

FINAL REPORT

IDENTITY CRIME

Model Criminal Law Officers' Committee of the
Standing Committee of Attorneys-General

March 2008

This Report was prepared by the Model Criminal Law Officers' Committee. It does not necessarily represent the views of the Standing Committee of Attorneys-General or an individual Attorney-General.

© Commonwealth of Australia 2008

ISBN: 1 921241 37 3

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600, or posted at <http://www.ag.gov.au/cca>.

COMMITTEE MEMBERS AND ADVISERS

Chair

South Australia: Mr Matthew Goode
Managing Solicitor
Legislation and Legal Policy Section
Attorney General's Department

Members

New South Wales: Ms Penny Musgrave
Director
Criminal Law Review Division
Attorney General's Department

Victoria: Mr Greg Byrne
Director
Criminal Law—Justice
Department of Justice

Western Australia: Mr George Tannin SC
State Counsel for Western Australia
State Solicitor's Office
Department of the Attorney General

Tasmania: Mr Nick Perks
Principal Crown Counsel
Office of the Director of Public Prosecutions

Northern Territory: Ms Fiona Hardy
Senior Law Officer
Legal Policy Division
Department of Justice

Australian Capital Territory: Ms Nicole Mayo
Principal Legal Officer
Criminal Law Group
Legislation and Policy Branch
Department of Justice and Community Safety

Australian Government: Dr Karl Alderson
Assistant Secretary
Criminal Law Branch
Attorney-General's Department

MCLOC Participant

Queensland:

Ms Virginia Sturgess
Assistant Director
Strategic Policy
Department of Justice and Attorney-General

Advisers

Dr Susan Cochrane
Principal Legal Officer
Criminal Law Branch
Attorney-General's Department

Ms Lauren Thomas
Legal Officer
Criminal Law Branch
Attorney-General's Department

Ms Louise Cairns
Senior Legal Officer
Criminal Law Branch
Attorney-General's Department

Contents

1	Introduction	1
	(a) <i>Background of the Model Criminal Code Officers' Committee—now known as Model Criminal Law Officers' Committee</i>	1
	(b) <i>Reference from Standing Committee of Attorneys-General to examine model offences on identity crime</i>	1
	(c) <i>Public consultation—Discussion Paper released in April 2007</i>	1
2	What is identity crime?	3
2.1	Identity and identification	3
2.2	False identity	3
2.3	Fictitious identity	4
2.4	Impact of identity crime	4
2.5	How does identity crime occur?	5
2.6	Definitions	7
3	Extent and cost of identity crime	9
4	Overseas responses to identity crime	11
4.1	United States of America	11
4.2	United Kingdom	12
4.3	Canada	12
4.4	Europe	12
4.5	South Korea	13
5	Existing legislative framework in Australia	14
5.1	Model Criminal Code offences	14
5.2	Model credit card skimming offence	16
5.3	Specific identity crime offences—South Australia and Queensland	17
5.4	Other possibly applicable offences	18
5.5	Less serious possibly applicable offences	23
6	Recommended model identity crime offences	25
6.1	Definitions	28
6.2	Dealing in identification information	30
6.3	Possession of identification information	36
6.4	Possession of equipment capable of making identification documentation	38
6.5	Certificate may be issued by Local Court in relation to victim of identity crime	42
7	On-selling identification information	45
Appendix A	Submissions received on the Identity Crime Discussion Paper	46

1 Introduction

(a) *Background of the Model Criminal Code Officers' Committee—now known as Model Criminal Law Officers' Committee*

On 28 June 1990, the Standing Committee of Attorneys-General (SCAG) placed on its agenda the question of the development of a national Model Criminal Code for Australian jurisdictions. To advance the concept, SCAG established a Committee consisting of an officer from each Australian jurisdiction with expertise in criminal law and criminal justice matters. Originally known as the Criminal Law Officers' Committee, the name was changed in November 1993 to the Model Criminal Code Officers' Committee (MCCOC). MCCOC released a large number of Discussion Papers and Reports on criminal law topics.¹

In July 2006, SCAG decided to rename the Committee the Model Criminal Law Officers' Committee to reflect its broader role of advising on criminal law issues that have been referred to it by SCAG and the fact that development of the Model Criminal Code is largely complete.

(b) *Reference from Standing Committee of Attorneys-General to examine model offences on identity crime*

The issue of identity crime has received considerable media and public attention in recent years. It is of major concern to government agencies, law enforcement bodies, private organisations, the financial sector and individuals. It is also an issue of international significance. Identity crime can be a central element in transnational crime.

Responding to identity crime was identified as a priority matter in the Commonwealth and States and Territories Agreement on Terrorism and Multi-Jurisdictional Crime, dated 5 April 2002.

In July 2004, the Committee sought SCAG's direction on whether model identity theft offences should be prepared. Ministers agreed that MCLOC should examine the issue of identity theft.

(c) *Public consultation—Discussion Paper released in April 2007*

On 20 April 2007, MCLOC released a discussion paper on identity crime for public consultation. The Discussion Paper was available at the Attorney-General's Department website <www.ag.gov.au>, the then Commonwealth Minister issued a press release, and the secretariat wrote to range of stakeholders, requesting their comment. Submissions were due on 12 June 2007.

¹MCCOC and MCLOC Discussion Papers and Reports can be found at the Australian Government Attorney-General's Department website at:
<http://www.ag.gov.au/www/agd/agd.nsf/Page/Model_criminal_code>.

Twenty-six submissions were made in response to the Discussion Paper. Submissions were received from a variety of organisations, including State Police forces, government agencies and associations. A list of those who provided submissions is at Appendix A. Submissions were generally supportive of establishing the proposed offences, but suggested amendments. The Committee adopted some of these suggestions in the model offences.

Parts 2 to 5 of this Final Report discuss the nature, extent and cost of identity crime, overseas responses to identity crime and the current legislative framework in Australia.

In Part 6, the Committee proposes its preferred model identity crime offences and analyses the suggestions made in the submissions. Part 7 discusses why the Committee no longer recommends the creation of an offence of on-selling identification information, as it did in the Discussion Paper.

2 What is identity crime?

2.1 Identity and identification

The possession of an identity is inseparable from an individual's sense of self and individuality.² Identity can be defined by how your identity is established; for example, by such identifiers as:

- physical or biometric identifiers—eg photographs, iris scans, fingerprints and voice prints
- written identifiers—eg drivers' licences and passports, and
- financial identifiers—including bank account, credit card and employment information.

The notion of identity is central to almost all aspects of life. At a general level, the recognition and differentiation of individuals and organisations is based on some form of identification.³ The United Kingdom Cabinet Office in a 2002 report⁴ discussed the terms 'attributed identity' and 'biographical identity'. 'Attributed identity' relates to those elements that are applied as a result of birth, such as birth name, date of birth, and parents' details. Biographical elements commence after birth. They include information about the person's interaction with society, from documents such as:

- electoral registers
- marital certificates
- educational or technical qualifications, and
- employment history.

2.2 False identity

Identity crime often involves the use of a false identity. False identities can relate to either natural persons (living or deceased) or to corporate entities, and can be established in the following ways:⁵

- the creation of a fictitious identity (identity fabrication)
- the alteration of one's own identity (identity manipulation), by changing one or more elements of identity—eg name, date of birth, address, or
- the theft or assumption of a pre-existing identity (identity theft), which may also involve subsequent manipulation.

² Cuganesan, S and Lacey, D, *Identity fraud in Australia: An evaluation of its nature, cost and extent*, Securities Industry Research Centre of Asia-Pacific, Sydney, 2003 ('SIRCA report'), p 1.

³ SIRCA report, p 1.

⁴ United Kingdom Cabinet Office, *Identity Fraud: A Study*, Economic and Domestic Secretariat, London; <http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf>.

⁵ ACPR, *Standardisation of definitions of identity crime terms: A step towards consistency*, Report Series No 145.3, March 2006, p 7.

2.3 Fictitious identity

When someone creates a false identity that is not based on a real person, that person has created a fictitious identity. It is also possible for someone to adapt their own identity to allow them to commit frauds. The UK Cabinet Office gives an example of a man who created 25 false names by using a combination of his own name and his mother's and wife's maiden names to commit tax fraud.⁶

Fraud rings that use fictitious identities often reuse and rearrange the same names over and over. A report by the USA firm ID Analytics refers to a case where a fraud ring committed identity fraud over two years using the same first names 'Jeremy' and 'Kendrick', and last names 'Watson' and 'Armstrong'.⁷

It has been estimated that over 88% of all identity fraud in the USA involves fictitious identities.⁸

2.4 Impact of identity crime

Identity crime can have a number of impacts.

