identity misuse that they had experienced in the previous year.

Respondents indicated that there were 19 different types of PII that had been misused (see Figure 37). Credit or debit card information was identified by respondents as being misused the most frequently (52%), followed by a person's name (37%), bank account information (25%) and address (25%). These results are consistent with those obtained in the 2013 AIC Survey and outlined in the Pilot Report.

These results are also fairly consistent with other research on this issue. For example, iDcare found that driver licences were the most targeted source of personal information, followed by taxation information,

bank account details, and credit or debit card details (iDcare 2014). Unpublished AFP data also indicates that driver licences and Medicare cards continue to be the most likely identity credentials to be used in the facilitation of identity crime. These are a relatively easy target for identity criminals due to their prevalence throughout the community, and the ease with which they can be altered compared with other identity credentials such as passports. It is also possible that driver licences are an attractive target because of the cursory scrutiny that they often receive compared with other credentials.

Figure 37: Types of PII that respondents reported as being misused in the previous 12 months




Note: in the 2014 survey, data was weighted to reflect the distribution of the population across jurisdictions. There were 460 survey participants who answered this question, and respondents could select multiple types of personal information.

Source: Smith & Hutchings 2014; Smith, Brown & Harris-Hogan forthcoming.

3. Impacts of identity crime

3.1 Direct cost of identity crime and misuse to government agencies

Key finding: There were just over 17,000 incidents involving misuse of identity recorded by Commonwealth agencies in 2012–13, which represents approximately 12.5% of the 135,600 frauds reportedly committed against Commonwealth agencies during this period. The direct and indirect costs of identity crime and misuse to Commonwealth government agencies is approximately \$28.5m.



The estimates presented in this section of the report 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). The figures used in these estimates are based on data from previous reports which have sought to quantify the cost of fraud committed against Commonwealth agencies (Jorna & Smith forthcoming). Further details of how these figures were obtained can be found in Appendix F.

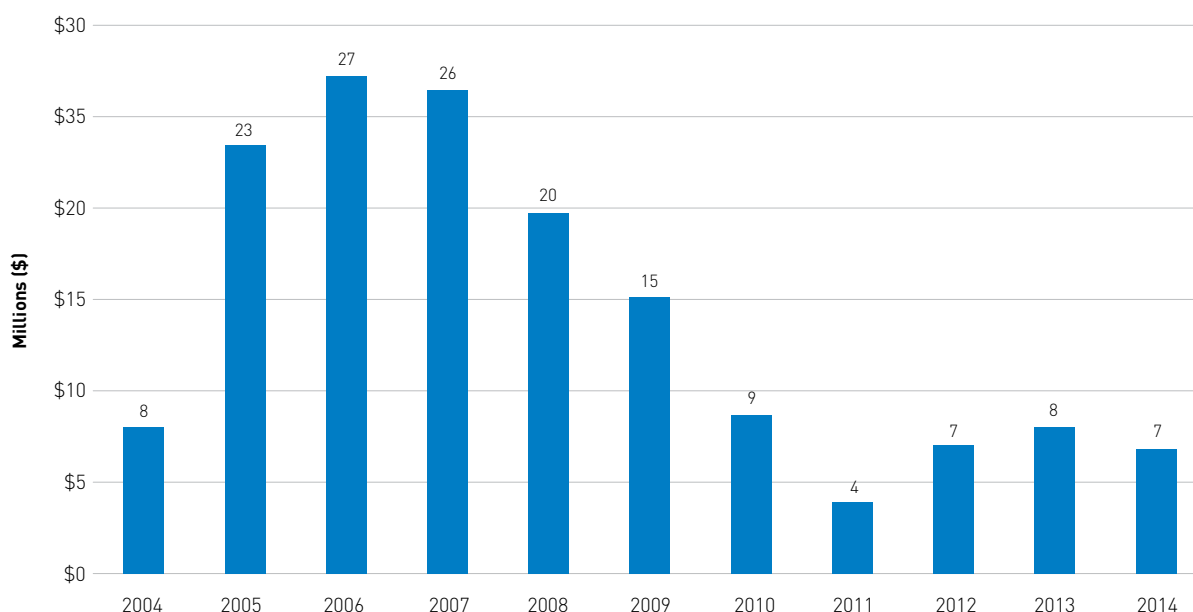
In 2012–13, Commonwealth agencies reported a total of 135,672 internal and external incidents of fraud worth \$207,102,705 (Jorna & Smith forthcoming). This equates to approximately \$1,526 per incident. Data provided by Commonwealth agencies for the annual Commonwealth Fraud Survey indicated that there were a total of 17,001 internal and external misuse of identity incidents recorded by Commonwealth agencies in 2012–13 (Jorna & Smith, forthcoming). As a proportion of the total fraud incidents reported by Commonwealth agencies, the 17,001 identity-related incidents represent approximately 12.5% of the total frauds reported to Commonwealth agencies. Figures from 2012–13 have been used, as figures for 2013–14 were not available at the time of publishing this report.

A series of calculations were performed using these data in line with the methodology used to estimate the costs of Commonwealth fraud in the AIC's 'Counting the costs of crime' report (Smith, Jorna, Sweeney & Fuller 2014), resulting in Commonwealth agencies incurring an estimated \$228,154,457 in indirect and direct losses as a result of fraud.

If it is assumed that identity crime represents 12.5% of all incidents of fraud experienced by Commonwealth agencies, identity crime as a proportion of all Commonwealth fraud would cost approximately \$28.5m.

Cost of benefits fraud

There was a large increase in the total recorded value of identity crime investigated by DHS between 2005 and 2009. This can be attributed to increased funding that the Department received in the 2003–2004 Federal Budget, which it used to expand the number of specialist identity fraud investigation teams within the agency. Since 2012, however, the total value of identity crime committed against DHS has remained relatively stable at around \$7m (see Figure 38).

Figure 38: Total value of identity fraud against DHS, by year, 2004 to 2014

Source: Department of Human Services.

Costs of identity crime to other government agencies

In addition to DHS (Centrelink); the Australian Taxation Office (ATO); the Department of Industry, Innovation, Science, Research and Tertiary Education (DIISRTE); Defence and AUSTRAC provided information regarding the estimated value of fraud or identity crime to their agencies during 2013–14.

The only state government agencies that provided information regarding the estimated cost of identity crime investigations were the Queensland Department of Transport and Main Roads and the Western Australia Department of Transport.

The Queensland Department of Transport and Main Roads and the Australian Transaction Reports and Analysis Centre (AUSTRAC) requested that their data remain confidential.

Australian Taxation Office (ATO)

In 2013–14, the ATO saved the Commonwealth government \$20,632,375 in protected revenue as a result of the identity fraud protective measures that it had implemented. For instance, tax returns that were cancelled as a result of the ATO's pre-issue program (whereby the ATO verifies the details and amounts reported in an income tax return before a notice of assessment is issued to the taxpayer), saved the Commonwealth government \$15,782,187. Tax returns that were cancelled as a result of a compromised TFN indicator being identified saved the Commonwealth \$1,777,065 in protected revenue. The ATO saved the Commonwealth a further \$3,073,123 as a result of cancelling income tax returns to protect TFNs.

Department of Industry, Innovation, Science, Research and Tertiary Education (DIISRTE)

DIISRTE advised that it identified 66 incidents of fraud in 2013–14 valued at \$1,555,741. However, no information was provided regarding how many, (if any) of these incidents involved identity crime.

Department of Defence

The Department of Defence detected one incident of identity crime during 2013–14. The estimated cost to the victim was \$3,561. No information was provided regarding the cost of this incident to the department.

Western Australia Department of Transport

The Western Australia Department of Transport estimated that it cost the agency approximately \$275,000 in 2013–14 to deal with 30 suspected identity fraud incidents involving WA driver licences. Note this figure only refers to the staffing costs for the facial recognition process.

3.2 Direct costs of identity crime and misuse to business

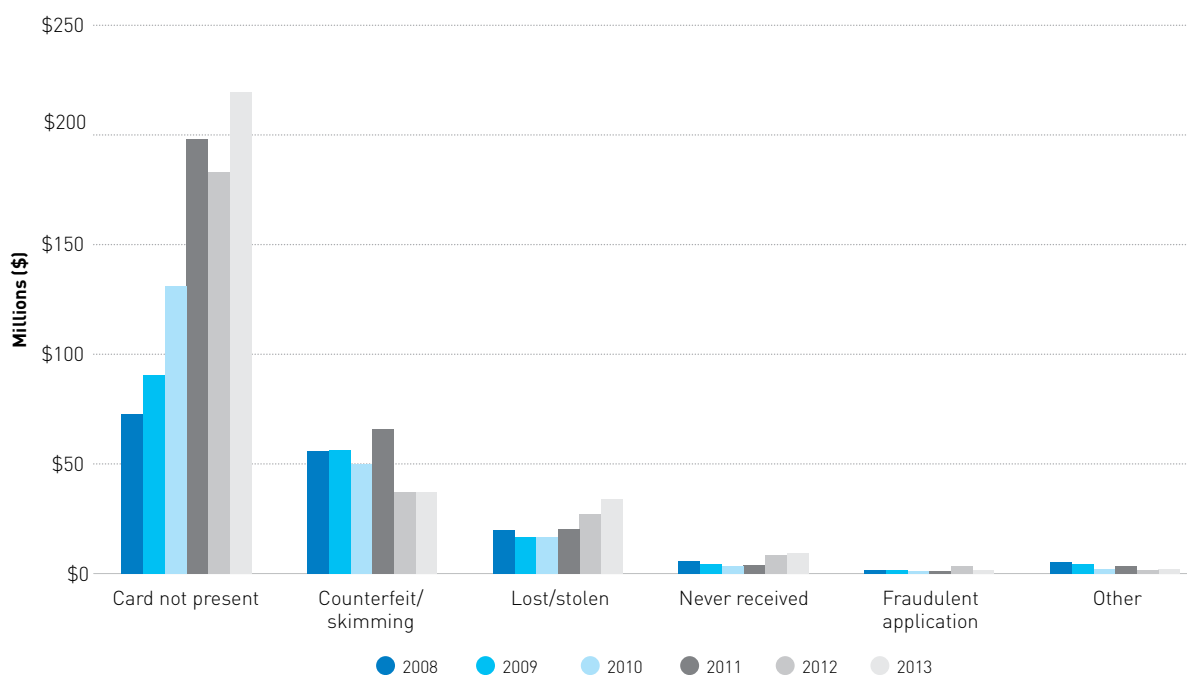
Key finding: The Association of Certified Fraud Examiners (ACFE) has estimated that organisations around the world lose an estimated 5% of their annual revenues to fraud (ACFE 2014). If it is assumed that around one fifth of these frauds possibly involved some form of identity crime, this would mean that organisations potentially lose around 1% of their revenue each year to identity crime.

An example of the financial impact of identity crime on Australian businesses is evident through data released by the Australian Payments Clearing Association (APCA) which revealed that fraudulent debit and credit card transactions cost Australian businesses around \$304m in 2013–14, with the majority of these frauds falling into the category of card-not-present fraud (see Appendix D).

Identity fraud involving transaction payment systems

In 2013–14, there were a total of 6.1b transactions involving a credit or debit card in Australia. Of these transactions, 1,543,197 were fraudulent. The total value of the fraudulent transactions was approximately \$304m (APCA 2014:7). It is reasonable to assume that the vast majority of such fraudulent transactions involve misuse of personal information, given the fact this type of activity usually involves someone misrepresenting themselves as the owner of another person's credit or debit card. Accordingly, these types of transactions could be classified as identity crimes. A breakdown of the different types of frauds involving credit and debit cards between 2008 and 2013, as well as the estimated value of these frauds is illustrated in Figure 39.

Figure 39: Cost of Australian credit and debit card fraud 2008–2013



Source: APCA 2014.

Case Study 7:

Four men, including a taxi driver, were arrested in a Sydney motel in August 2014 after it was discovered that the motel room was being used as a 'card-cloning den.' Police allegedly found 800 blank credit cards, a skimming device, and a card encoder. A number of laptops that were believed to have been used to download credit card data were also seized.

Police alleged that the men were part of a sophisticated fraud syndicate who skimmed details off the magnetic strip of credit cards as they were used in taxis and other locations around Sydney. The syndicate would then create replica cards from the stolen information and withdraw cash and make purchases.

The four men were charged with dealing in identification information and possessing equipment for the manufacture of identity documents. One of the men was charged with directing the activities of a criminal group and the other three were charged with participating in the activities of a criminal group.

Source: Sydney Morning Herald, 9 July 2014, <http://www.smh.com.au/digital-life/consumer-security/police-swoop-on-alleged-taxi-credit-card-fraud-syndicate-in-sydney-20140709-zt0wj.html>



Private sector organisations were not approached to provide data for this report due to time and resource constraints. However, 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 actually is within the Australian business community (KPMG 2013; PwC 2014). It must be emphasised that the KPMG surveys have only been administered to between 220 and 280 businesses from both Australia and New Zealand, and the surveys do not contain specific questions regarding identity crime.

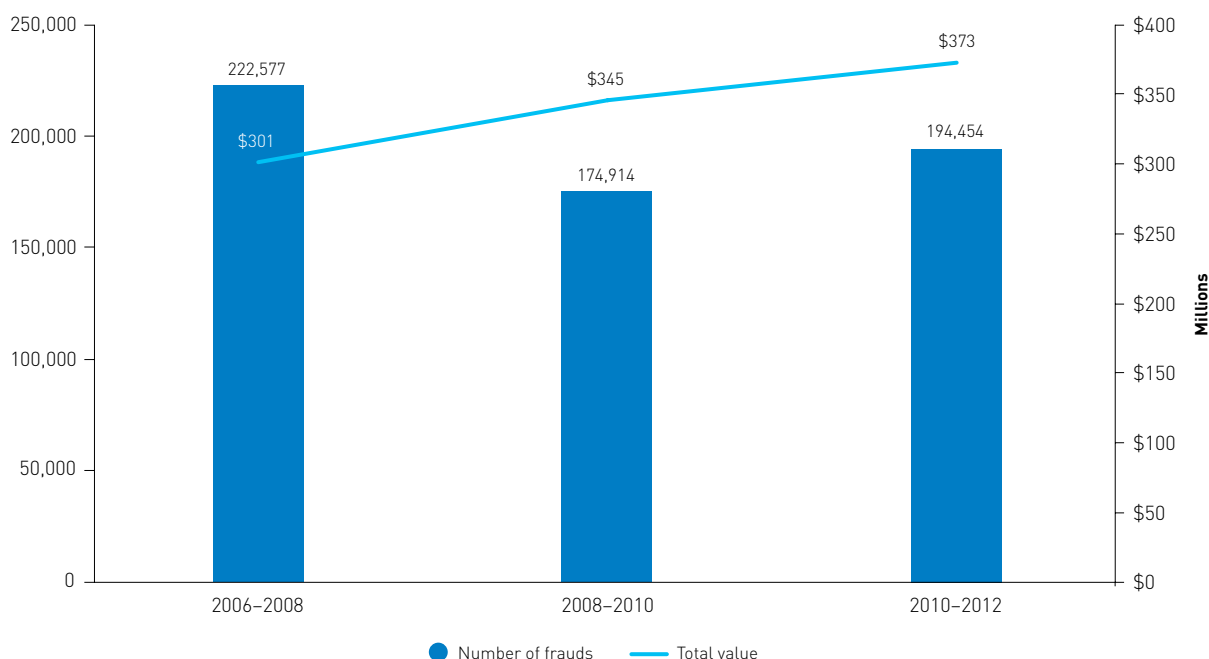
The most recent KPMG survey was conducted in 2012 and involved a number of Australian and New Zealand organisations in the public and private sectors. Participating organisations were asked to complete a questionnaire on their attitudes and responses to fraud, bribery and corruption. Businesses were also asked to consider the number of incidents of fraud that took place in their organisations between 1 February 2010 and 31 January 2012.

A total of 281 organisations responded to the survey from a number of different industries including:

- financial and insurance services;
- health care and social assistance;
- manufacturing; energy, gas, water and waste services;
- agriculture, forestry and fishing;
- professional, scientific and technical services, and
- construction.

