NATIONAL IDENTITY SECURITY STRATEGY

Identity crime and misuse in Australia

Key findings from the National Identity Crime and Misuse Measurement Framework Pilot

IDENTITY SECURITY

ISBN: 978-1-925118-34-6

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:

Business Law Branch
Attorney-General’s Department
3–5 National Cct
BARTON ACT 2600
Telephone: 02 6141 6666
copyright@ag.gov.au

Contents

Foreword

It is almost ten years since Australian governments recognised that tackling identity crime should be a national priority, with the agreement in 2005 to develop a *National Identity Security Strategy*. In 2007, this was formalised in an Intergovernmental Agreement to a National Identity Security Strategy, which provides a roadmap for collaboration between the Australian Government and states and territories to strengthen Australia's 'identity infrastructure'.

Since that time, Australians have seen more and more of their everyday interactions with government, business and each other move from face-to-face to online channels. Australians have the right to remain anonymous in a wide range of situations. But it is becoming increasingly important that people can have confidence in the identities of the people with whom they are conducting sensitive or high value transactions; and that their own identities can be protected when transacting online. Growth in the Australian digital economy creates real efficiencies for government and businesses and fosters greater opportunities for improving the wellbeing of all Australians. Unfortunately, it also creates new ways for criminals to defraud governments, businesses and individuals, assisted by the criminal misuse of an individual's identity.

Identity crime is one of the most prevalent criminal activities in Australia, affecting hundreds of thousands of Australians every year. Criminals can generate significant profits by stealing personal identity information, then manufacturing or selling fraudulent identity credentials to defraud businesses, individuals and financial institutions. Criminals also use these illicit identities to access government benefits and services to which they are not entitled. Identity crime also lies at the heart of some of the most heinous criminal activity in facilitating terrorism, human trafficking and many other serious offences, where a criminal needs to disguise their true identity.

Taking all these impacts into account, this report estimates the economic impact of identity crime to Australia is likely to exceed $1.6 billion dollars every year.

The development of new and innovative approaches to identity security should be informed by a comprehensive and reliable evidence base on identity crime. With this in mind, this report represents one of the first attempts by any government worldwide to develop an identity crime measurement framework at the national level.

Executive summary

Efforts to combat identity crime require a reliable evidence base that quantifies the complete nature and extent of the problem. In Australia and also internationally, there are limited sources of comprehensive, reliable data about identity crime and its consequences.

To address this gap in knowledge, the Council of Australian Governments (COAG) agreed in 2012 that work should be undertaken to develop a national measurement framework for identity crime to better inform efforts to implement the National Identity Security Strategy (NISS). This report presents the key findings from a pilot data collection exercise that was undertaken as part of the project established to develop this measurement framework.

One of Australia's most prevalent crimes

Key finding: Each year around 4 to 5% of Australians (around 750,000 to 937,000 people) experience identity crime resulting in a financial loss. However, the true extent of identity crime is likely to be unknown, as a considerable proportion of incidents go unreported.

Each year around 4–5 per cent of Australians experience identity crime resulting in a financial loss.

The Australian Institute of Criminology conducted a 5,000-person online community survey (the AIC Survey) in 2013 as part of this pilot. They found that 9.4 percent of respondents reported having their personal information stolen or misused in the previous 12 months, with five percent reporting that they suffered financial losses as a result (Smith & Hutchings 2014).

Identity crime is likely under-reported by both individual victims and organisations. For example, recent research has shown that only 50 percent of credit card fraud victims and 66 percent of identity theft victims reported the incident to a formal institution, such as law enforcement or a financial institution (ABS 2012).

Identity crime is one of the most prevalent crime types affecting Australians each year.

Key finding: Compared with other personal and theft-related crimes (i.e. assault, robbery, break-ins and motor vehicle theft), identity crime is one of the most prevalent crime types affecting Australians each year.

When compared with the results from similar self-report victimisation surveys on other personal and theft-related crimes, it can be seen that identity crime is one of the most prevalent offence types in Australia (i.e. four percent of the population or around 750,000 people) (ABS 2012). For example, survey data from the ABS show that in 2012–13 an estimated three percent of Australians aged 15 years and over (498,000 people) were victims of assault, 2.7 percent of households (239,700 households) were victims of at least one break-in, 0.4 percent of people (65,700 people) were victims of robbery, and 0.6 percent of households had their motor vehicle stolen (57,200 incidents) (ABS 2014a).

At least one data breach occurs every week in Australia, with an average of 19,000 records lost or stolen per incident, costing $138 per record and a total of $2.16m to the organisation involved.

Acquiring a fraudulent identity

Key finding: The price of fraudulent identity credentials suggests they are relatively cheap and easy to obtain. This is reflected in the variety of ways that these credentials are used to commit identity fraud. Information on data breaches (many of which go unreported) also suggests that the personal information needed to create fraudulent identity documents is also available to those willing to seek it out.

In the main, criminals will use one of two approaches to obtaining a fraudulent identity: either creating a fictitious identity; or stealing all, or parts of, personal information from another person (living or deceased). To get the personal information required to establish a fraudulent identity, some criminals will illegally access databases held by government agencies or private sector organisations and steal personal information, or obtain this information through traditional means such as stealing it from mailboxes. In other cases, personal information will be accidentally made publicly available. Research into data breaches shows that there is an average of one every week in Australia, with around 19,000 records lost or stolen per incident, at an average cost of $138 per record, costing the agency or organisation involved an average of $2.16m per incident (Ponemon Institute 2012).

Another approach is to purchase a fraudulent identity credential, such as a driver licence or Medicare card, on the 'black market'. Information provided by the Australian Federal Police indicated that the price of fraudulent identity credentials ranges from around $80 (Medicare cards), to around $350 (driver licences), and $1,500 (for an Australian passport to be altered by a professional document forger) up to $20,000-$30,000 (for a legitimately issued passport with fraudulent details). Although some fraudulent credentials are relatively cheap to acquire, the ability to use them to facilitate criminal activity largely depends on their quality and the intrinsic security features (i.e. counterfeited documents compared to legitimately-issued documents with fraudulent details). The cost attributed to fraudulent Medicare cards ($80) and driver licences ($350) was for counterfeit documents that were not the most recent versions that contain state-of-the-art security features.

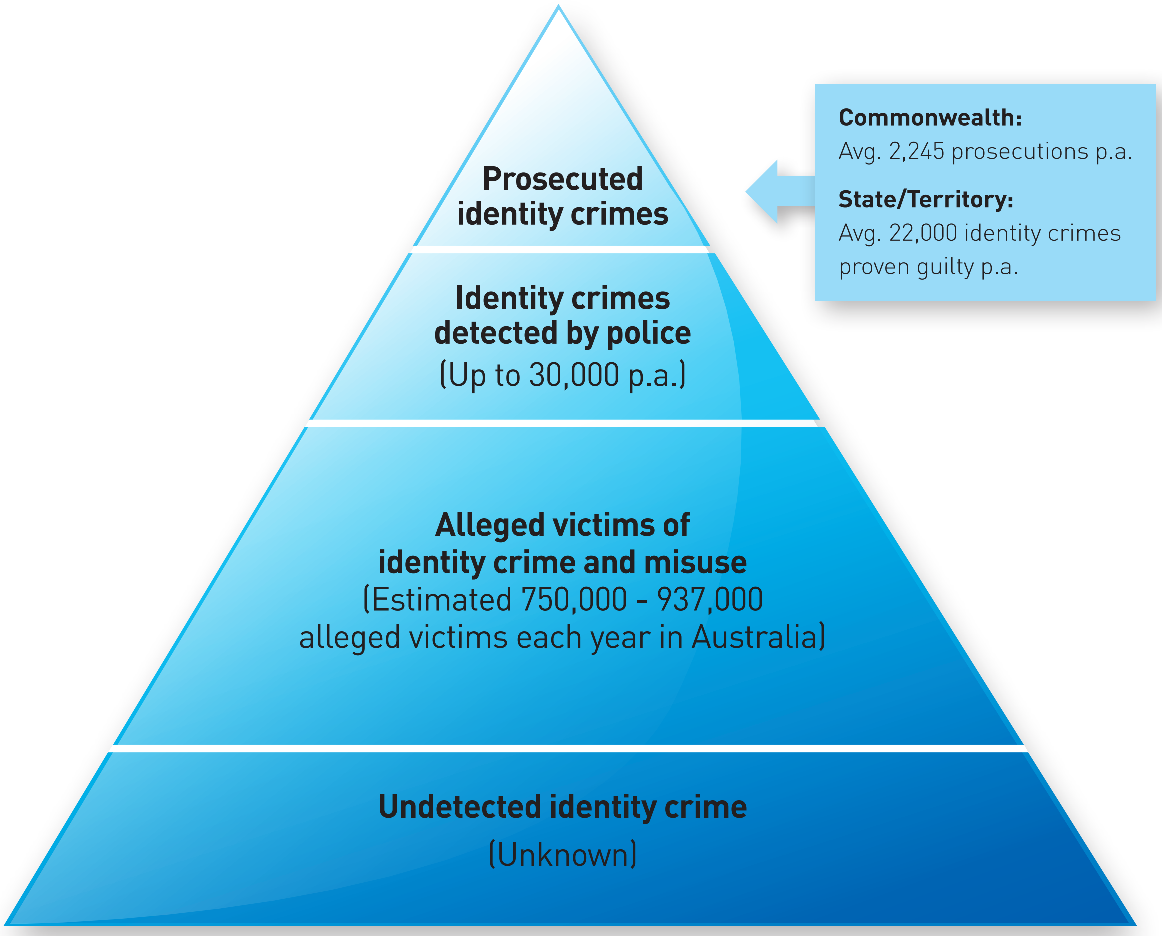
The price of fraudulent identity credentials ranges from around $80 (Medicare cards), to around $350 (driver's licences), up to $30,000 (for a legitimately issued passport with fraudulent details).

Identity crimes and the criminal justice system

Key finding: State and territory police detect up to an estimated 30,000 identity crimes each year, with around 24,000 offences proven guilty in a court of law. As identity crimes are often recorded under other related offences such as fraud, the actual number of identity crimes is likely much higher.

Data was collected to quantify the number of identity crime offences at each stage of the criminal justice process, from alleged victims, to identity crimes detected by police to the number that are prosecuted before the courts (see Figure 1).

Figure 1: Identity crime in Australia


Prosecuted identity crimes
Identity crimes detected by police
(Up to 30,000 p.a.)
Alleged victims of identity crime and misuse
(Estimated 750,000 - 937,000 alleged victims each year in Australia)
Undetected identity crime
(Unknown)
Commonwealth:
Avg. 2,245 prosecutions p.a.
State/Territory:
Avg. 22,000 identity crimes proven guilty p.a.

Due to the way identity crime statistics are collected in the criminal justice system, combined with the clandestine nature of these offences, and the fact that false or stolen identities are used to facilitate many other criminal activities besides fraud, it is highly likely that these numbers represent only a proportion of the true number of identity crimes committed in Australia each year.

Impacts on victims

Key finding: The majority of identity 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 to their mental or physical health, reputations or general wellbeing.

The consequences of identity crime for individuals can be serious, including financial loss, reputational damage as well as emotional and psychological harm.

While most victims of identity crime lose relatively small amounts of money, in some cases individuals have lost hundreds of thousands of dollars. The AIC Survey found that victims reported an average out-of-pocket loss of $4,101 per incident, with losses ranging between $1 and $310,000. However, as an indication of more typical cases, half of these victims lost less than $250 and three quarters lost $1,000 or less (Smith & Hutchings 2014).

The AIC Survey found that, on average, victims of identity crime will spend at least 18 hours dealing with the consequences of the incident, with victims of a total 'identity hijack' spending more than 200 hours (Smith & Hutchings 2014).

While financial losses suffered by victims can sometimes be recovered or reimbursed by financial institutions, the non-monetary impacts of identity crime can be equally if not even more significant to deal with. Victims of identity theft or misuse can suffer considerable psychological trauma and damage to their reputation, something that can be very difficult to repair.

On average, victims of identity crime spend at least 18 hours dealing with the consequences, with victims of a total 'identity hijack' spending more than 200 hours.

The AIC Survey found that 15 percent of respondents experienced mental or physical health impacts that led them to seek counselling or other medical treatment; while six percent reported being wrongly accused of a crime (Smith & Hutchings 2014).

Key finding: Only a small proportion of victims of identity crime report the incident to relevant organisations. Court-issued victims' certificates appear significantly underutilised as a mechanism to assist victims in recovering from the consequences of identity crime.

In some cases, victims may be eligible to apply for court-issued victims' certificates to assist in dealing with the consequences of identity theft, such as restoring credit ratings and recovering financial losses. However, the AIC Survey found that only around one in 10 victims of identity crime knew of the existence of these certificates, with fewer than one in 20 victims actually applying for one (Smith & Hutchings 2014). This suggests there is a general lack of awareness of these certificates in the community, that their availability is limited and/or that victims see them as being of limited value in recovering from the consequences of identity crime.

The identity crime victim support service provided by the not-for-profit organisation iDcare, is also another avenue victims can use to obtain assistance recovering from identity crime. However, this service was not operational during the pilot exercise and so could not provide data to inform the measurement framework.

Fewer than 2 in 5 victims of identity crime and misuse reported the incident to relevant authorities.

Prevention activities

Key finding: There are an increasing number of identity credentials that can be verified through the Document Verification Service (DVS), as well as a growing demand for the service amongst government and private sector organisations.

Many of the methodologies criminals use to commit identity crime are widely available from open sources. Some of these methodologies seek to exploit vulnerabilities in Australia's identity infrastructure that have been known for more than 15 years. One methodology known as "tombstone fraud" involves the theft and use of an identity belonging to a deceased person. In many cases this could be prevented through checks against death records whenever an application for an identity credential is lodged. Work is currently underway to improve national systems to make these checks more widely available.

> *Many of the methodologies used to commit identity crime exploit vulnerabilities in Australia's identity infrastructure that have been around for over 15 years.*

Key finding: As use of the DVS increases and counterfeit credentials become more easily detected, criminals are more likely to seek legitimately issued documents with fraudulent details.

The expansion of DVS use among government agencies and private sector organisations, which have a reasonable need to use the service in accordance with the *Privacy Act 1988*, will improve the ability to detect counterfeit identity credentials. As these counterfeit credentials become harder to use, there will be stronger incentives for criminals to seek legitimately issued documents with fraudulent details, both through methods such as the theft or takeover of real identities, or through compromising the processes of credential issuing agencies. To help prevent this from occurring on a widespread basis, the agencies that issue these credentials will need to strengthen their identity verification processes. Given the interdependencies of Australia's identity infrastructure, this will require a consistent, whole-of-government approach.

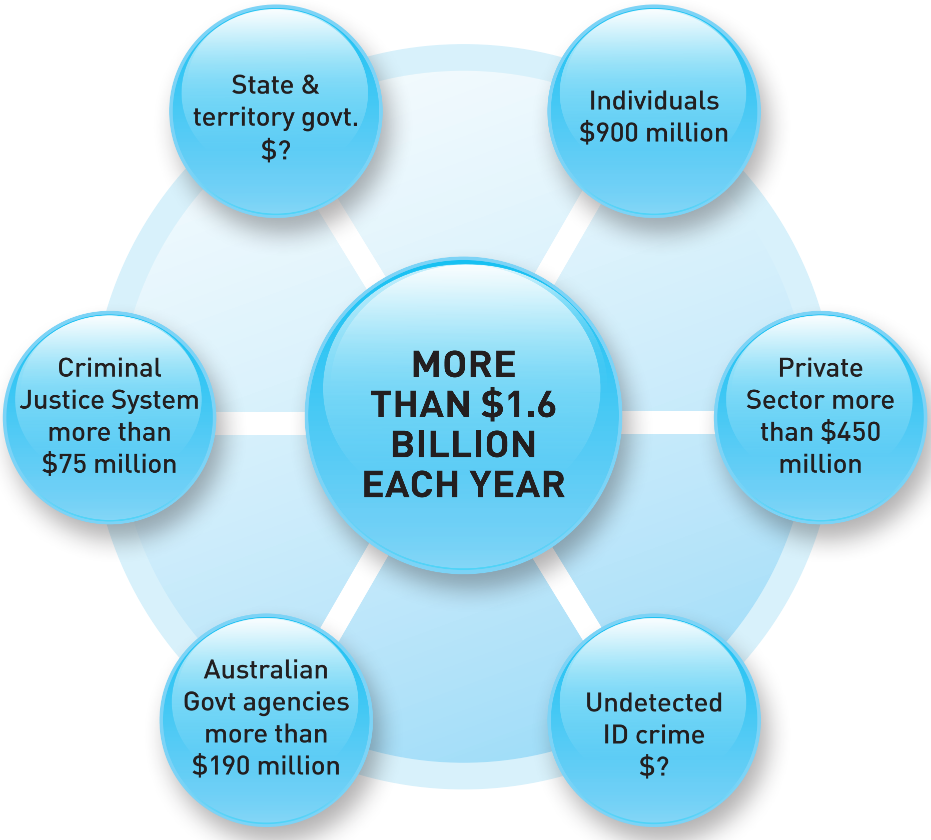
The economic impacts of identity crime

Key finding: The estimated economic impact of identity crime in Australia is likely to exceed $1.6 billion per year. In light of the limited data available and the underreporting of identity crime, by both individuals and organisations, this is likely to be a conservative estimate.

> *Identity crime seriously impacts the Australian economy, with estimates putting the direct cost at more than $1.6 billion per year.*

Based on an analysis of the data received during the pilot, the estimated *direct losses* from identity crime in Australia likely exceed $1.5 billion per year, with the *direct cost* of investigating and prosecuting these cases estimated at $75 million annually. These estimates include the direct financial losses suffered by individuals, government agencies and private sector organisations, as well as the estimated criminal justice system costs of investigating and prosecuting these cases (including the AFP, CDPP, state police and courts). These estimates are towards the conservative end of previous attempts to calculate the total cost of identity crime to Australia, which range from $800 million to $4 billion.

Figure 2: The economic impacts of identity crime


State & territory govt. $?
Individuals $900 million
Criminal Justice System more than $75 million
MORE THAN $1.6 BILLION EACH YEAR
Private Sector more than $450 million
Australian Govt agencies more than $190 million
Undetected ID crime $?

Data quality and availability

Key finding: Aside from underreporting, the single biggest limitation on efforts to measure identity crime is the lack of standardisation between organisations over definitions and how incidents are recorded.

In response to the requests for data and information about identity crime, a number of agencies indicated that they either do not collect, or could not provide data that would be useful for the pilot measurement indicators. For example, only two out of nine police agencies; two out of eight registries of births, deaths and marriages; and three out of eight consumer affairs departments could provide relevant data within the time and resources available.

To build a reliable evidence base, it will be necessary for governments to invest effort and resources into developing the capacity of current systems and practices to more accurately capture identity crimes.

At the Australian Government level, similar deficiencies in data availability were identified. Nevertheless, Australian Government agencies responsible for delivering key government services, such as the Department of Human Services and the Australian Taxation Office, collected and were able to provide valuable data for the purpose of measuring identity crime. Moreover, Australian Government agencies that issue identity credentials, such as the Australian Passport Office within the Department of Foreign Affairs and Trade, and the Department of Immigration and Border Protection, also provided detailed data and information.

Finally, the Australian Federal Police also provided valuable information about identity crime, including advice about recent operational matters arising from the work undertaken with the New South Wales Police Force as part of the joint Identity Security Strike Team.

To build a reliable evidence base, it will be necessary for a range of Australian, state and territory government agencies to invest time and resources into developing the capacity of current databases and recording practices to more accurately capture identity crimes.

The way forward

In addition to this report on key findings of the measurement framework pilot, a companion report on recommendations for improving the measurement of identity crime has been developed for further government consideration. This report provides further detail on the challenges to be addressed in improving data quality and availability and a potential approach to improving the monitoring and measurement of identity crime in Australia on an ongoing basis.

This will be important to help improve the national evidence base to inform future policy and operational responses to identity crime. Importantly, this includes efforts to raise awareness of the evolving nature and extent of identity crime—one of Australia's most prevalent crime types—and of the steps that individuals, businesses and governments can take to reduce the impacts of identity crime on the Australian community.

Background

Identity crime is a generic term that describes a range of activities/offences where a perpetrator uses an identity (some combination of personal information) that is fabricated, manipulated, stolen or assumed from another person in order to facilitate the commission of a crime(s).

Identity crime is rarely an end in itself, but 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 terrorist financing; gaining unauthorised access to sensitive information or facilities; and concealing other activities such as drug trafficking and procuring child exploitation material. It has also been used to facilitate the commission of terrorist acts.

Identity crime is rarely an end in itself, but an important element in a wide range of criminal activities—fraud, money laundering, drug trafficking and terrorism.

The diverse nature of identity crime reflects the critical role of identity information—being able to verify that a person is who they claim to be—in a great many transactions and services that take place across government, the private sector and the broader community every day. It is not surprising then that recent surveys indicate that identity crime is amongst the most prevalent crime types in Australia; and is a concern for a majority of Australians.

Identity crime generates significant profits for offenders and causes considerable financial losses to the Australian Government, private industry and individuals (AFP 2014). Internationally, identity-related crime is regarded as a serious and increasing criminal risk to governments and the wider community (OECD 2006; 3). In its most recent Organised Crime Threat Assessment, the Australian Crime Commission rated identity crime as one of the key enablers of serious and organised criminal activity (ACC 2013; 13). Organised crime costs Australians an estimated $15 billion each year (ACC 2013; 13). The ACC also assessed that the risks associated with identity crime were likely to increase in the future (ACC 2013; 21).

The pervasive impacts of identity crime are widely acknowledged by governments, business and the broader community. Despite this, a lack of comprehensive, reliable data makes it difficult to quantify the full extent of this crime, or to assess its costs and consequences for victims. As a result, the true extent of identity crime in Australia is likely to be both underreported and underestimated.

Despite the widespread impacts of identity crime, there are relatively few reliable information sources, within Australia or internationally, to accurately quantify the extent of this crime type.

The development of a National Identity Crime Measurement Framework has been identified as a priority activity to support implementation of the National Identity Security Strategy (NISS), which the Council of Australian Governments agreed to in 2012.

As part of the NISS work plan, the Australian Attorney-General's Department (AGD) is coordinating a project to assess the feasibility of establishing an ongoing program for monitoring and analysing data on identity crime. However, as a national initiative, it would not be feasible without support and input from a range of government agencies across all states and territories and the Australian Government.

By improving the available information and evidence on identity crime, the primary aims of this Measurement Framework are to:

- measure the extent of identity crime and misuse in Australia
- assess the effectiveness of policy and operational responses to identity crime and related efforts to implement the NISS.

Methodology

The methodology for the Measurement Framework involved developing a range of indicators that were designed to quantify not only the incidence of identity crime itself, but also its broader impacts and some of the activities that can be undertaken to prevent identity crime from occurring. AGD developed this methodology with assistance from the AIC (Bricknell & Smith, 2013; the AIC Report).

This methodology was then tested during an initial six-month pilot data collection exercise involving a range of Australian, state and territory government agencies, using a sub-set of these indicators. This exercise was focussed primarily on existing data held by government agencies, and other information that was available from public sources.

With the assistance of the Department of Foreign Affairs and Trade, AGD also commissioned the AIC to conduct a community survey to gauge the community experiences of, and attitudes toward, identity crime. The AIC Survey was administered online over a two-week period in September 2013, and garnered responses from a cross-section of 5,000 people.

This report provides key findings and preliminary observations on the nature and scale of identity crime in Australia. This will be used to assess whether or not to establish an ongoing monitoring program.

Limitations

Given the number of agencies that were approached with requests for data—over 50—the pilot exercise was conducted over a relatively short timeframe. Aside from the AIC Survey, there was limited additional funding available for the pilot; as such agencies needed to provide data, if available, using existing resources. In some cases, agencies indicated that they may have data to inform the exercise, but that it could not be provided in an accessible format within the timeframe and resources available.

Similarly, there are a range of private sector and other non-government organisations that hold valuable sources of information on identity crime, although it was beyond the scope of the pilot activity to explore non-government sources of data that were not otherwise publicly available. It is envisaged that these sources of information could be explored in any future phases of the project.

This report provides some of the key findings of the pilot data collection exercise and makes some preliminary observations on the nature and scale of identity crime in Australia. This may provide some insights into possible policy or operational responses to identity crime. However, the report is designed primarily to help raise broader awareness of the nature and extent of identity crime in Australia and for relevant ministers to use when assessing whether or not to establish an ongoing program of data collection, measurement and reporting to support implementation of the NISS.

Australia's national identity infrastructure

Unlike some countries, Australia does not have a national identity card. The systems that Australians rely upon to help establish and verify their identities—our national identity infrastructure—is an interdependent network of systems that has evolved over time by practice and convention, not necessarily by design. It is built on a range of documents, cards and other credentials that are issued by a range of government, business and other non-government organisations. While the primary purpose of these credentials was not to serve as evidence of a person's identity, they have become increasingly used in this way throughout the community.

Australia has a complex, federated network of identity infrastructure in which around 20 government agencies manage over 50 million core identity credentials.

In order to develop reliable and robust estimates of identity crime, it is important to understand the nature of Australia's identity systems. Within Australia's network of identity infrastructure, over 20 government agencies manage more than 50 million 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.