(a) Financial impacts

Identity crime can have a *direct* financial impact. For individuals, this may include the loss of savings. For business organisations, the direct financial impacts can include the cost of reporting and investigating identity crime cases, the cost of preventing the continued use of the identity, and the cost of restoring the business or organisation's reputation.

There may also be *indirect* financial impacts, in the form of damage to a person's credit rating, the creation of a criminal record in the person's name, and the efforts spent restoring records of transactions or credit history. For example, a victim may not become aware that identity crime has occurred until he or she is called upon by defrauded creditors to make good on defaulted loan payments. It has been claimed that individual victims of identity crime spend an average of two or more years attempting to fix their credit report and restore their credit rating.⁹

For a business or organisation, the indirect financial damage can be to its reputation or the opportunity cost resulting from forgoing benefit-generating activities to counter identity crime.¹⁰

On the other hand, for the perpetrators of identity crime, international statistics point to the risk–reward trade-off being significantly more favourable when compared to other kinds of crime.¹¹

⁶ United Kingdom Cabinet Office, *Identity Fraud: A Study*, Economic and Domestic Secretariat, London; <http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf>.

⁷ ID Analytics, *Creation of a fictitious identity or manipulation of one's own identity*, <<http://www.business.mcmaster.ca/IDTDefinition/defining/fictitious.htm>>.

⁸ ID Analytics, *US National Fraud Ring Analysis*, <<http://www.idanalytics.com/whitepapers/index.html>>.

⁹ Hatch M, 'The Privatisation of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century', *William Mitchell Law Review*, vol 27 no 3, 2001, pp1457–1502.

¹⁰ SIRCA report, p 43.

¹¹ SIRCA report.

(b) Psychological impacts

Identity crime can invade a person's privacy and sense of individuality. It can create trauma, stress and reduced participation in society for individual victims;¹² for example, the suffering caused to a family following the theft of the identity of a stillborn child, or the impact of the use of one family member's identity by another family member.

(c) Other intangible impacts

Identity crime may facilitate access to citizenship and/or social services such as medical services. It may also enable an offender to acquire a professional affiliation or qualification.

(d) National security impacts

It is not only individuals who commit identity crime-related offences. It has been recognised that organised crime groups are becoming increasingly involved in identity crime; for example, to facilitate the smuggling or trafficking of people. The 9/11 hijackers used fictitious social security numbers, false identities and fraudulent identification documents. A report issued by the French Senate in 2005 indicates that terrorist networks have systematically used false identity documents to obtain employment overseas, finance activities and avoid detection.¹³

2.5 How does identity crime occur?

The use of false identities by criminal offenders is not a recent phenomenon. The earliest English Act on forgery was passed in 1870 to deal with fake stock certificates.¹⁴

The United Nations recently released a report dealing with identity crime, which noted that unlike fraud, which is often the primary focus of offenders, identity-related crimes appear to be most commonly found as a constituent element of larger criminal offences or operations.¹⁵ Identity crime may encompass conduct from the illegal use of a person's credit card details to make purchases over the internet or telephone, through to the assumption by one person of another person's entire identity to open bank accounts, take out loans, and conduct other business illegally in that name. It may or may not involve financial fraud, and it can be used to cover up or enable various forms of criminal activity.

(a) Online techniques—general

Identity-related criminal activity is constantly evolving as new ways to gain access to or manipulate identity data are found.

A prevalent online method of obtaining personal details is phishing. Phishing email attacks are commonly perpetrated through the creation of fake emails purporting to be from trusted organisations such as banks. Typically, e-mails pretending to be from a bank are sent to individuals, directing the receiver to a fake website designed to look like the bank's

¹² Walker, J, 'Estimates of the Costs of Crime in Australia in 1996', in *Trends & Issues in Crime and Criminal Justice*, Australian Institute of Criminology, Canberra.

¹³ Paget, F, *Identity Theft White Paper*, <www.mcafee.com>, January 2007.

¹⁴ SIRCA report, p 8.

¹⁵ United Nations Economic and Social Council, *International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes*, <http://www.unodc.org/pdf/crime/15_commission/study-on-fraud-and-the-criminal-misuse-and-falsification-of-identity-first-draft.pdf>, 2007.

actual website. The person is asked to verify their personal log on details. When the victim enters his or her details, these are captured and subsequently used to withdraw funds from the account.

Other online techniques for procuring personal identifying information include:

- using a key logging device on computers, and
- stealing personal information in computer databases, and infiltration of organisations that store large amounts of personal information, such as government organisations and financial institutions.

(b) Online social interaction

Online social interaction, particularly social networking, is growing in popularity. However, some users of social networking websites engage in behaviour that puts them at risk of identity theft.

Online social interaction is essentially the use of the internet to meet others. For example:

- chat rooms
- social networking sites
- instant messaging
- virtual worlds, and
- web logs.

Research conducted by the National Cyber Security Alliance revealed that 74 per cent of social networking users divulge personal information, such as their e-mail address, name and birthday. Some users download unknown files, for example, respond to unsolicited emails or instant messages.

Placing personal information on online social interaction sites can provide enough information for perpetrators to steal an individual's identity and open accounts in the individual's name.

(c) Consumer scams

There are increasing reports of high volume scams or frauds involving low or no value, purporting to offer lottery, job or other opportunities.¹⁶

Consumer scams are crimes of dishonesty such as forgery, counterfeiting, online deception, and theft that are targeted at people who seek to purchase goods and services.

¹⁶ Russell Smith, *Trends and issues in crime and criminal justice*, No 331, Australian Institute of Criminology, February 2007; press release issued by Australian Government Minister for Justice and Customs on 4 March 2007.

<[http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/Page/Media_Releases_2007_1st_Quarter_2_March_2007_-_Scams_take_\\$1_billion-plus_toll_on_consumers](http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/Page/Media_Releases_2007_1st_Quarter_2_March_2007_-_Scams_take_$1_billion-plus_toll_on_consumers)>.

Potential victims can be those who use fixed line or mobile phones, computers and the internet, older people, and those who use professional advisers.¹⁷

These consumer scams may be used by crime groups to gather personal identification information which is then on-sold to other crime groups. However, supplying information may also involve the legitimate use of personal identification information. The original person or group of people may have no criminal intent, but sells the information on to a group which does intend to use the information for a criminal purpose.

As part of a whole-of-government approach to combat consumer fraud and scams targeted at consumers, the Australasian Consumer Fraud Taskforce was established in March 2005. It comprises all the governmental regulatory agencies and departments in Australia and New Zealand that have responsibilities for consumer protection. The Taskforce's 2007 campaign (SCAMS TARGET YOU - Protect Yourself) raised awareness about scams and fraud prevention.

(d) Traditional techniques

Techniques used to obtain personal information are not limited to high-tech or online methods such as credit card skimming devices and phishing. Other ways of procuring personal identifying information include:

- stealing mail or rummaging through rubbish (dumpster diving), and
- eavesdropping on public transactions to obtain personal data (shoulder surfing).

Identity crime can be difficult to detect as it can involve the use of lawful processes, such as a change of name¹⁸ (through a change of name certificate, managed and issued through Registrars of Births, Deaths and Marriages). However, the Committee notes that identities can also be adapted for lawful purposes; for example, the adoption of another identity for witness protection.

2.6 Definitions

There is no universally accepted definition of identity crime. In Australia and overseas,¹⁹ the term is often used interchangeably with the terms 'identity fraud' and 'identity theft' to cover a broad range of conduct involving the unauthorised or improper use of personal identification information.

The April 2007 Council of Australian Governments (COAG) Agreement²⁰ to a National Identity Security Strategy (NISS) includes the following definitions, which were developed

¹⁷ Russell Smith, Trends and issues in crime and criminal justice, No 331, *Australian Institute of Criminology*, February 2007.

¹⁸ ACPR, p 9.

¹⁹ ACPR, p 5.

²⁰ The Agreement, available at www.coag.gov.au, outlines the elements of a National Identity Security Strategy (NISS), including undertakings to further develop and implement the NISS to give effect to the COAG commitments. The NISS provides a framework for inter-governmental cooperation to strengthen Australia's personal identification processes.

by the Australian Centre for Policing Research²¹ based on the current use within Australasian policing:

Identity crime is 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.

Identity fraud is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.

Identity theft is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased.

²¹ ACPR, p 13.