There were a total of 194,454 incidents of fraud reported (see Figure 40). The total value of these frauds was estimated to be \$372.7m, or just over \$1.3m per organisation. Each fraud involved an average loss of \$1916. There were 20 much larger frauds which cost the agencies involved over \$1.0m each. For the purposes of this report, the estimated cost of identity crime against the private sector has been counted as 'serious fraud'.

Figure 40: Number and value of frauds against Australian and New Zealand businesses, by year (2006—2012) (number and dollar value)



Source: KPMG 2009, 2010 & 2013.

PwC's 2014 Global Economic Crime Survey found that 47% of the 79 Australian organisations surveyed experienced more than 10 fraud incidents in the 24 months prior to the survey, and 36% of Australian respondent organisations suffered losses in excess of \$1.0m in the 24 months prior to the survey (PwC 2014). While identity crime was not specifically mentioned in the PwC survey, it did indicate that 43% of respondents expressed concern about cyber-threats involving the theft or loss of PII.

While the KPMG and PwC surveys focussed on fraud more generally, rather than identity crime, it is reasonable to assume that identity crime would have played a role in a proportion of the 194,454 incidents of fraud that were reported in the KPMG survey.

As is evident in Figure 40 above, there has been an increase in the total value of the frauds experienced by organisations who have responded to the KPMG survey since 2006. It must be noted that the actual cost of fraud to Australian businesses would be considerably more than this, given that this figure reflects the cost of fraud for only 281 organisations, including organisations from New Zealand in 2010–12.

The Association of Certified Fraud Examiners (ACFE) has estimated that organisations around the world lose an estimated 5% of their annual revenues to fraud (ACFE 2014). While it is acknowledged that this figure is not specifically related only to Australian organisations, if it is assumed that around one fifth of these frauds possibly involved some form of identity crime, approximately 1% of an organisation's annual revenue could potentially be lost as a result of identity crime.

3.3 Direct cost to individual victims of identity crime and misuse

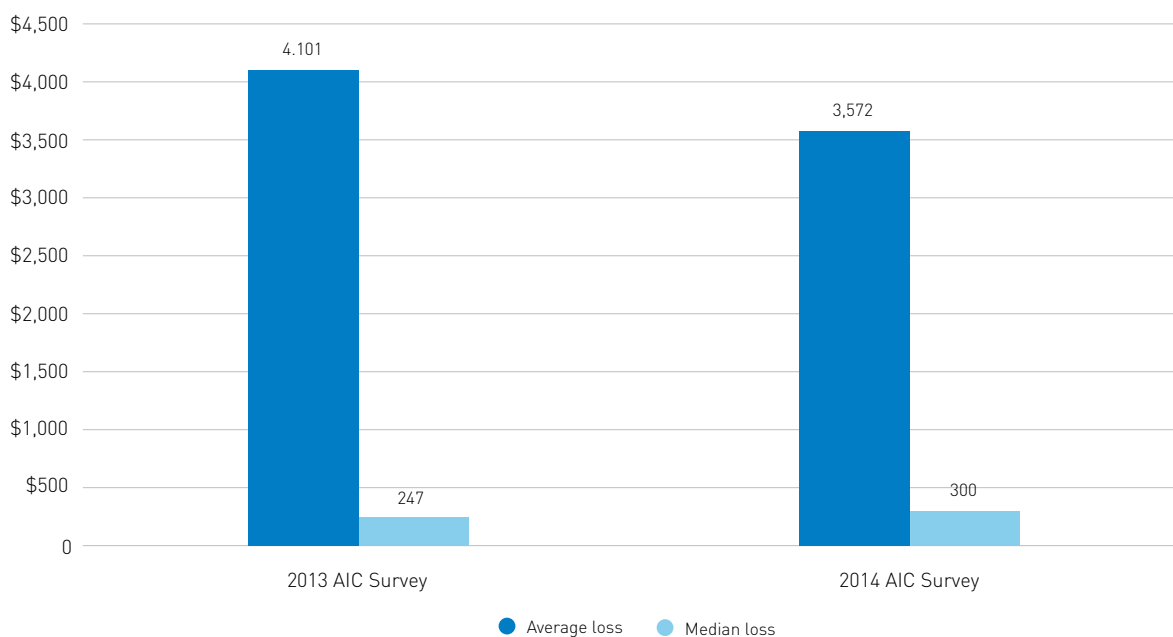
Key finding: The direct cost of identity crime and misuse to individual victims in Australia each year is around \$432m. This estimate is based on the methodology used to estimate the cost of personal fraud in the AIC's 'Counting the cost of crime' report (Smith, Jorna, Sweeney & Fuller 2014). Further details regarding the methodology used to calculate this estimate can be found in Appendix F.

The amount of money lost by victims of identity crime and misuse varies considerably. Some suffer substantial out-of-pocket losses, while most lose relatively small amounts. Data obtained in the AICs 2014 survey found that 4.8% of all respondents experienced out-of-pocket losses of between \$1 and \$200,000. This was similar to the results obtained in the 2013 AIC Survey, where 5.0% of all respondents reported out-of-pocket losses of between \$1 and \$310,000.

On average, respondents to the AICs surveys reported mean out-of-pocket losses of \$4,101 in the 2013 AIC Survey and \$3,572 in the 2014 AIC Survey; a small reduction between these two years. The majority of respondents in both surveys, however, reported smaller median out-of-pocket losses of \$247 in 2013 and \$300 in 2014 (see Figure 41) (Smith & Hutchings 2014; Smith, Brown & Harris-Hogan forthcoming).

These findings are similar to those obtained in other survey research conducted by iDcare and the ABS. Between October and December 2014, iDcare found that victims of identity crime incurred an average \$412 in out-of-pocket expenses (iDcare 2014), while the ABS's national survey found that victims of personal fraud lost an average of \$2,000, with a median loss of \$300 (ABS 2012).

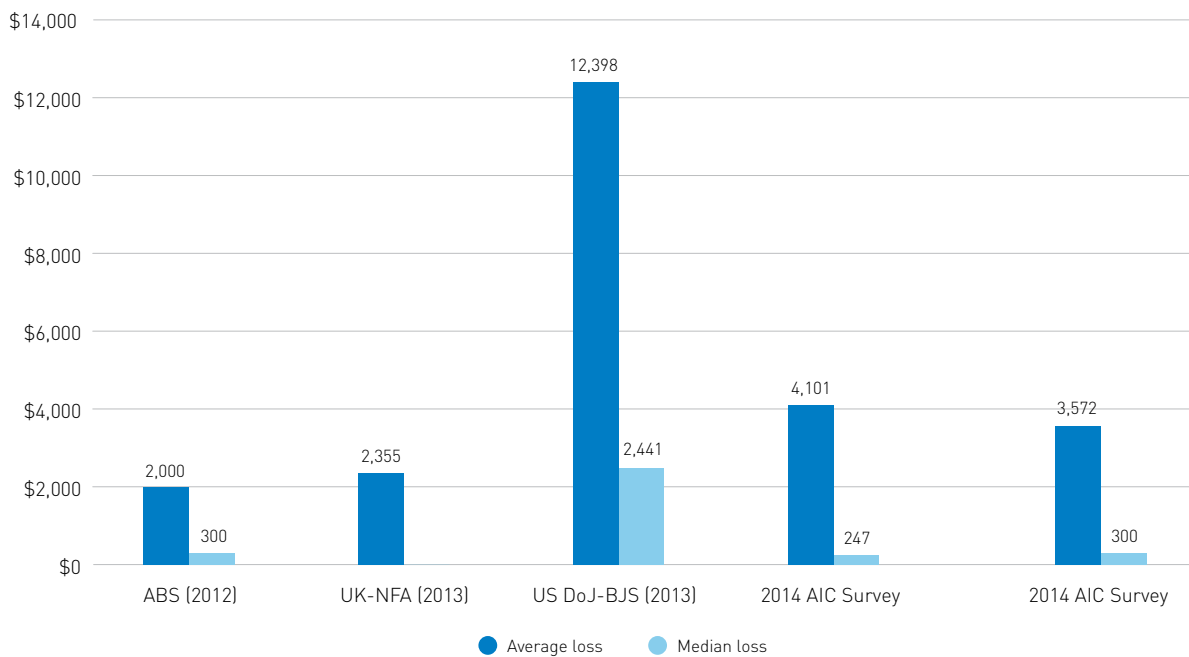
Figure 41: Average and median out-of-pocket losses suffered by victims of identity crime and misuse, by AIC survey (\$)



Source: 2013 and 2014 AIC Surveys.

The average out-of-pocket losses incurred by respondents to the 2014 AIC Survey were slightly higher than average loss of \$2,000 that the ABS found to be incurred by victims of personal fraud (ABS 2012), and approximately 72% less than the average direct losses incurred by victims of identity crime in the United States in 2012, namely US\$9,650 (AUD\$12,398). The average financial losses incurred by identity crime victims in the United Kingdom (UK) in 2012 were slightly less than the 2014 AIC Survey average, at a total of AUD\$2,355 (£1,203) (National Fraud Authority 2013). No data were available in relation to the median loss in the UK. A comparison of these figures is illustrated in Figure 42.

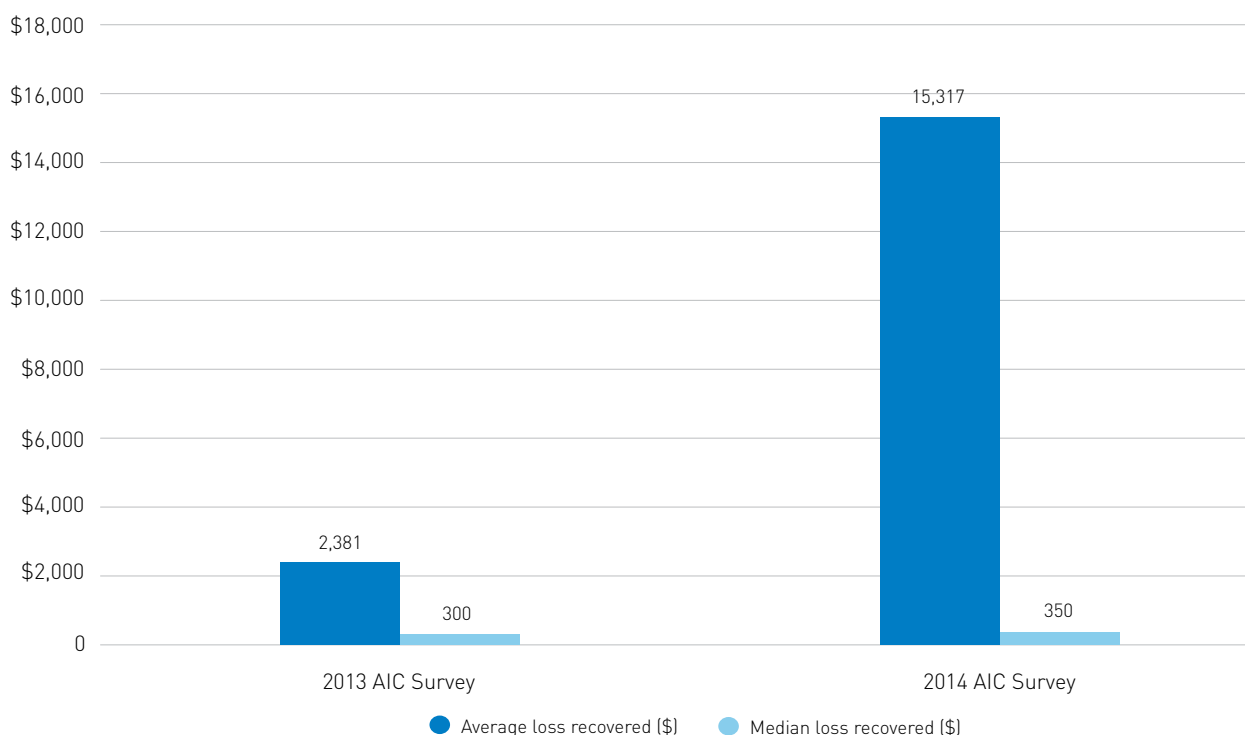
Figure 42: Average and median losses suffered by victims of identity crime and misuse, by survey (\$)



Source: ABS 2012; UK National Fraud Authority 2013; Harrell & Langton 2013; Smith & Hutchings 2014; Smith, Brown & Harris-Hogan forthcoming.

Note: All figures have been converted to Australian dollars.

Some victims of identity crime and misuse seek reimbursements and refunds for the financial losses they incur as a result of misuse of their personal information. Figure 43 illustrates the average and median loss amounts that respondents in the 2013 and 2014 AIC Surveys recovered as a result of reimbursements or by some other means. The average recovered loss in 2014 is considerably higher than that recorded in the 2013 AIC Survey due to one person reporting that they recovered \$2.0m (Smith, Brown & Harris-Hogan forthcoming).

Figure 43: Average and median recovered losses in AIC Surveys

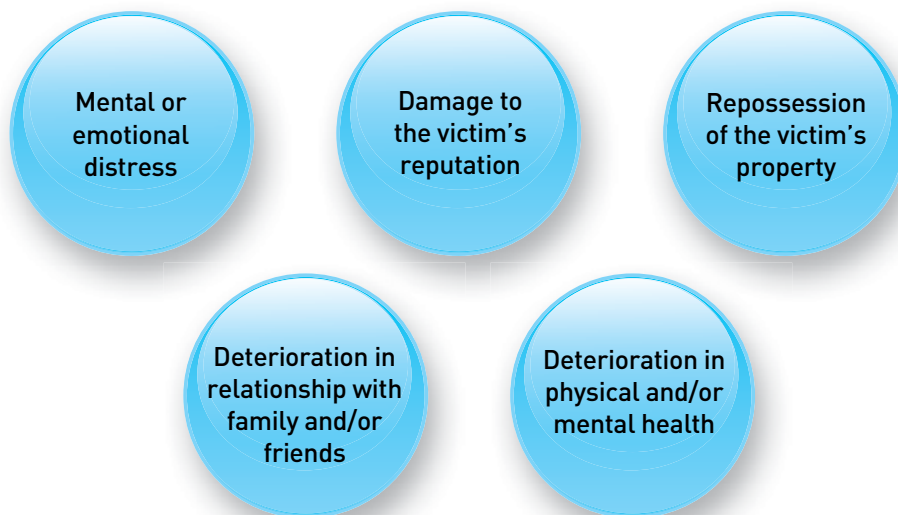
Source: 2013 and 2014 AIC Surveys.

3.4 Non-financial consequences of identity crime and misuse

Key finding: The impact of identity crime on victims is not limited to the financial losses that they may incur directly. In some cases, the non-financial consequences of these types of crimes on victims can be more severe than any economic loss they incur, affecting personal relationships, patterns of work and sleep and even the victim's mental health resulting in self-harm or suicide.

As illustrated in Figure 44, the non-financial consequences of identity crime on victims can be diverse.

Figure 44: Non-financial consequences of identity crime



Participants in the 2014 AIC survey were asked about the consequences they experienced as a result of their personal information being misused in the previous 12 months. These results are presented in Figure 45 and are very similar to those of the 2013 AIC Survey, indicating that there has not been a significant shift in the non-financial consequences experienced. Indeed, the most common non-financial consequences for victims in both surveys were being refused credit followed by mental or emotional distress.