While not traditionally considered as critical infrastructure, Australia's identity management systems have many of these characteristics. In the event that these systems are compromised or become unavailable for any length of time, there could be significant impacts to the Australian economy.

Australia's federated identity management system is characterised by interdependencies. Each agency that issues identity credentials within Australia relies upon those issued by other organisations to help verify their clients' identities. A breach of identity security in one organisation can have potentially serious 'downstream' consequences for the identity of an individual or another organisation, and affects the strength of the network as a whole.

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

Australia's identity systems are also highly dynamic. Each year hundreds of thousands of identity credentials are issued or renewed as people arrive in Australia, move interstate, get married, learn to drive, or need to access medical services.

Detecting and preventing the fraudulent use of identities in such a dynamic network of identity management systems presents significant challenges for the range of service delivery, regulatory and law enforcement agencies involved.

Definition of key terms

One of the key challenges in measuring identity crime is the lack of commonly agreed terms and definitions for this activity, both across Australia and internationally. However, there is an emerging consensus around the use of some of this terminology. Definitions for some of the key terms used throughout this report are included below. A more complete glossary is included in Appendix C.

Identity crime: *a generic term to describe activities/offences in which a perpetrator uses a fabricated, manipulated, or stolen/assumed identity to help them commit a crime(s).*

Identity fabrication: *the creation of a fictitious identity.*

Identity fraud: *gaining money, goods, services or other benefits or avoiding obligations by using a fabricated, manipulated, or stolen/assumed identity.*

Identity manipulation: *altering one or more elements of an identity (e.g. name, date of birth, address etc.).*

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.*

Identity takeover: *assuming parts or all of the identity of another person with their consent.*

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.*

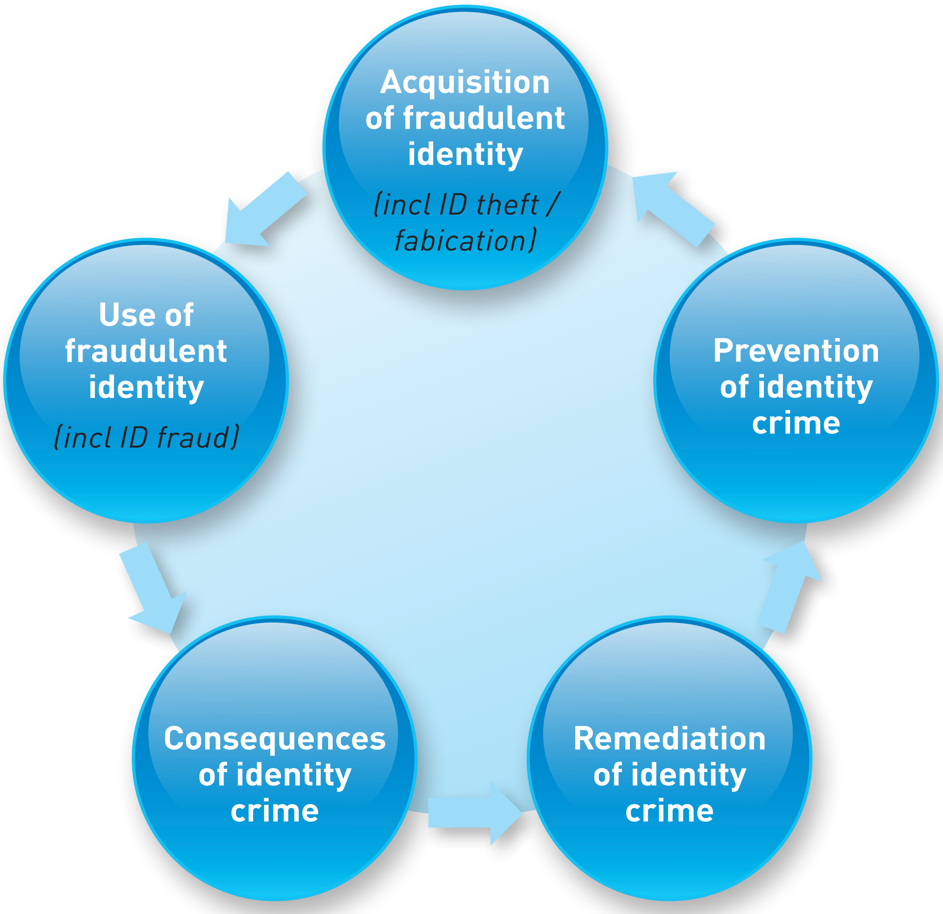
Identity Crime Conceptual Model

Most research that seeks to quantify identity crime concentrates on defining and/or categorising the nature of the associated offences. It often fails to adequately explore the other dimensions of the activity, particularly as they relate to factors that increase or mitigate identity crime risks (i.e. the likelihood and consequences of identity crime occurring).

To help address this issue, an Identity Crime Conceptual Model has been developed to identify and categorise the five key groups of activities involved not only in the commission of identity crimes, but also in prevention and remediating the consequences (see Figure 3).

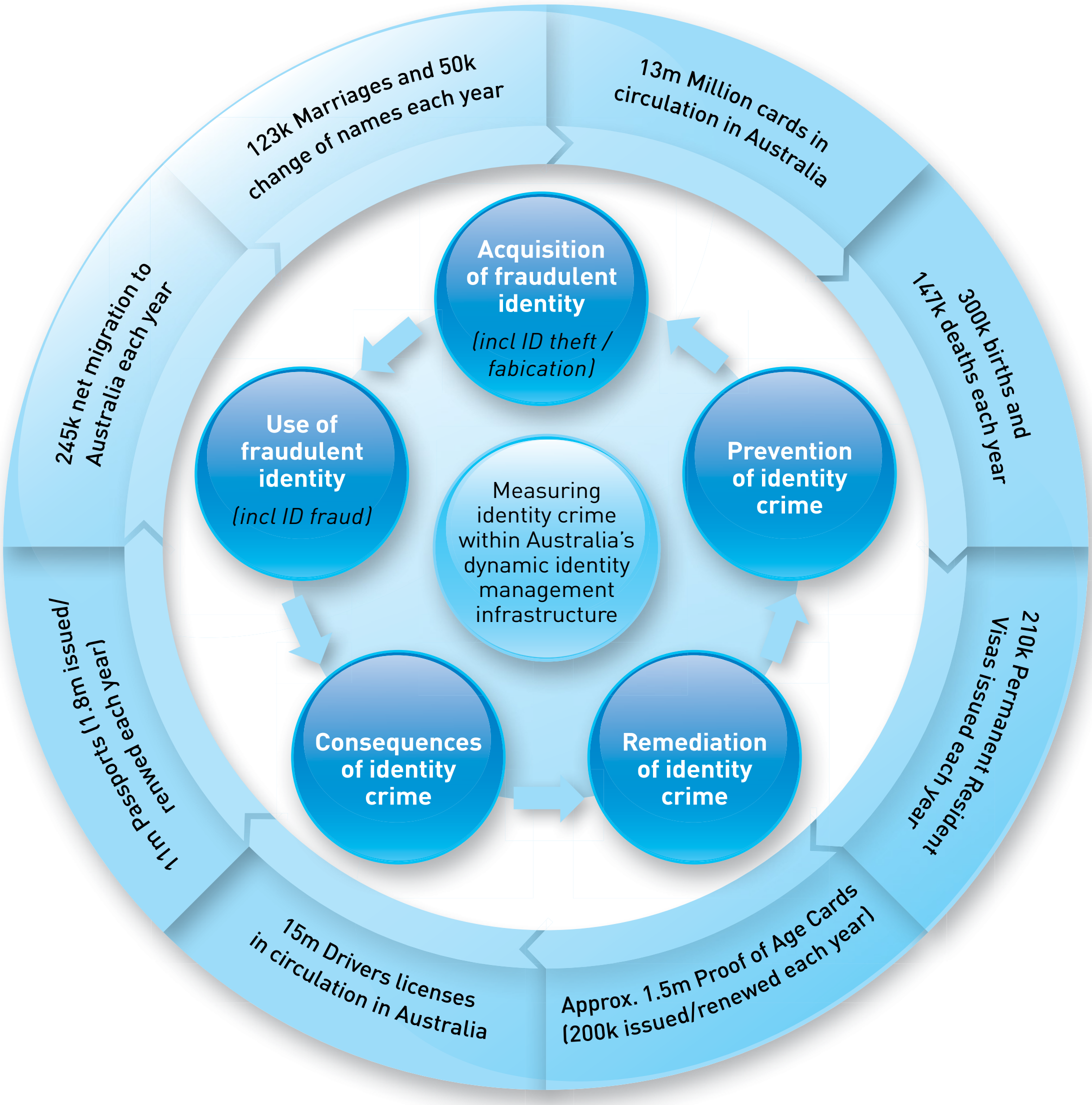
This Conceptual Model aims to provide a common understanding of identity crime and related activities for the purpose of the Measurement Framework project, as indicated in the following diagram.

Figure 3: Identity Crime Conceptual Model


Acquisition of fraudulent identity
(incl ID theft / fabication)
Use of fraudulent identity
(incl ID fraud)
Consequences of identity crime
Remediation of identity crime
Prevention of identity crime

Incidences of identity crime can number in the tens of thousands each year. While this is a significant figure, it is important to maintain a sense of the relative size of this activity in comparison with the vast majority of legitimate identity-related transactions that occur each year within Australia. This is illustrated in Figure 4.

Figure 4: Identity crime and Australia's identity infrastructure


123k Marriages and 50k change of names each year
13m Million cards in circulation in Australia
300k births and 147k deaths each year
210k Permanent Resident Visas issued each year
Approx. 1.5m Proof of Age Cards (200k issued/renewed each year)
15m Drivers licenses in circulation in Australia
11m Passports (1.8m issued/ renewed each year)
245k net migration to Australia each year
Acquisition of fraudulent identity (incl ID theft / fabication)
Prevention of identity crime
Remediation of identity crime
Consequences of identity crime
Use of fraudulent identity (incl ID fraud)
Measuring identity crime within Australia's dynamic identity management infrastructure

Measurement Framework indicators

The Measurement Framework aims to provide both a comprehensive picture of identity crime and related activities, and a robust basis for monitoring and measuring changes in these activities over time. To achieve this, a set of individual measurement indicators have been mapped against each category of activities identified in the Conceptual Model, as indicated below.

1. Acquisition of fraudulent identities

This component covers the activities associated with acquiring identities that are 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.

There are two indicators that 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 identities (as opposed to use of these identities), it is not feasible to extract this information from within currently available data sources. Most cases of identity crime that come to the attention of authorities involve both the fraudulent acquisition and use of identities but do not distinguish between these for reporting purposes.

2. Use of fraudulent identities

This component covers the activities associated with various uses of fraudulent identities, or the fraudulent use of legitimate (real) identities such as financial, taxation, immigration and criminal identity fraud (e.g. identity fraud to evade detection for other criminal activities).

There are five indicators that 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. Consequences of identity crime

This component covers some of the consequences of identity crime, including costs of the fraudulent use of identity credentials to individual victims, government agencies, business and the broader community.

There are four indicators that are 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 financial losses to victims of identity crime and misuse
- Indicator 3.4—number of identity crime victims experiencing other non-financial consequences.

4. Remediation of identity crime

This component covers the broader activities associated with the remediation of identity crime, 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 five indicators that are designed to measure identity crime prevention activities in this component:

Use of the DVS

- Indicator 5.1—the number of identity credentials able to be verified using 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 adopts robust online security practices to protect personal information.

Key findings

1. Acquisition of fraudulent identities

Fraudulent identity credentials can be obtained in a variety of ways. The methods for sourcing fraudulent credentials can be grouped into two main categories:

- identity theft/manipulation—instances where a criminal steals or otherwise acquires all, or parts of, a legitimate identity from another person; and
- identity fabrication—where a fictitious identity is created and manufactured onto a credential.

To establish a fraudulent identity, the offender requires personal identifying information (PII). Criminals can obtain PII from a wide range of source documents such as bank statements or utility bills that are discarded into the rubbish (commonly known as 'dumpster diving'—see Case Study 1), from malicious hacking of databases containing PII (data breaches), or PII can simply be made up (i.e. identity fabrication). There have even been cases where criminals have taken over the identities of people who are deceased (known as 'Tombstone Fraud'—see the in-depth case study at the end of this report).

Case Study 1 (2012): Personal information stolen from mailboxes used in superannuation identity fraud

Members of an organised criminal syndicate stole cheques, superannuation statements and personal bank statements from the mailboxes of unsuspecting victims and used this information to produce high-quality counterfeit identity documents. These documents were then used to conduct frauds against superannuation accounts. After assuming the victim's identity and setting up a Self-Managed Super Fund in their name, the syndicate member would contact the victim's superannuation provider and request that they 'roll over' the funds from the legitimate superannuation fund into the new, fraudulent Self-Managed Super Fund that they had established.

Following a coordinated multi-agency investigation, a total of 25 syndicate members were charged with more than 2,500 offences involving the laundering of over AUD$8 million in fraudulently obtained funds.

Source: AUSTRAC typologies and case studies report, 2012; 45
http://www.austrac.gov.au/files/typ_rprt12_full.pdf

1.1 Price of fraudulent identity credentials

Key finding: Medicare cards and driver licences—and to a lesser extent birth certificates—are more likely than other credentials to be used to facilitate identity crime. This is due to a range of factors including Australians' ubiquitous use of these cards as evidence of identity and the security features of the credentials. This emphasises the importance of verifying the information presented on these credentials with the issuing agency.

The price of fraudulent identity documents serves as an indicator of their availability on the black market and the extent to which they are used in identity related crime.

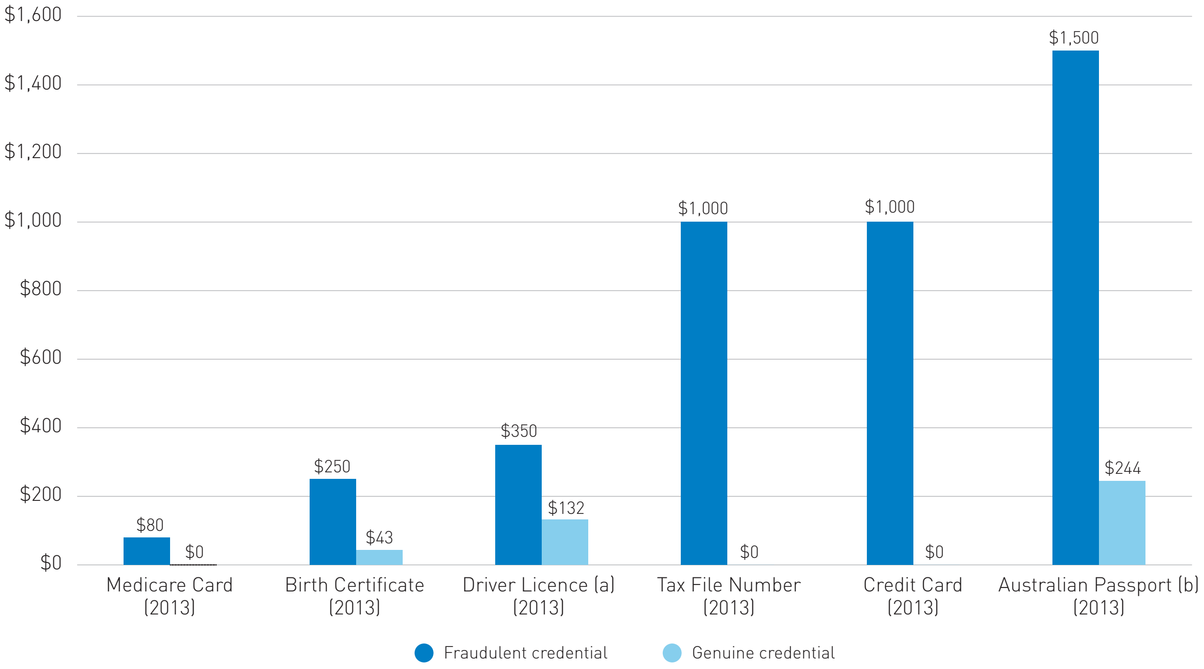
Just like narcotics, fraudulent identity credentials are an illicit commodity subject to the market forces of supply and demand. The price of fraudulent identity documents serves as an indicator of the availability of that type of fraudulent credential on the black market and the extent to which the credentials are used in identity-related crime.

The level of availability is, in turn, influenced by a number of factors: the financial *value* of the credential (e.g. credit/debit cards with an available balance); the *quality* of the credential, including whether it uses fabricated or legitimate identity information and contains the required security features; and the *utility* of the credential in facilitating other crimes (i.e. the extent to which it is accepted in the community, and the benefits it enables).

There is a key difference between credentials that are completely counterfeit and those that are legitimately issued but contain fraudulent personal information (i.e. those issued in a fraudulent identity, or issued to a person fraudulently using another person's real identity).

The pilot revealed two reliable sources of information for this indicator: DFAT's Australian Passport Office (APO), which provided information on the price of fraudulent passports; and the Australian Federal Police (AFP), which provided intelligence on the price of various other fraudulent credentials (see Figure 5).

Figure 5: Price of fraudulent and genuine Australian identity credentials



a: For a 5-year genuine driver licence.

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

Source: Australian Federal Police and Department of Foreign Affairs and Trade

The presence and complexity of the credential's security features will also affect the price of a fraudulent document. For example, counterfeit documents that have been manufactured using readily available printing equipment are more likely to be detected than legitimate documents that contain fraudulent information. For this reason, the cost to acquire fraudulent identity credentials can be used as an indicator of how vulnerable they are to forgery. Credentials with stronger security features are more difficult to reproduce and are likely to cost more on the illicit market.

Intelligence indicates that the price of fraudulent identity credentials can vary from around: $80 (counterfeit Medicare cards), to $250–$350 (counterfeit birth certificates and driver licences), to $1,500 (legitimately issued Australian passports to be altered by a professional document forger) and up to $30,000 (legitimately issued passport containing fraudulently obtained identity information). In many cases, these were not the most recent versions of the documents in question, which contain state-of-the art security features, but rather they were older versions that are easier to alter or reproduce.

Medicare cards—and to a lesser extent birth certificates and driver licences—appear more likely to be used in identity crime.

This emphasises the need for organisations to be able to verify the information presented on these credentials with the issuing agency.

The fact that Medicare cards are the cheapest fraudulent credential on the black market suggests that they are relatively easy to reproduce, particularly in light of the fact that they contain very few security features, such as a facial image or hologram.

Another potential measure of the availability of fraudulent credentials is their price relative to the legitimate versions of these documents. As indicated above (see Figure 5), the cost of fraudulent birth certificates and driver licences is between two and six times the cost of the official versions of these documents. By contrast, the cost of fraudulent passports and Tax File Numbers (TFNs) is between six and 16 times the cost of these credentials respectively (TFNs are free for individuals to apply, though applications through a registered tax agent may involve fees of around $60).

Finally, as use of the DVS increases, particularly among the private sector, the likelihood of counterfeit credentials being detected will also increase. The expected result is a displacement effect; criminals' use of counterfeit credentials will be replaced by legitimately issued documents containing fraudulent identity details. One potential avenue for criminals to obtain such legitimately issued fraudulent documents is to corrupt or exploit officials involved in the issuance of identity credentials (see Case Study 2). While there is not enough information about this case to ascertain whether any of the 650 licences issued contained fraudulent details, this case does illustrate the kinds of potential vulnerabilities that criminals could exploit to obtain 'legitimate' identity credentials issued with fraudulent details.

Case Study 2 (September 2012): Exploiting a corrupted employee to obtain an identity credential

Between 2005 and 2012, a Victorian man employed as an accredited tester for heavy vehicle licencing was alleged to have signed 650 fraudulent heavy vehicle certificates in return for cash payments. These certificates are used as evidence of passing a heavy vehicle driving test and are required to obtain the appropriate driver licence.

Source: The Age, 21 September, 2012
http://www.theage.com.au/victoria/truckies-face-retest-amid-licence-fraud-probe-20120921-26acr.html

It may also become more likely for criminals to obtain legitimate documents by purchasing them from individuals that are unlikely to need or use them. For example, criminals may look to target vulnerable members of the community (i.e. people in hospitals, nursing homes or serving long sentences in prison) and convince them to sell their identity credentials.

Finally, the joint AFP/NSW Police Identity Security Strike Team indicated that some organised criminal syndicates are now manufacturing high quality fraudulent credentials. Upon raiding the premises used by these syndicates, the strike team seized commercial grade printing equipment, batches of blank cards containing holograms and other security features, along with thousands of stolen images and personal details.

Conclusions about the cost to acquire fraudulent credentials

With the exception of DFAT, no credential issuing agency (such as an RTA or RBDM) was able to provide information on the estimated price of fraudulent versions of their credentials. If state and territory police agencies were to regularly collect intelligence on the cost to acquire fraudulent credentials, this would provide credential issuing agencies with a valuable indication as to the vulnerability of their credentials. This information would be useful as a measure of the extent to which these credentials are being used to facilitate identity crime—information that should inform any future changes to the security features or issuing processes for these credentials.

1.2 Number of reported data breaches

Key finding: There is limited reliable data on the true extent of data breaches in Australia. Nevertheless, data breaches, whether accidental or deliberate, will continue to present significant opportunities for obtaining personal identifiable information that is used in identity crime.

The types of personal information used to commit identity crime are increasingly being collected and stored in databases held by a variety of government agencies and private sector organisations. The aggregation of this information, particularly in electronic forms that are accessible online, increases the risk that they may be acquired through data breaches, either accidental or through deliberate attempts to steal personal information.

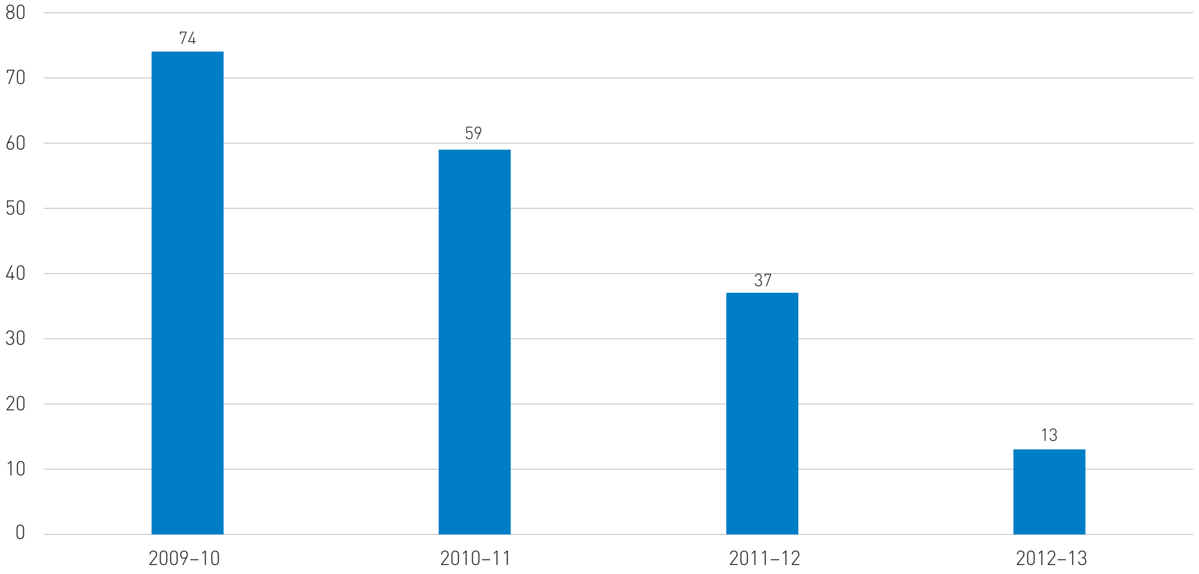
Case Study 3 (May 2013): Data breach affecting a major telecommunications provider

The owner of a marketing business was searching Google when he discovered that several large spreadsheets containing information about customers of a major telecommunications provider were freely accessible. One spreadsheet contained 1,677 records, including customer names, phone numbers, telephone plans and home addresses. Three other spreadsheets contained 8,201 records with names and telephone numbers. On 11 March 2014, the Office of the Australian Information Commissioner and the Australian Communications and Media Authority found that the telecommunications provider had breached privacy laws by failing to protect the personal information of 15,775 customers.

Source: Sydney Morning Herald, 16 May 2013
http://www.smh.com.au/it-pro/security-it/oops-google-search-reveals-private-telstra-customer-data-20130516-2jnmw.html
Source: Office of the Australian Information Commissioner, 11 March 2014
http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-of-15-775-customers

The Office of the Australian Information Commissioner (OAIC) collects data on the number of reported data breaches, as well as the number of own-motion investigations the OAIC initiates into privacy matters or information protection issues. The number of OAIC-initiated investigations has steadily declined over the four years from 2009–10 to 2012–13 (see Figure 6). This does not necessarily indicate there were fewer serious incidents involving suspected privacy breaches during that time. These figures provide no indication of the scale or complexity of these investigations, which can extend over more than one reporting period.