3 Extent and cost of identity crime

Studies have observed that the incidence, extent and cost of identity crime are increasing in a number of countries, including Australia. This has been attributed to numerous factors, including:

- the rise in high-speed information flows
- globalisation
- the increased use of remote communications to transact at a distance rather than traditional face-to-face interactions
- the ease with which documents can be forged using high-tech methods, and
- the widespread collection and dissemination of data about individuals by private sector and other organisations, which provides opportunities for easier access to personal information.²²

A great amount of information on individuals and other entities is readily available and accessible on the Internet. Recent survey data has revealed that many Australians are not vigilant in protecting the privacy of their personal information.²³ However, 62% of Australians are very or extremely concerned about unauthorised access to or misuse of their personal information.²⁴

Identity crime is a serious problem facing the Australian criminal justice system. It seriously affects victims, it costs the Australian economy a significant amount, and often facilitates more serious crimes, such as terrorism and people smuggling.

Accurate measurement of the cost of identity crime is difficult and there are relatively few statistics available on its impact in Australia. The Australian Institute of Criminology reported that approximately one quarter of incidents involving fraud reported to the Australian Federal Police involve 'the assumption of false identities'.²⁵ *Identity Fraud in Australia*, a 2003 report by the Securities Industry Research Centre of Asia–Pacific (SIRCA) for financial intelligence agency AUSTRAC, claimed that identity fraud cost Australian large business \$1.1 billion in 2001–02.²⁶

²² Lozusic R, *Fraud and Identity Theft*, Briefing Paper 08/2003, 30/05/2003 <<http://www.parliament.nsw.gov.au>>; SIRCA report.

²³ Unisys Security Index Australia, A Newpoll Survey, <<http://www.unisys.com.au>> December 2006.

²⁴ Unisys Security Index Australia, A Newpoll Survey, <<http://www.unisys.com.au>> May 2007.

²⁵ AIC, 'Identity Fraud', *Australian Institute of Criminology Newsletter*, Summer/Autumn 2002, no 17, p 3.

²⁶ SIRCA report. Note there is an estimation error of \$130 million.

An indication of the costs involved can be obtained from statistics held in other countries. The USA *2007 Identity Fraud Survey Report* found that eight million adults in the USA (or just under 4% of the adult population) were victims of identity fraud, with a total cost involved of US\$49.3 billion.²⁷

Of this loss, less than 10% was borne by the individuals whose identities were used or stolen, meaning that most of the loss was instead incurred by businesses or organisations.

The same study²⁸ found that there has been a gradual decrease in the cost of identity fraud since 2003. However, the time spent by victims in resolving identity fraud cases increased from 33 hours in 2003 to 40 hours in 2006. The study also found that only a small percentage of identity fraud occurred over the Internet, with most cases involving traditional offline channels.

As for identity crime more broadly, a 2004 study in the USA found that 3.6 million households (or 3% of the population) had at least one member who had experienced the use or attempted use of their personal information without permission in the last six months, with a loss to the individuals involved estimated at \$US3.2 billion.²⁹

In the United Kingdom, the impact of identity theft has been estimated at £1.7 billion over the three years to 2007, according to one Home Office committee.³⁰ Another UK survey by CIFAS, the UK's Fraud Prevention Service, found the number of victims of impersonation to be more than 67,000, with total cases of identity fraud reported at over 80,000.³¹ Other research by CIFAS³² indicates that deceased fraud (or impersonation of deceased persons) is the UK's fastest growing identity theft crime, estimated to cost the UK £250 million a year.

Canada has experienced significant problems with identity theft. Public Safety and Emergency Preparedness Canada estimated that, in 2002, total losses due to identity theft were approximately CAN\$2.5 billion.³³

²⁷ Javelin Strategy, *2007 Identity Fraud Survey Report*, <<http://www.javelinstrategy.com/research>>, accessed on 27 February 2007.

²⁸ Javelin Strategy, *2007 Identity Fraud Survey Report*, <<http://www.javelinstrategy.com/research>>, accessed on 27 February 2007.

²⁹ US Department of Justice Bureau of Justice Statistics, *Identity Theft 2004*, NCJ 212213.

³⁰ Home Office Identity Fraud Steering Committee, *Identity Theft, Don't Become a Victim*, <<http://www.identitytheft.org.uk>>.

³¹ CIFAS Online, *2006 Fraud Trends*, <http://www.cifas.org.uk/press_20070130.asp>.

³² CIFAS, *Deceased Frauds – Research Results – December 2004*, <http://www.cifas.org.uk/reports_deceased_fraud.asp>.

³³ Public Safety and Emergency Preparedness Canada, *Report on Identity Theft*, October 2004.

4 Overseas responses to identity crime

Identity crime is a widespread problem facing most countries. In developing an Australian legislative response to the issue, it is helpful to look at how some other countries have dealt with the problem. Below are descriptions of some jurisdictions' responses to identity crime. Many countries have data protection laws that address the improper use of information and which may also apply to identity crime. However, only offences specifically relating to identity crime have been included in the discussion.

4.1 *United States of America*

The USA has adopted a series of measures to tackle identity crime. In 1998, the United States Congress enacted a new specific criminal offence of identity theft in the *Identity Theft and Assumption Deterrence Act 1998*.³⁴

This identity theft offence, codified at 18 USC 1028(a)(7), prohibits the knowing use, transfer or possession, without authorisation, of a 'means of identification' of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes any offence under United States federal law, or any felony under United States state or local law. The penalty for a simple breach is a maximum of five years imprisonment and an aggravated offence attracts a penalty of 15 years imprisonment.³⁵

It should be noted that offences criminalising identity crime also exist at the state level in the United States.

The *Identity Theft and Assumption Deterrence Act* also creates a centralised victim assistance, complaint and consumer education service for victims of identity theft. This means that victims need not contact each of the relevant agencies separately. Instead, there is a 'joint fraud alert' that the three major credit reporting agencies administer. Victims can access assistance in the absence of a conviction for identity theft.

The *Fair and Accurate Credit Transactions Act 2003* introduced a series of protections for consumers. Consumers are able to obtain a free credit report on request, to help them monitor their financial information and provide an early alert of unlawful activity. Consumers can also place a fraud alert on their account. Once the alert has been placed on the account, credit reporting agencies must block potentially fraudulent information on consumer credit reports from being released. The fraud alert is effective for 90 days once the consumer provides proof of identity, with a possibility of extension to seven years once the consumer submits a police report. A national standard has been set, requiring merchants to truncate account numbers on credit or debit card receipts. Victims of identity theft can also obtain copies of the impostor's account application and transactions conducted in the victim's name once a police report has been filed. A conviction is not required.

³⁴ PSEPC report, see n 33, p 10.

³⁵ The aggravated offence was created by the *Identity Theft Enhancement Penalty Act 2004*.

The federal bank and thrift regulatory agencies have issued the *Guidelines requiring the Proper Disposal of Consumer Information*³⁶ underpinning the *Fair and Accurate Credit Transactions Act*. These guidelines require each financial institution to develop and maintain appropriate controls to ensure that it properly disposes of consumer information derived from a consumer's credit report.

4.2 United Kingdom

In the United Kingdom, the impact of identity theft was estimated in 2006 at £1.7 billion a year.³⁷ While the United Kingdom does not have a specific identity crime offence, some recently enacted laws target identity crime offences. The *Identity Cards Act 2006* created new criminal offences of being in possession of or controlling false identity documents, including genuine documents that have been improperly obtained or were issued to another person, without reasonable cause. These offences came into force on 7 June 2006 and cover both United Kingdom and foreign documents.³⁸

4.3 Canada

Canada is in a similar position to Australia in terms of existing legislation to combat identity crime. It does not have a specific identity crime offence; rather, it has traditional offences such as fraud and forgery to prosecute identity crime-related offences. In addition, Canada has offences that criminalise activities that are integral to the criminal misuse of personal information. But the preliminary steps of collecting, possessing and trafficking identity information are generally not captured by existing offences.

On 16 October 2007, the Canadian Government introduced legislation amending the Criminal Code, R.S.C 1985, c. C-46. The Bill creates the following offences:

- obtaining personal information from a third party by false pretence or by fraud, and
- selling or otherwise disclosing personal information obtained from a third party by a false pretence or by fraud.

The amendments permit police to intervene at an earlier stage of criminal operations, before identity fraud or other crimes that cause financial or other harm are attempted or committed.

The Act will come into force on a day to be fixed by order of the Governor in Council. As at 18 March 2008, it had not come into force.

4.4 Europe

Although identity crime is also a problem in Europe, one recent report notes that France, Germany and the Netherlands do not have specific offences covering identity crime. Like

³⁶ US *Federal Register*, Volume 69, Number 248, Rules and Regulations, Page 77610–7762128; <www.fdic.gov> December 28 2004.

³⁷ Home Office Identity Fraud Steering Committee, *Identity Theft, Don't Become a Victim*, <<http://www.identitytheft.org.uk>>.

³⁸ <<http://www.identity-theft.org.uk/what-is-being-done.htm>>.