Case Study 8:

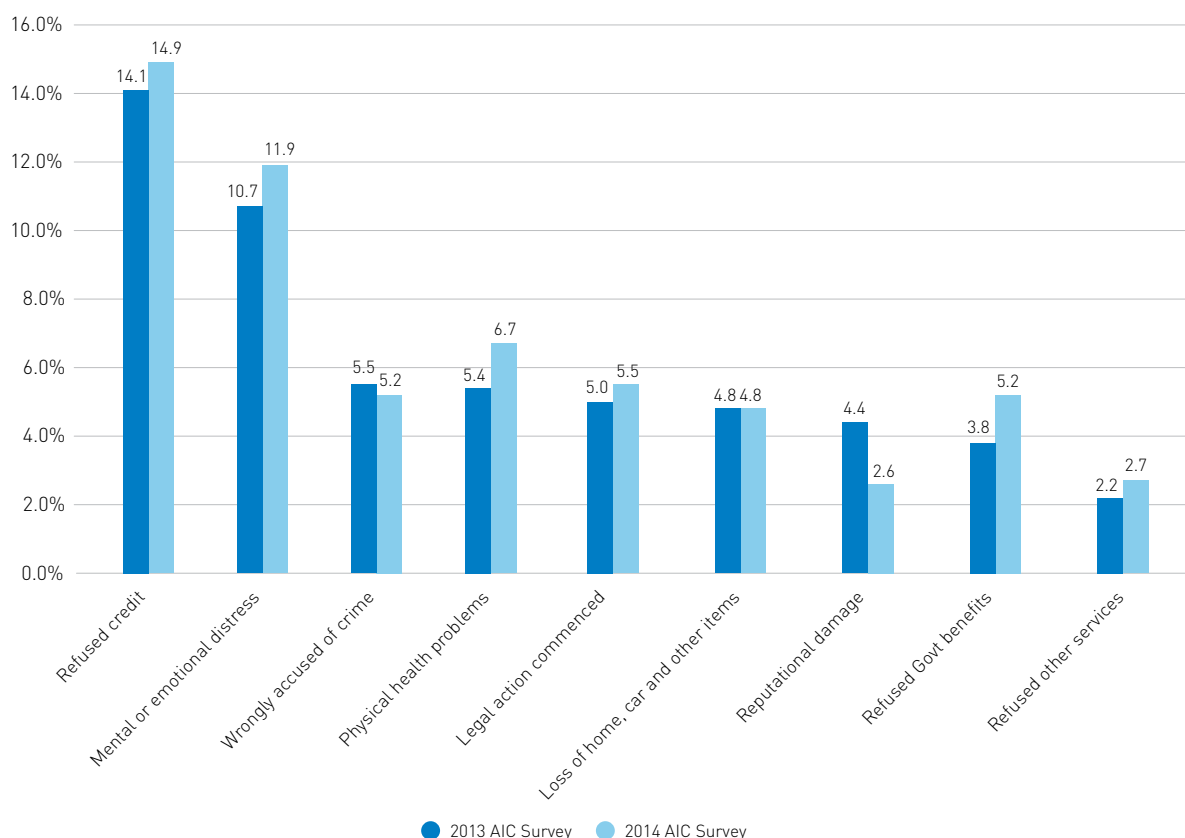
The victim alleged that after she separated from her husband, he committed a number of identity crimes against her, including falsifying signatures on documents to gain access to files, hacking her email account, stealing her passport and using her personal information to obtain government benefits.

The accused was also alleged to have used the stolen personal information to have the victim's tax rebate deposited into his account, as well as attempting to gain access to her bank accounts.

The victim also alleged that her ex-husband fraudulently made her the only Director of a company he established, which he then made insolvent by forging her signature. As a result of this conduct, the victim claimed that she was subsequently unable to access social welfare benefits as she was named a Company Director.

Source: iDcare, January 2015 (unpublished case studies).

Figure 45: Consequences experienced as a result of personal information being misused in the previous 12 months



Source: 2013 and 2014 AIC Surveys.

4. Remediation of identity crime

The amount of time that it takes for a victim to recover from the impact and consequences of identity crime varies depending on the extent of their victimisation. In cases that only involve one fraudulent application or transaction, the victim may only incur minimal inconvenience and financial impost. In more serious cases such as those involving a complete takeover of the victim's identity, it may take the victim over 200 hours to obtain new credentials and sort out the consequences of the crime (CIFAS 2013).

4.1 Average time by victims spent in remediation activity

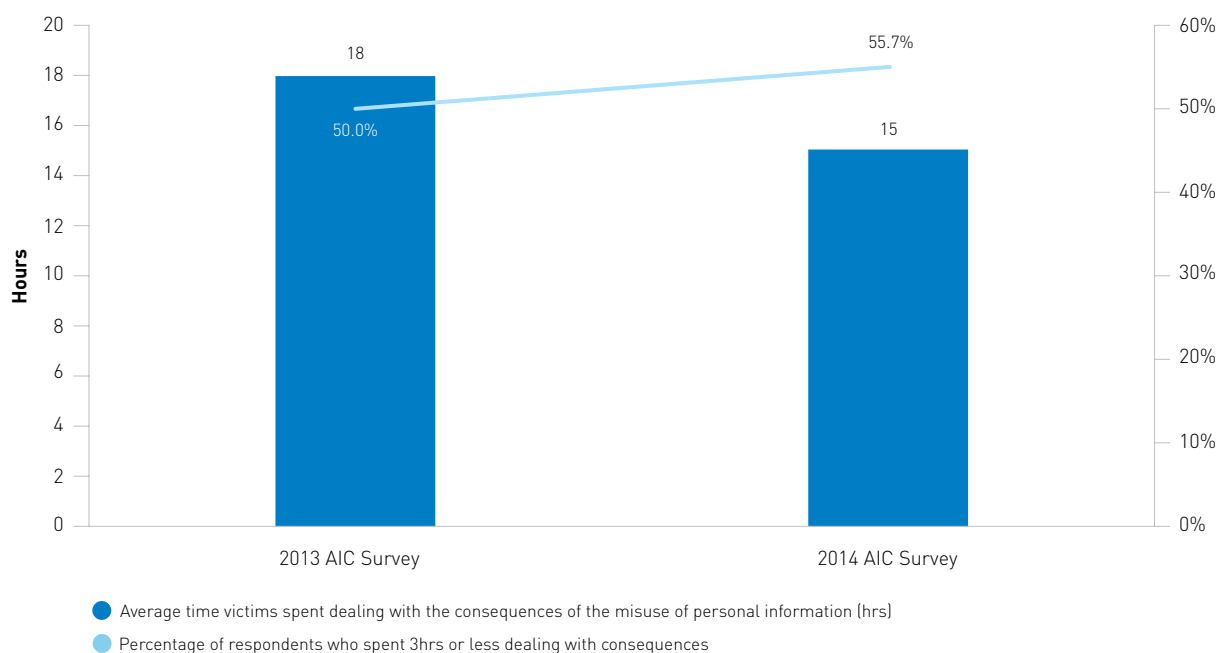
Key finding: Respondents in the 2014 AIC Survey who experienced misuse of their personal information in the previous 12 months spent an average of 15.3 hours dealing with the consequences—slightly less than the average of 18.1 hours reported in the 2013 Survey—although almost 56% of these respondents spent less than three hours dealing with the consequences.

The level of emotional distress experienced by victims of identity crime has been found to be related to the length of time that victims spend resolving problems caused by the crime (Harrell & Langton 2013). While it would appear that the majority of victims are able to deal with the consequences fairly quickly and with little financial impost, the consequences for those victims forced to deal with the consequences for months and years afterwards can be devastating.

In addition to the indirect consequences of identity crime, victims sometimes need to spend a substantial amount of their own time and money dealing with the repercussions of this type of crime. Several studies have been conducted in Australia and internationally to examine the average amount of time that victims spend dealing with the consequences of identity crime.

In the 2014 AIC Survey, survey participants who had experienced misuse of their personal information in the previous 12 months were asked how many hours they had spent dealing with the consequences. This included the amount of time that was taken to reinstate their credit rating, and arrange for new credit or debit cards to be issued (Smith, Brown & Harris-Hogan forthcoming). As demonstrated in Figure 46 below, respondents in the 2014 AIC Survey spent less time dealing with the consequences, compared with respondents in the 2013 Survey (15.3 hours compared with 18.1 hours). Additionally, there were a greater percentage of respondents in the 2014 AIC Survey who spent three hours or less dealing with the consequences of the misuse of their personal information, compared with respondents in the 2013 AIC Survey (56% compared with 50%).

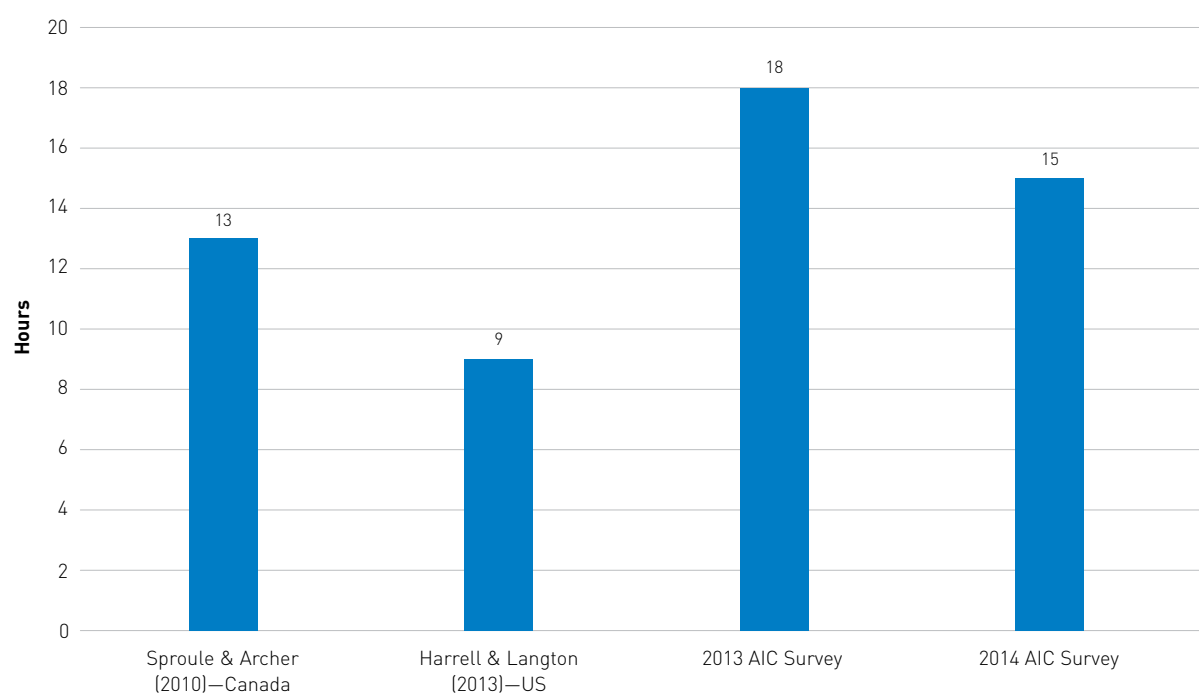
Figure 46: Time spent by victims dealing with consequences of misuse of personal information, AIC Surveys



Source: 2013 and 2014 AIC Surveys.

The average amount of time respondents spent dealing with the consequences of the misuse of their personal information in the 2013 and 2014 AIC Surveys is higher than the average amount of time that studies in Canada and the United States found victims of identity crime have had to spend dealing with the consequences. A comparison of the relevant findings of these studies can be seen in Figure 47 below.

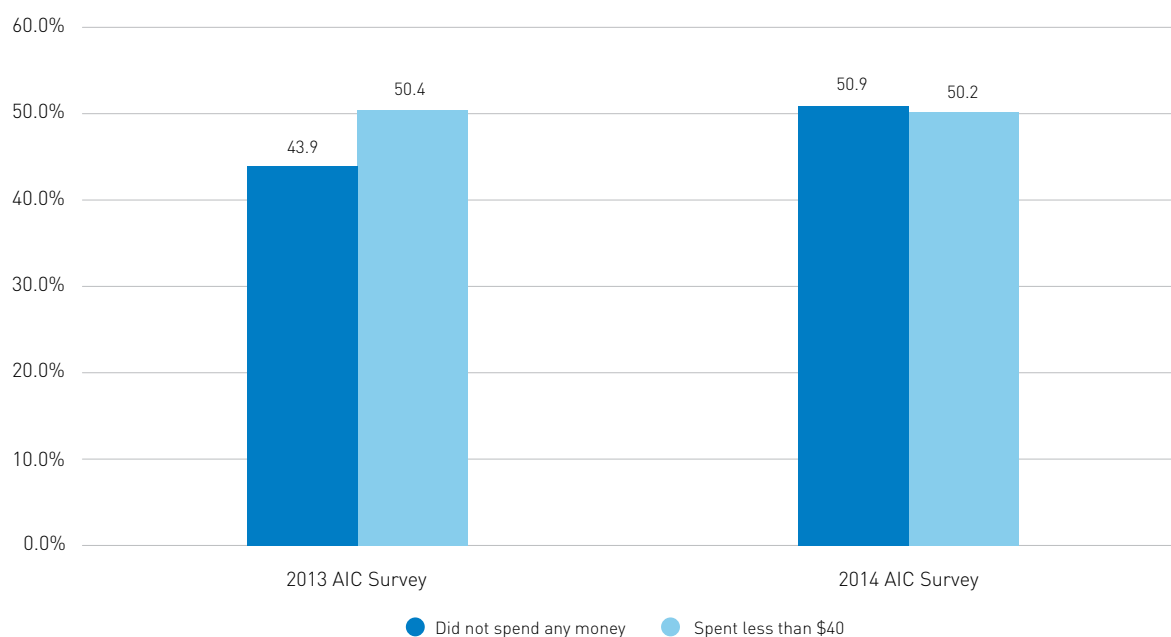
Figure 47: Average time victims spent dealing with the consequences of the misuse of personal information (hrs)



Source: Sproule & Archer 2010; Harrell & Langton 2013; Smith & Hutchings 2014; Smith, Brown & Harris-Hogan forthcoming.

In addition to the amount of time spent dealing with the consequences of the misuse of personal information, respondents in the 2014 AIC Survey who had experienced misuse of their personal information in the previous 12 months were also asked how much money they had spent dealing with the consequences of the misuse. A comparison of the 2013 and 2014 AIC Survey results can be found in Figure 48.

Figure 48: Amount of money spent dealing with the consequences of misuse of personal information



Source: 2013 and 2014 AIC Surveys.

4.2 Number of enquiries to government agencies regarding assistance to recover identity information

Key finding: Reporting of identity crime to state and territory consumer affairs agencies appears to be very low

Consumer Affairs agencies from Victoria, New South Wales, Western Australia and Queensland provided data regarding the numbers of identity crime related enquiries that they received in 2013–14. A comparison of the number of enquiries received by each of these agencies is illustrated in Figure 49.

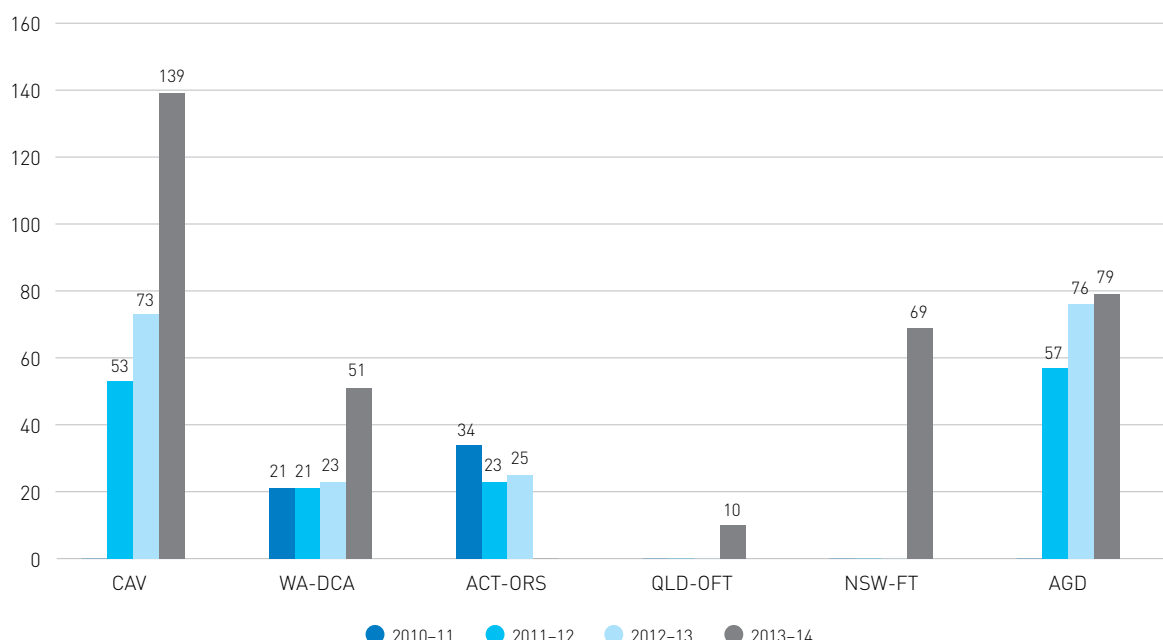
Of the jurisdictions which responded to the data request, Consumer Affairs Victoria recorded the highest number of identity-related enquiries, with a total of 136 identity fraud enquiries or requests for information, and three identity fraud disputes received between July 2013 and June 2014 (see Figure 49). Of these, nine were referred to Victoria Police and another five were referred to an agency other than the police. The remaining 125 enquiries were referred to an unspecified agency.