Figure 6: Number of own-motion investigations initiated by the OAIC, by year (2009–10 to 2012–13)



Source: Office of the Australian Information Commissioner 2011a, 2012a & 2013a

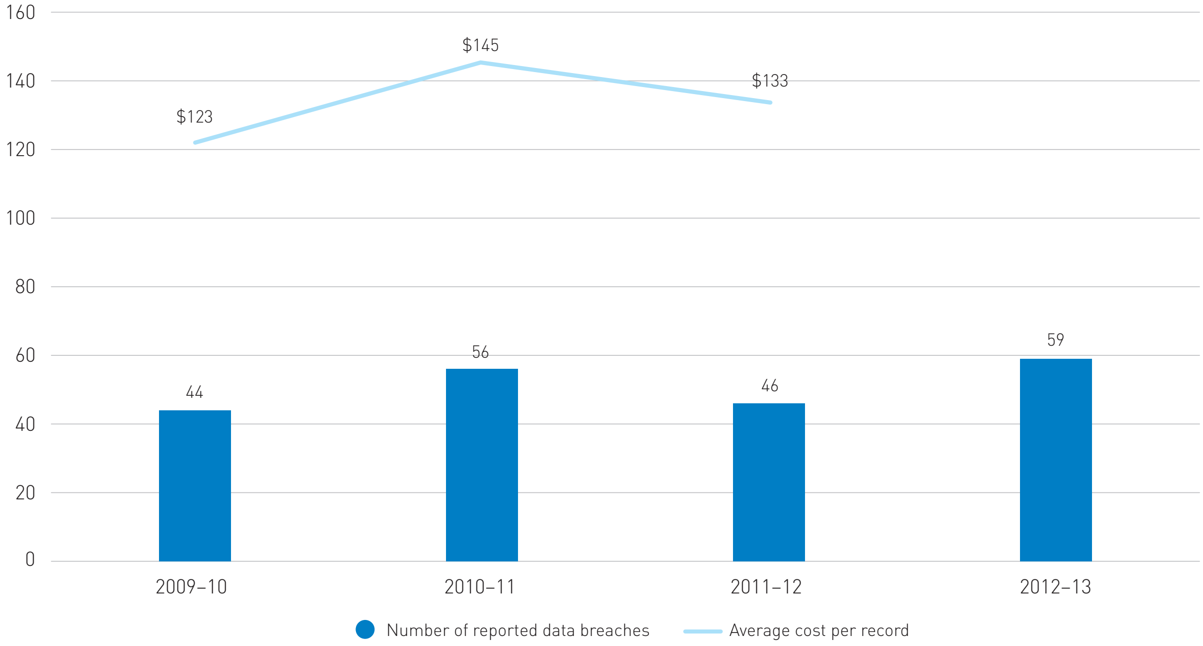
Another measure of the availability of information that can be used to facilitate identity crime is the number of reported data breaches. The OAIC has developed guidelines that encourage organisations to report serious data breaches involving personal information (OAIC 2012b). However, Australian organisations are not obliged under law to report data breaches, so the number of incidents reported to the OAIC is likely to be significantly less than the actual number of breaches in Australia.

On its own, the number of data breaches reported to the OAIC has limitations as a measurement indicator. Aside from being only a subset of total data breach incidents, the number of reported data breaches does not distinguish between the number of records involved in each breach, or their significance. This level of information is not available from the OAIC as it does not uniformly require or capture this amount of detail when it accepts a complaint regarding identity crime or theft.

The 22 data breach incidents examined in 2011 involved an average of 19,000 records lost or stolen, at an average cost of $138 per record. The average financial impact on the organisation involved was $2.2m.

However, other research by the Ponemon Institute provides some further insights into the nature of data breaches experienced by Australian organisations. The Australian data breaches (n=22) examined by the Ponemon Institute between 2009–10 and 2011–12 involved estimated average losses of between $123 and $145 per record (see Figure 7).

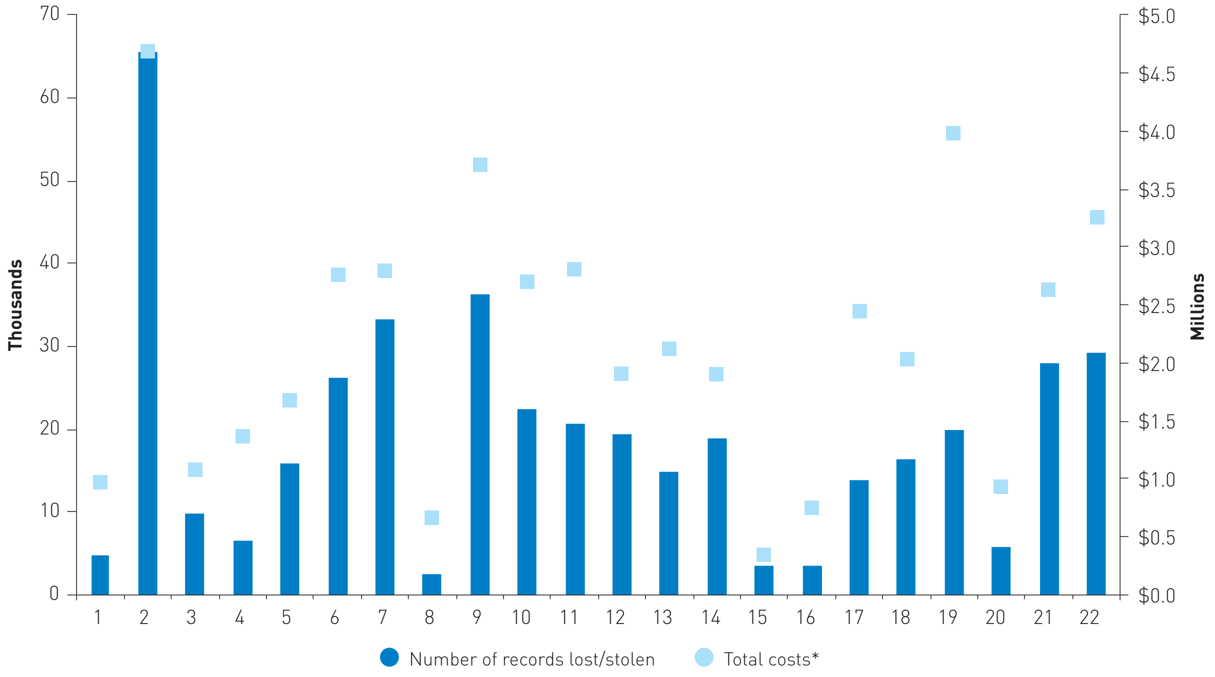
Figure 7: Number of voluntarily reported data breaches to the OAIC and the average cost per lost or stolen record, by year (2009–10 to 2012–13)



Source: Office of the Australian Information Commissioner 2011a, 2012a & 2013a; Ponemon Institute 2012 & 2013

Further detail is available on the 22 incidents examined in the 2011 Ponemon Study (see Figure 8). Analyses show that these incidents involved the loss or theft of an average of 19,000 records per incident, at an average cost of $138 per record. The average total financial impact on the organisation or agency involved was $2.2m (Ponemon 2012).

Figure 8: Size of data breaches (records lost) and total cost to the organisation, 2011



* Includes the costs associated with detection, notification, post-incident response and loss to business activity.

Source: Ponemon Institute 2011

Based on the data above, which indicates that an average Australian data breach costs $2.2 million and involves 19,000 records, the annual impact of reported data breaches alone could be over $100 million in costs and could involve the compromise of almost 100 million records.

It is likely that a considerable proportion of data breaches involve the loss or theft of personal information that is ultimately used in identity crime. Recent American data suggests that one in four data breach notification recipients in the US became a victim of identity fraud (Javelin Strategy & Research 2013).

2. Use of fraudulent identities

The government agencies participating in the pilot were asked to provide de-identified statistics on the number of recorded instances of identity crime and misuse. Some agencies were only able to provide limited data, some were able to provide a few case studies, and some were able to provide both case studies and data. This section provides an overview of the responses that were received.

2.1 Number of identity crime incidents recorded by government agencies

Key finding: Identity crime incidents are detected by a range of government agencies across a wide variety of fraud types including: welfare, passport, immigration, conveyancing, taxation and other financial frauds.

Offenders will often endeavour to use fraudulent identities against multiple different targets, including government agencies, financial institutions and non-government organisations. In light of the time and resources available during this pilot, it was only possible to collect data and information about the number of recorded incidents of identity crime against government agencies.

For the pilot, Australian Government agencies responsible for service delivery—i.e. Department of Human Services (DHS) and Australian Taxation Office (ATO)—or the issuing of identity credentials—i.e. Australian Passport Office (APO) and Department of Immigration and Border Protection (DIBP)—were able to provide some statistics[1].

Benefits fraud

Using a stolen or fabricated identity, individuals can claim government benefits to which they are not entitled. For the pilot, data was sourced on the total number of fraud investigations in recent years, as well as the number identified as identity fraud (see Figures 9 and 10).

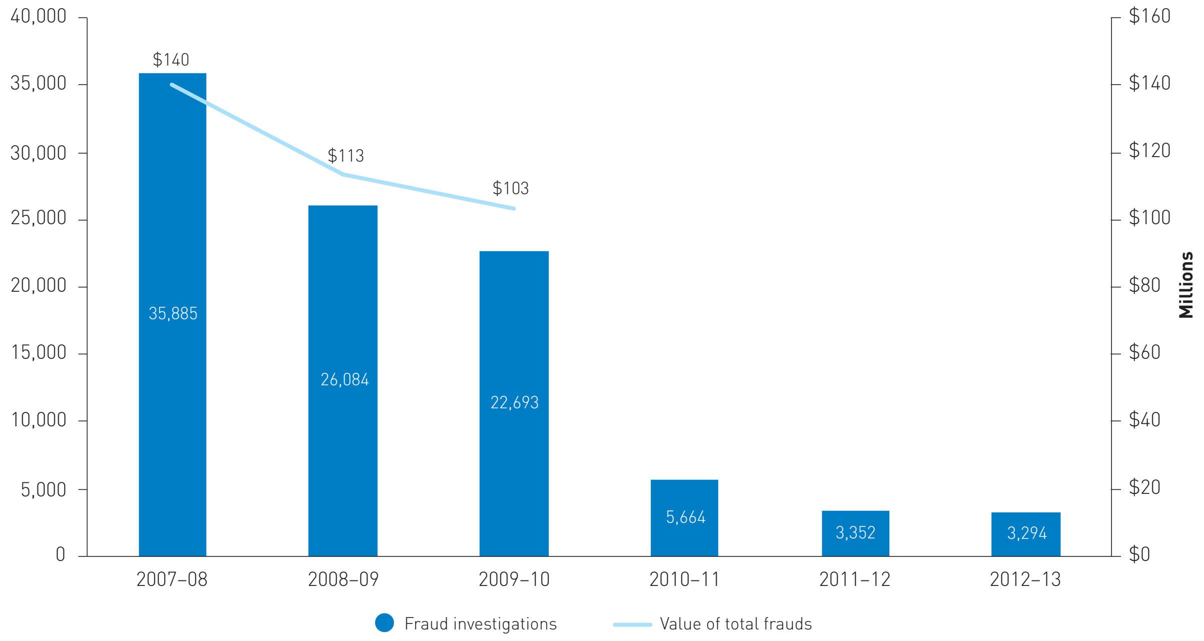
Case Study 4 (March 2009): Identity fraud against the Department of Human Services

Following the Victorian bushfires in February 2009, a 55 year old man created 112 fictitious identities that were used to claim disaster relief payments totalling $116,800. The man was convicted of two counts of obtaining property by deception and was sentenced to 3 years and 9 months imprisonment and ordered to repay the money he had obtained.

Commonwealth Director of Public Prosecutions, *2009–10 Annual Report*. Available at: http://www.cdpp.gov.au/case-reports/george-hebaiter/

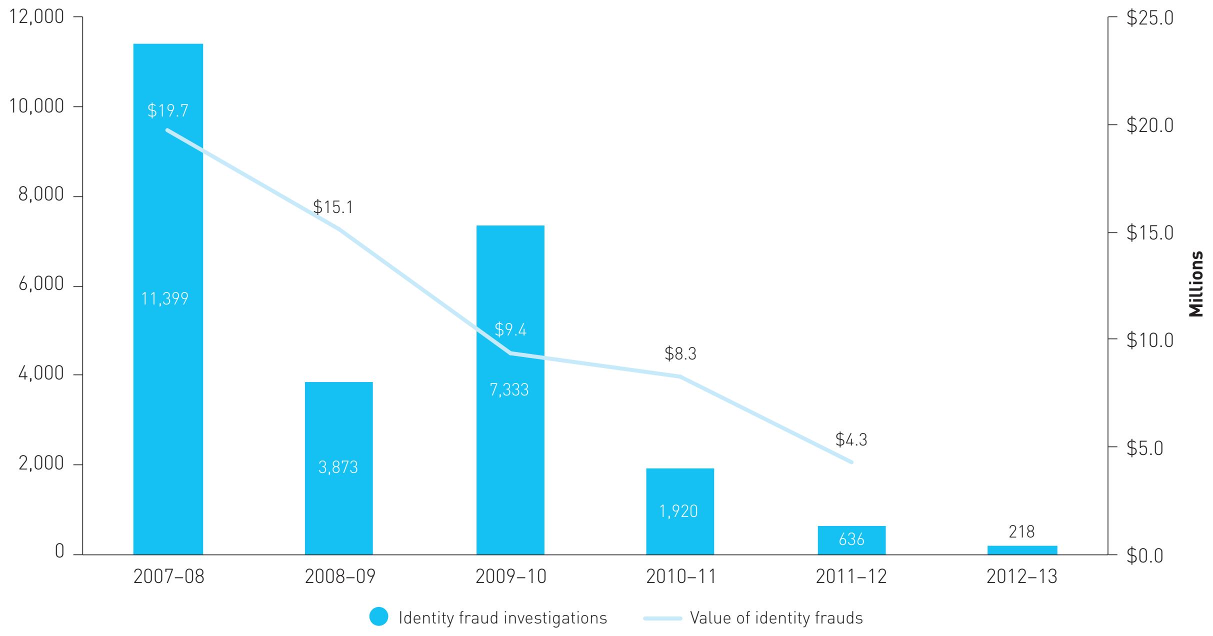
[1] Due to some variability in the characterisation of agency definitions regarding identity-related crimes, it may be difficult to directly compare data produced by different agencies in all cases.

Figure 9: Total number of DHS fraud investigations and total value, by year, 2007-08 to 2012–13



Source: DHS 2009, 2010, 2011, 2012, 2013 and unpublished data.

Figure 10: Total number of DHS identity fraud investigations and total value, by year, 2007-08 to 2012–13



Source: DHS 2009, 2010, 2011, 2012, 2013 and unpublished data.

In 2010–11 DHS (Centrelink) implemented a new intelligence database and case management system to record details of cases of suspected fraud that progressed to an investigation or evaluation. This is a subset of an unknown larger number of cases that were submitted to DHS investigators for review.

The total number of DHS fraud investigations has declined over the three years to 2012–13: from 5,664 investigations in 2010–11, to 3,294 investigations in 2012–13. Over the same period, the number of DHS identity fraud investigations have also declined from 1,920 incidents in 2010–11, to just 218 incidents in 2012–13. This is a decrease in incidents of 42 percent and 89 percent respectively.

Before 2010–11, DHS (Centrelink) systems recorded all cases of suspected fraud, including those that did not progress to formal investigation or prosecution. While these figures are not directly comparable with data from 2010–11 onwards, they do indicate a consistent decline in the number of fraud incidents detected by DHS over the last six years.

During the three years from 2007-08 to 2009–10, total DHS fraud investigations declined from 35,885 (valued at $140m) to 22,693 (valued at $103m) (see Figure 9). Over the same period, the number of DHS identity fraud investigations have also declined from 11,399 incidents in 2007-08 (valued at $20m), to 7,333 incidents (valued at $9m) in 2009–10 (see Figure 10). This is a decrease in incidents of 37 percent and 36 percent respectively.

These declines are partly associated with increased government funding that enhanced the specialised fraud investigation teams within DHS. This has meant that frauds are now detected sooner, before large debts can be accumulated. Another driver for the apparent decline in both the incidence and value of detected frauds was changes in both the overall quantum of cases being reported, along with changes in the way the cases were classified and processed.

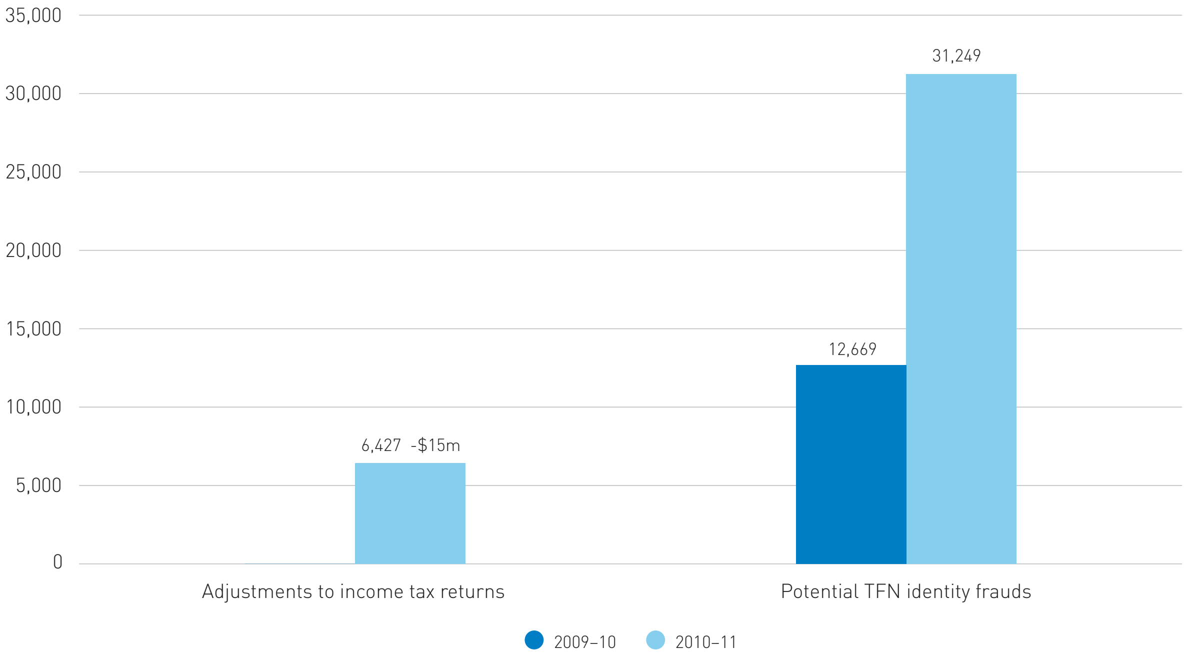
Taxation identity fraud

As part of a suite of initiatives designed to detect fraud and identity crime, the ATO uses their Identity Crime Model to flag suspicious cases for further review before they are processed. In 2010–11, the ATO identified 6,427 income tax returns that involved identity fraud, with a combined value of $15 million (see Figure 11).

In 2011, the ATO further re-engineered processes relating to the potential compromise of TFNs. This followed recommendations by the Commonwealth Ombudsman after an investigation into the way the ATO responded to incidents where TFNs were compromised or incorrectly linked (Commonwealth Ombudsman 2010).

These changes resulted in increased detections of potential TFN identity fraud cases, from 12,669 in 2009–10 to 31,249 in 2010–11 (see Figure 11). Advice provided by the ATO outlined that this increase can be attributed to a combination of an actual rise in the incidence of identity crime as well as improved fraud-detection processes.

Figure 11: Taxation identity fraud incidents (income and TFNs) and value of protected revenue



Source: Australian Taxation Office unpublished data

The AIC also regularly reports on fraud against Commonwealth agencies. In the most recent *Fraud Against the Commonwealth 2009–2010 Annual Report to Government* (Lindley, Jorna & Smith 2012), a total of 2,859 external fraud incidents involving the unauthorised use of another person's TFN or Australian Business Number were reported.

Case Study 5 (February 2011): Identity fraud against the Australian Taxation Office

The offender believed he could boost his income by creating 17 bogus companies and submitting fraudulent activity statements for each of them. Using the GST Identity Fraud Model, the ATO quickly identified his claims as suspect. Once detected, the ATO undertook a detailed investigation where it became evident that a serious offence had occurred. The offender was charged with obtaining and attempting to obtain a financial benefit by deception, was sentenced to five years imprisonment and had to pay $312,075 in reparations.

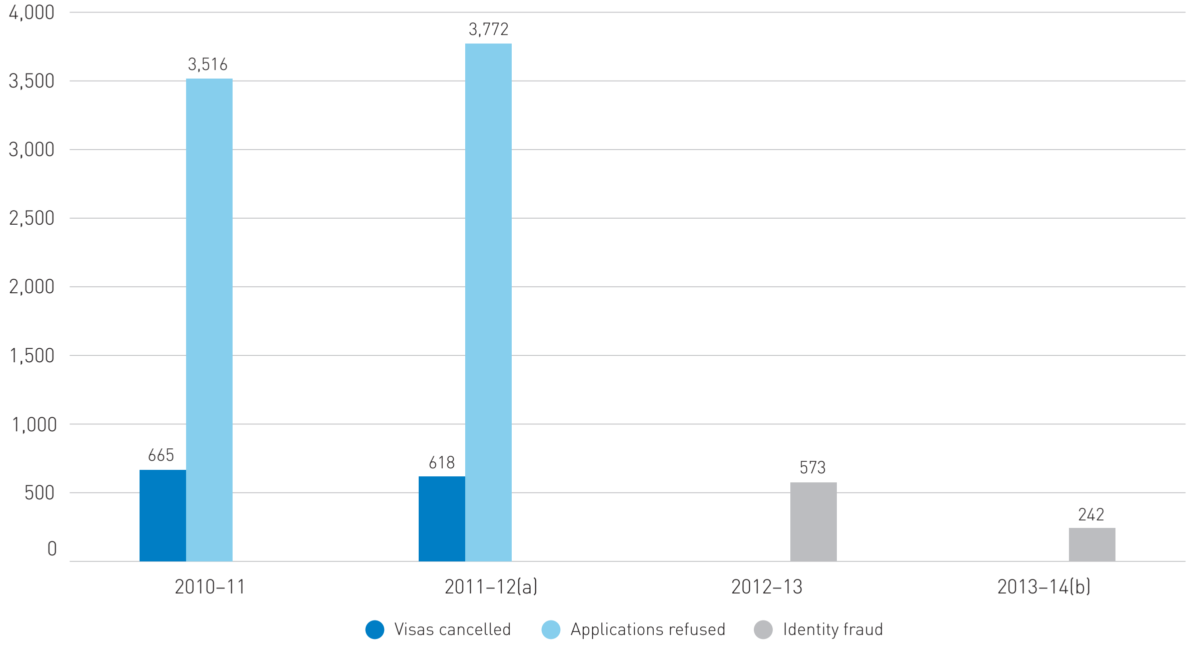
Australian Taxation Office, 2011—Targeting tax crime: A whole-of-government approach.

Available at: http://www.ato.gov.au/General/Tax-evasion-and-crime/In-detail/Targeting-Tax-Crime-magazine/2011/Targeting-tax-crime--A-whole-of-government-approach---February-2011/?page=8

Immigration identity fraud

The Department of Immigration and Border Protection (DIBP) collects a variety of statistics on fraud and identity crime related to immigration visas. For the pilot, the DIBP supplied data on the number of visa cancellations and visa application refusals due to fraud (see Figure 12). These statistics relate to fraud generally, as well as cases further categorised as identity fraud, which includes instances where a person has altered an aspect of their biographical data in an effort to facilitate entry to Australia.

Figure 12: Immigration fraud and identity fraud incidents, by type and year, 2010–11 to 2013–14



a: 618 visa cancellations due to fraud as at 31 December 2012

b: 242 identity frauds detected between 1 July and 31 December 2013

Source: Department of Immigration and Border Protection unpublished data.

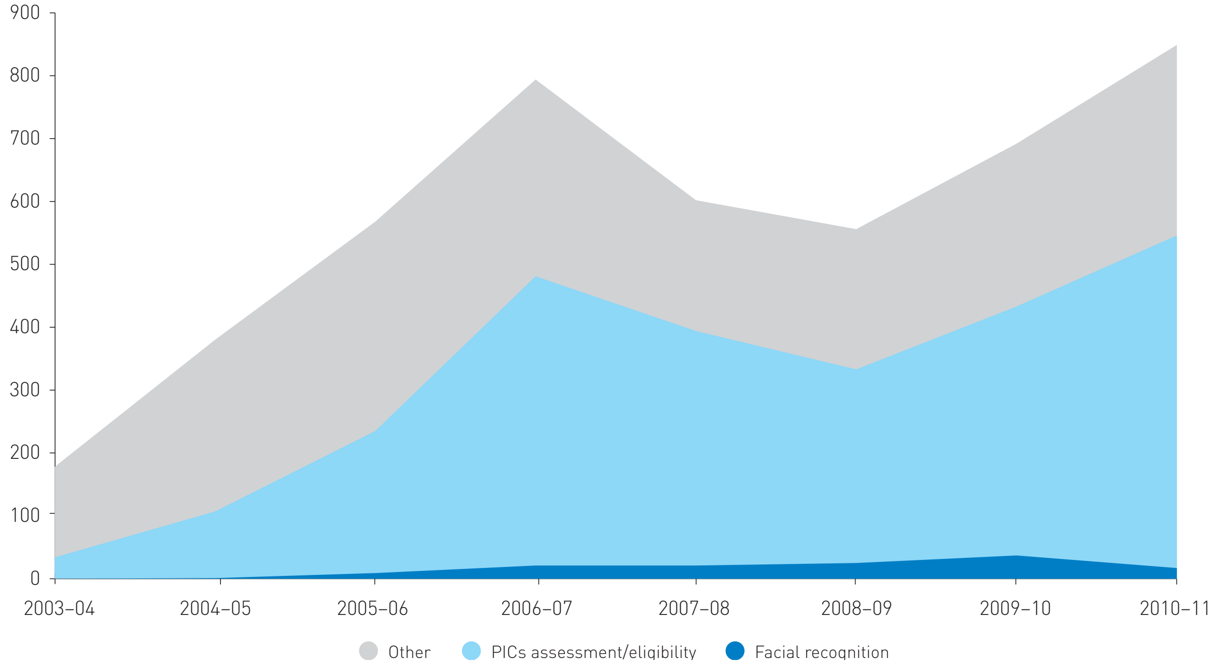
In 2010–11, 665 visas were cancelled as a result of fraud, with the number likely to be higher in 2011–12, as the 618 cases presented are only the number of detected frauds in the first half of the 2011–12 financial year. The DIBP also provided data on the number of identity frauds against visas, with 573 recorded incidents in 2012–13, and a further 242 incidents in the first half of the 2013–14 financial year.