Canada, there are laws that can be used to prosecute offences such as forgery or data abuse, but a specific offence is yet to be enacted for identity crime.³⁹ In 2004, the European Commission developed an Action Plan for 2004-2007 to prevent fraud on non-cash means of payment. The Plan acknowledges that fraud is evolving rapidly and often involves identity theft. The Plan sets out a number of initiatives to combat identity theft.⁴⁰

The Netherlands has recognised the impact of identity theft, with a report to the Dutch Parliament stating that identity theft costs the country 5 billion euros a year.⁴¹

Many European countries (as well as some non-European countries) are parties to the Council of Europe Convention on Cybercrime. In Article 1, the Convention sets out some of the substantive criminal law offences that should be enacted at the national level. These offences relate in many cases to conduct that is part of identity crime. Article 2 deals with illegal access to computer data. Article 3 deals with illegal interception of data and Article 4 deals with data interference.

Article 5 deals with system interference and Article 6 deals with misuse of devices that could commit any of the offences in Articles 2–5. Articles 7 and 8 deal with computer-related forgery and fraud respectively. Identity crime itself is not set out as an offence in any of the articles of the Convention and therefore no offence is required to be enacted by any of the ratifying countries.

One of the most notable aspects of the Convention is Chapter 3, which deals with international cooperation. The inclusion of this chapter emphasises that these kinds of offences are not inhibited by borders, and that dealing with these crimes successfully hinges in many cases on effective and efficient international cooperation.

4.5 South Korea

Possibly the most novel approach to the identity theft problem comes from South Korea. It has been reported that the South Korean government will implement legislation that will make it mandatory for financial institutions to compensate customers who are victims of online fraud and identity theft.⁴²

However, if customers are careless with their data, they will not be entitled to compensation. This would place a greater onus on financial institutions to maintain a high level of security to prevent identity theft.⁴³

³⁹ Owen, K, Keats, G, and Gill, M, *The Fight Against Identity Theft*, June 2006, p 4.

⁴⁰ van der Meulan, N, *The Spread of Identity Theft: Developments and Initiatives within the European Union*, May 2007.

⁴¹ van der Meulan.

⁴² Article posted 14 December 2005 at <http://www.schneier.com/blog/archives/2005/12/korea_solves_th.html>

⁴³ Article posted 14 December 2005 at <http://www.schneier.com/blog/archives/2005/12/korea_solves_th.html>.

5 Existing legislative framework in Australia

Offences that can currently be used to prosecute identity crime are scattered through State, Territory and Commonwealth legislation on a range of subjects. The difficulty with using most of these offences is that they require the prosecution to prove another associated criminal act, such as theft, fraud or forgery. With the exception of South Australia and Queensland, it is not currently an offence in Australia to assume or steal another person's identity, except in limited circumstances.⁴⁴ It is what is done with the identity that generally attracts law enforcement attention.⁴⁵ There is no single offence that comprehensively criminalises identity crime in its own right.

5.1 Model Criminal Code offences

As with credit card skimming, there can be difficulties in adapting existing Model Criminal Code offences of theft, forgery and fraud to identity crime (see Credit Card Skimming Report, pp 7–10).

(a) Model Criminal Code theft offences

The phrase 'identity theft' is a misnomer, as identity theft does not actually deprive a person of their identity. The offence of theft or larceny traditionally involves an appropriation of the personal property of another with the intention to deprive him or her of that property permanently.⁴⁶ Wrongfully accessing or using a person's personal information or forging proof of identity documents, without taking any physical document or thing, would not deprive the person of the ability to use that information.

The use of identifying information relating to another person or to a fictional person to pass one's self off as that person can be conceptualised as fraud or deceit. This conceptualisation focuses on the use of false personal information rather than the way the information is accessed or obtained.

Section 16.7 of the Model Criminal Code (going equipped for theft, robbery, burglary or other offences) criminalises possession, while not at home, of an article with intent to use it in the course of, or in connection with, any theft or related offence. This offence could apply, for example, where a defendant had in his or her possession information used to identify another person and the defendant intended to use that information to commit a fraud offence such as obtaining property by deception. The prosecution has to prove that the defendant:

- knew he or she had the article, and
- intended to use it for the purpose of theft or a related offence.

⁴⁴ For example, there are offence provisions for the falsification or concealment of an identity with the intention of deceiving or misleading etc: section 8U of the *Taxation Administration Act 1953* (Cth).

⁴⁵ ACPR, p 9.

⁴⁶ See, for example, subsection 131.1(1) of the *Criminal Code Act 1995* (Cth).

It may be difficult for the prosecution to prove the defendant had the necessary intent to use the article for fraud. Where it can be shown that an article is made or adapted for theft, fraud or a related offence, that will be evidence from which inferences can be drawn that the defendant had the article for that purpose.⁴⁷ It may be possible to show that personal identifying information 'is made or adapted for'⁴⁸ a fraud offence. For example, a defendant may have an invoice showing that the defendant used another person's credit card details to purchase goods.

The offence of going equipped for theft, robbery, burglary or other offences is a preparatory offence and for that reason carries a maximum penalty of only three years imprisonment.

(b) Model Criminal Code forgery offences

Section 19.3 of the Model Criminal Code criminalises the making of a false document with the intention that the person or another will dishonestly use it to:

- induce a person to accept the document as genuine—s 19.3(a) or
- obtain a gain or cause a loss or to influence the exercise of a public duty—s 19.3(b).

This offence could apply, for example, where a person has manufactured a counterfeit identifying document, such as a driver's licence or passport, to purchase goods.

Similar offences apply where the person uses (s 19.4) or possesses (s 19.5) a false document.

One difficulty with these offences in their application to identity crime is that they are limited to false 'documents'. The term 'document' is defined broadly to include cards. However, it may not apply where the forgery has occurred on an electronic record; for example, where a fake website has been created to lure a bank's customers to provide their financial details.

The maximum penalty for offences under ss 19.3–19.5 is seven years and six months imprisonment.

(c) Model Criminal Code fraud offences

Unlike the Model Criminal Code forgery offences, the fraud offences in ss 17.2 (obtaining property by deception) and 17.3 (obtaining a financial advantage by deception) do specifically extend to electronic records or systems. The term 'deception' is defined to include 'conduct by a person that causes a computer system or any machine to make a response that the person is not authorised to cause it to do'. Section 17.3 could therefore apply to a situation where a person sets up a fake website to lure a bank's customers to provide their financial details.

The maximum penalty under both ss 17.2 and 17.3 is 10 years imprisonment.

⁴⁷ Final Report on *Chapter 3 – Theft, Fraud, Bribery and Related Offences*, December 1995, p 103.

⁴⁸ See, generally, *Nac* (2002) 163 CCC (3d) 1 (SCC).

While the misappropriation or misrepresentation of an identity is a common factor in many instances of fraud, identity crime by itself will not usually constitute a criminal offence without something more, such as intent to obtain property or a benefit, or to avoid a detriment.⁴⁹

5.2 Model credit card skimming offence

In its Report on Credit Card Skimming, the Committee commented on the difficulties of applying the model credit card skimming offence to identity theft because of the differences between the two offences.⁵⁰

(a) Kind of information used

In credit card skimming, the personal information involved is that used to access funds, credit or other financial benefits—including account numbers, credit card numbers, a person's user identification name or number, and a person's password for ATM or Internet access. This is reflected in the model credit card skimming offence in subsection 3.3.5(1) of the Model Criminal Code, which defines 'personal financial information' as 'information relating to a person that may be used, whether alone or in conjunction with other information, to access funds, credit or other financial benefits'. It does not cover personal identifying information such as a name, address, date of birth, driver's licence number or biometric data.

On the other hand, in the case of identity theft, the personal information involved is all information used to identify the person. It includes some of the forms of information used in credit card skimming (for example, a person's credit or debit card). However, information that identifies a person for the purpose of the person accessing his or her funds (such as a password) may not necessarily form an aspect of the person's identity.

(b) Purpose for which the information is used

The purpose of credit card skimming is likely to be to obtain a financial benefit for the perpetrator, to the detriment of the victim.

In contrast, identity theft may involve activities that do not have the purpose of obtaining a financial benefit, and do not achieve that result. For example, identities may be misused for the purpose of smuggling people between borders for the purposes of organised crime or terrorism.

⁴⁹ See the crime of fraud in section 409 of the *Criminal Code Act Compilation Act 1913 (WA)*.

⁵⁰ Report on *Chapter 3 – Credit Card Skimming Offences*, p 28.

5.3 Specific identity crime offences—South Australia and Queensland

South Australia was the first Australian jurisdiction to enact an offence specifically criminalising identity theft. In March 2007, Queensland also enacted a specific identity theft offence through the *Criminal Code and Civil Liability Amendment Act 2007* (Qld). The offence carries a maximum penalty of three years imprisonment.