In 2013–14, NSW Fair Trading received 61 potential identity fraud enquiries and eight identity fraud complaints. Three of the people who made an enquiry were advised to contact police. However, NSW Fair Trading did not refer any enquiries or complaints to police directly.

The Western Australia Department of Commerce received 47 enquiries and four complaints in relation to potential identity fraud in 2013–14. Six of these enquiries and complaints were referred to police. The police also referred two incidents to the WA Department of Commerce.

The Queensland Office of Fair Trading received ten enquiries where a consumer alleged their identity may have been misused, or believed they were the victim of identity theft. No information was provided in relation to how many of these enquiries (if any) were referred to police for further investigation.

Figure 49: Enquiries received in relation to identity crime, by agency and year, 2010–11 to 2013–14



Source: Consumer Affairs Victoria (CAV); Western Australian Department of Consumer Affairs (WA-DCA); Australian Capital Territory Office of Regulatory Services (ACT-ORS); Queensland Office of Fair Trading (QLD-OFT); NSW Fair Trading (NSW-FT); Commonwealth Attorney-General's Department (AGD).

When compared with the ABS' 2010–11 Personal Fraud Survey results which indicated that there were approximately 702,100 Australians victims of identity fraud in the twelve months prior to interview (ABS 2012), the number of identity crime enquiries reported by the state and territory consumer affairs agencies appears to be very low. This may be due to a lack of awareness in the community that misuse of personal information is actually a crime, or it may be that members of the public do not realise that consumer affairs agencies can possibly assist them if they believe they have fallen victim to identity crime.

Attorney-General's Department (AGD)

In the 2014 calendar year, the AGD received 79 enquiries relating to the theft or misuse of personal information, as well as enquiries from individuals and organisations seeking guidance about identity security. Of these enquiries, 49 were received via emails, 18 were web enquiries submitted through the AGD website and 12 were phone calls.

The categories to which the enquiries related are outlined in Table 4 below:

Table 4: Reason for contacting AGD

Issue/Reason for contact	Number of enquiries
Lost/stolen documents ^a	20
Scams	11
Identity fraud	6
Identity theft	20
Unsafe disclosure of personal information	4
Cyber-security	5
Organisation privacy practices ^b	9
Other (n.e.c)	4
Total	79

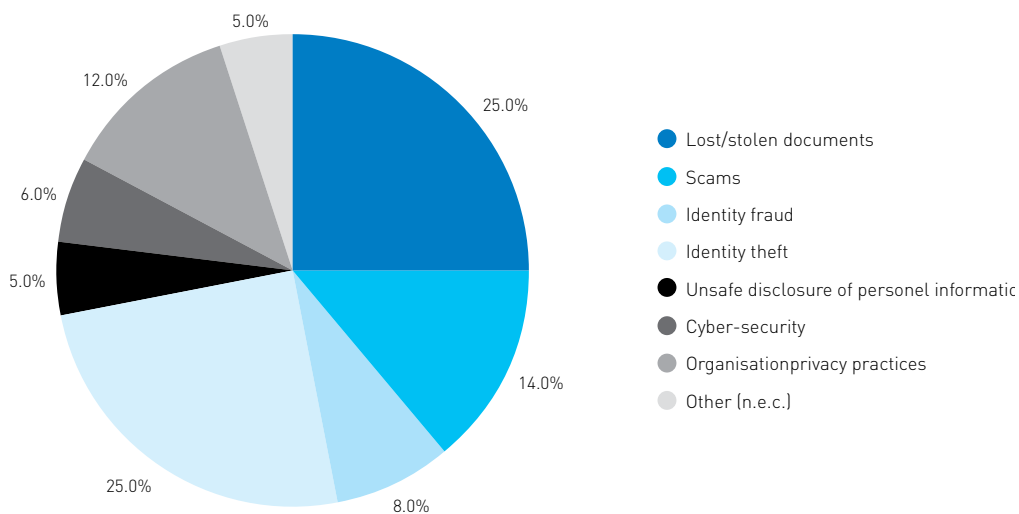
a. Includes instances where personal information and documents have been stolen in electronic formats.

b. Includes businesses and government agencies seeking guidance in relation to best practices for collecting, using and disclosing personal information.

Note: The abbreviation n.e.c stands for 'not elsewhere classified'.

The distribution of these enquiries is illustrated below in Figure 50.

Figure 50: Enquiries received by the AGD by subject matter



Source: Attorney-General's Department, unpublished data.

Office of the Australian Information Commissioner (OAIC)

The OAIC received a total of 67 enquiries that may have been related to identity crime in 2013–14. These enquiries were in relation to a number of National Privacy Principles (NPP), Information Privacy Principles (IPP) and Australian Privacy Principles (APP). The majority of enquiries (30) related to Part IIIA of the *Privacy Act 1988* [Cth] which regulates consumer credit reporting in Australia.

The second most prevalent issue about which the OAIC received enquiries which may have related to identity crime involved NPP 4, with 16 enquiries (see Table 5). NPP 4 places an obligation on organisations to take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

Table 5: Number of enquiries possibly related to identity crime received by the OAIC in 2013–14

Issue	Number of enquiries possibly involving identity related issues
NPP 1	3
NPP 2	8
NPP 4	16
NPP 6	3
IPP 4	1
Part IIIA <i>Privacy Act 1988</i>	30
Privacy generally	2
APP 11	4
Total	67

Source: OAIC unpublished data.

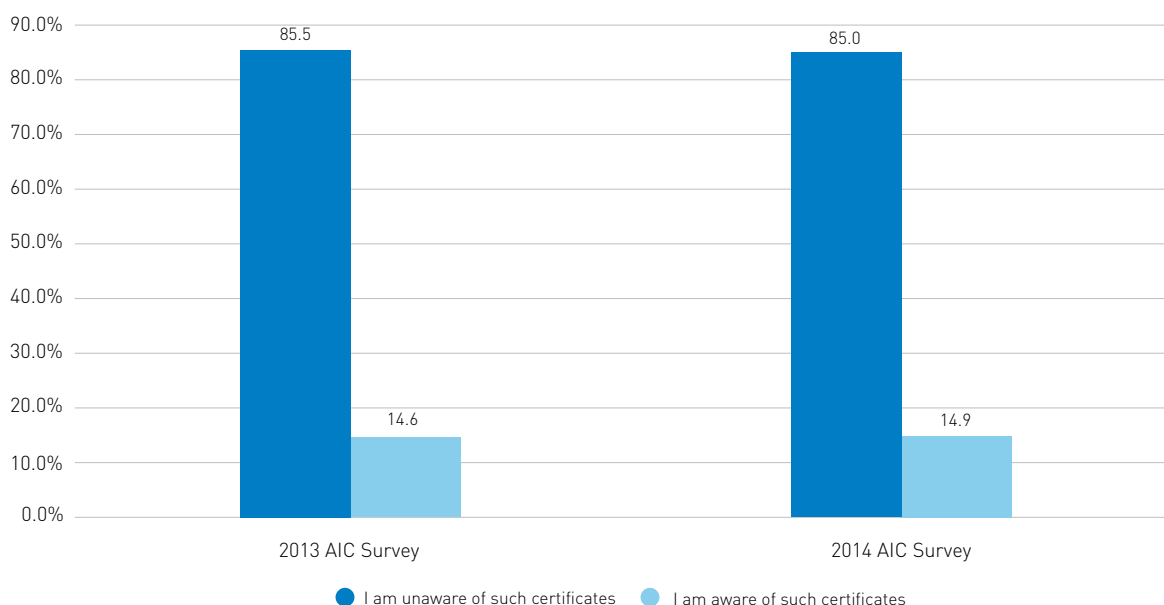
4.3 Number of applications for victims' certificates

Key finding: 'Victims of Identity Crime' Certificates continue to be under-utilised, with no certificates being issued at the Commonwealth level in 2013–14. In 2014, only 15% of respondents in the AIC's 2014 Identity Crime and Misuse Survey indicated they were even aware that victims' certificates exist.

Victims' Certificates record the name of the victim and describe the circumstances in which the person has been a victim of identity crime. They are designed to assist victims by providing evidence of the victim's true identity (AGD 2015c). Whilst the certificates do not compel organisations to take particular action—such as re-establishing the victim's credit rating or removing fraudulent transactions from the victim's record—they may assist victims in their negotiations with organisations to re-establish their identity credentials (AGD 2015c). Provisions regarding Victims' Certificates are found in Division 375.1 of the *Criminal Code Act 1995* [Cth] as well as in the criminal law statutes of some states.

The low uptake rate of these certificates can partially be 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). Other reasons for the low usage rates could be that victims are choosing not to apply for one, or are simply not aware that the certificates exist. Indeed, this would appear to be supported by results from the AIC's 2013 and 2014 Surveys which found that approximately 85% of respondents were unaware of the existence of Victims' Certificates (see figure 51 below).

Figure 51: Respondents' awareness of victims' certificates



Source: 2013 and 2014 AIC Surveys.

Note: Data were weighted to reflect the distribution of the population across jurisdictions. Percentages may not total 100.

5. Prevention of identity crime

5.1 Range of identity credentials verifiable using the Document Verification Service (DVS)

Key finding: The DVS can be used to verify information on the majority of government-issued identity credentials that are most commonly relied upon as evidence of identity.

The DVS is a secure, online system that provides for automated checks of the accuracy and validity of information regarding certain government documents that are often presented as evidence of a person's identity. The DVS enables users to match the biographical data on identity credentials with the records of the issuing authority, and in this regard, plays an important role in detecting fraudulent documents.

5.2 Number of government agencies using the DVS

Key finding: As at 30 June 2014, 16 government agencies were users of the DVS, compared to 12 at 30 June 2013.

This is a substantial increase, with just over 2.1m transactions being conducted as at June 2014. Government organisations accounted for 87% of that total.

5.3 Number of private sector organisations using the DVS

Key finding: There were 52 private sector organisations registered to use the DVS as at 30 June 2014—just a few months since private sector access to the service commenced. Private sector use of the DVS is expected to increase significantly throughout 2014–15 and beyond.

When first introduced in 2011, the DVS was only available for use by government agencies. Following a decision to expand access in 2012–13, private sector organisations that are required to identify their customers under Commonwealth law, and who meet the necessary requirements of the *Privacy Act 1988* [Cth] have been able to access this service.

While the DVS has been well utilised by private sector organisations, the usage rates have not been as high as government agencies. It is possible that this may be attributed to the fact that private sector agencies incur a fee each time they use the DVS, whereas government agencies are able to use the service free of charge.

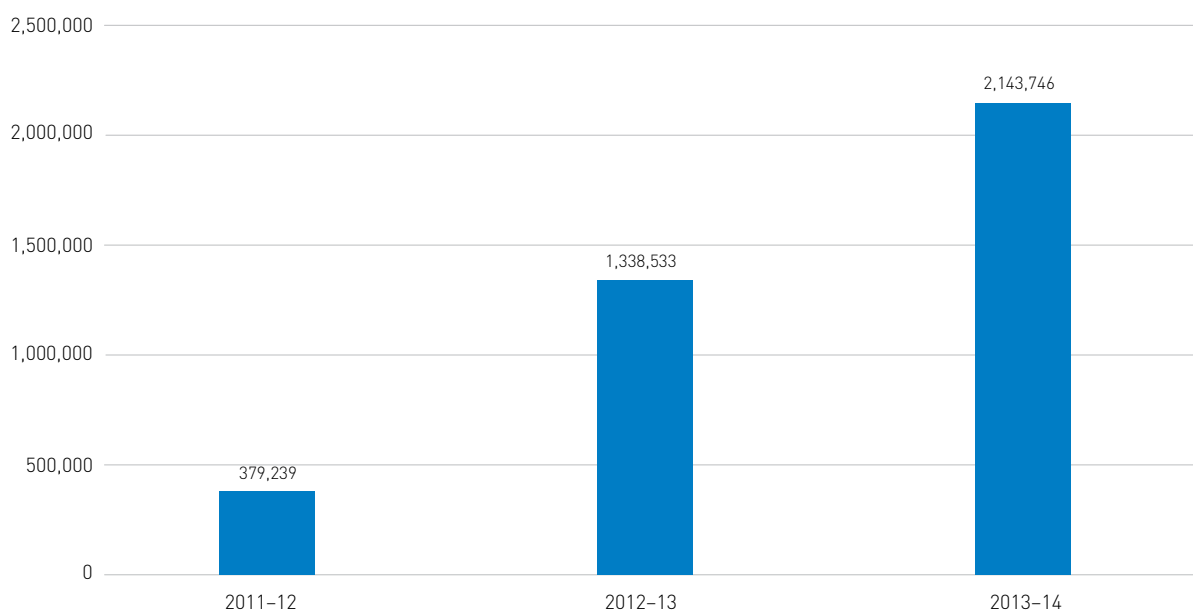
5.4 Number of DVS transactions each year

Key findings: Document verifications using the DVS have increased from 379,239 transactions in 2011–12 to over 2.1m transactions in 2013–14—an increase of approximately 465%. The number of DVS transactions that took place between 2012–13 and 2013–14 also increased by almost 60%.

The numbers of DVS transactions that have taken place since 2011–12 have increased considerably, jumping from 379,239 transactions in 2011–12 to over 2.1m transactions in 2013–14 (see Figure 52)—an increase of approximately 465%.

DVS transactions also increased by almost 60% between 2012–13 and 2013–14, with a total of 2,143,746 document verifications using the DVS in 2013–14, compared with 1,338,533 verifications in 2012–13. Government organisations accounted for 87% of the total document verifications.

Figure 52: Number of DVS transactions, by year (2011–12 to 2013–14)



Source: Attorney-General's Department unpublished data.

Note: These figures include repeat transactions, for example where data entry errors occur. Some validation attempts can involve numerous transactions.

5.5 Online security practices—individuals, business and government

Key finding: The majority of Australians have taken steps to counter the threats posed by cybercrime on their home computers. However, a considerable number of Australians appear to have overlooked the threats posed by cybercrime (and identity crime) arising from smartphone usage.

Research suggests that Australians who have had their personal information misused change their behaviour in a number of ways, with the top three behavioural changes involving changing of passwords; exercising greater care when reviewing financial statements, and exercising greater care when using or sharing personal information.

Whilst studies have found larger organisations to be well-equipped to deal with the threats posed to their businesses by cybercrime, small and medium-sized businesses often do not have the same capacity to deal with cybercrime incidents. Accordingly, they are often a relatively easy target for cybercriminals.

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. Indeed, research conducted by Norton as part of its Cybercrime Report in 2013 found that 60% of Australian adults had been a victim of cybercrime at some point in their lifetime, and 46% had been a victim of cybercrime in the previous year [Norton 2013].