Passport identity fraud

In 2012, the Australian National Audit Office (ANAO) published an audit report that examined the management of e-passports, which included analysis of new passport frauds and the way they were detected (see Figure 13) (ANAO 2012). These new passport frauds relate to instances where individuals have sought to obtain a passport issued in another name or have a second passport issued. The number of detected fraud cases involving new e-passports increased from 178 in 2003–04 to 849 in 2010–11

(ANAO 2012; 67). This increase is attributed to a combination of the increasing number of passports that are issued each year (up from 1.1 million in 2003-04 to 1.8 million in 2010–11) and greater investigative capability, rather than to an increase in the rate or incidence of fraud (ANAO 2012; 68–69).

Figure 13: Passport frauds, by detection method and year, 2003-04 to 2010–11



Notes: 'Other' detection methods include up to 12 other categories such as fraud detected at the border, by other agencies such as the AFP and information from informers.

PICs stands for Passport Issuance and Control system.

Source: ANAO 2012

For this pilot, DFAT analysed passport records between 2010–11 and 2011–12 and reported the number of identity-related passport frauds (see Table 1), that is those cases where an individual has supported a passport application with fraudulent credentials.

Table 1: Identity-related passport frauds, by year, 201011 and 2011–12

	2010–11	2011–12
Identity fraud against passport	127	83

Source: DFAT—APO unpublished data

Lost and stolen passports

Another method for undertaking identity-related passport fraud is to obtain a genuinely issued passport that has been lost or stolen and then modify the information and/or image contained within the document to create a 'new' credential.

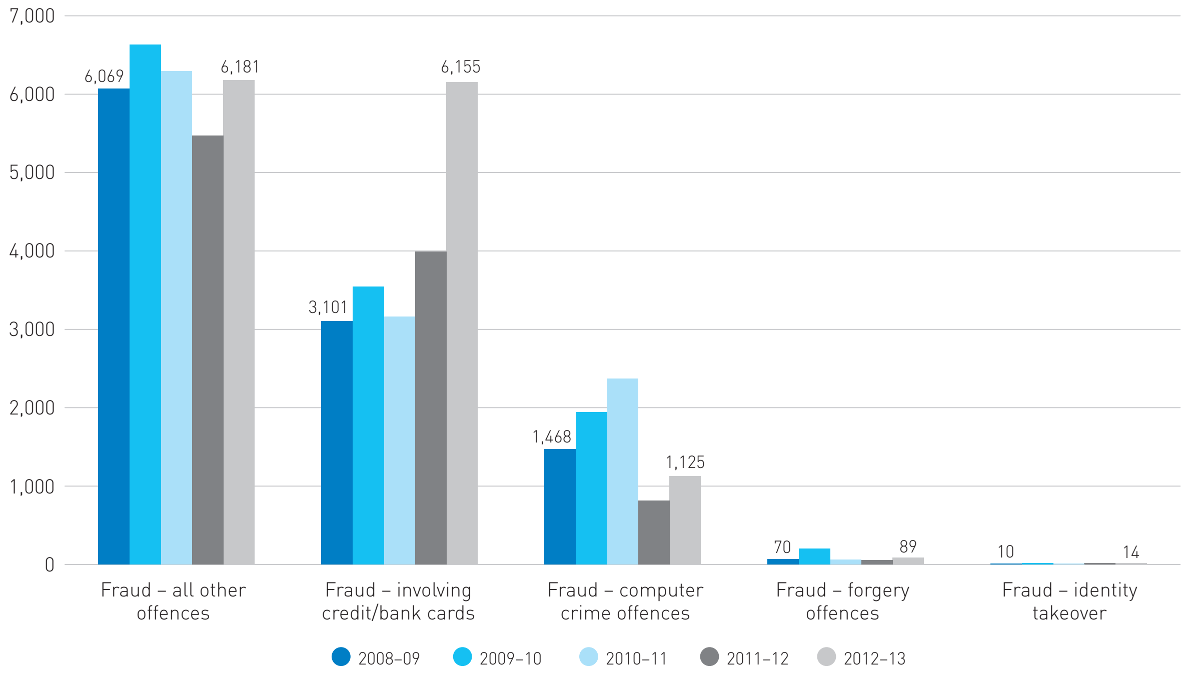
In 2010–11, 34,681 Australian passports were reported as lost or stolen. As soon as a passport is reported as lost or stolen, DFAT will record the passport number and then cancel it to ensure that it cannot be used for travel purposes. These passports could, however, continue to be fraudulently presented in the community more broadly, and would only be detected where they are verified through systems such as the DVS.

DFAT has indicated that older passports, which could more easily be altered by professional document forgers, have now been phased out. There are no known instances where an individual has successfully altered the electronic chip in newer generations of e-passports, which have been issued since late 2005. As the older generation passports expire, all Australians will transition to the new e-passports. This is expected to occur by early 2016.

Identity fraud detected by state and territory police

Requests were sent to all state and territory police agencies to obtain data on the number of recorded identity crime incidents and related offences (e.g. fraud, forgery and impersonation). Within the three-month data collection period, only the Queensland Police Service (QPS) was able to provide relevant statistics from its QPRIME data recording system (see Figure 14).

Figure 14: Fraud offences detected by the Queensland Police Service, by offence type and year, 2008–09 to 2012–13



Note: This data is preliminary and may be subject to change.

Source: Queensland Police Service

The QPS data indicate that while most categories of fraud offences have remained relatively stable over recent years, frauds involving credit/bank cards increased from 3,101 in 2008–09 to 6,155 in 2012–13, an increase of almost 200 percent.

Police data systems record crimes under the Australian Bureau of Statistics standard offence classification codes, known as the *Australian and New Zealand Standard Offence Classification (ANZSOC) 2011* (ABS 2011). While there are specific ANZSOC codes that relate to fraud, deception and forgery offences, there are no specific codes that apply to identity crimes such as stealing someone's identity or possessing a fraudulent identity credential. Identity crimes are usually recorded under broader offence categories such as fraud.

As such, it was not feasible for the pilot to identify the number of fraud offences recorded by all police agencies that were identity crimes. This would have required detailed analysis, and in some cases manual counts, of thousands of records.

Despite these limitations, it is possible to use the QPS data to calculate an approximate estimate of the total number of frauds detected by police across Australia, as well as the number and proportion of these incidents that involve identity crimes.

Across the five years for which QPS data were provided (2008–09 to 2012–13) there was an annual average of 11,770 fraud offences detected. Based on the proportion of Australians that live in Queensland (20% as at 30 June 2013), a national fraud estimate can be calculated by multiplying the Queensland figure by five. This produces a rough national estimate of 58,851 frauds detected by police in 2012–13.

In the United Kingdom, the Credit Industry Fraud Avoidance Service (CIFAS) observed that a considerable proportion of all fraud can be classified as identity crime, in that '50 percent of all frauds identified during 2012 relate to the impersonation of an innocent victim or the use of completely false identities' (CIFAS 2012). Within Australia, the Australian Federal Police has previously estimated that the proportion of fraud that is identity crime would be in the region of 25 percent (House of Representatives Standing Committee on Economic Finance and Public Administration 2000; EFPA 164).

Assuming that between 25–50 percent of the estimated national fraud figure calculated above (58,851 frauds) is identity crime, then there was somewhere in the order of 15,000–30,000 identity crimes detected by police in Australia in 2012–13.

The experience of the joint AFP/NSW Police Identity Security Strike Team indicates that a single identity crime investigation can involve around 2,000 fraudulent identities that, in turn, can be used to facilitate hundreds of different offences, which may or may not be fully identified.

Available data suggests that there was somewhere in the region of 15,000–30,000 identity crimes detected by police in Australia in 2012–13.

It is highly likely that these estimates represent only a proportion of the true number of identity crimes committed in Australia each year.

Given that false or stolen identities are used to facilitate such a broad range of other criminal activities, it is highly likely that the above estimates represent only a proportion of the true number of identity crimes committed in Australia each year.

Identity fraud detected by registries of births, deaths and marriages (RBDM)

When a birth, death or marriage occurs in Australia, the event and the parties involved are registered with the relevant RBDM, with the details recorded on the appropriate certificate. These certificates are relied upon as documentary evidence of both the commencement of an identity (i.e. birth certificates) and of changes to identity details over time (i.e. marriage and change of name certificates).

For the pilot, all of the state and territory RBDMs were asked to provide data on the number of incidents of identity crime and misuse involving certificates that they issue. Only Western Australia and New South Wales RBDMs were able to provide relevant statistics (see Table 2).

Table 2: Incidents of identity crime and misuse involving RBDM certificates, by year

New South Wales RBDM			Western Australia RBDM		
Year	Fraudulent Certificates	Unauthorised Amendments	Year	Fraudulent Certificates	Unauthorised Amendments
2010	Birth—7 CoN—2	Birth–40	2010–11	Birth–3	Birth–0
2011	Birth—15 CoN—0	Birth–65	2011–12	Birth–3	Birth–1
2012	Birth—26 CoN—1	Birth–33	2012–13	Birth–1	Birth–0
2013	Birth—10 CoN—1	Birth–19			

Note: CoN stands for Change of Name

Source: New South Wales & Western Australian Registry of Births, Deaths and Marriages

The number of birth certificates recorded as fraudulent is far less than one percent of the total number of birth certificates that are issued in just one year. For example, in 2012 there were over 95,000 births registered in New South Wales (NSW RBDM 2013) and in the same year only 59 birth certificates were recorded as fraudulent or containing unauthorised amendments.

The price of fraudulent birth certificates indicates that these documents are more widely available than these figures would otherwise indicate. This is likely because most government agencies and private sector organisations do not have arrangements in place to notify the relevant RBDM when they detect a certificate that is suspected to be fraudulent. It is likely, therefore, that RBDMs are not notified of the majority of incidents involving fraudulent versions of their certificates.

Driver licence fraud

While not initially intended to be used as an identity document, in practice driver licences have arguably become the key identity credentials used by Australians. Of the eight road transport and licensing agencies that were approached during the pilot, only Roads Corporation Victoria (VicRoads) and the South Australian Department of Transport advised that they had data and information about incidents of identity fraud. Media reports also indicate that VicRoads and the WA Department of Transport have recently undertaken projects to use facial recognition technology to help identify fraudulent driver licences (see Case Study 6). However, no statistics on fraudulent licences were able to be provided by any road agency before the completion of the pilot exercise.

Case Study 6 (October 2012): False Victoria driver licences detected through facial biometric auditing

Following a 2007 Ombudsman's report that found the driver licensing system was vulnerable to corruption, VicRoads used facial recognition software over a four year period (2007–2010) to audit around 700,000 driver licences. The audit identified 600 suspected frauds that were referred to police.

Source: The Australian, 29 October, 2012
http://www.theaustralian.com.au/news/vicroads-goes-hi-tech-to-end-driving-licence-fraud/story-e6frg6n6-1226504896204#

Conveyancing identity fraud

Purchasing a property is the highest value transaction that most Australians will undertake in their lifetime. To help guard against fraud in property transactions, land titles agencies, conveyancers and other property professionals need to take reasonable steps to verify the identity of their clients. In all jurisdictions, there are legislative protections for cases of conveyancing identity fraud under which the relevant state or territory government can compensate the affected property owner. While no quantitative data was available on incidents of identity crime among conveyancing transactions, there are a number of cases that have come to public attention (for example see Case Study 7).

Case Study 7 (June 2010): Fraudulent property sale

Using fraudulent identity documents in the owner's name, Nigerian-based scammers successfully convinced a Perth real estate agent to sell an investment property worth $485,000. The owner of the property, who was living in Cape Town at the time, was only alerted to the fraud when the offenders also tried to sell his primary residence and he was contacted by a concerned neighbour.

Source: WA Today, 13 September, 2010
http://www.watoday.com.au/wa-news/property-scam-highlights-need-for-greater-security-reiwa-20100913-15952.html

Conclusions about incidents of identity crime and misuse against government agencies

Based on the available data provided by a handful of government agencies, it is hard to make definitive conclusions about identity crime trends, or to establish a reliable baseline of identity crime against government agencies. Certain types of identity crimes, such as taxation and passport identity frauds, have been increasing considerably in recent years. On the other hand, an examination of data on identity-related benefits fraud reveals that both the number of investigations and values involved have been declining in recent years.

Overall, findings indicate that where agencies have recently developed new approaches to detecting identity crime, such as the ATO's Identity Crime Model, the number of detected incidents has increased.

Where agencies have recently developed new approaches to detecting identity crime, the number of recorded incidents has increased.

2.2 Prosecutions for identity crime and other related offences

Key finding: There are an estimated 24,000 prosecutions for identity-related crimes each year in Australia, although prosecution statistics only ever measure a relatively small sub-set of the total incidents of criminal activity.

Rather than specific identity crime offences, most identity criminals are prosecuted for the crimes that are enabled by using a false or stolen identity, such as fraud (i.e. obtaining benefit by deception). This may be because these offences attract higher penalties or are more appropriate to the overall circumstances of the conduct.

There are a wide variety of different Commonwealth offences under which people committing identity crime offences can be prosecuted. The specific offence provision that criminals are prosecuted under is largely dictated by the nature, circumstances and target of the identity-related offences that are committed. For example, offenders who obtain financial advantage by deception (i.e. fraud), make false or misleading statements to an Australian Government agency, or forge government-issued identity documents will likely be prosecuted under the *Criminal Code (Cth)*. Offenders, who target the Department of Immigration and Border Protection, such as by providing false documents to obtain a visa, will likely be prosecuted under the *Migration Act 1958*.

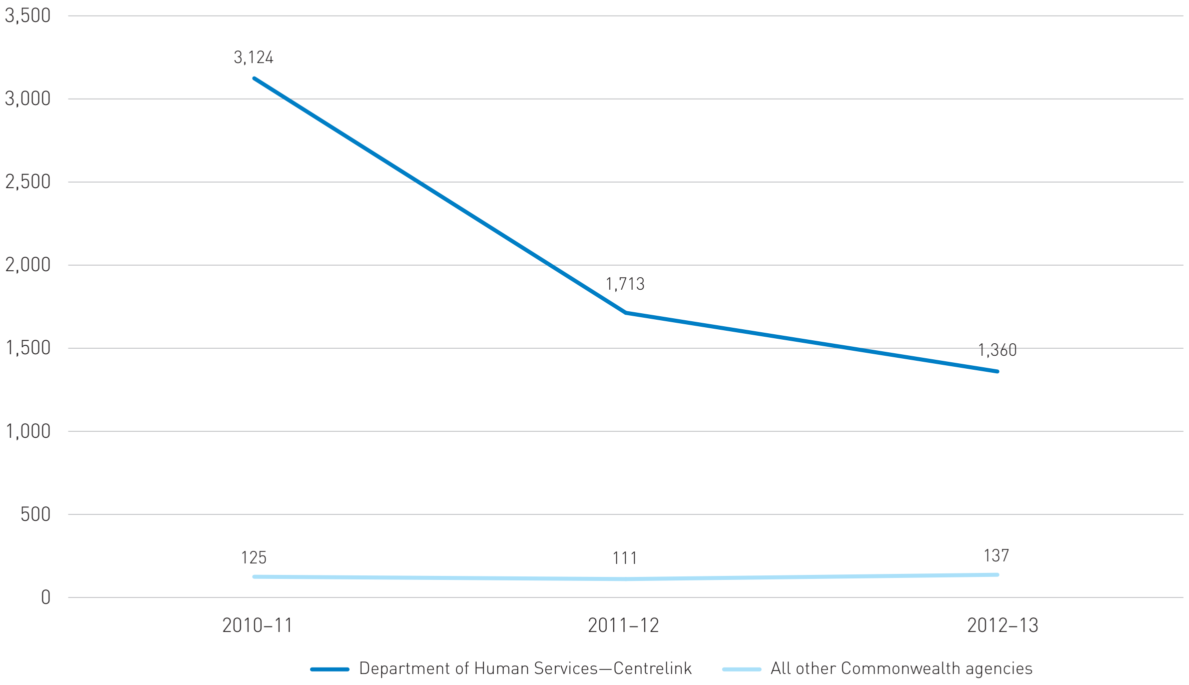
Offenders who commit identity-related offences against Australian Government agencies may be prosecuted by the Commonwealth Director of Public Prosecutions (CDPP). For the pilot, the CDPP provided a suite of prosecution statistics relating to identity crime offences under the *Criminal Code (Cth)* over the last three financial years (2010–11, 2011–12 and 2012–13), and other Commonwealth offences under which offenders can be prosecuted for identity-related crime (see Figure 15 and Table 3).

Case Study 8 (February 2007): Identity fraud committed by Medicare employee

Over a five year period, the offender used her position as a Medicare Branch Manager to create 65 false identities under which 387 fraudulent claims were made, totalling $156,034. The offender was charged with 65 counts of obtaining property by deception and was sentenced to 8 years imprisonment.

Commonwealth Director of Public Prosecutions. *2010. 2009–10 Annual Report*. Available at: http://www.cdpp.gov.au/case-reports/marita-quetcher/

Figure 15: Total number of Commonwealth prosecutions for fraudulent conduct, by referring agency, 2010–11 to 2012–13



Note: Data as at 25/11/13

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

Source: Commonwealth Director of Public Prosecutions

These figures indicate that over the last three financial years (2010–11 to 2012–13) DHS (Centrelink) has made 94 percent of all referrals for Commonwealth prosecutions (both summary and on indictment) for fraudulent conduct. It can also be seen that while the number of prosecutions referred by all other Australian Government agencies has remained relatively stable, the number of DHS prosecutions have more than halved over this period, from 3,124 in 2010–11 to 1,360 in 2012–13.

The vast majority (96%) of Commonwealth defendants prosecuted for identity-related crimes over the three years to 2012–13 are prosecuted for offences of fraudulent conduct (see Table 3). Only a small number are prosecuted for offences that may be more directly associated with identity crime, such as forgery or possessing/manufacturing false documents. Only one defendant was prosecuted for a specific identity crime offence.

This illustrates the limitations of using identity crime offence prosecutions as an indicator of identity-related crime. While not all fraud offences involve identity-related crime, research from the United Kingdom indicates that a significant proportion (more than 50%) of all fraud is enabled through the use of a false or stolen identity (CIFAS 2013). Australian data illustrates that most identity criminals are being prosecuted for the offences that are enabled using a false or stolen identity (e.g. fraudulently obtaining benefit by deception), rather than the offences of acquiring and possessing a fraudulent identity.

Table 3: Number of defendants[a] prosecuted by the CDPP, by Act and year (2010–11 to 2012–13)[b]

	2010–11	2011–12	2012–13
Divisions 370, 372, 375 *Criminal Code*—Identity crime	0	0	1
Divisions 133-137 *Criminal Code*—Fraudulent conduct	3,215	1,796	1,458
Divisions 144-145 *Criminal Code*—Forgery	31	19	24
Division 480 *Criminal Code*—Financial information offences	12	10	9
Section 234 *Migration Act 1958*—False documents	17	16	29
Anti-Money Laundering and Counter Terrorism Financing Act 2006, sections 135-138	3	4	2
Section 24 *Financial Transactions Report Act 1988*— Opening account etc. in false name	10	7	9
Part XIII *Customs Act 1901*—Penal provisions (section 233BAB)	16	7	13
Part 14 *Trademarks Act 1995*—sections 146-148	8	10	9
Total	**3,312**	**1,869**	**1,554**

(a) 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 3,289, 1,854, and 1,535 unique defendants prosecuted in 2010–11, 2011–12, and 2012–13 respectively.

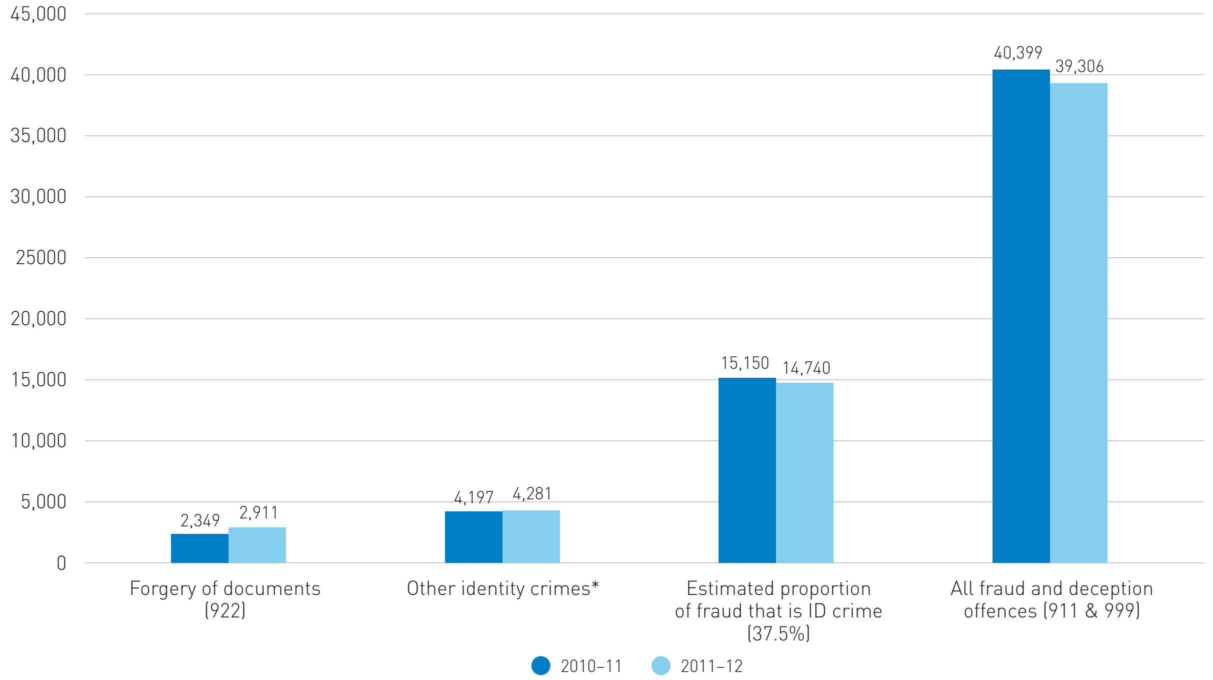
(b) As at 25/11/13

Source: Commonwealth Director of Public Prosecutions

State and territory identity crime prosecutions

States and territories also have specific identity crime offences, such as dealing or possessing fraudulent or stolen identification information, or manufacturing counterfeit credentials. Criminal courts data on state and territory prosecutions from the Australian Bureau of Statistics (ABS 2014b; *Criminal Courts, Australia* series Cat. No. 4513.0) also suggests that, like Commonwealth offences, many state and territory identity crimes are prosecuted under other fraud related offences (see Figure 16).

Figure 16: Number of identity crime offences and frauds proven guilty in all state/territory courts, by offence category and year, 2010–11 and 2011–12



* Includes identity crimes coded under the following ANZSOC codes: 322, 829, 831, 923, 931, 932, 933, 991, 1111, 1542, 1543, 1549, 1559, 1612, 1631, and 1694.

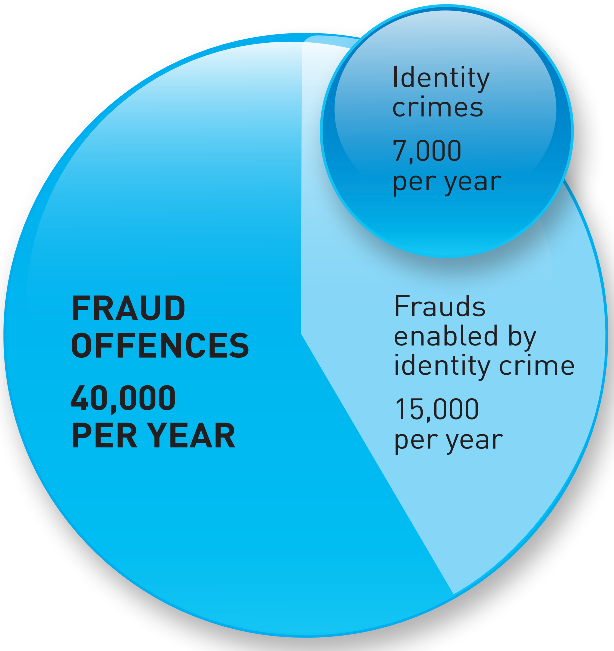
Note: Excluded from this data is identity crimes prosecuted in the Australian Capital Territory Magistrates' and Children's Courts in 2010–11 and Tasmanian Higher Courts for both 2010–11 and 2011–12

Source: ABS Customised report (2014).