(a) South Australia

In 2003, South Australia introduced specific identity theft offences. The offences, in Part 5A of the *Criminal Law Consolidation Act 1935* (SA), criminalise the following conduct:

- the assumption of a false identity (including falsely pretending to have a particular qualification or have, or be entitled to act in, a particular capacity)—s 144B
- the misuse of personal identification information—s 144C
- the production and possession of prohibited material— ss 144D(1) and (2), and
- the possession of equipment for making prohibited material—ss 144D(3).

Section 144A of the Act defines key terms, including ‘false identity’, ‘personal identification information’ and ‘prohibited material’. ‘Personal identification information’ is broadly defined as information used to identify the person, including the person’s name, address, date of birth and voice print, and biometric data relating to the person. The definition of personal identification information specifically includes ‘the person’s credit or debit card, its number, and data stored or encrypted on it.’ For a body corporate, ‘personal identification information’ includes the number of any bank account established in the body corporate’s name or of any credit card issued to the body corporate.

The offences do not apply to under-age persons who attempt to enter age-restricted venues or purchase age-restricted items, such as cigarettes or alcohol.

The *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA) amended the *Criminal Law (Sentencing) Act 1988* (SA) by providing for the issue of a certificate, on application by the victim of the offence, where a court convicts a person of an offence involving the assumption of another person’s identity or use of another person’s personal identification information. The certificate contains details of the offence, the name of the victim and any other matters the court considers relevant.

(b) Queensland

Queensland’s new s 408D of the Criminal Code is based on the model credit card skimming offence that was endorsed by MCCOC in its Discussion Paper of March 2004. The Queensland offence is quite broad, which should ensure that the full range of conduct that can constitute identity theft is captured. The new provision applies to a person who possesses ‘identification information’ for the purpose of committing or facilitating the commission of an indictable offence.

The definition of ‘identification information’ covers a broad range of conduct which can be described as ‘identity theft’ and ‘identity fraud’. It covers conduct involving another entity’s identification information where:

- (a) the entity is alive or dead
- (b) the entity exists or does not, or
- (c) the entity consents to the use of the identification information or does not.

The offence includes a list of examples of information that would be considered 'identification information', both for an individual and for a body corporate.

The Queensland offence does not contain an express exception (as in the South Australian Identity Theft Act) to cover the situations of a person under 18 using a fake identity to gain entry to premises, or to buy alcohol or tobacco. However, as s 408D requires an intent to commit, or facilitate the commission of, an indictable offence, this conduct would not be captured because using a fake identity to gain entry to premises or to buy alcohol or tobacco is a summary offence.

5.4 Other possibly applicable offences

Outlined below are some of the existing offences under Commonwealth, State and Territory laws that could apply to identity crime. Many of these offences are longstanding and well-established; for example, those relating to fraud or impersonation. The list is illustrative rather than exhaustive.

(a) Commonwealth

The *Criminal Code Act 1995* (Cth) implements the Model Criminal Code offences dealing with theft, fraud, bribery and related offences (Parts 7.2, 7.3, 7.4, 7.6 and 7.7), computer offences (Part 10.7), and financial information offences, including credit card skimming (Part 10.8).

Division 474 of Part 10.6, and Divisions 477 and 478 of Part 10.7, cover cybercrimes such as hacking, denial of service attacks, virus propagation and website defacements. Part 10.8 targets credit card skimming and internet banking fraud, including phishing. It draws on the provisions of the Council of Europe Convention on Cybercrime, referred to earlier. The offences are phrased in similar terms to the model credit card skimming offence in that they refer to dishonestly obtaining or dealing in personal financial information.

As discussed above, consumer scams can use online deception to target people who seek to purchase goods and services. These consumer scams may be used by crime groups to gather listings of personal identification information which is then on-sold to other crime groups. The *Spam Act 2003* (Cth) goes some way to addressing this issue by creating offences for sending, or causing to be sent, spam (defined as unsolicited commercial electronic messages) that have an Australian link. The offences carry penalties of up to \$1.1 million a day for repeat corporate offenders.

(b) New South Wales

In New South Wales, the more serious offences in the *Crimes Act 1900* (NSW) that could be used to prosecute identity crime include:

- inducing persons to enter into certain arrangements by misleading statements (s 185A), maximum penalty of five years imprisonment

- impersonating the owner of stock or property (s 184A), maximum penalty of 10 years imprisonment
- directors omitting certain entries (s 174) or wilfully destroying, altering, falsifying (s 175), or cheating or defrauding (s 176), maximum penalty of 10 years imprisonment
- obtaining money by deception (s 178BA), by false or misleading statements or false pretences (s 179), maximum penalty of five years imprisonment
- making and using false instruments (s 300), maximum penalty of 10 years imprisonment
- making or using copies of false instruments (s 301), maximum penalty of 10 years imprisonment
- custody of false instruments (s 302), maximum penalty of 10 years imprisonment
- making or possession of implements for making false instruments (s 302A), maximum penalty of 10 years imprisonment
- giving false or misleading information (s 307B), maximum penalty of two years imprisonment
- unauthorised access, modification or impairment with intent to commit serious indictable offence (s 308C), carrying a penalty the same as that for the intended serious indictable offence
- unauthorised modification of data with intent to cause impairment (s 308D) and unauthorised impairment of electronic communication (s 308E), both carrying maximum penalties of 10 years imprisonment
- possession of data with intent to commit a serious computer offence (s 308F) and producing, supplying or obtaining data with intent to commit a serious computer offence (s 308G), both carrying penalties of three years imprisonment, and
- unauthorised access to or modification of restricted data held in a computer (s 308H) and unauthorised impairment of data held on computer disk, credit card or other device (s 308I), both summary offences with maximum penalties of two years imprisonment.

(c) Victoria

In Victoria, the more serious offences in the *Crimes Act 1958* (Vic) that could be used to prosecute identity crime include:

- making false statements (s 247), maximum penalty of five years imprisonment
- obtaining property by deception (s 81), maximum penalty of 10 years imprisonment
- obtaining financial advantage by deception (s 82), maximum penalty of 10 years imprisonment
- falsification of documents (s 83A), maximum penalty of 10 years imprisonment, and

- fraudulently inducing persons to invest money, maximum penalty of 15 years imprisonment.

Under the Victorian *Health Services Act 1988* (Vic), impersonation of an authorised officer carries a maximum penalty of 120 penalty units.

(d) Queensland

Section 408C of the Criminal Code is cast in broad terms. It applies to a person who dishonestly obtains property or a benefit, causes a detriment, or applies to his or her own use or the use of any person property belonging to another. The maximum penalty is five years imprisonment or 10 years imprisonment in certain circumstances.⁵¹

The term ‘property’ is widely defined in s 4 of the Code. However, s 408C (3) extends it to include credit, service, any benefit or advantage, anything evidencing a right to incur a debt or to recover or receive a benefit, and releases of obligations.

Section 408C applies to most conduct covered by Queensland’s identity crime provision, and may also include on-supplying identification information. However, unlike the new s 408D offence, which requires proof of intent to commit an indictable offence, the s 408C offence requires the prosecution to prove dishonesty.

Other general provisions in the Queensland Criminal Code that could be used to prosecute identity crime in Queensland include:

- computer hacking and misuse (s 408E), penalty range of two to 10 years imprisonment
- forgery and uttering (s 488), maximum penalty of three years imprisonment to life, depending on what the thing forged purports to be
- attempts to procure unauthorised status (s 502), maximum penalty of three years imprisonment
- instruments and materials for forgery (s 510), maximum penalty of 14 years imprisonment, and
- personation in general (s 514), maximum penalty of three years imprisonment or 14 years imprisonment if the offender falsely pretends to be a person entitled to any specific property and the offender intends to obtain such property.

(e) Western Australia

In Western Australia, the more serious offences in the *Criminal Code 1913* (WA) that could be used to prosecute identity crime include:

- fraud (s 409), maximum penalty of seven years imprisonment or 10 years imprisonment where the person deceived is of or over the age of 60 years
- forgery and uttering (ss 473–474), maximum penalty of two years imprisonment or \$8,000

⁵¹ For example, where the property or yield to the offender is of a value of \$5,000 or more.

- procuring or claiming unauthorised status (s 488), maximum penalty of three years imprisonment
- personation of a person with the intent to defraud any person (s 510), carrying a penalty of imprisonment for three years. If the representation is that the offender is a person entitled by law to any specific property and the offender commits the offence with the intent to obtain such property, he or she is guilty of a crime and is liable to imprisonment for 14 years, and
- personation of the owner of shares or an interest in a company, maximum penalty of 20 years imprisonment.