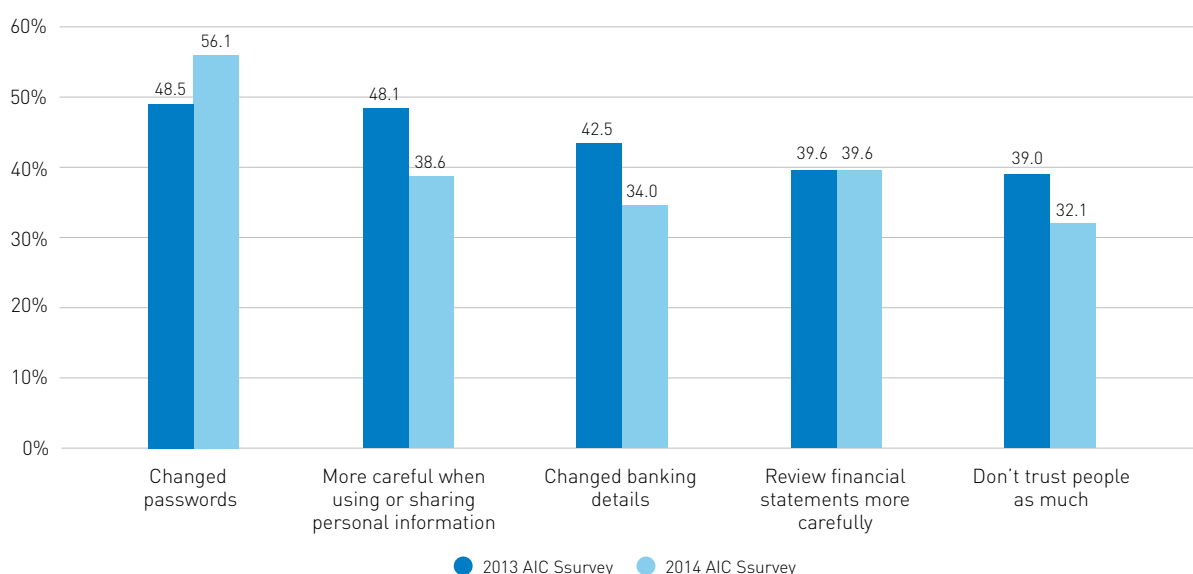
According to the ABS, 83% of Australian households had access to the Internet from home in 2012–13, compared with just 64% in 2006–2007 (ABS 2014c). Despite such a high level of Internet access, a survey undertaken by the Australian Communications and Media Authority (ACMA) regarding the online security practices of Australians, found that only 54% of Australian adults were confident in their ability to actually manage the security of their personal information online (ACMA 2011).

Although just over half of Australian adults expressed confidence about managing the security of their personal information online, internet security is clearly an issue that the majority of Australian internet users have considered at some point. Indeed, the use of anti-virus and other software to counter the threat of cybercrime has been found to be quite high among Australian internet users, with the ABS finding that 90% of the 15.3m people who had access to a computer at home had anti-virus and firewall software, and 13% had filtering software (it should be noted that it was possible to select more than one type of security measure) (ABS 2011a).

Despite this vigilance with home computers, research suggests that Australians have overlooked the security risks posed by cybercrime (and identity crime) involving smartphones. Of Australian respondents interviewed as part of Norton's research, 32% indicated that they had experienced cybercrime as a result of using their smartphones, and 59% of mobile device users indicated that they were not aware that security devices for mobile phones existed (Norton 2013).

In regard to the ways in which individuals change their behaviour following the misuse of their personal information, the five most common behaviour changes identified by respondents in these surveys are illustrated in Figure 53 below.

Figure 53: Behaviour changes arising from the misuse of personal information



Source: 2013 and 2014 AIC Surveys.

Note: Respondents were able to select more than one response for this survey question.



Business

One of the more recent studies conducted to determine the attitudes of the Australian business community towards cybercrime was the *2012 Cyber Crime and Security Survey: Systems of National Interest* (CERT Australia, 2012). A total of 255 organisations from a number of business sectors responded to the survey, which found that over 90% of respondents used anti-virus software, firewalls and anti-spam filters; and almost 60% of respondents reported using some sort of intrusion detection system. Small and medium-sized businesses often do not have the same capacity as larger organisations to deal with cybercrime incidents. Accordingly, they are often a relatively easy target for cybercriminals (Verizon 2012).

Government agencies

A number of policy frameworks and guidelines have been produced in an effort to assist government agencies to effectively deal with the threat of cyber-attacks; for example, the Attorney-General's Department (AGD) Protective Security Policy Framework (PSPF) for government agencies (AGD 2015b).

The Australian Signals Directorate (ASD) (formerly the Defence Signals Directorate) also advises the Australian Government about matters relating to the security and integrity of information. To assist government agencies in this regard, the ASD has developed a list of strategies to mitigate the risk of cybercrime attacks (ANAO 2014).

At least 85% of the targeted cyber intrusions to which the ASD responds could be prevented by following the top four mitigation strategies outlined in its *Strategies to Mitigate Targeted Cyber Intrusions* (ANAO 2014). These include:

- application whitelisting;
- patching applications and operating systems and
- using the latest versions, plus
- minimising administrative privileges (ASD 2012).

An additional tool that may be used by both state/territory governments and Commonwealth agencies is the 2014 Australian Government Information Security Manual—Controls (ISM) (ASD, 2014). This guide provides government agencies with strategies to detect, report and manage cyber security incidents.

Although many government agencies have taken positive steps to address the threats posed by cybercrime, it would appear that there are still a number of ways in which these cybercrime defences can be added to or improved. The security of government ICT systems has been the subject of a number of audits at both the Commonwealth and state levels. For instance, in 2013–14, the Australian National Audit Office (ANAO) conducted an audit entitled *Cyber Attacks: Securing Agencies' ICT Systems* (ANAO 2014). Seven Commonwealth agencies were audited, and a number of recommendations were made by the ANAO (ANAO 2014:29–30).

At the state level, an audit was conducted by the Victorian Auditor-General into the Victorian Government's Information Security Management Framework (Victorian Auditor-General 2013). This audit found that a number of Victorian agencies were '*potentially exposed to cyber-attacks, primarily because of inadequate ICT security controls and immature operational processes*' (Victorian Auditor-General 2013: x).

6. Estimating the economic impact of identity crime to Australia

Key findings: It is estimated that the total cost of identity crime in Australia is approximately \$2b including direct and indirect costs, but excluding prevention and response costs. If the estimated costs associated with preventing and responding to identity crime by government, business and individuals are included (\$350m), the estimated total economic impact of identity crime in Australia is approximately \$2.4b.

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.

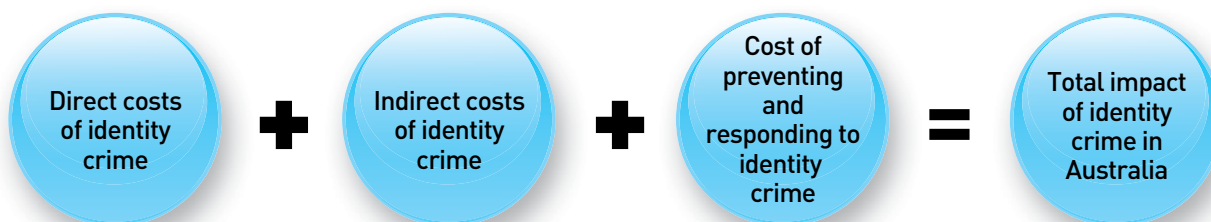
Several attempts have been made in the past to estimate the cost and economic impact of identity crime in Australia. The most recent attempt was made by the AGD in the Pilot Report, where it was estimated that identity crime in Australia cost the Australian economy \$1.6b (AGD 2014b).

The estimates presented in this report 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). Personal fraud victimisation survey data (ABS 2012) as well as officially recorded police statistics about fraud have also been relied upon.

The present methodology differs from that used in previous estimates of the cost of identity crime such as that presented in the Pilot Report, making direct comparisons inappropriate.

The methodology used to calculate the cost of identity crime can essentially 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 E and F.

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 below.

Figure 55: Formula for direct costs of identity crime

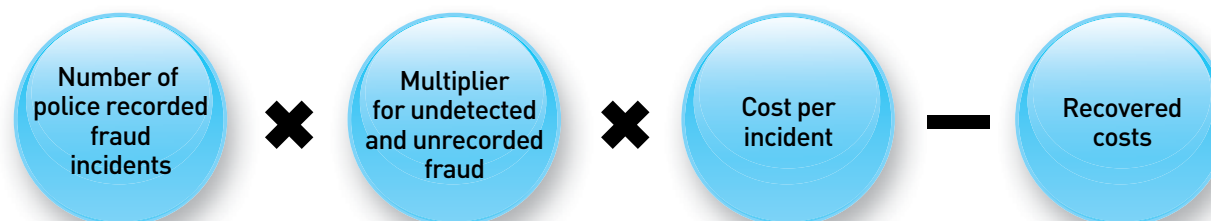


Table 6 below presents the data for each element of this formula. These figures have been rounded to the nearest whole number. Further details regarding the methodology, and data used in the calculation process are contained in Appendices E and F.

Table 6: Data for calculating direct cost of identity crime

Fraud category	Incidents	Multiplier	Cost per incident	Recovered costs	Total direct cost
Commonwealth fraud	135,672	1.15	\$1,526	\$9,936,641	\$228,154,457
Personal fraud	1,438,296	N/A ^a	\$300	N/A	\$431,488,800
Serious fraud	300	2.2	\$1,500,000	N/A	\$990,000,000
Police recorded fraud	85,605	4	\$4,229 per unrecorded fraud; \$26,819 per recorded fraud	N/A	\$3,381,911,130

a. Multiplier is inapplicable because incident numbers are derived from a victimisation survey.

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

In the absence of relevant Australian research, reliance has been placed on the work of Harrell & Langton (2013) in the United States, who found that 6% of all identity theft victims reported indirect losses as a result of their most recent incident of identity theft. 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. Victims reported a mean indirect loss of US\$4,168 (AU\$5,366) and a median loss of US\$30 (AU\$40).

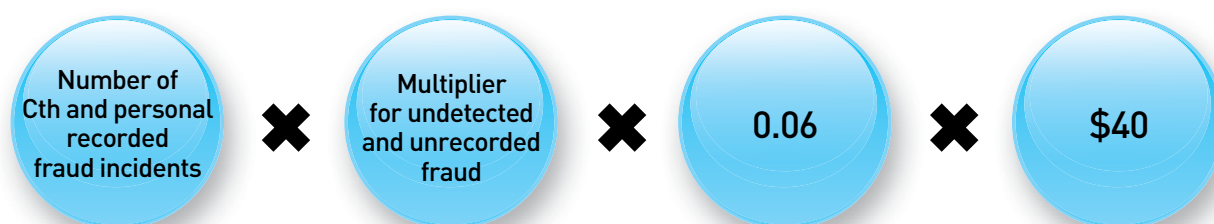
For each of the four categories of fraud examined in this report, the median or mean was used, where appropriate, as the value to determine the amount that indirect losses contributed to the cost of each fraud category.

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 below.

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



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

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

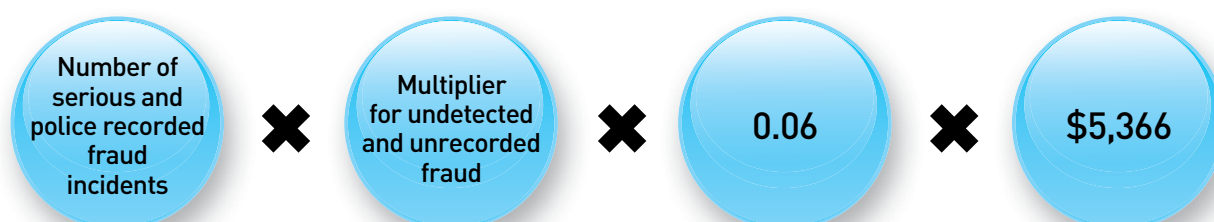


Table 7 presents data for each element of these formulae. These figures have been rounded to the nearest whole number. Further details regarding the methodology, and data used in the calculation process are contained in Appendices E and F.

Table 7: Data for calculating indirect cost of identity crime

Fraud category	Incidents (after multiplier applied)	# incidents considering only 6% had indirect loss	Total indirect cost after multiplying by median or mean
Commonwealth fraud	156,023	9,361	\$374,440
Personal fraud	1,438,296	86,298	\$3,451,920
Serious fraud	660	40	\$214,640
Police recorded fraud	342,420	20,545	\$110,245,543

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

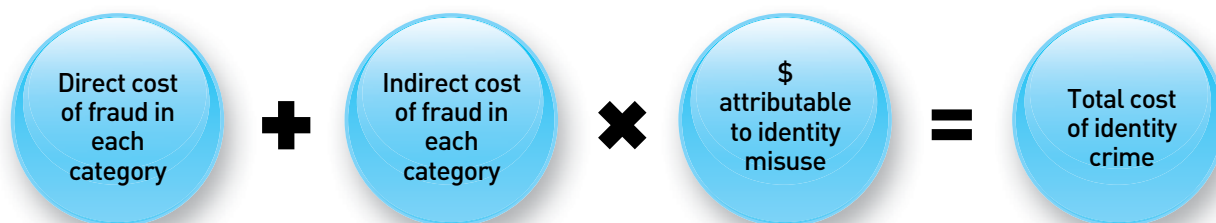


Table 8 below presents the data for each element of this formula. As is apparent from this table, the estimated cost of identity crime in Australia was approximately \$2b for 2013–14. Further details regarding the methodology, and data used in the calculation process are contained in Appendices E and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

Table 8: Data for calculating total cost of identity crime

Fraud category	Direct cost	Indirect cost	% ID Crime	ID Crime Cost
Commonwealth fraud	\$228,154,457	\$374,440	12.5	\$28,566,112
Personal fraud	\$431,488,800	\$3,451,920	100	\$434,940,720
Serious fraud	\$990,000,000	\$214,640	15	\$148,532,196
Police recorded fraud	\$3,381,911,130	\$110,245,543	40	\$1,396,862,669
Total				\$2,008,901,697

Calculating the costs of responding to and preventing identity crime

The estimated costs associated with responding to and preventing 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.

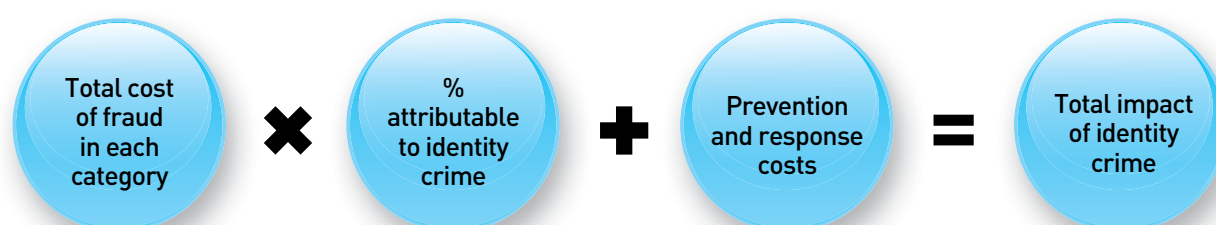
An attempt was made to assess costs for as many Commonwealth and state and territory agencies as possible. The agencies considered, and the costing details of the percentage of identity-related crime costs incurred by the agencies and organisations, are presented in Appendix E2.

The total estimated cost of prevention and response activities was approximately \$350m.

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 below. 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 \$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 \$350m is added to this total, it is estimated that the economic impact of identity crime in Australia would be approximately \$2.4b.

Conclusions

Research conducted over many years has suggested that identity crime is one of the most prevalent types of crime in Australia; generating substantial profits for offenders and considerable financial losses to individuals, business organisations and government agencies.

This report has sought 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, and has also attempted to estimate the economic impact of this crime for Australia in 2013–14. In doing so, the report builds on the AGD's development of a National Identity Crime and Misuse Measurement Framework which sought to establish 'baseline' estimates on the prevalence and impact of identity crime using data for 2012–13.

A large number of government agencies at both the Commonwealth and state and territory levels provided valuable data for inclusion in this report. This is to be commended, as it is only through the sharing of this information and analysis that the extent of identity crime in Australia can be better understood.

Despite this, there are a number of difficulties involved in accurately determining the prevalence and impact of identity crime and misuse in Australia. The under-reporting of identity crime victimisation; difficulties in linking data breaches to identity crime incidents; inconsistencies in the ways in which agencies record identity crimes; and problems of estimating the percentage of fraud that involves misuse of identity information, means that achieving an accurate picture of the true prevalence of this crime is problematic.

Work is underway to improve the quality and availability of information on identity crime and misuse in Australia. This will be an ongoing effort involving police, courts and government agencies across the Commonwealth, states and territories; as well as the private sector and other non-government organisations. It will assist future iterations of this research in presenting a more accurate picture of the true prevalence and cost of identity crime in Australia, and to guide efforts under the *National Identity Security Strategy* to reduce the impacts of identity crime on the Australian community.

References

All URLs are current at 8 July 2015.