Quantifying the true number of identity crimes proven guilty 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 frauds. Based on the assumption that 37.5 percent (i.e. halfway between 25% and 50%) of fraud involves identity crime, ABS data shows that around 22,000 identity crimes were proven guilty in 2010–11 and 2011–12.

To provide a clear picture of the relationship between identity crime and other types of fraud, data presented in Figure 17 shows that of the 40,000 frauds proven guilty each year in state and territory courts, around 15,000 are enabled by the use of stolen or fabricated identities. In addition, there are also around 7,000 'core' identity crime offences proven guilty each year, including activities such as forgery, possessing equipment to manufacture fraudulent credentials and making false representations.

Figure 17: Estimated number of identity crime and fraud offences proven guilty in state and territory courts each year



Conclusions around identity crime prosecutions

Prosecution data provided by the CDPP and ABS shows that there are thousands of identity crimes prosecuted each year, with available data showing a slightly downward trend. As with police data recording systems, most identity crime offences are recorded as frauds. This makes it very difficult to separate those frauds that are enabled using fraudulent identities and those committed through other methods.

As with police data recording systems, most identity crime offences are categorised as frauds in prosecution statistics.

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

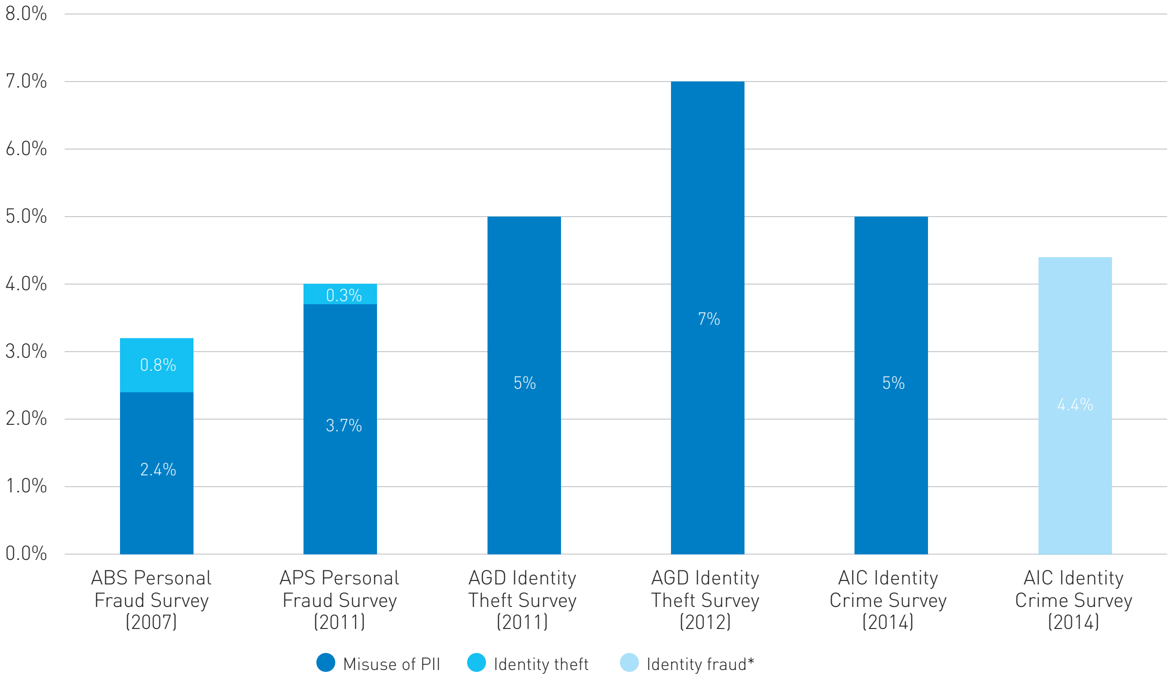
Key findings: The number of people who experience identity crime or misuse each year appears to be rising. The proportion of Australians who report being a victim of identity crime is significantly higher than other personal and theft-related offences.

Key finding: Identity crime is significantly underreported by both individual victims and organisations. Recent research indicates that half of credit card fraud victims and a third of identity theft victims did not report the incident to a formal institution, such as law enforcement or a financial organisation.

Recent identity crime survey data

As part of the pilot, AGD and DFAT commissioned the AIC to undertake a survey on the rate of identity crime victimisation among the Australian community. The AIC Survey sought to build on other recent identity crime survey research conducted by the ABS (2008 and 2012) and AGD (2011 and 2012a). The headline findings from each of these surveys are presented in Figure 18. In general, findings indicate that around four to five percent of respondents experienced identity crime in the previous 12 months, of which a large proportion was identity fraud (mostly credit card fraud).

Figure 18: Proportion of respondents reporting identity crime victimisation or misuse of personal information, by survey and year



* Includes credit card fraud.

Note: The AGD surveys asked respondents about their victimisation in the previous six months, whereas the reference period in the other surveys was 12 months.

Source: ABS 2008 & 2012; AGD 2011 & 2012; Smith & Hutchings 2014.

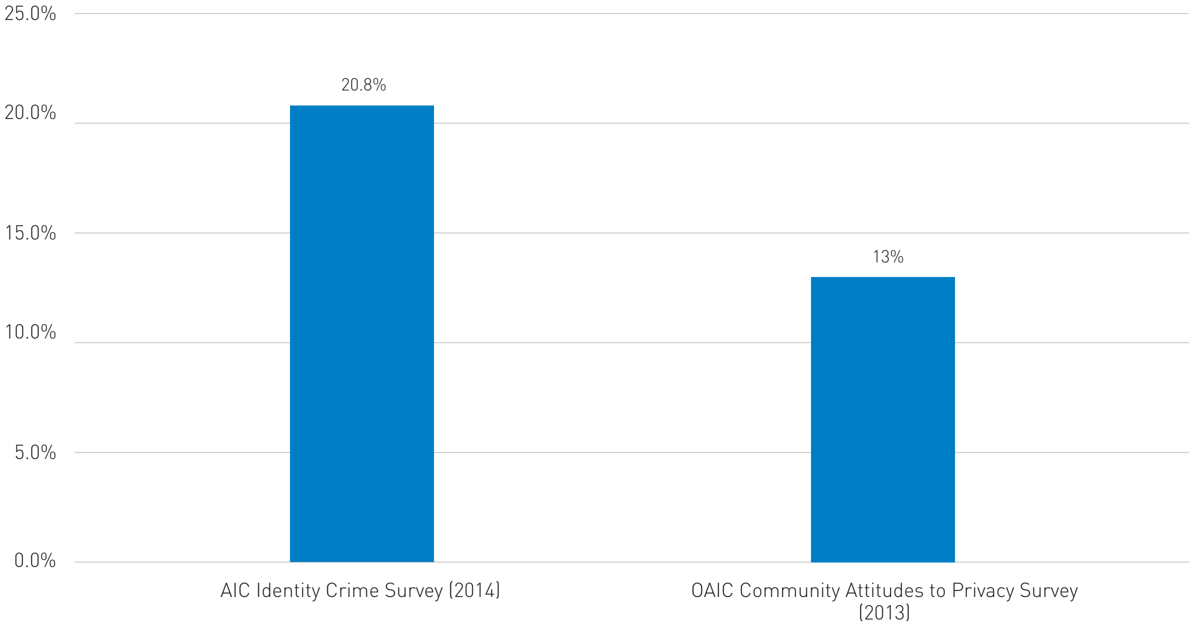
Differences in the headline victimisation rate between the surveys is likely due to the different sampling methodologies, data collection techniques employed, and focus of questions asked of respondents.

Recent survey data show that 9.4% of respondents reported having their personal information stolen or misused in the previous 12 months, with 5% reporting losing money as a result.

The AIC Survey adopted a broader definition of 'identity misuse' than those conducted by the ABS (2008 and 2012) and AGD (2011 and 2012a), which focussed primarily on identity crime. The AIC Survey asked participants whether they had experienced misuse of their personal information in the previous 12 months, whereas the scope of the ABS questions was more specific[2]. The AGD surveys asked participants whether their identity information had been stolen or misused in the previous six months or so.

The AIC Survey and another survey conducted by the OAIC on community attitudes to privacy also provide an indication of the lifetime prevalence of identity crime amongst Australians (see Figure 19).

Figure 19: Proportion of survey respondents reporting having ever been a victim of identity theft or misuse, by survey



Source: Smith & Hutchings 2014; OAIC 2013b

[2] The ABS survey asked respondents whether in the last 12 months, they had been aware of anyone using their credit cards to make purchases or withdraw cash without their permission, or using their personal details, such as driver's licence or tax file number in stolen, fraudulent or forged documents, without their permission.

The highlights of the various Australian identity crime surveys conducted in recent years suggest that:

- between four and five percent of people are victims of identity crime that results in a financial loss each year
- around 9.4 percent of people may experience some form of misuse of their personal information, including identity crime, per year
- between 13 and 21 percent of people have experienced identity crime or misuse *at some point in their life*
- the majority of identity crime victims, perhaps around nine in 10, experience credit card fraud, or other less serious frauds, and in around half of these cases they are reimbursed by a financial institution
- a small but significant proportion of victims, perhaps around one in 10, experience more serious cases of identity theft which involved considerable financial and other consequences.

Similar surveys conducted in the United States and the United Kingdom produced broadly comparable findings. The most recent Identity Theft Supplement to the National Crime Victimisation Survey (NCVS) conducted by the Bureau of Justice Statistics in the United States found that 16.6 million people (7% of the population aged 16 years or older) were victims of one or more incidents of identity theft in 2012, with 85 percent involving the fraudulent use of financial information such as credit cards or bank account details (Harrell & Langton 2013). A 2012 survey by the then National Fraud Authority in the United Kingdom found that 4.3 million adults (8.8% of the population) had been a victim of identity fraud in the previous 12 months, with 27 percent reporting that they had been a victim at some point in their life (NFA 2013; 30).

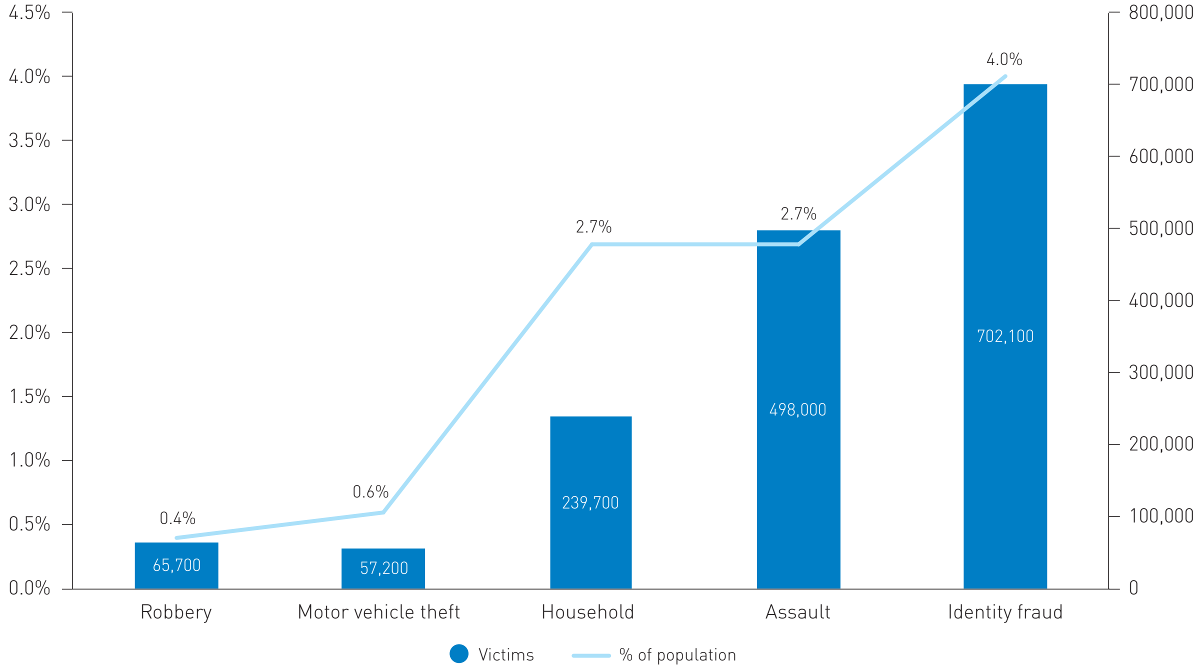
Identity crime victimisation compared with other personal and theft-related crimes

ABS survey data in Figure 20 shows that in 2012–13 an estimated three percent of Australians aged 15 years and over (498,000 people) were victims of assault, 2.7 percent of households (239,700 households) were victims of at least one break-in to their home, garage or shed, 0.4 percent (65,700 people) were victims of robbery, and 0.6 percent of households had their motor vehicle stolen (57,200 incidents) (ABS 2014a).

This indicates that identity crime is one of the most prevalent crimes affecting Australians each year, in that a greater proportion of people report being a victim of identity crime than assault, robbery, household break-ins or motor vehicle theft.

More Australians report experiencing identity crime each year than assault, robbery, household break-ins or motor vehicle theft.

Figure 20: Number of victims and proportion of population, by offence type



Source: ABS 2014a.

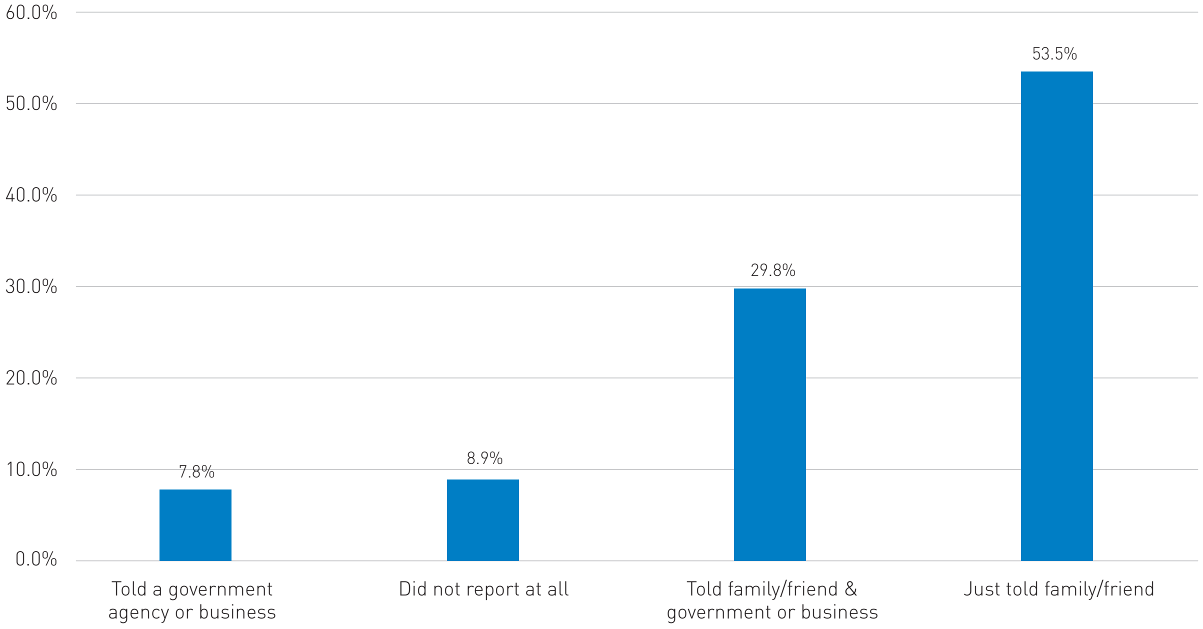
Underreporting

Despite the apparent prevalence of identity crime, it is highly likely that the full extent of this crime type is not being captured due to underreporting, with only around 40-60 percent of identity crime victims lodging a formal report about the incident to a government agency or private sector organisation.

Recent research by the ABS has shown that half of credit card fraud victims and one third of identity theft victims did not report the incident to a formal institution, such as law enforcement or a financial institution (ABS 2012).

The AIC Survey results show that only around two in five people reported the incident formally, while just over half only told a friend or family member (see Figure 21).

Figure 21: Reporting experience of identity crime and misuse, by type of report



Source: Smith & Hutchings 2014

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

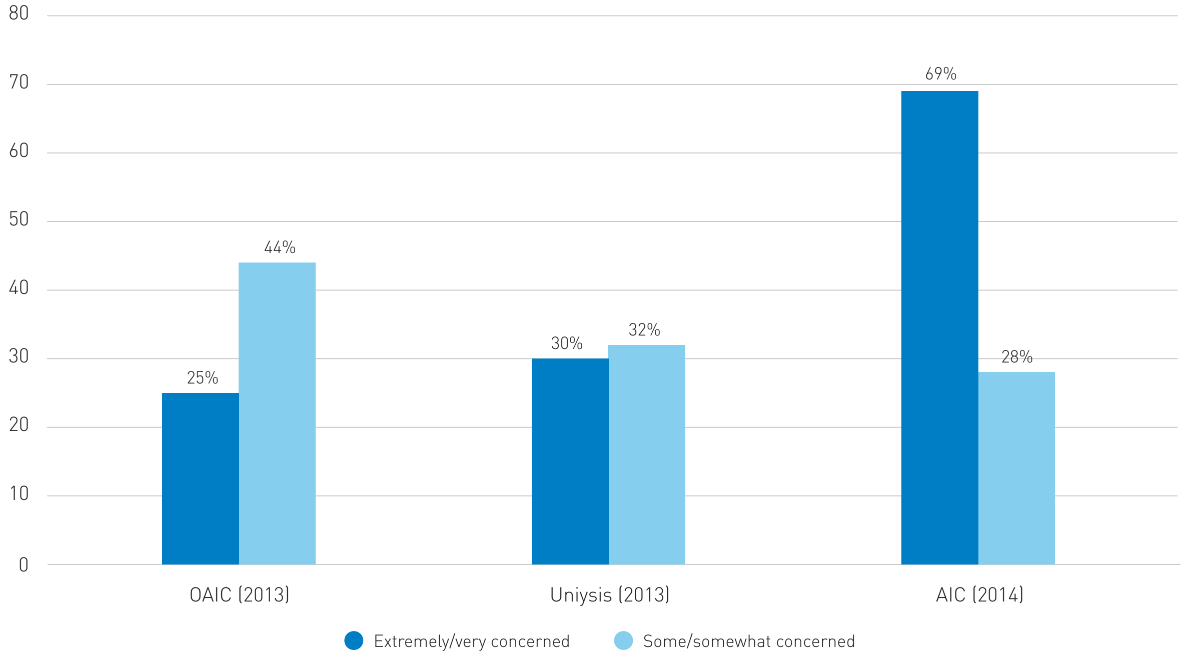
Key findings: Identity crime continues to be of serious concern to a large number of Australians, with around two-thirds of survey respondents expressing concern about becoming a victim of identity crime in the next 12 months.

In addition to direct impacts on victims, identity crime appears to be a significant concern to Australians more broadly. Findings from recent surveys show that between one quarter and two thirds of respondents perceive identity crime to be a serious problem (see Figure 22).

In addition to the AIC and OAIC surveys mentioned above, Unisys has undertaken annual surveys since 2006 that gauge community concern about a range of security-related issues. Responses to the 2013 Unisys Security Index survey show that, across all of the issues canvassed—which included national security threats and serious health epidemics—the two issues that rated highest in terms of level of concern were:

- unauthorised access to/misuse of personal information (62%)
- other people obtaining/using credit card/debit card details (60%) (Unisys 2013).

Figure 22: Level of concern about identity crime and misuse, by survey



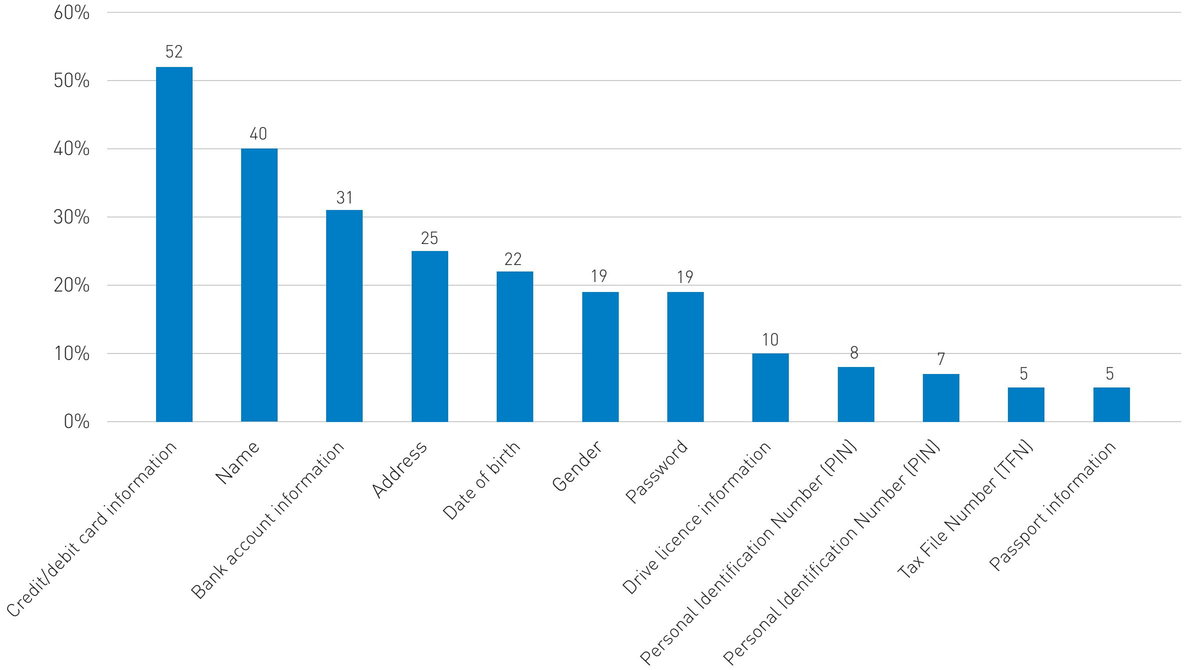
Source: OAIC 2013b; Unisys 2013; Smith & Hutchings 2014.

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

Key findings: The types of information most susceptible to identity theft include financial information (credit card numbers and bank account details) and other biographic information (name, date of birth). Passwords were also identified as vulnerable in around one in five cases of identity crime and misuse. Organisations that use this information to transact with their clients need to take adequate precautions to ensure that it remains protected.

For the most serious occasion of victimisation, the AIC Survey asked respondents about the types of personal identifying information (PII) that they perceived to be most at risk of misuse. Respondents believed that credit/debit card information was the most susceptible to misuse, followed by name and bank account information (see Figure 23).

Figure 23: Types of PII that respondents reported was misused in previous 12 months



Note: 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.

3. Consequences of identity crime

3.1 Direct cost of identity crime and misuse to government agencies

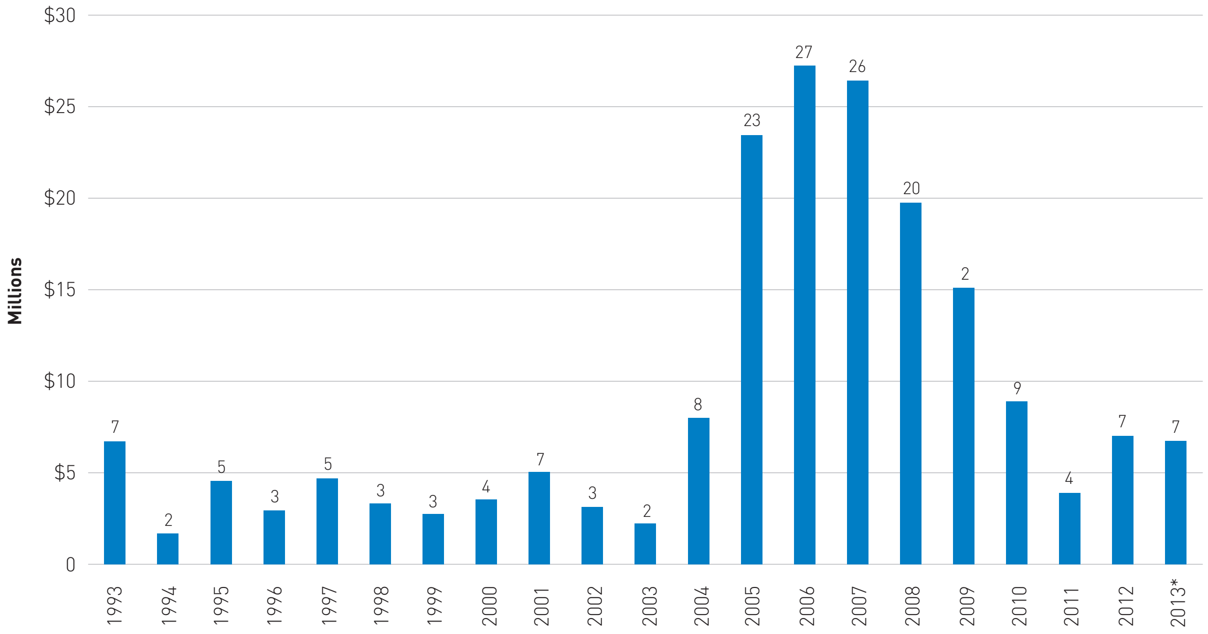
Key findings: The total direct losses and associated costs of identity crime to government agencies are difficult to estimate, but they are likely in the order of several hundred million dollars each year. Where an agency invests additional effort and resources in detecting and investigating this activity, the amount of incidents detected is likely to increase considerably.