(f) South Australia

In South Australia, the more serious offences in the *Criminal Law Consolidation Act 1935* (SA) that could be used to prosecute identity crime include:

- theft (s 134), maximum penalty of 10 years imprisonment
- deception (s 139), maximum penalty of 10 years imprisonment or for an aggravated offence 15 years imprisonment, and
- dishonest dealings with documents (s 140), maximum penalty of 10 years imprisonment or for an aggravated offence 15 years imprisonment.

Subsection 140(6) of the Act also contains an offence of possession, without lawful excuse, of any article for creating a false document or for falsifying a document. The maximum penalty for this offence is imprisonment for two years.

(g) Tasmania

In Tasmania, the more serious offences in the *Criminal Code 1924* (Tas) that could be used to prosecute identity crime include:

- insertion of false information as data (s 257E)
- acquiring a financial advantage (s 252A)
- personation in general (s 288)
- obtaining goods by false pretences (s 250), and
- obtaining execution of a security by false pretences (s 251).

Instead of providing separate maximum penalties, the Tasmanian Criminal Code provides for a general maximum term of imprisonment of 21 years (except for murder) and leaves it to the courts to place the various crimes into different categories of gravity.

(h) Australian Capital Territory

In the Australian Capital Territory, the more serious offences in the *Criminal Code 2002* (ACT) that could be used to prosecute identity crime include:

- obtaining property (s 326) or a financial advantage (s 332) from someone else by deception both carry a maximum penalty of 10 years and/or \$100,000 (money value of 1,000 penalty units).
- general dishonesty (s 333), including doing something with intent to dishonestly obtain a gain from someone else, or with intent to dishonestly cause a loss to someone else, maximum penalty of five years and/or \$50,000 (money value of 500 penalty units)
- conspiracy with intent to dishonestly obtain a gain from a third person, or with intent to dishonestly cause a loss to a third person, or with intent to dishonestly influence a public official in the exercise of the official's duty as a public official, maximum penalty of 10 years and/or \$100,000 (money value of 1,000 penalty units)
- making false or misleading statements on oath or in statutory declarations (s 336A), maximum penalty of five years and/or \$50,000 [money value of 500 penalty units]
- offences under Part 4.2 of the Code relating to unauthorised access, modification and impairment of data and electronic communications to or from a computer, and the production, supply etc of data, and
- forgery and related offences, maximum penalty of 10 years and/or \$100,000 (money value of 1,000 penalty units).

In the ACT, giving false or misleading statements carries a penalty of one year's imprisonment, while general dishonesty carries a maximum penalty of five years imprisonment.

(i) Northern Territory

In the Northern Territory, the more serious offences in the *Criminal Code 1983* (NT) that could be used to prosecute identity crime include:

- unlawful access to data with the intent to cause harm or gain benefit, and also unlawful use (s 276B), maximum penalty of 10 years imprisonment
- personation of a person named in a certificate (s 274), maximum penalty of seven years imprisonment
- unlawful modification of data (s 276C), maximum penalty of 10 years imprisonment, and
- falsification of registers (s 265), maximum penalty of seven years imprisonment.

5.5 *Less serious possibly applicable offences*

There is longstanding law on the use of identity, covering impersonation, pretending to have certain qualifications and misuse of identity cards. Some examples are set out below.

- Impersonation in official contexts, such as where it is done to obtain a ballot paper in an election
 - *Parliamentary Electorates and Election Act 1912* (NSW), s 66L—False Statements
 - *Electoral Act 2002* (Vic), s 148—False Information
 - *Electoral Act 1992* (Qld), s 347—Impersonation of authorised officer
 - *Electoral Act 1907* (WA), s 190—Electoral offences
 - *Electoral Act 1985* (SA), s 69—Entitlement to vote
 - *Electoral Act 2004* (Tas), s 183—False or misleading statements or declarations
 - *Electoral Act 1992* (ACT), s 311—Electoral papers—unauthorised possession
 - *Electoral Act 2004* (NT), s 21—Entitlement to be enrolled for a division, and
 - *Electoral Act 1918* (Cth), s 339—Other offences relating to ballot-paper etc.
- Offences for representing that one is qualified or registered to work in various trades and professions
 - *Sheriff Act 2005* (NSW), s 9—Impersonation of sheriff’s officers
 - *Gas Industries Act 2001* (Vic), s 199—Impersonation of Inspector
 - *Prostitution Act 1999* (Qld), s 283—False representation that a person is a registered agent
 - *Legal Practice Act 2003* (WA), s 129—Practitioner making false representation to be certificated
 - *Fisheries Act 1989* (SA), s 29—False representation of a Fisheries Officer
 - *Fertilizers Act 1993* (Tas), s 18—Impersonating an Inspector
 - *Criminal Code 2002* (ACT), s 360—Impersonating territory public official
 - *Totalisator Licence and Regulation Act 2004* (NT), s 100—Impersonation of an inspector, and
 - *Australian Federal Police Act 1979* (Cth), s 63A—Personation etc. of protective service officers or special protective service officer.
- Offences for impersonating public officers
 - *Police Act 1990* (NSW), s 204—Impersonation of police officers
 - *Nurses Act 1993* (Vic), s 62A—Impersonating a nurse
 - *Criminal Code* (Qld), s 97—Personating public officers
 - *Fire and Emergency Services Authority of Western Australia Act 1998* (WA), s 38C - Impersonation of a member of staff
 - *Electricity Act 1996* (SA), s 88—Impersonation of officials etc
 - *Criminal Code* (Tas), s 290—Personating public officers
 - *Criminal Code* (ACT), s 3.8362 - Impersonating police officer
 - *Police Administration Act 2006* (NT), s 38C—Impersonation of member of staff section 154, and
 - *Criminal Code* (Cth), s 148.1—Impersonation of an official by a non-official.
- Misuse of particular types of government-issued identification, such as motor vehicle drivers’ licences

- *Road Transport (Driver Licensing) Act 1998* (NSW), s 22—Obtaining driver’s licence by false statements
- *Road Safety Act 1986* (Vic), s 71—Obtaining licence etc. by false statements
- *Transport Operations (Road Use Management) Act 1995* (Qld), s 26—Fraud and unlawful possession of licences
- *Road Traffic Act 1974* (WA), s 97—Offences
- *Motor Vehicles Act 1959* (SA), s 96(3)—Falsely representing to be the person on the licence
- *Vehicle and Traffic Act 1999* (Tas), s 64—Offences of dishonesty
- *Road Transport (Driver Licensing) Act 1999* (ACT), s 30—Unlawful possession of licence etc.
- *Motor Vehicles Act 1978* (NT), s 11—Obtaining a permit, licence by misrepresentation, and
- *Australian Passports Act 2005* (Cth), s 32—Improper use of or possession of an Australian travel document.

6 Recommended model identity crime offences

Section 5 outlines many offences that already apply to some forms of identity crime. However, there are gaps in the coverage of those offences. Accordingly, the Committee recommends the creation of specific identity crime offences that would comprehensively cover identity fraud and identity theft.

The Committee's view is that any gaps in existing laws should be remedied with general offences wherever possible. Any proposal for specific or narrowly applied offences should be based on a clear need. The Committee considers that, in the case of identity crime, there is such a need.⁵²

The Committee therefore recommends the creation of the following model offences to cover identity crime:

- dealing in identification information,
- possession of identification information with the intention of committing, or facilitating the commission of, an indictable offence, and
- possession of equipment to create identification information, in certain circumstances.

The complete text of the recommended model provision is set out below.

3.3.6 Identity fraud

(1) Definitions.

In this section:

deal in identification information, includes make, supply or use any such information

identification documentation means any document or other thing that contains or incorporates identification information and that is capable of being used by a person for the purpose of pretending to be, or passing himself or herself off as, another person (whether living or dead, real or fictitious, or an individual or a body corporate)

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

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

⁵² The offences would be included in the Model Criminal Code, Chapter 3 (Theft, fraud, blackmail, forgery, bribery and related offences), Part 3.3 (Fraud) after credit card skimming and related offences (section 3.3.5).

- (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) a financial account number, user name or password,
- (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.

(2) Dealing in identification information.

A person who deals in identification information with the intention of committing an indictable offence, or of facilitating the commission of an indictable offence, is guilty of an offence.

Maximum penalty: Imprisonment for 5 years.

(3) Possession of identification information.

A person who possesses identification information with the intention of committing an indictable offence, or of facilitating the commission of an indictable offence, is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

Possession of equipment used to make identification documentation.