Association of Certified Fraud Examiners (ACFE) 2014. *Report to the Nations on Occupational Fraud and Abuse, 2014 Global Fraud Study*. <http://www.acfe.com/rtn/docs/2014-report-to-nations.pdf>

Attorney-General's Department 2015a. *Document Verification Service website*. Canberra: <http://www.dvs.gov.au/Pages/default.aspx>

Attorney-General's Department 2015b. *Protective Security Policy Framework website*. Canberra: <http://www.protectivesecurity.gov.au/Pages/default.aspx>

Attorney-General's Department 2015c. *Victims of Commonwealth Identity Crime*. Canberra: <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/VictimsofCommonwealthidentitycrime.aspx>

Attorney-General's Department 2014a. *Cyber Emergency Response Team (CERT) website*. Canberra: <http://www.ag.gov.au/RightsAndProtections/CERT/Pages/default.aspx>

Attorney-General's Department 2014b. *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 2012a. *Identity Theft: Concerns and Experiences*, Di Marzio Research, Donvale: Victoria. http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity

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>

Attorney-General's Department 2011. *Identity Theft: Concerns and Experiences*, Di Marzio Research, Donvale: Victoria. http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity

Attorney-General's Department 2001. *Scoping Identity Fraud*. An abridged version of a report on Identity Fraud Risks in Commonwealth Agencies: Canberra.

Australian Bureau of Statistics 2015. *Crime Victimisation, Australia, 2013–14*, ABS Cat No.4530.0, Canberra: <http://www.abs.gov.au/ausstats/abs@.nsf/mf/4530.0>

Australian Bureau of Statistics 2014. *Household Use of Information Technology, Australia, 2012–13*, ABS Cat. No. 8146.0, Canberra: <http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/D0DD505F12749281CA257C89000E3F5E?opendocument>

Australian Bureau of Statistics 2013. *Australian Demographic Statistics, June 2013*, ABS Cat. No. 3101.0, Canberra: <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3101.0Main+Features1Jun%202013?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/E6838CDEE01D34BCA25722E0017B26B>

Australian Bureau of Statistics 2011a. *Household Use of Information Technology, Australia, 2010–11*. ABS Cat. No. 8146.0, Canberra: <http://www.abs.gov.au/ausstats/abs@.nsf/0/192B7AFC26FF3538CA25796600152BDF?opendocument>

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) 2014. *Targeting Scams – Report of the ACCC on scams activity 2013*. Canberra: <https://www.accc.gov.au/system/files/Targeting%20Scams%202013.pdf>

Australian Crime Commission 2013. *Organised Crime in Australia 2013*, Canberra: <http://www.crimecommission.gov.au/sites/default/files/files/ACC%20OCA%202013.pdf>

Australian Cybercrime Online Reporting Network (ACORN) 2015. *Australian Cybercrime Online Reporting Network website*. <http://www.acorn.gov.au/>

Australian Federal Police (AFP) 2014. *Platypus Magazine*. Jan–June 2014. <http://www.afp.gov.au/~media/afp/pdf/p/platypus115.pdf>

Australian National Audit Office (ANAO) 2014. *Cyber Attack: Securing Agencies' ICT Systems*. Audit Report No. 50 - 2013–14. Canberra: http://www.anao.gov.au/~media/Files/Audit%20Reports/2013%202014/Audit%20Report%2050/AuditReport_2013-2014_50.pdf

Australian Payments Clearing Association (APCA) 2014. *Australian Payments Fraud Details and Data*. <http://apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2014.pdf>

Australian Signals Directorate (ASD) 2014. *2014 Australian Government Information Security Manual – Controls*. Canberra: http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf

Australian Taxation Office (ATO) 2014. *Annual Report 2013–14*. Canberra: http://annualreport.ato.gov.au/sites/default/files/downloads/n0995-10-2014_js32662_w.pdf

- CERT Australia 2012. *Cyber Crime and Security Survey Report 2012*. Commonwealth of Australia: Canberra. <http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf>
- 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 2014. *Annual Report 2013/14*. Canberra: <http://www.cdpp.gov.au/wp-content/uploads/CDPP-Annual-Report-2013-2014.pdf>
- Credit Industry Fraud Avoidance Service (CIFAS) 2013. *Is identity fraud serious?*, United Kingdom, http://www.cifas.org.uk/is_identity_fraud_serious
- 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>
- Cuganesan S & Lacey D 2003. *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, Sydney: SIRCA.
- Department of Foreign Affairs and Trade (DFAT) 2014. *Annual Report 2013-2014*. Canberra: <http://dfat.gov.au/about-us/publications/corporate/annual-reports/annual-report-2013-2014/dfat-annual-report-2013-14.pdf>
- Department of Foreign Affairs and Trade (DFAT) 2014. *Annual Report 2012-2013*. Canberra: <http://dfat.gov.au/about-us/publications/corporate/annual-reports/annual-report-2012-2013/index.html>
- Department of Foreign Affairs and Trade (DFAT) 2014. *Annual Report 2011-2012*. Canberra: http://dfat.gov.au/about-us/publications/corporate/annual-reports/annual-report-2011-2012/pdf/DFAT_AR_2011-12.pdf
- Department of Human Services 2008-2014. *Annual Reports*, Canberra: <http://www.humanservices.gov.au/corporate/publications-and-resources/annual-report/>
- Harrell E & Langton L 2013. *Victims of Identity Theft, 2012*. Bureau of Justice Statistics, Office of Justice Programs, US Department of Justice. <http://www.bjs.gov/content/pub/pdf/vit12.pdf>
- 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*.
- Javelin Strategy and Research 2012. *2012 Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier*, <https://www.javelinstrategy.com/brochure/239>
- Jorna P & Smith RG forthcoming. *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>

KPMG 2010. *Fraud and Misconduct Survey 2010*. <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/Fraud-Survey-2010.aspx>

KPMG 2009. *Fraud Survey 2008*. <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/Fraud-Survey-2008.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

Lozusic R 2003. *Fraud and Identity Theft*, Briefing Paper No. 8/03, New South Wales Parliamentary Library Research Service: Sydney. [http://www.parliament.nsw.gov.au/prod/parlament/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146/\\$File/08-03.pdf](http://www.parliament.nsw.gov.au/prod/parlament/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146/$File/08-03.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.

National Fraud Authority 2013. *Annual Fraud Indicator – June 2013*, London: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf

Northern Territory Police, Fire and Emergency Services 2014. *Annual Report 2013-14*. Darwin: <http://www.pfes.nt.gov.au/Publications-and-forms.aspx>

Norton 2013. *2013 Norton Report – Country Report: Australia*, Symantec: <http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-australia.pdf>

NSW Bureau of Crime Statistics and Research (BOCSAR) 2014. *NSW Recorded Crime Statistics 2014*. <http://www.bocsar.nsw.gov.au/Documents/RCS-Annual/RCS2014.pdf>


Office of the Australian Information Commissioner 2014. *OAIC Annual Report – 2013-14*, Canberra: <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/>

Office of the Australian Information Commissioner 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

Office of the Australian Information Commissioner 2012. *Data breach notification: A guide to handling personal information security breaches*, Canberra. <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>

Office of the Australian Information Commissioner 2012a. *OAIC Annual Report – 2011-12*, Canberra: <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201112/>

- Office of the Australian Information Commissioner 2011. *OAIC Annual Report – 2010-11*, Canberra: <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201011/>
- Ponemon Institute 2014. *2014 Cost of Data Breach Study: Australia*, http://www-935.ibm.com/services/multimedia/2014_report_au_en_codb_V5.pdf
- 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:///a:icsf/downloads/catherine.emami/Downloads/global-economic-crime-survey-2014%20\(3\).pdf](file:///a:icsf/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>
- Richards K 2009. *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Research and Public Policy Series 102, Australian Institute of Criminology: Canberra. <http://www.aic.gov.au/documents/3/B/3/%7B3B3117DE-635A-4A0D-B1D3-FB1005D53832%7Drpp102.pdf>
- 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, Brown R, & Harris-Hogan S forthcoming. *Identity crime and misuse in Australia: Results of the 2014 online survey*. Australian Institute of Criminology: Canberra.
- 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, Sweeny 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 2014. *Annual Report 2013-14*. Adelaide: https://www.police.sa.gov.au/__data/assets/pdf_file/0008/58616/Annual-report-2013-2014__INTERNET.pdf
- Sproule S & Archer N 2010. Measuring identity theft and identity fraud. *International Journal of Business Governance and Ethics* 5(1-2): 51-63.
- Tasmanian Department of Police and Emergency Management 2014. *2013-14 Crime Statistics Supplement*. <http://www.police.tas.gov.au/wp-content/uploads/2013/10/2013-14-Crime-Statistics-Supplement-.pdf>



Unisys 2014. *Australia Unisys Security Index – Australia – May 2014*. <http://www.unisyssecurityindex.com/system/reports/uploads/314/original/Unisys%20Security%20Index%20Australia%20Report%20May%202014.pdf?1400743320>

Unisys 2013. *Australia Unisys Security Index – May 2013*. <http://www.unisyssecurityindex.com/usi/australia/reports>

Verizon 2012. *2012 Data Breach Investigations Report*. http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Victorian Auditor-General 2013. *WoVG Information Security Management Framework*, PP No. 281, Victoria: <http://www.audit.vic.gov.au/publications/20131127-WoVG-Info-Security/20131127-WoVG-Info-Security.pdf>

Victoria Police 2014. *Crime Statistics 2013-14*. Melbourne: http://www.police.vic.gov.au/content.asp?a=internetBridgingPage&Media_ID=72176

Western Australia Police Service 2014. *Monthly Verified Crime Statistics 2013-14*. <http://www.police.wa.gov.au/Aboutus/Statistics/Crimestatistics/tabid/1219/Default.aspx>

Appendix A—Graphs of state and territory police data

The nature of identity offences differs between Australian jurisdictions. Some states such as Queensland, South Australia, New South Wales, Western Australia and Victoria have introduced specific identity crime provisions into their criminal statutes. Other jurisdictions, such as the Australian Capital Territory (ACT), continue to rely on more general deception and dishonesty offences to capture identity crimes, thus making inter-jurisdictional comparisons difficult.

The manner in which identity-related offences are reported also differs between jurisdictions. Police data systems record crimes using the Australian Bureau of Statistics (ABS) standard offence classification codes, known as the *Australian and New Zealand Standard Offence Classification (ANZSOC) 2011* (ABS, 2011), whereby specific codes apply to crimes such as fraud, deception and forgery. However, there are no codes for identity-related crimes, which means identity crimes are often recorded under more general crime categories like fraud.

It has also been suggested by some law enforcement agencies that some identity offences may be being overlooked in preference for the more serious crimes that the identity crime facilitates. For instance, a person might be prosecuted solely for the fraud offence, despite having also committed the identity crime to facilitate that fraud. As a result, accurate data about the real incidence of identity crime is difficult to obtain.

The Australian Federal Police (AFP) recorded 34 incidents involving identity crime in 2013–14. Of these:

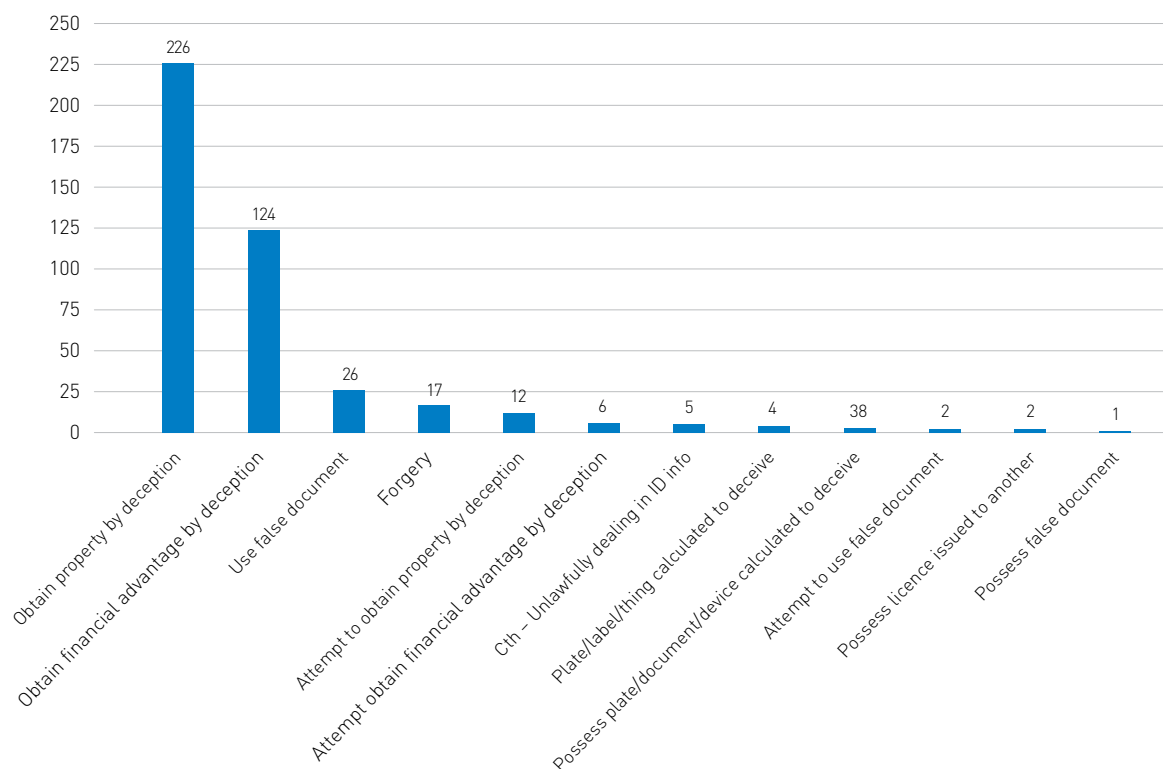
- 8 incidents related to fraud offences;
- 14 incidents explicitly related to identity crime;
- 5 related to aviation identity crime;
- 1 related to an international law enforcement agency request;
- 3 related to migration issues;
- 1 related to money laundering, and
- 2 offences involved a Commonwealth employee.

These 34 incidents do not represent all the offences investigated by the AFP during 2013–14 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.

Identity-related offences in the ACT

The ACT does not have specific identity crime offences, and instead, records these types of offences under more general deception and dishonesty offences. It is therefore difficult to compare the ACT's data with other jurisdictions. In the ACT, obtaining property by deception and obtaining financial advantage by deception were the most commonly applied identity-related offences in 2013–14 (see Figure 60).

Figure 60: Total number of identity-related offences in the ACT—2013–14



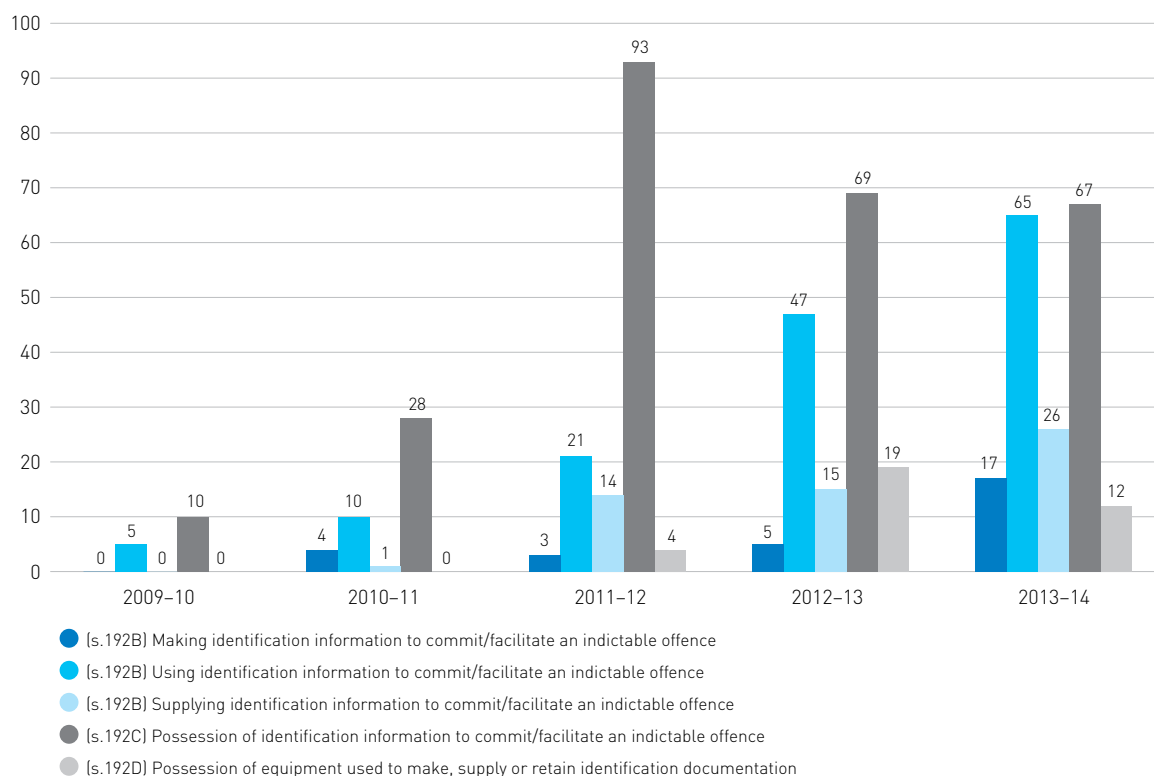
Source: ACT Policing unpublished data.