Due to limited available data, it is difficult to accurately quantify the direct cost of identity crime and misuse to government agencies. However, it is possible to produce a range of estimates that are based on the average number of offences, associated losses, as well as prevention and remediation costs.

Cost of benefits fraud

Within the constraints of available Centrelink data, the overall value of identity frauds between 1992 and 2013 is shown in Figure 24. Analysis of the data reveals that over this 21 year period, there was an annual average of $8.9m worth of identity fraud detected by DHS.

Figure 24: Total value of identity fraud against DHS (Centrelink), by year, 1/07/1992 to 30/04/2013



* To 30 April 2013

Source: Department of Human Services—Centrelink

The 2003–04 Federal Budget committed funding to expand the specialist identity fraud investigation teams within DHS, including the development of Tactical Intelligence Analysts based in Sydney, Melbourne, Brisbane and Canberra. As a result, it can be seen in Figure 24 that between 2005 and 2009 there was a considerable spike in the value of identity fraud detected by DHS.

There are also detailed findings from an AIC study on welfare fraud in Australia which show that in 2008–09 there were 3,873 investigations conducted into possible identity frauds, with 166 referrals for prosecution, and $15.1 million in debts and savings (Prenzler 2012; 64). In general, the report observes that around 3,000 cases are prosecuted each year, representing about 0.04 percent of all Centrelink customers, with the losses in these cases adding up to approximately $40.5m per year and involving approximately $120.9m per year in gross savings and amounts targeted for recovery (Prenzler 2012; xii).

Case Study 9 (December 2005): Centrelink benefits fraud using fictitious identities

Over a six year period, a Queensland nurse created four adult identities and registered that these persons had given birth to nine sets of twins. These fabricated identities were then used to claim family assistance payments from Centrelink worth $622,000. The offender was charged with 10 counts of obtaining benefit by deception and was sentenced to seven years imprisonment.

Source: ABC News, 16 December, 2005

http://www.abc.net.au/news/2005-12-16/nurse-jailed-for-massive-centrelink-fraud/763254

Costs of identity crime to other government agencies

Apart from the ATO that provided data on the number and value of income tax returns that were withheld due to identity crime in 2010–11 (6,427 returns worth $15m), no other government agency that participated in the pilot (either Australian or state and territory) was able to provide information about the costs to the agency of identity crime.

Estimated cost to investigate and prosecute identity crimes

Data presented in Table 4 shows the estimated annual *direct costs* to law enforcement agencies and criminal courts associated with investigating and prosecuting identity crimes. While there are variations in the time periods for which these figures apply, these estimates are based on the data available and are meant for indicative purposes only.

Table 4: Estimated annual direct costs of investigating and prosecuting identity crimes, by agency and year

Agency	Year	Unit of measurement	Total fraud cost	Average identity crime costs
AFP[a]	2010–11	Fraud investigations	$12,796,214	$4,798,580
CDPP	2012–13	Defendants prosecuted	$34,495,692	$12,935,885
State courts	2011–12	Defendants prosecuted	$66,000,000	$24,750,000
State police	2012–13	Fraud investigations	$90,000,000	$33,750,000
Total			**$203,291,906**	**$76,234,465**

a: Jorna & Smith 2013.

These estimates are based on the assumption that a single identity crime case costs state courts and police $3,000 per incident; the mid-point between the ABS (2012) average loss per personal fraud incident ($2,000) and the direct out-of-pocket losses per incident ($4,101) reported in the AIC Survey (Smith & Hutchings 2014). While this rough estimate of investigation and prosecution costs is not ideal, without more reliable cost data provided by state courts and police, it is very difficult to determine whether this $3,000 incident cost estimate is too high, or too low. For more detail about how the individual costs in Table 4 were calculated, see Appendix D.

3.2 Direct costs of identity crime and misuse to business

Key findings: Identity crime costs businesses at least $140 million each year. While the number of incidents has fluctuated, the financial impact of identity crime is consistently on the rise. This underscores the need for the private sector to play an active role in detecting and preventing identity crime.

Within the time and resources available during the pilot, it was not possible to engage private sector organisations about the cost of identity crime and misuse. Consequently, data for this indicator was sourced from recent KPMG surveys on fraud and misconduct affecting Australian and New Zealand businesses (KPMG 2009, 2010 & 2013) (see Figure 25). The surveys ask respondents about incidents occurring in the previous 24 month period.

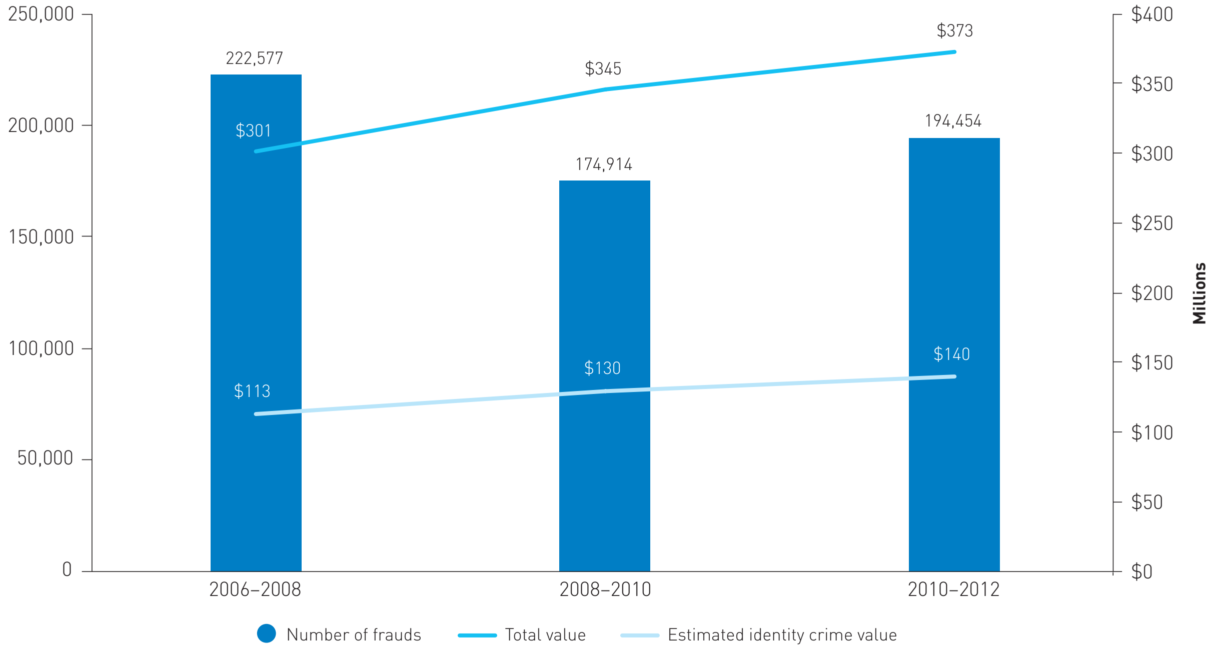
The most recent survey obtained responses from 281 private sector organisations across a range of industries including: financial and insurance services; health care and social assistance; manufacturing, energy, gas and water providers; and construction, as well as several other key industries.

Data presented in Figure 25 shows that while the number of all recorded frauds has fluctuated, the total value of these frauds has consistently increased, from $301m in 2006–2008 to $373m in 2010–2012. Estimates of the cost of identity-related frauds to business can be calculated based on the range that between 25-50 percent of all frauds involve some form of identity crime. If this is the case, the cost of identity fraud to Australian and New Zealand business in 2010–2012 was at least $140 million. However, these cost estimates are based on the survey responses provided by only 281 organisations and, as such, the total identity crime costs to all private sector organisations are certainly going to be many times higher.

Over the last four years the value of identity crime against businesses has been increasing, from $113m in 2006–2008 to $140m in 2010–2012.

These cost estimates are based on the responses provided by 281 organisations and, as such, the total identity crime costs to all private sector organisations are certainly going to be many times higher.

Figure 25: Number and value of frauds against Australian and New Zealand businesses, by year (2006—2012)

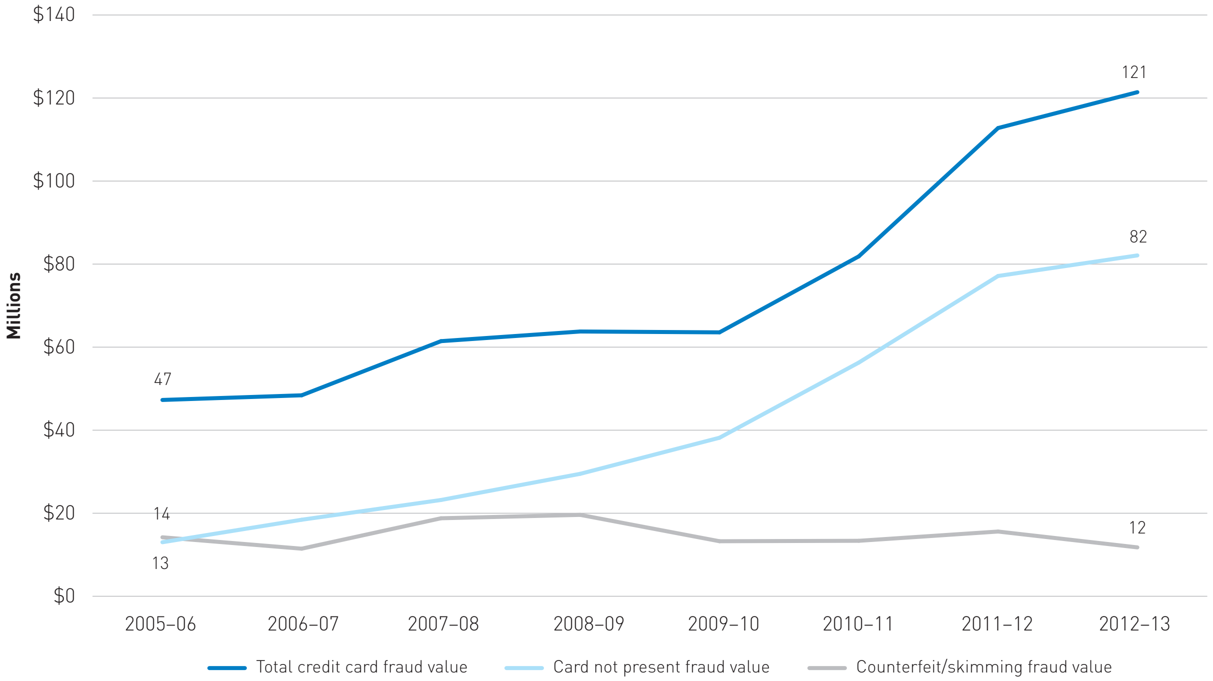


Source: KPMG 2009, 2010 & 2013

Payment identity fraud

The Australian Payments Clearing Association (APCA) monitors payment systems in Australia's financial sector, particularly non-cash transactions such as cheques, direct debit/credits, EFTPOS and ATM transactions as well as high value payments. The APCA publishes annual statistics on the number of fraudulent payments made in Australia (see Figure 26).

Figure 26: Value of credit card frauds, by fraud type and year (2005–06 to 2012–13)



Source: Australian Payments Clearing Association 2006–2013

Data presented in Figure 26 shows that the total value of credit card fraud is being driven upwards by card-not-present fraud (where a fraudulent transaction is made using only the credit card details and not the physical card). In 2005–06 there were just over $13 million worth of CNP frauds, while in 2012–13 the value reached over $82 million, an increase of 600 percent in just eight years.

It is difficult to estimate the proportion of these credit card frauds that are identity crime-related, as this category comprises a range of fraud methodologies. These include transactions on lost/stolen cards; frauds where a recently issued card has been intercepted and used before reaching the owner; fraudulent applications involving stolen, fabricated or manipulated identity information; counterfeit/skimming; card-not-present frauds; and other miscellaneous frauds—all of which could be conducted using cards held by individuals or organisations.

In the last eight years there has been a 600% increase in the value of card-not-present frauds.

There is some debate as to whether credit card fraud should be considered as identity crime or rather classified as a type of financial fraud. This is in part because many victims of credit card fraud are reimbursed by financial institutions and so do not experience any significant impacts (although these costs may be passed on in other ways such as increased fees). However, as credit card fraud generally involves the use of the card holder's name or other personal information, it has been included within the definition of identity crime for the purpose of the pilot. This view is supported by the results of the AIC Survey, which indicate that respondents thought that credit card details should be considered as personal information.

Case Study 10 (October 2011): Inter-agency investigation busts fake credit card syndicate

Following a collaborative investigation between the Australian Federal Police, New South Wales Police Force, New South Wales Roads and Maritime Services, and Department of Immigration and Border Protection, a sophisticated fake credit card syndicate was busted. After raiding two properties in Sydney, police officers found 12,000 blank credit cards and hundreds of blank NSW driver licences in addition to equipment and computer files used to manufacture fraudulent documents. It is estimated that the fake credit cards could have been used to complete $30m in fraudulent transactions.

Source: ABC News, 20 October, 2011
http://www.abc.net.au/news/2011-10-19/police-strike-30m-fake-credit-card-syndicate/3579592

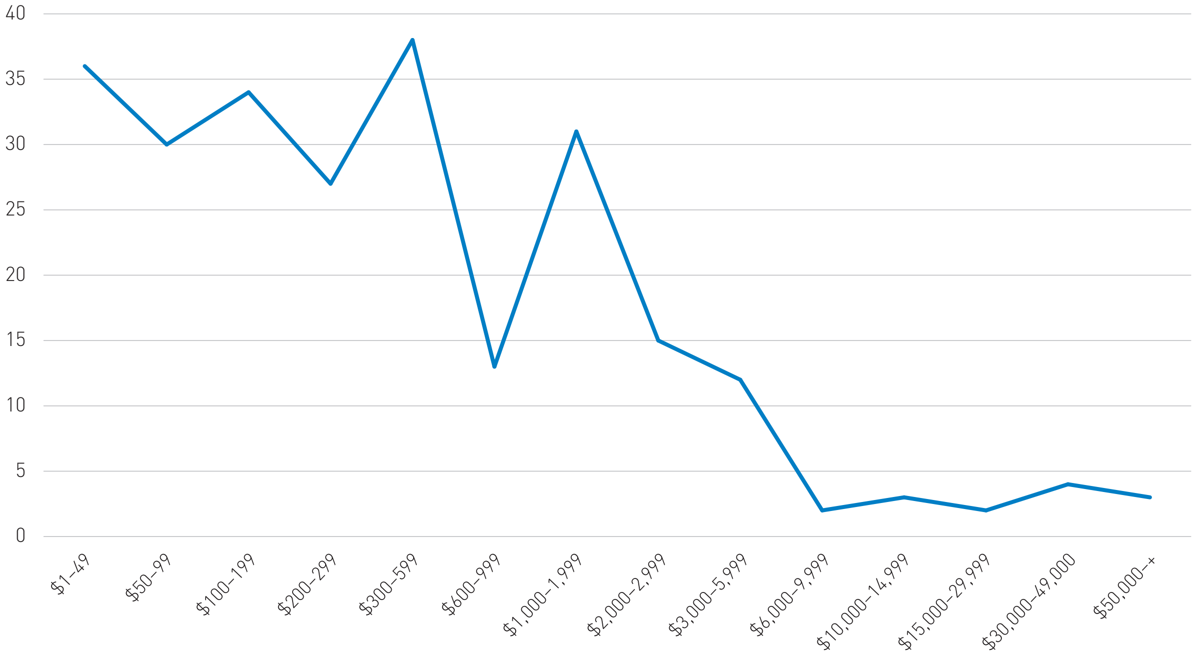
3.3 Direct financial losses to victims of identity crime and misuse

Key findings: The majority of identity victims lose relatively small amounts of money of 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 to their mental or physical health, reputations or general wellbeing.

The AIC Survey asked respondents about financial losses suffered as a result of misuse of their personal information. Of the 4,995 participants, 250 respondents (five percent or one in 20) reported losing money ranging between $1 and $310,000, with a median loss of $247 per victim (i.e. half the victims lost more than $247 and half lost less than that).
The distribution of the financial losses that victims reported experiencing in the previous 12 months is presented in Figure 27. It can be seen that the vast majority of victims lost an amount less than $1,000.

Victims of identity crime suffer out-of-pocket losses of $4,101 per incident.

Figure 27: Distribution of financial losses experienced by victims in the preceding 12 months

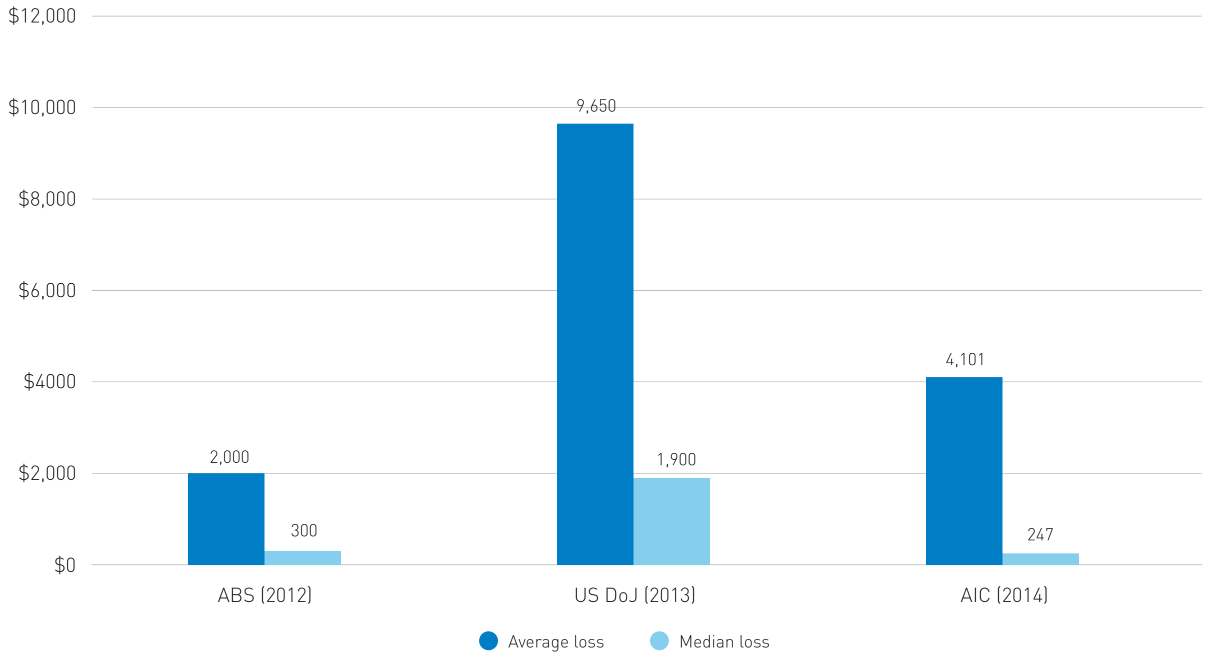


Source: Smith & Hutchings 2014

Survey respondents were also asked whether they were able to recover any losses or were reimbursed by banks or other organisations. Responses indicate that on average victims were able to recover $2,381 (although 45 percent did not recover any money), leaving an average out-of-pocket loss of $4,101 per victim (Smith & Hutchings 2014) (see Figure 28).

These findings are similar to those produced by the ABS (2012), which found that three in five personal fraud victims (60%) lost money at an average of $2,000 per person (median $300). Comparable data from the United States shows that two-thirds of identity theft victims (66%) reported a direct financial loss, at an average of $USD9,650 per victim (median $USD1,900) (Harrell & Langton 2013; 6).

Figure 28: Average and median financial losses suffered by victims of identity crime and misuse, by survey



Source: ABS 2012; Harrell & Langton 2013; Smith & Hutchings 2014

3.4 Number of identity crime victims experiencing non-financial consequences

Key findings: In addition to financial losses, many victims of identity crime experience other mental and physical health impacts. The stress and frustration of trying to regain control of one's identity information and financial reputation can also damage family and social relationships.

There are only a small number of studies that have sought to measure the non-monetary impact of identity crime victimisation, such as the emotional and psychological harm.

Results from the AIC Survey show that one in 10 victims (11%) experienced mental or emotional distress that required counselling or other treatment, while one in 17 (6%) were wrongly accused of a crime (i.e. the criminal who stolen the identity information used it to commit an offence for which the victim was accused) (Smith & Hutchings 2014).

11% of identity crime victims required counselling or other treatment; 6% were wrongly accused of a crime.

It has been observed that 'few people realise that identity theft may have long term, unexpected consequences which may significantly impact the life of the victim' (Identity Theft Resource Centre 2010; 24). Indeed, an American survey conducted in 2008 found that the psychological trauma experienced by some identity crime victims was similar to that experienced by victims of violent crime (Van Vliet & Dicks

2010). Coming to terms with the fact that your identity has been stolen and used to commit crimes can be a very difficult situation for many victims to deal with, in that 'the psychological distress caused by the crime itself is heightened when victims encounter difficulties clearing their name' (Lawson 2011; 18).

Identity crime affects not only the individuals who are victimised, but can also have negative impacts on the victim's friends and family. It has been shown that the stress and frustration of trying to regain control of one's identity information and financial reputation can damage family and social relationships (Lawson 2011; 18). When identity information is stolen and used to commit other offences, the damage caused to the victim's reputation can take years to repair (see Case Study 11).

Case Study 11 (September 2004): The non-financial consequences of identity theft

A 46-year-old British man regularly shopped online from large well-known retailers. His credit card details were stolen and used by an offender in Jakarta, Indonesia to purchase child exploitation material. The victim was arrested by the British police as part of a criminal investigation into child exploitation. When his employer discovered that he had been arrested for allegedly downloading child exploitation material, he was dismissed from his job as a well-paid executive. His close friends and family refused to talk to him anymore. It took the victim almost four years to clear his name and repair the damage to his reputation.

Source: BBC UK, 3 April, 2008
http://news.bbc.co.uk/2/hi/uk_news/magazine/7326736.stm

4. Remediation of identity crime

This component seeks to measure the different activities associated with helping victims of identity crime to recover their identity and restore the damage caused to their credit rating and reputation.

4.1 Average time by victims spent in remediation activity (i.e. recovering their identity)

Key findings: The average amount of time victims spend recovering from identity theft ranges from 10 to 18 hours. A small but significant number of victims, around one in 20, spend over 200 hours recovering their identity. These more complex cases can involve identities that are stolen and used to commit other serious criminal offences. The damage caused to the victim's reputation can often take years to repair.

Victims of identity crime will spend an average of 18 hours dealing with the consequences, with some spending more than 200 hours.

There have been several recent studies that examine the length of time it takes victims to deal with the consequences of identity crime (see Table 5). Respondents to the AIC Survey spent an average of 18 hours dealing with the consequences of identity crime and misuse, including time taken to fix their credit rating and other financial information (Smith & Hutchings 2014). Results from a

Canadian survey were in-line with Australian findings, in that victims spent an average of 13 hours in remediation activity. Findings from surveys conducted in the United Kingdom and United States show that victims of identity crime spend slightly longer in remediation activity than Australian victims.

Table 5: Estimates of the time spent by victims remediating the consequences of identity crime

Country	Source	Year	Time spent by victims
Australia	AIC (Smith & Hutchings 2014)	2013	Range: 0-500 hours Average 18.1 hours 5% spent over 60 hours
Australia	Lacey (2013)	2013	Average: 10.2 hours Some victims spent more than 200 hours
United Kingdom	CIFAS (2012)	2012	Typical victim spends between 3–48 hours Victims of a 'total hijack' spent 200 hours
United States	Harrell & Langton (2013)	2012	52% spent 1 day or less 19% spent 2–7 days 18% spent 8 days to <1 month
Canada	Sproule & Archer (2008)	2008	Average of 13 hours per victim, up to 17 hours when credit card fraud is excluded

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

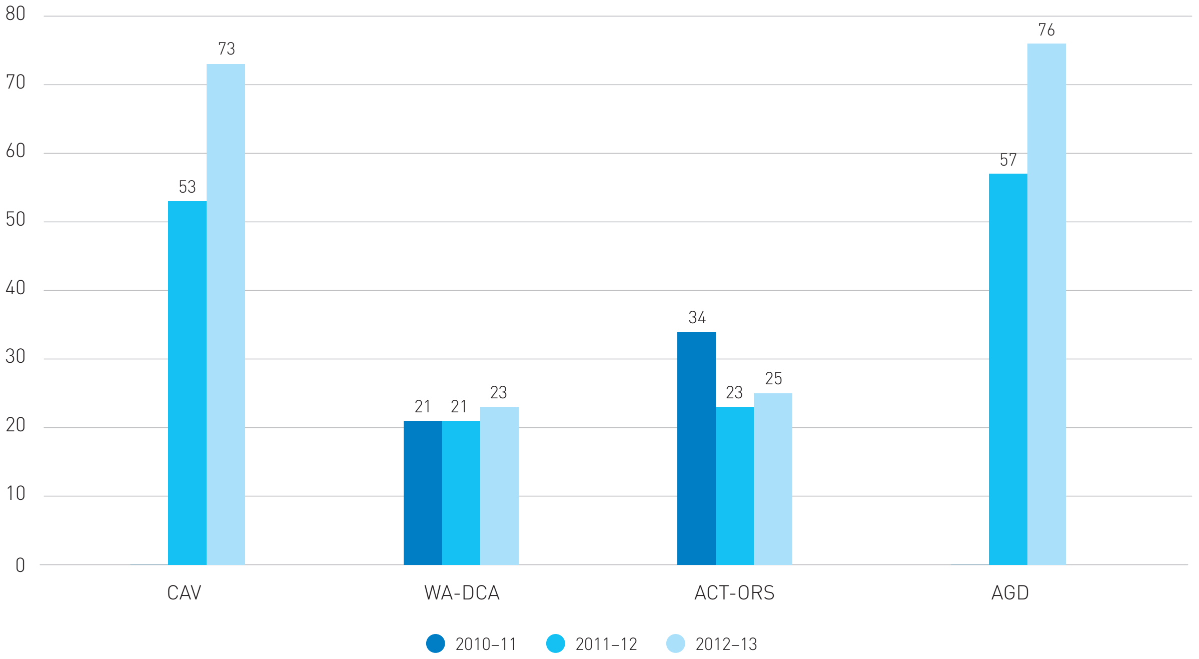
Key findings: The proportion of identity crime victims who report their experience to government agencies is relatively small (around 1 in 5). The reasons for this may be that victims are unaware of the reporting processes available to them, or that they do not consider there is value in reporting the crime to these agencies.