(4) A person who possesses equipment that is capable of being used to make identification documentation, with the intention that the person or another person will use the equipment to commit an offence against this section, is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

(5) This section applies:

- (a) to a person who intends to commit, or facilitate the commission of, an offence even if committing the offence concerned is impossible or the offence concerned is to be committed at a later time, and
- (b) in the case of an offence against subsection (2) or (3), whether or not the person to whom the identification information concerned relates consented to the dealing in, or possession of, the identification information.

(6) Subsections (2) and (3) do not apply to dealing in, or the possession of, a person's own identification information.

(7) It is not an offence to attempt to commit an offence against this section.

Notes.

1. Alternative verdict provision under subsection (3) for persons who are charged with an offence against subsection (2) is a matter for each jurisdiction.

2. It is intended that the law of the local jurisdiction inform the meaning of “indictable offence” and related issues (including whether offences under the law of other jurisdictions are included and whether it is necessary to establish the status of the offence concerned).

Suggested additional provision for inclusion in the criminal procedure law of the relevant jurisdiction (adjustments will have to be made to reflect the manner in which Magistrates Courts are described in the relevant jurisdiction.)

Certificate may be issued by Local Court in relation to victim of identity crime

(1) In this section, **victim** of an alleged offence under section 3.3.6, means a person whose identification information is the subject of an offence.

(2) The Local Court may issue a certificate under this section if satisfied, on the balance of probabilities, that an offence against section 3.3.6 has been committed and that the certificate may assist with any problems the offence has caused in relation to the victim’s personal or business affairs.

(3) The certificate is to:

- (a) identify the victim of the offence, and
- (b) describe the manner in which identification information relating to the victim was used to commit the offence.

(4) The certificate may contain such other information as the Court considers appropriate.

(5) The certificate is not to identify the perpetrator or any alleged perpetrator of the offence.

(6) The Court may issue a certificate under this section whether or not:

- (a) the perpetrator of the offence is identifiable, or
- (b) any criminal proceedings have been or can be taken against a person in respect of the offence, or are pending.

(7) The Court may issue a certificate under this section on the Court’s own initiative or on application by the victim of the offence.

(8) The certificate is not admissible in any criminal proceedings in relation to the offence.

The elements of the model provisions are set out individually and explained below.

6.1 Definitions

Model definition of identification information.

(1) Definitions.

In this section:

deal in identification information, includes make, supply or use any such information

identification documentation means any document or other thing that contains or incorporates identification information and that is capable of being used by a person for the purpose of pretending to be, or passing himself or herself off as, another person (whether living or dead, real or fictitious, or an individual or a body corporate)

identification information means information relating to a person (whether living or dead, real or fictitious, or 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, and 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.

Discussion Paper

The Discussion Paper proposed that the model identity crime offences should cover the broadest possible range of identification information. Both the Queensland *Criminal Code* and the South Australian *Criminal Law Consolidation Act 1985* adopt broad definitions of the information covered. The definitions encompass and extend beyond financial information (as in the case of model credit card skimming) to include biometric data, voice prints, a body corporate's name and ABN, and a series of numbers or letters intended for use as a means of personal information.

Submissions and commentary

The Office of the New South Wales Privacy Commissioner and the Association of Building Societies and Credit Unions agreed that identification information needs to be defined as broadly as possible, noting that the definition needs to be broad enough to cover changes in technology.

The Office of the Privacy Commissioner said:

[I]n the Office's experience a technologically neutral definition that is contingent on context for an application, like that used in the Privacy Act, or alternatively a definition that seeks to identify the features of information that render it 'personal identification information' is likely to be more effective and less likely to become outdated than a list of information to be included in the information.

Section 408D of the *Criminal Code* (Qld) contains a broad definition of identification information which is technologically neutral. This definition also refers to 'identification information', rather than 'personal identification information', which is more appropriate, given that the offence is to also apply to identification information of a body corporate.

Conclusion

The Committee maintains its recommendation that the definition of identification information be based on s 408D of the *Criminal Code* (Qld).

6.2 *Dealing in identification information*

(1) **Definitions.**

In this section:

deal in identification information, includes make, supply or use any such information...

(2) **Dealing in identification information.**

A person who deals in identification information with the intention of committing an indictable offence, or of facilitating the commission of an indictable offence, is guilty of an offence.

Maximum penalty: Imprisonment for 5 years.

...

(5) This section applies:

- (a) to a person who intends to commit, or facilitate the commission of, an offence even if committing the offence concerned is impossible or the offence concerned is to be committed at a later time, and
- (b) in the case of an offence against subsection (2) or (3), whether or not the person to whom the identification information concerned relates consented to the dealing in, or possession of, the identification information.

(6) Subsections (2) and (3) do not apply to dealing in, or the possession of, a person's own identification information.

(7) It is not an offence to attempt to commit an offence against this section.

Notes.

1. Alternative verdict provision under subsection (3) for persons who are charged with an offence against subsection (2) is a matter for each jurisdiction.
2. It is intended that the law of the local jurisdiction inform the meaning of "indictable offence" and related issues (including whether offences under the law of other jurisdictions are included and whether it is necessary to establish the status of the offence concerned).

Discussion Paper

The Discussion Paper recommended a broad identity crime offence to the following effect.

To convict a person of identity crime under the model offence, the prosecution would have to prove:

- (a) that the person captured, used or transferred the personal identification information belonging to another person—whether the person to whom the information relates is alive or dead, real or fictional
- (b) that the person captured, used or transferred that personal identification information with the intent to commit, or facilitate the commission of, an indictable or serious offence.

It would not be a defence that the person to whom the information relates consented to the capture, use or transfer of the information.

Submissions and commentary

The Committee received several submissions on this proposal, addressing various aspects.

Application to a body corporate

The Australian Customs Service, the South Australian Police Force, the Australian Bankers' Association and the Australian Taxation Office suggested that the offence apply to both individuals and corporate offenders.

The offence is intended to apply to all persons in the legal sense, including bodies corporate, in line with the general approach in Australian law—eg s 22(1) of the *Acts Interpretation Act 1901* (Cth).

Therefore, this component of the offence did not undergo any changes.

Making identification information

The Australian Taxation Office suggested the offence include the creation of identification information. This offence is partially covered in s19.3 of the Model Criminal Code, which criminalises the making of a false document with the intention that the person or another will dishonestly use it. However, this does not extend to the situation where the forgery has occurred on an electronic record; for example, where a fake website has been created to lure a bank's customers to provide their financial details. Accordingly, ss (1) of the model offence provides that dealing in identification information includes making, supplying or using identification information.

The Committee considered having the offence also apply to the impersonation of another person, but decided that this did not fit within the scope of this Paper or draft offence provision.

Dealing in identification information

Rather than using the terms 'captured, used or transferred,' the Committee decided to use the broader term 'dealing' to encapsulate all of the terms. Dealing is defined to include 'making,' 'supplying' and 'using'.

Intention to commit

The Australian Bankers' Association, the New South Wales Police Force, the Queensland Police Force, Denise Lofthouse (a former police officer) and the Australian Taxation Office suggested that the onus for the offence be reversed. The Australian Taxation Office said:

The ATO considers that (in place of the intent element) a person who is proved, beyond reasonable doubt, to have captured, used or transferred the PII [personal identification information] should be guilty of the offence unless that person can establish, on the balance of probabilities, 'a lawful or reasonable excuse' for that capture, use or transfer.

Victoria Legal Aid expressed its strong support for maintaining the onus on the prosecution to prove that the accused had intent to commit an offence. The Committee supports Victoria Legal Aid's submission as it is a longstanding principle of criminal law that a defendant is presumed to be innocent and that the prosecution must prove every element of an offence relevant to the guilt of the person charged.

The New South Wales Police Force said:

We are, however, concerned that it may sometimes be difficult to establish the element of intention in the absence of an admission or any other type of direct or strong circumstantial evidence.

The fact that it is difficult for the prosecution to prove an element of an offence is not in itself a sound justification for reversing the onus of proof. This kind of statutory formula (eg without lawful excuse or without reasonable excuse) should be regarded with caution. Consider the offence of possession of implements of gaming or cheating without lawful excuse. The effect of the offence is to make every possession of those implements presumptively unlawful. The escape is a lawful excuse. That makes sense only if possession of the things in question ought to be presumptively unlawful. That in turn depends on what an instrument of gaming might entail. For example, it is not sensible to presume that every possession of a pack of cards is unlawful.

Indictable offence

The Commonwealth Director of Public Prosecutions (CDPP) suggested the offence should cover situations where the person captured, used or transferred the identification information with the intent to commit an offence punishable by 12 months imprisonment or more. The CDPP made the following comment in its submission:

In relation to the requirement concerning the intent to commit an indictable or serious offence, this office notes that if the offence was framed so that the intent was to commit an

indictable offence punishable by 2 years, it would not cover the situation where a person used the false identity to obtain a financial advantage from the Commonwealth (section 135.2 of the *Criminal Code 1995* (Cth)) which has a penalty of 12 months imprisonment or more.