Identity related offences in Western Australia

There were 197 identity crime investigations carried out by Western Australia Police (WAPOL) in 2013–14. WAPOL estimated that victims lost a total of \$952,734, or approximately \$4,832 per offence. Each identity crime investigation took approximately 81 days to complete.

Identity-related offences in Victoria

There were a total of 187 identity-related offences recorded in Victoria in 2013–14, with the most common identity offence being possession of identification information with the intention of using the information to commit or facilitate an indictable offence. This was followed by the offence of making, using or supplying identification information to commit or facilitate an indictable offence. These results indicate a trend in the types of identity-related crimes being recorded by VICPOL, with these offences consistently being the most frequently applied of all the Victorian identity-related offences since 2009–10 (see Figure 61).

Figure 61: Identity crime related offences 2013–14 (Victoria)

Source: Victoria Police unpublished data.

Identity related offences in Queensland

There were a total of 572 identity-related offences recorded in Queensland in 2013–14. These offences related to;

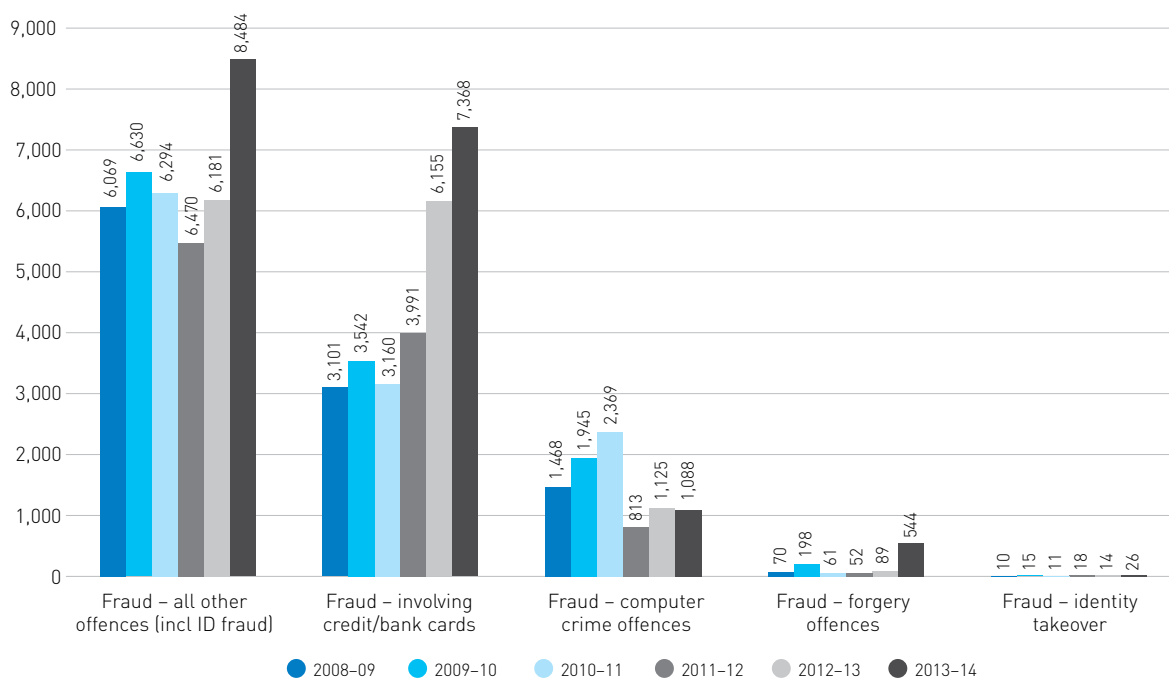
- possessing false identity documents;
- use of another identity;
- use of a fictitious identity, and
- identity takeover.

In 2013–14, recorded fraud offences involving credit or bank cards increased to their highest level in Queensland since 2008, with 7,368 offences of this nature recorded (see Figure 62). This is an approximately 20% increase on the number of offences recorded in 2012–13, and a 138% increase on the 3,101 credit and bank card fraud cases recorded in 2008–09.

The increase may be attributed to society's increasing use of online shopping and the consequent reliance on credit cards to complete these transactions. The Australian Payments Clearing Association (APCA) finding that 'card-not-present' fraud has increased in Australia from 45% of total card frauds in 2008, to 72% of all card frauds in 2013 (APCA, 2014) appears to support this view.

More general fraud offences also increased to their highest levels since 2008 in Queensland during the reporting period, with 8,484 general fraud offences (including identity fraud) recorded in 2013–14, compared with 6,181 offences in 2012–13 (see Figure 62 below).

Figure 62: Fraud offences detected by the Queensland Police Service, by offence type and year, 2008–09 to 2013–14



Source: Queensland Police Service unpublished data.

Note: Fraud-forgery offence data for 2013–14 are not directly comparable with previous years.

Appendix B—Measurement framework indicators

Table B1 –Measurement indicators of identity crime and misuse and data sources

Indicators	Description	Data source
1. Acquisition of fraudulent IDs		
1.1 The price of fraudulent identity credentials	The cost to illicitly acquire real Australian credentials or identities.	Data from law enforcement (and other government) agencies on the cost to illicitly acquire the most common identity credentials such as: <ul style="list-style-type: none"> • driver licences • Australian passport • Medicare card • birth certificate.
1.2 Number of reported data breaches	Acts as a proxy measure of organisational cyber security arrangements for protecting personal information.	Privacy (Information) Commissioners.
2. Use of fraudulent IDs		
2.1 Number of identity crime and misuse incidents recorded by government agencies.	Estimates the known (or detected) incidence of identity crime and or misuse, based on incidents recorded in Australian 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 Number of prosecutions for identity crime and other related offences	The number of prosecutions for identity related offences is used as a proxy for the number of serious incidents of identity crime and misuse that occur in Australia.	CDPP ABS Police (State & Territory)
2.3 Number of people who self-report being victims of identity crime or misuse	Estimates the victimisation rate based on self-report data, collected in specialised crime victimisation or consumer surveys.	AIC survey ABS surveys AGD surveys

Indicators	Description	Data source
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
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
3. Consequences of ID crime		
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.	Unisys 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
3.4 Number of identity crime victims experiencing non-financial consequences	Seeks to quantify the non-monetary harm caused by identity crime victimisation.	AIC Academic literature

APPENDIX B—MEASUREMENT FRAMEWORK INDICATORS

Indicators	Description	Data source
4. Remediation of ID crime		
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) spend trying to resolve the issue of having their identity stolen or misused.	ACCC ABS AGD 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 ABS CDPP
5. Prevention of ID Crime		
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
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
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
5.4 Number of DVS transactions each year	The number of validation transactions through the DVS each year	AGD
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 AIC Norton Verizon

Appendix C—Government agencies involved in this report

Table C1—Australian Government agencies involved in the Identity Crime and Misuse Monitoring Report 2015

Australian Government agency
Australian Bureau of Statistics
Australian Competition and Consumer Commission
Australian Crime Commission
Australian Electoral 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
Department of Defence
Department of Foreign Affairs and Trade—Australian Passport Office
Department of Human Services
Department of Human Services—Centrelink
Department of Immigration and Border Protection
Department of Industry, Innovation, Science, Research and Tertiary Education
Office of the Australian Information Commissioner

APPENDIX C—GOVERNMENT AGENCIES INVOLVED IN THIS REPORT

Table C2—State/territory government agencies involved in the Identity Crime and Misuse Monitoring Report 2015

State/territory government agency	
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
	Office of Fair Trading
	Department of Justice and Attorney-General
	Department of Transport and Main Roads
SA	South Australia Police
	Births, Deaths and Marriages Registration Office
	Consumer and Business Services
	Department of Planning, Transport and Infrastructure
WA	Western Australia Police
	Department of Commerce—Consumer Protection
	Department of Transport
ACT	ACT Policing
	Office of Regulatory Services

Appendix D—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>

Data Breach: *an incident that resulted in confirmed disclosure of information to an unauthorised party*

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 Guidelines 2011]

Identity crime: *a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of 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)

Appendix E—Calculating the cost of identity crime

Table E1: Total direct and indirect costs of identity crime in Australia

Fraud category	Reference period	Incidents	Cost per incident	Total cost	Multipliers	Indirect costs	Incidents after multipliers applied	Total cost (\$m) [after multipliers applied and including indirect costs]	% ID Crime	Applying % ID crime to total
Cth fraud (including undetected and unreported, less recovered)	2012–13	135,672	\$1,526	\$207,102,705	1.15	\$374,440	156,023	\$228,528,897	12.5%	\$28,566,112
Personal fraud (based on National Victimisation Surveys)	2013	1,438,296	\$300	\$431,488,800	NA	\$3,451,920	1,438,296	\$434,940,720	100%	\$434,940,720
Serious fraud	2011	300	\$1,500,000	\$450,000,000	2.2	\$214,640	660	\$990,214,640	15%	\$148,532,196
Police recorded fraud (excl. above categories)	2013–14	85,605	\$26,819 per recorded fraud; \$4,229 per unrecorded fraud	\$2,295,840,495 in recorded fraud costs; \$1,086,070,635 in unrecorded fraud costs	4	\$110,245,543	342,420 (85,605 recorded; 256,815 unrecorded)	\$3,492,156,673	40%	\$1,396,862,669
Total										\$2,008,901,697

Source: Derived from Smith, Jorna, Sweeney & Fuller 2014.

Table E2: Total costs of preventing and responding to identity crime in Australia

Jurisdiction	Portfolio / Type	Division	Annual recurrent expenditure \$	Crime %	Crime cost \$	% ID Crime	ID Crime Cost \$
Commonwealth	Attorney-General	Attorney-General	\$800,000,000	20.00%	\$160,000,000	1.00%	\$1,600,000
		ACLEI	\$6,000,000	100.00%	\$6,000,000	0.50%	\$30,000
		ACC	\$98,000,000	100.00%	\$98,000,000	10.00%	\$9,800,000
		Customs	\$1,450,000,000	15.00%	\$217,500,000	5.00%	\$10,875,000
		Aust Federal Police	\$1,370,000,000	70.00%	\$959,000,000	5.00%	\$47,950,000
		Aust Inst Criminology	\$5,000,000	100.00%	\$5,000,000	2.00%	\$100,000
		ALRC	\$3,000,000	25.00%	\$750,000	0.20%	\$1,500
		ASIO	\$394,000,000	30.00%	\$118,200,000	0.50%	\$591,000
		AUSTRAC	\$67,000,000	100.00%	\$67,000,000	1.50%	\$1,005,000
		Immigration	\$2,369,100,000	30.00%	\$710,730,000	3.00%	\$21,321,900
		Human Services	\$5,738,400,000	20.00%	\$1,147,680,000	3.00%	\$34,430,400
		Passports	\$200,949,000	10.00%	\$20,094,900	5.00%	\$1,004,745
		Tax	\$3,587,538,000	10.00%	\$358,753,800	5.00%	\$17,937,690
		CrimTrac	\$4,000,000	100.00%	\$4,000,000	2.50%	\$100,000
		Federal Court	\$91,000,000	10.00%	\$9,100,000	0.50%	\$45,500
		Federal Magistrates' Court	\$53,000,000	10.00%	\$5,300,000	0.50%	\$26,500
		High Court	\$19,000,000	30.00%	\$5,700,000	0.20%	\$11,400
		CDPP	\$92,000,000	100.00%	\$92,000,000	1.00%	\$920,000
		Parliamentary Counsel	\$12,000,000	15.00%	\$1,800,000	0.20%	\$3,600



APPENDIX E—CALCULATING THE COST OF IDENTITY CRIME

Jurisdiction	Portfolio / Type	Division	Annual recurrent expenditure \$	Crime %	Crime cost \$	% ID Crime	ID Crime Cost \$
Queensland	Criminal Courts	Supreme, County, Mag, Childrens'	\$182,900,000	100.00%	\$182,900,000	0.30%	\$548,700
	Coroners' Court		\$14,000,000	50.00%	\$7,000,000	0.10%	\$7,000
	Corrections	Prisons & Community Corrections & transport	\$175,792,000	100.00%	\$175,792,000	0.50%	\$878,960
	Justice & Attorney-General	Criminal Justice	\$298,824,000	100.00%	\$298,824,000	1.00%	\$2,988,240
		Human Rights	\$38,069,000	50.00%	\$19,034,500	0.05%	\$9,517
Queensland		Crime & Misconduct Commission	\$16,607,000	100.00%	\$16,607,000	0.50%	\$83,035
		Witness protection	\$5,975,000	100.00%	\$5,975,000	0.30%	\$17,925
	Queensland Police		\$1,785,100,000	80.00%	\$1,428,080,000	2.00%	\$28,561,600
	Qld DPP		\$40,700,000	100.00%	\$40,700,000	0.50%	\$203,500
	Criminal Courts	Supreme, District, Mag, Childrens'	\$146,000,000	100.00%	\$146,000,000	0.30%	\$438,000
Queensland	Coroners' Court		\$12,600,000	50.00%	\$6,300,000	0.10%	\$6,300
	Corrections	Prisons & Community Corrections & transport	\$159,547,000	100.00%	\$159,547,000	0.50%	\$797,735
	Attorney-General	Forensic Services	\$20,329,000	100.00%	\$20,329,000	0.30%	\$60,987
		Police Complaints Authority	\$1,326,000	100.00%	\$1,326,000	0.50%	\$6,630
		Justice Portfolio	\$19,041,000	50.00%	\$9,520,500	1.00%	\$95,205
South Australia	South Australia Police		\$669,200,000	80.00%	\$535,360,000	2.00%	\$10,707,200

Jurisdiction	Portfolio / Type	Division	Annual recurrent expenditure \$	Crime %	Crime cost \$	% ID Crime	ID Crime Cost \$
	SA DPP		\$38,933,000	100.00%	\$38,933,000	0.50%	\$194,665
	Criminal Courts	Supreme, District, Mag, Childrens'	\$67,300,000	100.00%	\$67,300,000	0.30%	\$201,900
	Coroners' Court		\$3,000,000	50.00%	\$1,500,000	0.10%	\$1,500
	Corrections	Prisons & Community Corrections & transport	\$80,917,000	100.00%	\$80,917,000	0.50%	\$404,585
	Western Australia						
	Attorney-General	General	\$128,105,000	50.00%	\$64,052,500	0.50%	\$320,263
		Corruption and Crime Commission	\$32,747,000	100.00%	\$32,747,000	0.50%	\$163,735
	Western Australia Police		\$1,122,300,000	80.00%	\$897,840,000	2.00%	\$17,956,800
	WA DPP		\$18,302,000	100.00%	\$18,302,000	0.50%	\$91,510
	Criminal Courts	Supreme, District, Mag, Childrens'	\$130,500,000	100.00%	\$130,500,000	0.30%	\$391,500
	Coroners' Court		\$4,800,000	50.00%	\$2,400,000	0.10%	\$2,400
	Corrections	Prisons & Community Corrections & transport	\$135,491,000	100.00%	\$135,491,000	0.50%	\$677,455
Tasmania							
	Attorney-General and Justice	Victims of Crime	\$7,970,000	100.00%	\$7,970,000	0.10%	\$7,970
		Protective Jurisdictions	\$1,811,000	50.00%	\$905,500	0.10%	\$906
		Legislation development	\$602,000	50.00%	\$301,000	0.10%	\$301
		Anti-Discrimination	\$1,191,000	10.00%	\$119,100	0.05%	\$60
	Tasmania Police		\$218,800,000	80.00%	\$175,040,000	2.00%	\$3,500,800
	Tasmania DPP		\$6,289,000	100.00%	\$6,289,000	0.50%	\$31,445