This indicator tabulates enquiries made to government agencies by individuals seeking assistance to restore compromised identities. While most agencies participating in the pilot were asked to provide information about calls for assistance, only three consumer affairs agencies could provide relevant statistics.

Departments of Consumer Affairs

Figure 29 presents the data provided by Consumer Affairs Victoria, the Western Australian Department of Consumer Affairs, and the Australian Capital Territory Office of Regulatory Services. Also shown is data collected from alleged identity crime victims who contacted the Australian Attorney-General's Department during 2012 and 2013.

Figure 29: Request for assistance from alleged identity crime victims, by agency and year, 2010–11 to 2012–13



Source: Consumer Affairs Victoria (CAV); Western Australian Department of Consumer Affairs (WA-DCA); Australian Capital Territory Office of Regulatory Services (ACT-ORS); Australian Attorney-General's Department (AGD).

Only 8% of victims reported the incident to a government agency or business—54% just told a friend or family member.

Considering recent survey findings, which indicate that between four and five percent of respondents (an estimated 700,000 to 900,000 Australians aged 15 years and over) are victims of identity crime and suffer financial loss each year, the numbers presented in Figure 29 appear to be exceptionally low. The AIC Survey sought to better understand why victims do not report the incident, and for those who do report it, who they contacted and how satisfied they were with the response. Of the survey respondents who reported being a victim of identity crime or misuse in the previous 12 months, almost one in 10 (8.9%) did not report the incident in any way, while more than half (53.5%) just told a friend or family member (Smith & Hutchings 2014). Of those who did report the matter, only one in 12 (7.8%) reported it to a government agency or private business, most commonly the police or their financial institution (Smith & Hutchings 2014).

For victims who stated why they didn't report their experience, the common barriers were not believing that the police or other authority could do anything (40%), followed by being too embarrassed (24%) and not knowing how or where to report (23%) (Smith & Hutchings 2014).

Office of the Australian Information Commissioner

The OAIC also receives enquiries and complaints each year from members of the public. The OAIC supplied data on the number of enquiries, complaints and own motion investigations undertaken in 2012–13, categorised by whether the matter related to privacy or credit reporting (see Table 6).

Table 6: Number of enquiries, complaints and own motion investigations (OMIs) received by the OAIC in 2012–13

	Privacy matter	Credit reporting matter	Total
Enquiry	1,538	1,072	2,610
Complaint	229	400	629
OMIs	13	1	14

Source: Office of the Australian Information Commissioner

4.3 Number of applications for victims' certificates

Key findings: There is a lack of community awareness of the potential assistance that victims' certificates can provide to victims of identity crime. Only around one in seven victims were aware of the existence of these certificates and fewer than one in 30 victims actually applied for one, although no Commonwealth certificates have been issued in the last three years.

A victims' certificate can assist an individual, who has been a victim of identity crime, in dealing with organisations, including financial institutions for the purpose of restoring their credit rating or removing fraudulent transactions.

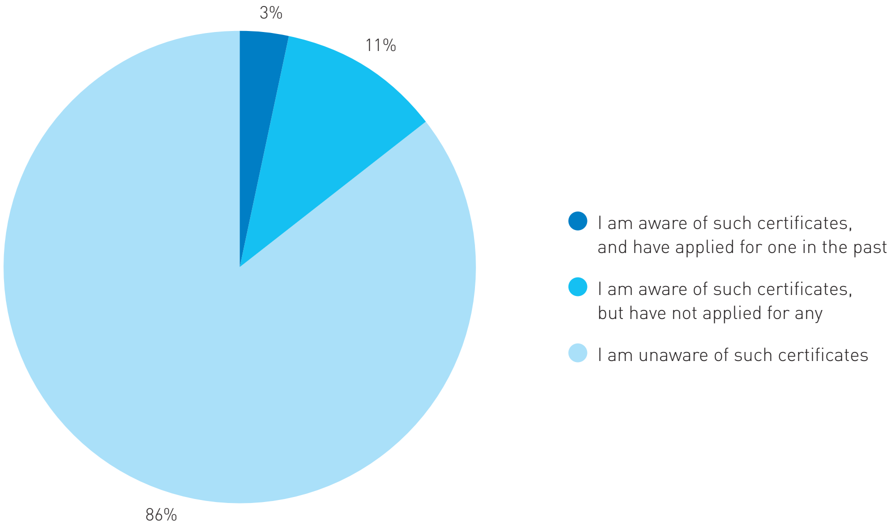
Only 1 in 7 victims of identity crime knew of the existence of victims' certificates, with less than 1 in 30 applying for one.

Under Division 375.1 of the *Criminal Code Act 1995* (Cth), victims of Commonwealth identity crimes can apply to a state or territory magistrate for a Commonwealth Victims' Certificate. Advice provided by the CDPP indicated that no Commonwealth Victims' Certificates have been issued in the last three years.

Legislation in Victoria (Part 4a, S89F, *Sentencing Act 1991*) and Western Australia (Part VI, D3, S494 *Criminal Code Act 1913*) also allows for certificates to be issued for victims of identity crime in those two jurisdictions. It was not possible to obtain data during the pilot to indicate how many victims' certificates were issued in these two jurisdictions.

The fact that no Commonwealth victims' certificates have been issued indicates that many victims may not be aware of the potential assistance they can provide. This is supported by the AIC Survey results which showed that only around one in 10 victims of identity crime knew of the existence of victims' certificates, with fewer than one in 20 victims actually applying for one (Smith & Hutchings 2014) (see Figure 30).

Figure 30: Respondents' awareness of victims' certificates



Source: Smith & Hutchings 2014

5. Prevention of identity crime

5.1 Number of identity credentials able to be verified using the DVS

Key findings: There are an increasing number of identity credentials that can be verified through the DVS, including four of the five credentials that have been identified through this project as being at most risk of misuse (i.e. Medicare cards, driver licences, birth certificates and passports).

The DVS enables user organisations to match the biographical data presented on identity credentials with the issuing authority, and is a useful tool for detecting fraudulent documents.

If a person presents an organisation with a document such as a passport or a driver licence as evidence of their identity, the organisation can use the DVS to check the authenticity of the document with the relevant issuing agency (AGD 2014a). As at February 2014, there are 10 core identity credentials that can be verified through the DVS: passports; citizenship certificates; registration by descent certificates; visas and Immicards; driver licences; birth, marriage and change of name certificates; and Medicare cards.

The DVS is increasingly being used to verify personal information on Australian identity credentials—which will strengthen the evidence of identity processes for government and the private sector.

5.2 Number of government agencies using the DVS

Key findings: An increasing number of government agencies are using the DVS across Australia, although coverage amongst key government credential issuing agencies is not yet universal, with only a quarter of RTAs and RBDMs currently using or planning to use the DVS by the end of 2014.

As of 31 March 2014 there are 17 government and 151 private sector users fully approved to use the DVS (see Table 7). Data presented in Table 7 indicates that there is currently only limited usage of the DVS by government agencies. For example, only one of the eight RTAs and eight RBDMs currently use or are planning to use the DVS by the end of 2014.

Table 7: Government agencies' use of the DVS

	Current users		
Agency	**Using DVS**	**Access from**	**Future users**
Australian Government			
Australian Taxation Office	Yes	June 2012	-
Department of Foreign Affairs and Trade	Yes	March 2010	-
Department of Immigration and Border Protection	Yes	March 2010	-
Department of Human Services—Medicare	-	-	By end of 2015
ComSuper	Yes	March 2012	-
Australian Financial Security Authority	Yes	December 2013	-
State/territory			
Road Transport Authorities	Yes—NSW	March 2010	VIC—June 2015
Roads & Maritime Services	Yes—NSW	March 2009	-
Registries of Births, Deaths & Marriages	Yes—NSW	September 2010	QLD—end 2014
Offices of State Revenue	Yes—NSW, VIC, SA, QLD, WA	NSW—July 2011 VIC—August 2012 SA—August 2012 QLD—March 2012 WA—Dec 2013	-
State Electoral Commissions	Yes - NSW	March 2011	-

Source: Attorney-General's Department

5.3 Number of private sector organisations using the DVS

Key findings: There is strong demand for use of the DVS amongst private sector organisations, particularly those with legislative obligations to verify the identities of their customers. There is scope for significant further growth in the number of user organisations which have a reasonable necessity to verify a person's identity in accordance with the Privacy Act 1988.

The DVS was originally only available to government agencies. However, in 2012–13 Australian governments decided that the use of the service should be extended to private sector organisations. Currently, those organisations that have an authority or requirement under law to identify their customers are eligible to use the service. This includes companies operating in the financial and telecommunications services sectors.

As at 31 March 2014, there have been around 250 new applications from private sector organisations to use the DVS and 151 of these private sector applications have been approved.

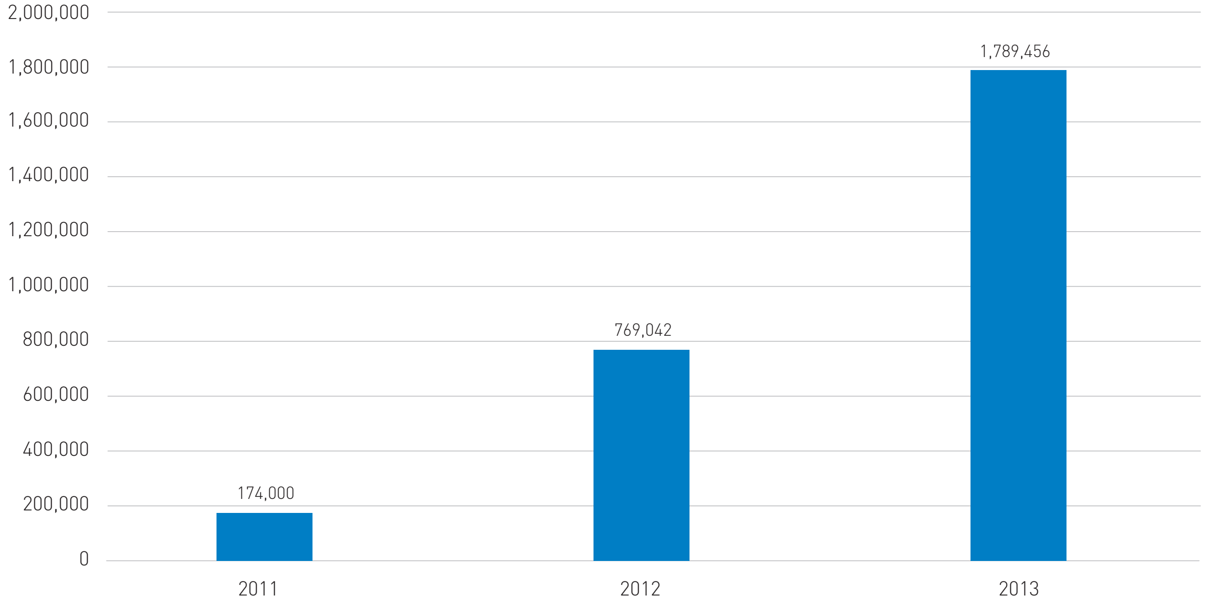
Although private sector access to the DVS has only been made available for a few months, the relatively large number of applications across various sectors demonstrates the utility of this service, as a cost effective means of strengthening identity verification processes.

5.4 Number of DVS transactions each year

Key findings: There has been rapid growth in the number of DVS verifications over recent years, albeit from a modest baseline, which is expected to continue into the future. This reflects growth in DVS user organisations and the range of documents that are able to be verified through the service.

In recent years the numbers of DVS transactions (i.e. validations of an identity credential) have steadily increased, from around 175,000 in 2011 to 1.8 million in 2013 (see Figure 31).

Figure 31: Number of DVS transactions, by year (2011–2013)



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

Source: Attorney-General's Department

5.5 Online security practices—individuals, business and government

Key findings: Most Australians adopt at least basic online security practices; and Australia's experience compares favourably in relative, international terms. However, surveys suggest that almost half of Australians are not confident in their ability to manage security of personal information online; only just over a third educate themselves about the most current ways to protect against identity theft; and there are areas where behaviours could be improved to help protect against identity crime.

A range of sources across government and the private sector produce data on Australians' online security practices. This provides a potentially rich source of information from which to develop indicators on the use of preventative measures for online identity crime. Unfortunately, this was not able to be completed in the time available for the pilot project. However, some general observations can be made. Further analysis of the available data is required in order to develop reliable indicators of the impact of the online security practices in preventing identity crime.

Individuals

Available data on Australians' online security practices presents somewhat of a mixed picture. Recent research by the Australian Communications and Media Authority (ACMA) indicates that just over half of Australian adults (54%) were confident in their ability to manage the security of their personal information online (ACMA 2013).

Australia was rated third out of 20 countries that were included in the latest global survey of online security practices by Microsoft. This survey of 10,000 people (including 530 Australians) measured individuals' behaviour in relation to a range of online security practices (Microsoft 2014).

While good in relative international terms, Australia received a score of 39 out of a possible 100 (Malaysia rated highest with a score of 42—the global average was 34). A significant majority (over 80%) of Australian respondents reported using at least some protections such as anti-virus software. But just over a third of respondents indicated that they limit the amount of personal information that appears online (36%), or educate themselves about the most current ways to protect against identity theft (37%) (Microsoft 2014).

The latest results from the 2013 Norton Report show that a considerable proportion of adults experienced cybercrime in the previous 12 months (46% or 5 million adult Australians), with almost two-thirds (60%) reporting having experienced cybercrime at some point in their lifetime (Norton 2013).

The survey also sought to examine the types of behaviours that may increase the likelihood of cybercrime victimisation (and potentially also identity theft), with results showing that:

- one third (32%) of smartphone users experienced mobile cybercrime in the past 12 months
- half (53%) of adults used public or unsecured Wi-Fi to share information
- when using public or unsecured Wi-Fi, around one quarter did shopping online or mobile banking (27% and 25% respectively) (Norton 2013).

Business

Some information is available on the online security practices of Australian businesses through the *2012 Cyber Crime and Security Survey: Systems of National Interest* (the Australian Cyber Crime and Security survey), conducted by Australia's national computer emergency response team (CERT Australia), located within AGD (see AGD 2014b).

This survey found that a significant majority (more than 80%) of businesses surveyed used anti-virus software, spam filters, firewalls and other access controls; with almost 60% also using more sophisticated measures such as intrusion detection systems (AGD 2012b).

The companies that took part in this survey were primarily the owners and operators of critical infrastructure (e.g. energy providers, defence industry, communications, banking/financial and water services) and other 'systems of national interest'. These businesses receive information and advice from CERT Australia on a regular basis. They would be expected to have a greater awareness of cyber security threats and a greater capacity to implement the necessary protective measures.

These results are unlikely to be representative of the online security practices of the broader private sector, including many of the small to medium sized businesses that handle many Australians' personal information. A comprehensive survey of the security practices of these types of business has not been conducted since the AIC's Australian Business Assessment of Computer User Security (ABACUS) survey in 2006–07 (Richards, 2009).

Government agencies

Information on the online security practices of government agencies is collected for various purposes.

In November 2013, the Victorian Auditor-General released an audit report into the Victorian Government's Information Security Management Framework (Victorian Auditor-General 2013). Overall, the report found that 'agencies are potentially exposed to cyber attacks, primarily because of inadequate ICT security controls and immature operational processes' (Victorian Auditor-General 2013). The audit also found that while the appropriate information security policy and framework is in place for the 20 agencies categorised as the 'inner Whole-of-Victorian-Government' (WoVG) arrangements, 'the remaining outer WoVG agencies—of which there are more than 500—are not required to conform to any specific policy or standard' (Victorian Auditor-General 2013) (For a discussion of some of the deficiencies in the Victorian Government's Cyber Security, see Cowan 2013).

At least 85 percent of the targeted cyber intrusions that the Australian Signals Directorate (formally known as the Defence Signals Directorate, or DSD) responds to could be prevented by following the top four mitigation strategies listed in its Strategies to Mitigate Targeted Cyber Intrusions (DSD 2012).

However, comprehensive information on cyber security practices and incidents is not as accessible as information on the practices of individuals and businesses, in part because of the potential sensitivity of this information. Developing measurement indicators for the online security practices of government agencies requires further analysis and may best be done as part of any related work to measure the nature and extent of cybercrime and other cyber security threats.

Estimating the economic impact of identity crime to Australia

Key finding: The total economic impact of identity crime in Australia could well exceed $1.6 billion annually.

Apart from the limitations in available data from government agencies and other public sources, it is possible to produce some estimates of the total economic impacts of identity crime to Australia.

Table 8 shows the estimated *direct losses* attributable to identity crime and misuse, over various 12 month periods and sectors, including businesses, government and individuals. Due to a lack of available data, it was not possible to calculate the economic impact of identity crime on state and territory government agencies.

The total of these *direct losses* is just over $1.5 billion. In light of the underreporting of identity crime, by both individuals and organisations, it is likely that these estimates are fairly conservative.

Table 8: Estimated direct losses to identity crime, by agency and year

Agency	Year	Unit of measurement	Loss to who	Total fraud cost	Average ID crime costs
PI[a]	2012	Data breach	Businesses	$131,760,000	$49,410,000
KPMG[b]	2012	Fraud incidents	Businesses	$865,480,000	$324,555,000
Cth fraud[c]	2009–10	Fraud incidents	Government	$495,534,658	$185,825,497
ABS	2010–11	Personal fraud incidents	Individuals	$2,400,000,000	$900,000,000
APCA	2012–13	Payment frauds	Financial institutions	$121,413,912	$45,530,217
Total				**$4,014,188,570**	**$1,505,320,714**

a: Ponemon Institute 2012

b: KPMG Survey of Fraud, Bribery & Corruption 2012

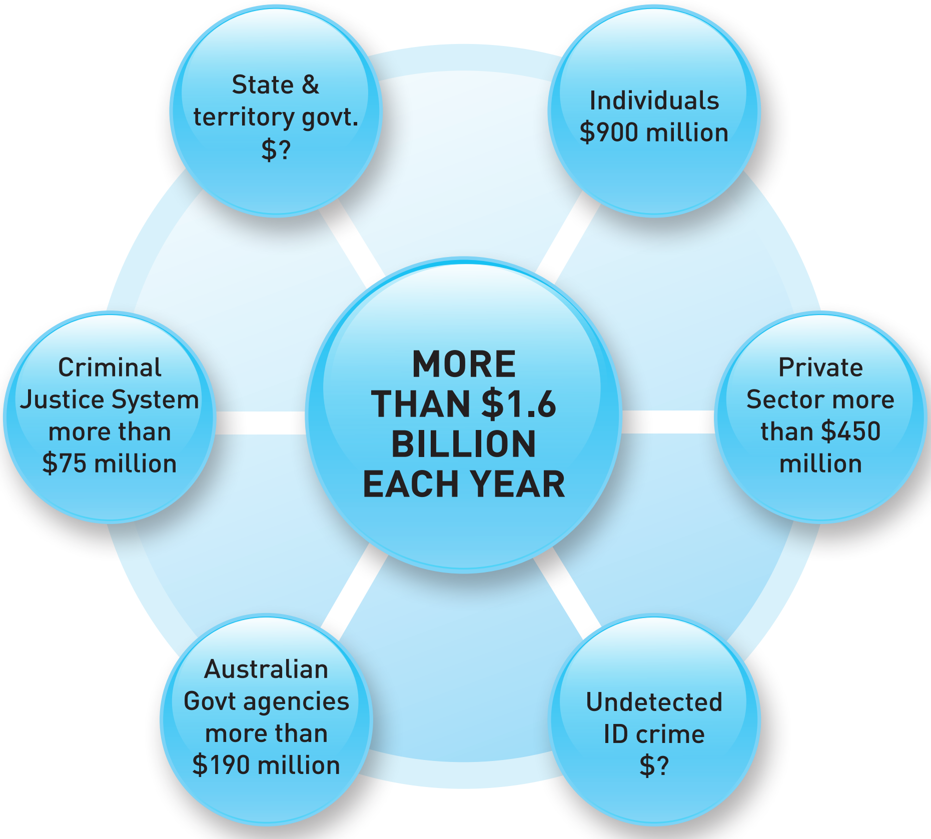
c: AIC Fraud against the Commonwealth 2009–10 annual report to government

Any attempt to calculate the direct losses attributable to identity crime will need to rely on a number of assumptions. The identity crime losses presented in Table 8 are based on the assumption that 37.5 percent of total fraud costs are identity crime. This percentage is the mid-point between two previous estimates of the proportion of all frauds that involve identity crime (i.e. 25% - AFP 2000; 50% - CIFAS 2012), noting that the percentage of fraud involving the misuse of personal information varies considerably across sectors, depending on the identity crime methodologies employed.

Direct losses to identity crime likely exceed $1.6 billion each year—$250m to government, $450m to business and $900m to individuals.

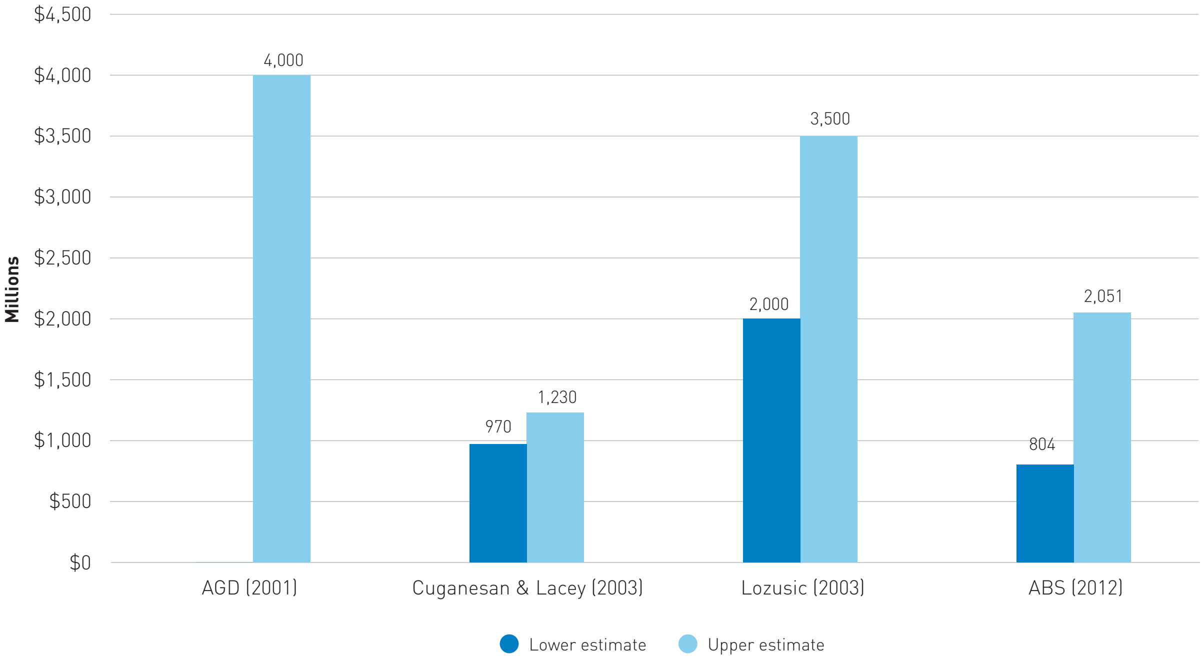
When combined with the estimated direct costs of investigating and prosecuting identity crimes calculated earlier (i.e. $75 million per annum), the total economic impact of identity crime in Australia could well exceed $1.6 billion annually (see Figure 32).

Figure 32: The economic impact of identity crime


State & territory govt. $?
Individuals $900 million
Criminal Justice System more than $75 million
MORE THAN $1.6 BILLION EACH YEAR
Private Sector more than $450 million
Australian Govt agencies more than $190 million
Undetected ID crime $?

This estimate is towards the conservative end of previous attempts to measure the total impact of identity crime in Australia, which have ranged between $800 million and $4 billion each year (see Figure 33).

Figure 33: Total estimated cost of identity crime, by source



The variations in these estimates are largely due to the definitional issues and differences in the methodologies used in calculating the final cost estimate.