APPENDIX E—CALCULATING THE COST OF IDENTITY CRIME

Jurisdiction	Portfolio / Type	Division	Annual recurrent expenditure \$	Crime %	Crime cost \$	% ID Crime	ID Crime Cost \$
Northern Territory	Criminal Courts	Supreme, District, Mag, Childrens'	\$17,600,000	100.00%	\$17,600,000	0.30%	\$52,800
	Coroners' Court		\$400,000	50.00%	\$200,000	0.10%	\$200
	Corrections	Prisons & Community Corrections & transport	\$71,647,000	100.00%	\$71,647,000	0.50%	\$358,235
	Justice	Community Justice Policy	\$3,481,000	100.00%	\$3,481,000	0.30%	\$10,443
		Legal Policy	\$2,544,000	80.00%	\$2,035,200	0.10%	\$2,035
		Research & Statistics	\$1,651,000	100.00%	\$1,651,000	0.10%	\$1,651
ACT		Community Justice Grants	\$7,596,000	50.00%	\$3,798,000	0.05%	\$1,899
		Anti-Discrimination Commission	\$1,209,000	50.00%	\$604,500	0.05%	\$302
	NT Police		\$277,800,000	80.00%	\$222,240,000	2.00%	\$4,444,800
	NT DPP		\$9,770,000	100.00%	\$9,770,000	0.50%	\$48,850
	Criminal Courts	Supreme, District, Mag, Childrens'	\$20,200,000	100.00%	\$20,200,000	0.30%	\$60,600
	Coroners' Court		\$1,100,000	50.00%	\$550,000	0.10%	\$550
ACT	Corrections	Prisons & Community Corrections & transport	\$124,012,000	100.00%	\$124,012,000	0.50%	\$620,060
	Justice & Community Safety	Policy advice	\$9,430,000	100.00%	\$9,430,000	0.10%	\$9,430
		Protection of Rights	\$9,110,000	50.00%	\$4,555,000	0.10%	\$4,555
		Access to law & justice	\$147,000	100.00%	\$147,000	0.05%	\$74
		Court security	\$952,000	100.00%	\$952,000	0.04%	\$381

Jurisdiction	Portfolio / Type	Division	Annual recurrent expenditure \$	Crime %	Crime cost \$	% ID Crime	ID Crime Cost \$
	ACT Police		\$148,500,000	80.00%	\$118,800,000	2.00%	\$2,376,000
	ACT DPP		\$8,912,000	100.00%	\$8,912,000	0.50%	\$44,560
	Criminal Courts	Supreme, District, Mag, Childrens'	\$13,200,000	100.00%	\$13,200,000	0.30%	\$39,600
	Coroners' Court		\$1,100,000	50.00%	\$550,000	0.10%	\$550
	Corrections	Prisons & Community Corrections & transport	\$15,135,000	100.00%	\$15,135,000	0.50%	\$75,675
All States & Territories							
	Forensic mental health		\$248,000,000	100.00%	\$248,000,000	0.05%	\$124,000
	Legal aid		\$270,000	100.00%	\$270,000	0.50%	\$1,350
	Juvenile Justice		\$640,000,000	100.00%	\$640,000,000	0.50%	\$3,200,000
	Victim compensation		\$177,000,000	100.00%	\$177,000,000	0.20%	\$354,000
	Child protection for criminal acts		\$1,500,000,000	100.00%	\$1,500,000,000	0.05%	\$750,000
	Violence against women support		\$124,000,000	100.00%	\$124,000,000	0.03%	\$37,200
	Voluntary services for crime		\$76,000,000	100.00%	\$76,000,000	0.06%	\$45,600
	Security industry		\$4,857,000,000	70.00%	\$3,399,900,000	0.50%	\$16,999,500
	Insurance administration		\$670,000,000	100.00%	\$670,000,000	0.03%	\$201,000
	Household precautions		\$2,360,000,000	100.00%	\$2,360,000,000	0.20%	\$4,720,000
	Conveyancing		\$2,000,000,000	5.00%	\$100,000,000	0.05%	\$50,000
	Births, Death, Marriages		\$54,000,000	10.00%	\$5,400,000	3.00%	\$162,000
	Road traffic		\$3,500,000,000	10.00%	\$350,000,000	4.00%	\$14,000,000
	Consumer affairs		\$402,000,000	5.00%	\$20,100,000	2.00%	\$402,000
TOTAL					\$24,110,372,500		\$349,854,612

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

Appendix F—Methodology for estimating the cost of identity crime

Cost of identity crime against Commonwealth agencies

In 2012–13, Commonwealth agencies reported a total of 135,672 internal and external incidents of fraud worth \$207,102,705 (Jorna & Smith forthcoming). This equates to approximately \$1,526 per incident. If this figure is inflated to cover the incidents for which an estimated cost was not reported and if a multiplier of 1.15 is applied to account for frauds that were undetected or unreported (Smith, Jorna, Sweeney & Fuller 2014), it is estimated that there were 156,023 incidents of fraud with an estimated loss of \$238,091,098. According to Jorna & Smith (forthcoming) a total of \$9,936,641 in recovered funds and reparations was recouped by Commonwealth agencies in 2012–2013. Deducting this from the total leaves a net total loss of \$228,154,457.

There were a total of 17,001 internal and external misuse of identity incidents recorded by Commonwealth agencies in 2012–13. This time period has been used, as figures for 2013–14 were not available at the time of publishing this report. Applying the multiplier of 1.15 mentioned above gives a total of 19,551 misuse of identity incidents recorded by Commonwealth agencies. Dividing these 19,551 identity incidents by the total 156,023 fraud incidents suggests that approximately 12.5% of Commonwealth fraud incidents were identity related.


In the United States, Harrell & Langton (2013) found that 6% 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\$4,168 and a median loss of US\$30. 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 that US\$30 is equivalent to AUD\$40, a total of \$374,440 in indirect costs needs to be added to the net total loss of \$228,154,457. Accordingly, Commonwealth agencies incurred \$228,528,897 in indirect and direct losses.

If it is assumed that identity crime represents 12.5% of all incidents of fraud experienced by Commonwealth agencies, identity crime as a proportion of all Commonwealth fraud would cost approximately \$28.5m.

Cost of identity crime against individuals

In 2010–11, the ABS conducted a survey of 26,405 Australian households in an effort to determine the prevalence of personal fraud in Australia. For the purposes of the ABS survey, personal fraud included scams, credit card fraud, identity fraud and identity theft (ABS, 2012). The survey was completed by one representative aged over 15 years from each household who had agreed to participate. The survey found that three in five victims (60%) of personal fraud, or 713,600 people, had lost money as a result of the fraud. This equated to an average loss of \$2,000 per victim, and a median loss of \$300.

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 2013 was used to determine the percentage of Australia's population who would have been aged over 15 years in 2013. 83% of Australia's population of 23,130,900 was aged over 15 years at June 2013 (ABS 2013). This equates to 19,198,647 people.



The ABS found that 6.7% of people aged over 15 years had experienced at least one incident of personal fraud (assuming credit card fraud, identity theft or scams all involved misuse of personal information) in the 12 months prior to interview in 2010–11. The AIC found that 8.7% of respondents in a similar survey it conducted in 2014 had experienced misuse of their personal information in the previous 12 months (Smith, Brown & Harris-Hogan forthcoming). The average of these two victimisation rates (7.7%) was used for the purposes of the identity crime estimate in this report.

Assuming that 7.7% of people aged over 15 years experienced personal fraud, there would have been 1,478,296 victims of personal fraud in 2013. The ABS (2012) found that 40,000 cases of personal fraud (3.4% of 1,188,100 victims of all types of personal fraud) were reported to police. Although not every matter that is reported to police is recorded, it is reasonable to deduct the 40,000 cases that were reported to police to avoid double-counting. Therefore, it is estimated that there were 1,438,296 victims of personal fraud in 2013.

According to the ABS (2012), victims of personal fraud lost an average of \$2,000, with a median loss of \$300. The AIC also found that victims who had experienced misuse of their personal information in the previous year lost an average of \$3,572, with a median loss of \$300 (Smith, Brown & Harris-Hogan forthcoming). Given the mean for both surveys 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 \$300 to calculate the direct cost of personal fraud. Accordingly, the total direct cost of personal fraud to individuals in Australia in 2013 was \$431,488,800.

If, as in the case of fraud against Commonwealth agencies, it is assumed that 6% of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell & Langton 2013), and victims had a median loss of AUD\$40, a total of \$3,451,920 in indirect costs needs to be added to the net total loss of \$431,488,800. Accordingly, individual victims of personal fraud incurred \$434,940,720 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 \$1.0m (KPMG 2013). Only 46% of the major incidents of fraud were reported to police (KPMG 2013).

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

APPENDIX F—METHODOLOGY FOR ESTIMATING THE COST OF IDENTITY CRIME

If, as noted above, it is assumed that 6% of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell & Langton 2013), and victims had an average loss of US\$4,168 (AUD\$5,366), a total of \$214,640 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 \$990,214,640 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 \$148,532,196.


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

In 2013–14, there were 126,305 fraud and dishonesty offences recorded by police throughout Australia (BOCSAR 2014; WA Police 2014; Dept. Police and Emergency Management 2014; SA Police 2014; Vic Police 2014; NT Police, Fire and Emergency Services 2014; Unpublished data from ACT Policing and QLD Police). Added to this are 72 referrals from Commonwealth agencies that were accepted by the AFP in 2012–13 (Jorna & Smith forthcoming). The financial loss associated with these 72 cases alone was \$102,426,346 or \$1,422,588 per matter (Jorna & Smith forthcoming). Accordingly, it is estimated that there were a total of 126,377 recorded fraud offences in Australia in 2013–14.

From these 126,377 recorded fraud offences, the 112 incidents of fraud against the Commonwealth that were referred to state and territory police by federal agencies in 2012–13 need to be deducted (Jorna & Smith forthcoming). A further deduction of 40,000 incidents should be made to reflect the 40,000 incidents of personal fraud that were reported to police in 2010–11 (ABS 2012), as well as the 660 serious fraud incidents estimated above. This brings the total estimated number of officially recorded fraud incidents to 85,605.

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 85,605 by a multiplier of 4.0 in order to determine the total number of recorded and unrecorded frauds. This results in a total of 342,420 recorded and unrecorded fraud offences. Deducting the 85,605 recorded fraud offences from the total 342,420 fraud incidents, yields 256,815 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 & Jorna 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 2013 would have been \$26,819, and \$4,229 respectively. Applying these figures to the estimated 85,605 recorded and 256,815 unrecorded frauds yields totals of \$2,295,840,495 for recorded frauds and \$1,086,070,635 for unrecorded frauds. This gives a grand total of \$3,381,911,130.

If, as noted above, it is assumed that 6% of all identity theft victims experienced indirect losses as a result of their most recent incident of identity theft (Harrell & Langton, 2013), and victims had an average loss of US\$4,168 (AUD\$5,366), a total of \$110,245,543 in indirect costs needs to be added to the total loss of \$3,381,911,130. 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 \$3,492,156,673.

For the purposes of this report, it has been estimated that up to 40% of police-recorded fraud and deception offences involve identity crime. This estimate is based on discussions with experts in this area, and recent observations by the United Kingdom's Credit Industry Fraud Avoidance Service (CIFAS) which found that 41% of all frauds recorded by CIFAS in 2014 involved instances of identity fraud (CIFAS 2015).

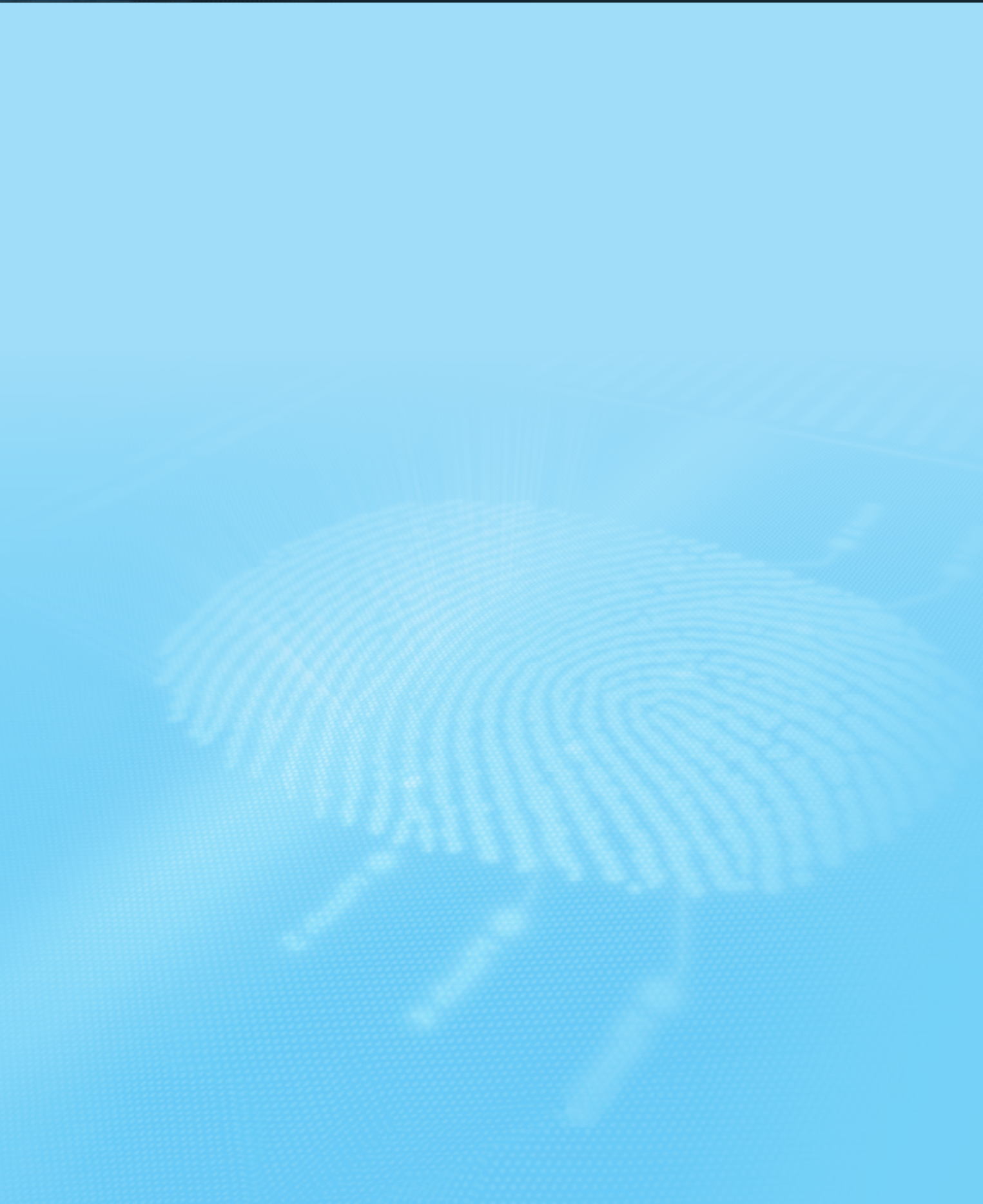
If it is assumed that 40% of police recorded and unrecorded fraud incidents involve identity crime, then it is estimated that the cost of identity crime as a proportion of police recorded and unrecorded fraud is \$1,396,862,669.

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 approximately \$350m. 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 and 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 2011-2012 Budget allocations for each agency or the agencies' 2011-2012 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 E.





IDENTITY SECURITY