In 2001, AGD published a report on the scope of identity crime, which estimated the total cost of identity-related fraud to the Australian economy at $4 billion (AGD 2001). This is around $5.5 billion in 2013 dollars and was based on the Reserve Bank of Australia inflation calculator with an annual inflation rate of 2.8 percent (RBA 2014).

The estimate calculated by Lozusic (2003) of total impacts of between $2.5–$3 billion (around $3.2–$4 billion in 2013 dollars) sought to account for the total direct losses to identity crimes, as well as the indirect costs (such as prevention and remediation) to business and government agencies.

The estimate by Cuganesan and Lacey (2003) of impacts of up to $1.2 billion ($1.57 billion in 2013 dollars) similarly took into account the direct losses to identity crimes, as well as the indirect costs associated with detection, investigation, prevention, recovery and restoration.

Finally, the ABS (2012) estimated the direct cost to individual victims of all personal fraud offences to be between $804 million and $2.05 billion. While these are frauds that are not limited to identity crime, and in this sense would be overestimates, they do not take into account losses experienced by organisations, and in this sense could be underestimates.

Conclusion

The importance of measuring identity crime

This report marks an initial attempt to develop a measurement framework for identity crime and misuse in Australia. Development of the report would not have been possible without the assistance of a broad range of government agencies across the Australian Government and the states and territories, in the form of information, analysis and encouragement throughout the preparation and conduct of the pilot data collection exercise.

The report makes some initial findings on the nature and extent of identity crime, based on collection and analysis of data by agencies conducted on a 'best endeavours' basis. The methodology and findings in the report provide a firm basis for further work and will benefit from being refined over time.

While it has an ambitious objective, the National Identity Crime and Misuse Measurement Framework project has demonstrated that development of such a framework is both feasible and necessary.

As one of the most prevalent types of crime in Australia, identity crime is a serious and increasing criminal risk to governments and the wider community (OECD 2006; 3). It generates significant profits for offenders and causes considerable financial losses to the Australian Government, private industry and individuals (AFP 2014).

But despite its widespread impacts, a lack of comprehensive data makes it difficult to quantify the full extent of identity crime, or to assess its costs and consequences for victims. As a result, identity crime is likely to be both underreported and its impacts underestimated.

The National Identity Crime and Misuse Measurement Framework project is an important step in improving the measurement of identity crime in Australia. From undertaking this pilot, it is evident that the greatest challenges to this effort are: the underreporting of incidents by victims (both individuals and organisations), and a lack of standardisation in definitions and recording practices.

Addressing these challenges will require concerted, sustained effort by a range of organisations. A companion report produced as part of this project offers recommendations for how this work might be taken forward. This is necessary if we are to properly quantify the impacts of identity crime and to develop the most effective policy and operational responses to minimise the harm that it causes to the Australian community.

Identity crime in depth: a case study

'Charles' was able to obtain a wide range of genuine Australian identity documents, issued with fraudulently obtained personal information. He used some of these documents himself and sold others to his criminal associates to help avoid detection for other serious criminal activity.

This is a real life case study. It shows how vulnerabilities in the processes supporting one type of identity credential can have flow-on effects to other agencies that form part of Australia's federated identity infrastructure; and which can be exploited by criminals to establish, use and sell fraudulent identities.

From the late 1990s to 2011, Charles searched through cemeteries in Queensland, New South Wales, Victoria and the Australian Capital Territory for the names and dates of birth of children who had died within a couple of months of being born. Using this identifying information, Charles then requested copies of the death certificates for these children.

Once he had obtained the details of the parents, Charles then manufactured *counterfeit* driver licences in their names, using photos taken from social media sites such as Facebook. With these two documents, he obtained the official birth certificates issued by the Registry of Births, Deaths and Marriages.

Charles then used the official birth certificates and *counterfeit* driver licences in the same name to open bank accounts and obtain credit cards. These bank accounts and credit cards, accompanied by the birth certificates, were then used to obtain genuine Medicare cards.

With these documents he was then able to obtain *genuine* driver licences issued in the same names.

Finally, Charles used these legitimately issued (but fraudulently obtained) identity kits to support applications for Australian passports. In total, he was able to obtain 10 genuinely issued Australian passports in various different names.

The identity kits were then sold to associates of Charles who were members of outlaw motorcycle gangs. The kits were sold for $9,000 without a passport and $30,000 with a passport.

Charles was also able to fraudulently obtain Australian Citizenship Certificates through an alternative method of 'tombstone fraud', using the names of children who had died during transit from the United Kingdom to Australia in post—World War II migration.

Charles' identity crimes went undetected for over nine years. Ultimately he was arrested by police for drug-related crimes and while in custody made admissions to the identity frauds. Charles was imprisoned for a total of 4 years 6 months, with a single non-parole period of 2 years 6 months.

References

2007 Intergovernmental agreement to a National Identity Security Strategy http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Inter%20Government%20Agreement%20to%20a%20National%20Identity%20Security%20Strategy%20[94.2KB%20PDF].pdf

Attorney-General's Department, (2014a), *Document Verification Service website*, Canberra: http://www.dvs.gov.au/Pages/default.aspx

Attorney-General's Department, (2014b), *Cyber Emergency Response Team (CERT) website*, Canberra: http://www.ag.gov.au/RightsAndProtections/CERT/Pages/default.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), *Cyber Crime & Security Survey Report 2012*, Canberra: http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%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, (2014a), *Crime Victimisation, Australia, 2012–13*, ABS Cat. No. 4530.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/D7B1A6CCDEF87612CA257B16000E06DE? opendocument

Australian Bureau of Statistics, (2014b), *Criminal Courts, Australia,* ABS Cat. No. 4513., Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/mf/4513.0

Australian Bureau of Statistics, (2013a), *Crime Victimisation, Australia, 2011–12*, ABS Cat. No. 4530.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/F716C0FC12B1517ECA257B16000E0DB3? opendocument

Australian Bureau of Statistics, (2013b), *Migration, Australia, 2011–12 and 2012–13*, ABS Cat. No. 3412.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/3412.0Chapter32011–12%20and%202012–13

Australian Bureau of Statistics, (2013c), *Births, Australia, 2012*, ABS Cat. No. 3301.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/mf/3301.0

Australian Bureau of Statistics, (2013d), *Deaths, Australia, 2012*, ABS Cat. No. 3302.0, Canberra: http://www.abs.gov.au/ausstats/abs@.nsf/mf/3302.0

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

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

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

Australasian Centre for Policing Research (ACPR), (2006), *Standardisation of definitions of identity crime terms: A step towards consistency*, Report Series No. 145.3, South Australia: http://www.anzpaa.org.au/anzpire/acpr-publications

Australian Communications and Media Authority (ACMA), (2013), *Digital footprints and identities: Community attitudinal research*, Melbourne: http://www.acma.gov.au/~/media/Regulatory%20Frameworks/pdf/Digital%20footprints%20and%20identities%20community%20attitudinal%20research%20pdf.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 Federal Police (AFP), (2014), *Identity Crime*, AFP website: http://www.afp.gov.au/policing/fraud/identity-crime

Australian National Audit Office (ANAO), (2012), *Management of e-passports*, Audit Report No. 33—2011–12, Canberra. http://www.anao.gov.au/~/media/Uploads/Audit%20Reports/2011%2012/201112%20Audit%20Report%20No33.pdf

Australian Payments Clearing Association (APCA), (2006-2013), *Payment Statistics—Fraud Statistics*, Sydney: http://www.apca.com.au/payment-statistics/fraud-statistics/archive-releases

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

Commonwealth Ombudsman, (2010), *Australian Taxation Office: Resolving Tax File Number Compromise*, Report 12/2010, Canberra. http://www.ombudsman.gov.au/files/ATO_resolving-TFNcompromise.pdf

Council of Australian Governments (COAG), (2012), *National Identity Security Strategy*, http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/NationalIdentitySecurityStrategy.aspx

Cowan, P., (2013), Big holes discovered in Vic Govt's cyber security, itNews: http://www.itnews.com.au/News/365679,big-holes-discovered-in-vic-govts-cyber-security.aspx#ixzz35XVturKj

Credit Industry Fraud Avoidance Service (CIFAS), (2013), *Is identity fraud serious?*, United Kingdom, http://www.cifas.org.uk/is_identity_fraud_serious

Criminal Code Act 1995 (Cth), http://www.austlii.edu.au/au/legis/cth/consol_act/cca1995115/sch1.html

Cuganesan, S and Lacey, D, (2003), *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, Sydney: SIRCA.

Department of Human Services, (2008-2013), *Annual Reports*, Canberra: http://www.humanservices.gov.au/corporate/publications-and-resources/annual-report/

Defence Signals Directorate (DSD), (2012), *Top four mitigation strategies to protect your ICT system*, Canberra: http://www.asd.gov.au/publications/csocprotect/Top_4_Mitigations.pdf?&verNov12

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/index.cfm?ty=pbdetail&iid=4821

House of Representatives Standing Committee on Economics, Finance and Public Administration, (2000), *Numbers on the Run: Review of the ANAO Report No.37 1998-99 on the Management of Tax File Numbers*, Transcripts of public hearings: 05/04/2000, EFPA 164. http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=efpa/tfnaudit/report.htm

Identity Theft Resource Centre, (2010), *Identity Theft: The Aftermath 2009*, California: http://www.idtheftcenter.org/ITRC-Surveys-Studies/aftermathstudies.html

Javelin Strategy & Research, (2013), *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters*, https://www.javelinstrategy.com/brochure/276

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

Lacey, D, (2013), *Identity Theft and Misuse in Australian and New Zealand: iDcare Report on Establishing a Trans-Tasman Identity Theft Victim Support Centre*, Gold Coast. http://www.idcare.org/idcare-aus-nz

Lawson, P, (2011), *Responding to Victims of Identity Crime: A Manual for Law Enforcement Agents, Prosecutors and Policy-Makers*, International Centre for Criminal Law Reform and Criminal Justice Policy, Canada: http://icclr.law.ubc.ca/sites/icclr.law.ubc.ca/files/publications/pdfs/00%20Victims%20of%20Identity%20Crime%20Manual.pdf

Lindley, J, Jorna, P. & Smith, R.G., (2012), *Fraud against the Commonwealth 2010–11 annual report to government*. Australian Institute of Criminology, Monitoring Reports: Canberra http://www.aic.gov.au/publications/current%20series/mr/1-20/18.html

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/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146/$ File/08-03.pdf

Ludington, S, (2006), *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, Maryland Law Review, Vol. 66, pp. 140-193. http://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=5&ved=0CEMQFjAE&url=http%3A%2F%2Fscholarship.law.duke.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D5492%26context%3 Dfaculty_scholarship&ei=qhDwUq6nGca6lQXM1IC4Bg&usg=AFQjCNEAtBThhSLLS-pl_-bjpe1oBEz_IQ

Microsoft, (2014), *2013 Microsoft Computing Safety Index*: http://www.microsoft.com/security/resources/mcsi.aspx

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

New South Wales Registry of Births, Deaths & Marriages (NSW RBDM) (2013), *Statistics from 1996 to 2012: Births*, Department of Attorney-General & Justice, Sydney: http://www.bdm.nsw.gov.au/resources/statsinfo.pdf

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

Office of the Australian Information Commissioner, (2013a), *OAIC Annual Report—2012–13*, Canberra: http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201213/

Office of the Australian Information Commissioner, (2013b), *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, (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, (2012b), *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, (2011a), *OAIC Annual Report—2010–11*, Canberra: http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201011/

Office of the Australian Information Commissioner, (2011b), *Vodafone Hutchison Australia: Own motion investigation report*, Canberra. http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-omi-reports/vodafone-hutchison-australia

Organisation for Economic Co-Operation and Development (OECD), (2006), *Report on Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities*, http://www.oecd.org/ctp/crime/identity-fraud-tax-evasion-and-money-laundering-vulnerabilities.htm

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

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

Prenzler, T, (2012), *Responding to welfare fraud: The Australian experience*, Research & Public Policy Series 119, Australian Institute of Criminology: Canberra. http://www.aic.gov.au/media_library/publications/rpp/119/rpp119.pdf

Reserve Bank of Australia (RBA), (2014), *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

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.

Smith, R, Jorna, P, Sweeny, J & Fuller, G, (forthcoming), *Counting the costs of crime in Australia—2011 update*, Research and Public Policy Series, Australian Institute of Criminology: Canberra.

Sproule, S and Archer, N, (2008), *Measuring Identity Theft in Canada: 2008 Consumer Survey*, MeRC Working Paper No.23, McMaster University. http://merc.mcmaster.ca/working-papers/23.html

Van Vliet, J, (2010), Stolen Identities: *A Qualitative Study on the Psychological Impact of Identity Theft*, University of Alberta: http://news.ualberta.ca/newsarticles/2011/04/uofaresearcherfindsthepsychologicaleffectsofidentitytheftlingerswithvictims

Unisys, (2013), *Australia Unisys Security Index—May 2013*, http://www.unisyssecurityindex.com/usi/australia/reports

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

Case Studies:

Case Study 1: Australian Transaction Reports and Analysis Centre (AUSTRAC), (2012), *AUSTRAC typologies and case studies report*, Pg. 45. http://www.austrac.gov.au/files/typ_rprt12_full.pdf

Case Study 2: Levy, M, (2012), *Truckies face retest amid licence fraud probe*, The Age, published 21 September. http://www.theage.com.au/victoria/truckies-face-retest-amid-licence-fraud-probe-20120921-26acr.html

Case Study 3: Grubb, B, (2013), *Oops: Google search reveals private Telstra customer data*, Sydney Morning Herald, published 16 May. http://www.smh.com.au/it-pro/security-it/oops-google-search-reveals-private-telstra-customer-data-20130516-2jnmw.html

Office of the Australian Information Commissioner, *Telstra breaches privacy of 15,775 customers*, Media release published 11 March 2014. http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-of-15-775-customers

Case Study 4: Commonwealth Director of Public Prosecutions, *2009–10 Annual Report.* Available at: http://www.cdpp.gov.au/case-reports/george-hebaiter/

Case Study 5: Australian Taxation Office, (2011), *Targeting tax crime: A whole-of-government approach*. Available at: http://www.ato.gov.au/General/Tax-evasion-and-crime/In-detail/Targeting-Tax-Crime-magazine/2011/Targeting-tax-crime--A-whole-of-government-approach---February-2011/?page=8

Case Study 6: Harris, A, (2012), *VicRoads goes hi-tech to end driving licence fraud*, The Australian, published 29 October. http://www.theaustralian.com.au/news/vicroads-goes-hi-tech-to-end-driving-licence-fraud/story-e6frg6n6-1226504896204#

Case Study 7: Styles, A, (2010), *Property scam highlights need for greater security: REIWA*, WA Today, published 13 September. http://www.watoday.com.au/wa-news/property-scam-highlights-need-for-greater-security-reiwa-20100913-15952.html

Case Study 8: Commonwealth Director of Public Prosecutions. 2010. *2009–10 Annual Report*. Available at: http://www.cdpp.gov.au/case-reports/marita-quetcher/

Case Study 9: ABC News, (2005), *Nurse jailed for massive Centrelink fraud*, published 16 December. http://www.abc.net.au/news/2005-12-16/nurse-jailed-for-massive-centrelink-fraud/763254

Case Study 10: ABC News, (2011), *Police strike $30m fake credit card syndicate*, published 20 October. http://www.abc.net.au/news/2011-10-19/police-strike-30m-fake-credit-card-syndicate/3579592

Case Study 11: Sigsworth, M, (2008), *'I was falsely branded a paedophile'*, BBC UK, published 3 April. http://news.bbc.co.uk/2/hi/uk_news/magazine/7326736.stm

Appendix A—Summary of key findings

1. Acquisition of fraudulent identities

Indicator 1.1—Key finding: Medicare cards and driver licences—and to a lesser extent birth certificates—are more likely than other credentials to be used to facilitate identity crime. This is due to a range of factors including Australians' ubiquitous use of these cards as evidence of identity and the security features of the credentials. This emphasises the importance of verifying the information presented on these credentials with the issuing agency.

Indicator 1.2—There is limited reliable data on the true extent of data breaches in Australia. Nevertheless, data breaches, whether accidental or deliberate, will continue to present significant opportunities for obtaining personal identifiable information that is used in identity crime.

2. Use of fraudulent identities

Indicator 2.1—Identity crime incidents are detected by a range of government agencies across a wide variety of fraud types including: welfare, passport, immigration, conveyancing, taxation and other financial frauds.

Indicator 2.2—There are an estimated 24,000 prosecutions for identity-related crimes each year in Australia, although prosecution statistics only ever measure a relatively small sub-set of the total incidents of criminal activity.

Rather than specific identity crime offences, most identity criminals are prosecuted for the crimes that are enabled by use of a false or stolen identity, such as fraud (i.e. obtaining benefit by deception). This may be because these offences attract higher penalties or are more appropriate to the overall circumstances of the conduct.

Indicator 2.3—Key findings: The number of people who experience identity crime or misuse each year appears to be rising. The proportion of Australians who report being a victim of identity crime is significantly higher than other personal and theft-related offences.

Identity crime is significantly underreported by both individual victims and organisations. Recent research indicates that half of credit card fraud victims and a third of identity theft victims did not report the incident to a formal institution, such as law enforcement or a financial organisation.

Indicator 2.4—Identity crime continues to be of serious concern to a large number of Australians, with around two-thirds of survey respondents expressing concern about becoming a victim of identity crime in the next 12 months.

Indicator 2.5—The types of information most susceptible to identity theft include financial information (credit card numbers and bank account details) and other biographic information (name, date of birth). Passwords were also identified as vulnerable in around one in five cases of identity crime and misuse. Organisations that use this information to transact with their clients need to take adequate precautions to ensure that it remains protected.

3. Consequences of identity crime

Indicator 3.1—The total direct losses and associated costs of identity crime to government agencies are difficult to estimate, but they are likely in the order of several hundred million dollars each year. Where an agency invests additional effort and resources in detecting and investigating this activity, the amount of incidents detected is likely to increase considerably.

Indicator 3.2—Identity crime costs businesses at least $140 million each year. While the number of incidents has fluctuated, the financial impact of identity crime is consistently on the rise. This underscores the need for the private sector to play an active role in detecting and preventing identity crime.

Indicator 3.3—The majority of identity victims lose relatively small amounts of money of 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 to their mental or physical health, reputations or general wellbeing.

Indicator 3.4—In addition to financial losses, many victims of identity crime experience other mental and physical health impacts. The stress and frustration of trying to regain control of one's identity information and financial reputation can also damage family and social relationships.

4. Remediation of identity crime

Indicator 4.1—The average amount of time victims spend recovering from identity theft ranges from 10 to 18 hours. A small but significant number of victims, around one in 20, spend over 200 hours recovering their identity. These more complex cases can involve identities that are stolen and used to commit other serious criminal offences. The damage caused to the victim's reputation can often take years to repair.

Indicator 4.2—The proportion of identity crime victims who report their experience to government agencies is relatively small (around 1 in 5). The reasons for this may be that victims are unaware of the reporting processes available to them, or that they do not consider there is value in reporting the crime to these agencies.

Indicator 4.3—There is a lack of community awareness of the potential assistance that victims' certificates can provide to victims of identity crime. Only around one in seven victims were aware of the existence of these certificates and fewer than one in 30 victims actually applied for one, although no Commonwealth certificates have been issued in the last three years.

5. Prevention of identity crime

Indicator 5.1—There are an increasing number of identity credentials that can be verified through the DVS, including four of the five credentials that have been identified through this project as being at most risk of misuse (i.e. Medicare cards, driver licences, birth certificates and passports).

Indicator 5.2—An increasing number of government agencies are using the DVS across Australia, although coverage amongst key government credential issuing agencies is not yet universal, with only a quarter of RTAs and RBDMs currently using or planning to use the DVS by the end of 2014.

Indicator 5.3—There is strong demand for use of the DVS amongst private sector organisations, particularly those with legislative obligations to verify the identities of their customers. There is scope for significant further growth in the number of user organisations which have a reasonable necessity to verify a person's identity in accordance with the *Privacy Act 1988*.

Indicator 5.4—There has been rapid growth in the number of DVS verifications over recent years, albeit from a modest baseline, which is expected to continue into the future. This reflects growth in DVS user organisations and the range of documents that are able to be verified through the service.

Indicator 5.5—Most Australians adopt at least basic online security practices; and Australia's experience compares favourably in relative, international terms. However, surveys suggest that almost half of Australians are not confident in their ability to manage security of personal information online; only just over a third educate themselves about the most current ways to protect against identity theft; there are areas where behaviours could be improved to help protect against identity crime.

Appendix B—Measurement framework pilot indicators

Table B1—Pilot project 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: • 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 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)

Indicators	Description	Data source
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
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.	Academic literature

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) ACMA Microsoft

Appendix C—Government agencies involved in pilot

Table C1—Australian Government agencies involved in the Measurement Framework pilot project

Australian Government agency
AusTrac
Australia Competition and Consumer Commission
Australia Federal Police
Australia Post
Australian Communications and Media Authority
Australian Crime Commission
Australian Customs and Border Protection Service
Australian Electoral Commission
Australian Institute of Criminology
Australian Securities and Investments Commission
Australian Security Intelligence Organisation
Australian Taxation Office
Commonwealth Director of Public Prosecutions
CrimTrac
Department of Broadband, Communications and the Digital Economy
Department of Defence
Department of Families, Housing, Community Services, Indigenous Affairs—Social Services
Department of Foreign Affairs and Trade—Australian Passport Office
Department of Human Services—Centrelink
Department of Human Services—Medicare
Department of Immigration and Citizenship
Department of Industry, Innovation, Science, Research and Tertiary Education
Department of Infrastructure and Transport
Department of Veterans' Affairs
Office of the Australian Information Commissioner

Table C2—State/territory government agencies involved in the Measurement Framework pilot project

State/territory government agency	
NSW	New South Wales Police Force
	Register of Births, Deaths and Marriages
	Department of Transport
	Department of Roads and Maritime Service
	Department of Fair Trading
VIC	Victoria Police Service
	Register of Births, Deaths and Marriages
	Roads Corporation Victoria—VicRoads
	Consumer Affairs Victoria
QLD	Queensland Police Service
	Register of Births, Deaths and Marriages
	Department of Justice and Attorney-General
	Department of Transport and Main Roads
SA	South Australia Police
	Register of Births, Deaths and Marriages
	Consumer and Business Services
	Department of Planning, Transport and Infrastructure
WA	Western Australia Police
	Register of Births, Deaths and Marriages
	Department of Consumer Affairs
	Department of Transport
TAS	Tasmania Police
	Register of Births, Deaths and Marriages
	Department of Premier and Cabinet—Proof of Age Cards
	Department of Infrastructure, Energy and Resources
	Department of Consumer Affairs and Fair Trading—DoJ
ACT	Australian Capital Territory Policing
	Register of Births, Deaths and Marriages
	Department of Transport
	Office of Regulatory Services

Appendix D—Definition of key terms

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 direct losses caused by identity crime

Table E1: Estimated direct losses attributed to identity crimes and misuse, by agency and value ($)

Agency	Year	Unit	Estimated Unit Cost	Multiplier	Total Fraud Cost	25% ID Crime	50% ID Crime	Average ID Crime Costs
PI[a]	2012	Data Breach	$2,160,000	61 breaches	$131,760,000	$32,940,000	$65,880,000	$49,410,000
KPMG[b]	2012	Aust & NZ Organisations	$3,080,000	281 organisations	$865,480,000	$216,370,000	$432,740,000	$324,555,000
Cth Fraud[c]	2009–10	Cth Agencies	$9,716,366	51 agencies	$495,534,666	$123,883,667	$247,767,333	$185,825,500
ABS	2010–11	Individuals	$2,000	1,200,000 people	$2,400,000,000	$600,000,000	$1,200,000,000	$900,000,000
APCA	2012–13	Payment Fraud	$197	614,960 transactions	$121,147,120	$30,286,780	$60,573,560	$45,430,170
Total					**$4,013,921,786**	**$1,003,480,447**	**$2,006,960,893**	**$1,505,220,670**

a: Ponemon Institute 2012

b: KPMG Survey of Fraud, Bribery & Corruption 2012: http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Documents/fraud-bribery-corruption-survey-2012-fraud-facts.pdf

c: AIC Fraud against the Commonwealth 2009–10 annual report to government: http://www.aic.gov.au/publications/current%20series/mr/1-20/18/04_exec_summ.html

Table E2: Estimated direct costs of investigating and prosecuting identity crimes, by agency and value

Agency	Year	Unit	Estimated Unit Cost	Multiplier	Total Fraud Cost	25% ID Crime	50% ID Crime	Average ID Crime Costs
AFP[a]	2010–11	Fraud investigation	$209,774	61 cases	$12,796,214	$3,199,054	$6,398,107	$4,798,580
CDPP	2012–13	Defendant prosecuted	$22,198	1554 defendants	$34,495,692	$8,623,923	$17,247,846	$12,935,885
State courts	2011–12	ID crimes proven guilty	$3,000	22,000 offences	$66,000,000	$16,500,000	$33,000,000	$24,750,000
State police	2012–13	Detected ID crime	$3,000	30,000 offences	$90,000,000	$22,500,000	$45,000,000	$33,750,000
Total					**$203,291,906**	**$50,822,977**	**$101,645,953**	**$76,234,465**

a: Jorna & Smith 2013.

IDENTITY SECURITY