Victoria Legal Aid said that ‘serious offence’ should be defined and that offences that are triable summarily should be excluded from the definition as it believes that many of those offences are less serious.

As the term ‘serious offence’ is not defined or commonly used, it was decided that using the term ‘indictable offence’ would be the best option. ‘Indictable offence’ is a key demarcation of the seriousness of an offence, which is used by all States and Territories. ‘Indictable offence’ is defined in the following ways:

- in the federal jurisdiction, it includes all offences punishable by more than 12 months imprisonment⁵³
- in Queensland, it includes all crimes and misdemeanours,⁵⁴ and
- in New South Wales, it includes offences which can be prosecuted before a judge and jury.⁵⁵

Therefore, the Committee recommends that the offence include the requirement that there be intent to commit, or facilitate the commission of, an indictable offence.

With or without consent

Victoria Legal Aid and the New South Wales Council for Civil Liberties suggested that a defence should be created where it is alleged that the defendant intended to commit an offence against a person who gave consent. Victoria’s Legal Aid submission gave the following example:

A 15 year old uses his mother’s E-bay account and credit card details to purchase an item on the internet. The prosecution alleges that he used the identification information with the intention of committing theft.⁵⁶ The fact that the defendant had his mother’s permission to use the account and credit card should be a complete defence to the charge.

In the Committee’s view, a person who uses the identification information of another person with that other person’s consent does not intend to commit an indictable offence, and would not be caught by the dealing in identification information provision. The Committee maintains its recommendation that the offence should apply regardless of whether the person whose identity is used or assumed consented to such use.

⁵³ Section 4G of the *Crimes Act 1914* (Cth).

⁵⁴ Section 3 of the *Criminal Code 1899* (Qld).

⁵⁵ Section 21 of the *Interpretation Act 1987* (NSW).

⁵⁶ Section 74 of the *Crimes Act 1958* (Vic).

In addition, after further consideration, the Committee's view is that the offence should also apply when it is impossible to commit the indictable offence at the time that the offence is to be committed.

Attempt to commit an offence

Given that this is a preparatory offence, the Committee decided that there should not be an offence of attempting to commit the offence. This has been made explicit by ss (7) of the model offence.

Telecommunications interception

The Australian Federal Police and the South Australian Police Force recommended that telecommunications interception warrants be available for obtaining evidence in relation to this offence. The South Australia Police Force said:

With the acknowledgement that Identity Crime is becoming synonymous with organised crime as an accepted means to fund their activities, it is necessary to give consideration to enabling Telecommunications Interception legislation to be utilised in the investigation of instances of Identity Crime.

The Australian Federal Police said:

To satisfactorily fight sophisticated identity crime syndicates, law enforcement agencies must commit to medium to long term investigations using a full suite of investigative tools, including telephone intercepts, surveillance devices, controlled operations, coercive powers, and other discovery tools.

The Australian Federal Police believes that it would be difficult for the prosecution to prove that the offender has intent to commit another crime without the ability to obtain a telecommunication interception warrant. The Australian Federal Police said:

Electronic surveillance has been critical to many of the AFP's successes in disrupting organised identity crime over the last 3 years and limiting the opportunity to expand access to that investigative option would diminish our operational capability to combat increased sophistication and organisation in identity crime.

Telecommunication interception provisions could apply to this offence by:

- amending the *Telecommunications (Interception and Access) Act 1979* (Cth) to specifically incorporate identity crime offences (irrespective of the penalty), or
- setting the penalty for identity crime offences to a maximum of at least seven years, which would allow investigations under the telecommunication interception legislation as it stands.

Recent trends in criminal investigation show that telecommunications interception is a

major and very effective crime fighting weapon. However, maximum sentences should be set in a principled manner by reference to the comparative seriousness of the offence (and not by reference to the investigative tools that may or may not be available as a consequence). A case for amending the definition of offences for which telecommunications interception is available would need to be put to the Commonwealth.

The Committee has drawn the submissions concerning telecommunications interception and electronic surveillance to the attention of relevant officers for consideration separately from this report.

Penalty

The majority of submissions supported the increase of the penalty to more than three years imprisonment as a maximum penalty.

The Victorian Police Force recommended that the offence carry a maximum penalty of 10 years because:

Victoria Police believes that one's identity should be considered sacrosanct. The long-term damage that can be caused by someone taking over one's identity can often be irreparable. The proposed higher penalty should be to reflect the seriousness if the mischief sought is to be prevented.

However, as Victoria Legal Aid pointed out, the offence is preparatory in nature and for that reason should not attract high penalties. Nevertheless, the preparatory nature of the offence needs to be balanced with the seriousness of the offence and the impact that it has on society.

The Committee considered having a tiered penalty system with a maximum penalty of five years imprisonment for a person who intended to commit an indictable offence, and a penalty of 12 months imprisonment for a person who intended to commit a less serious offence. However, the Committee decided that the courts should have the discretion in sentencing a person to take into account the seriousness of the offence to which the identity crime was directed.

Accordingly, the Committee recommends maximum penalty of five years imprisonment.

Conclusion

After considering stakeholder comments, the offence has undergone some significant changes since the release of the Discussion Paper. The main changes are:

- the offence applies to making identification information
- the offence applies to supplying identification information
- the offence has a maximum penalty of five years imprisonment, and
- it is not an offence to attempt to commit an offence against the provision.

6.3 Possession of identification information

(3) Possession of identification information.

A person who possesses identification information with the intention of committing an indictable offence, or of facilitating the commission of an indictable offence, is guilty of an offence.

Maximum penalty: Imprisonment for 3 years ...

(5) This section applies:

...(b) in the case of an offence against subsection (2) or (3), whether or not the person to whom the identification information concerned relates consented to the dealing in, or possession of, the identification information.

(6) Subsection (2) and (3) do not apply to dealing in, or the possession of, a person's own identification information.

Notes.

1. Alternative verdict provision under subsection (3) for persons who are charged with an offence against subsection (2) is a matter for each jurisdiction.
2. It is intended that the law of the local jurisdiction inform the meaning of "indictable offence" and related issues (including whether offences under the law of other jurisdictions are included and whether it is necessary to establish the status of the offence concerned).

Discussion Paper

The Discussion Paper did not recommend the creation of an offence for possessing or obtaining identification information. However, several submissions called for such an offence.

Submissions and commentary

The New South Wales Police Force, the South Australian Police Force, the Victorian Police Force and Denise Lofthouse suggested that a separate offence for the mere possession of identification information be developed. It was suggested that this offence not require an intent to commit another offence.

The Victorian Police recommended that:

There should be a prima facie offence of possession of personal identification belonging to another included as part of the model identity crime offences.

Such an offence would, in the Committee's view, be too broad and could cover situations in which possession of identification information would otherwise be lawful.

The NSW Police stated:

It may be appropriate to consider an offence such as possession of personal identification information with a presumed intention to on-sell it or use it to commit another offence. This may cover situations in which a person has been found in the possession of personal identification information that they have not actually on-sold/supplied or used to commit a subsequent indictable or serious offence, but where no reasonable or lawful explanation can be provided as to why they are in possession of the information.

The Committee does not consider that a presumed unlawful intention should be applied to this offence. There are many situations in which a person could be in possession of another person's identification information—for example, a person looking after their spouse's wallet while their spouse is playing sport.

However, the Committee agrees that there should be a separate, broadly cast offence that covers possessing identification information when it is intended to use that information to commit, or facilitate the commission of, an indictable offence.

Penalty

The possession offence is a preparatory offence, which requires intent to commit, or to facilitate the commission of, a further offence. Traditionally, the Committee has set lower maximum penalties for preparatory offences. The Committee therefore recommends that the offence carry a maximum penalty of three years imprisonment.

Conclusion

The Committee recommends that it be an offence to possess identification information with the intention of committing, or facilitating the commission of, an indictable offence.

6.4 Possession of equipment capable of making identification documentation

(4) Possession of equipment used to make identification documentation.

A person who possesses equipment that is capable of being used to make identification documentation with the intention that the person or another person will use the equipment to commit an offence against this section, is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

Discussion Paper

The Discussion Paper recommended a separate, specific offence of the possession of equipment to manufacture identification information, where the offender is *reckless* with respect to the information being used for an unlawful purpose.

The Discussion Paper stated that, in order to convict a person of the offence of the possession of equipment to manufacture identification information, the prosecution would have to prove:

- that the person possessed equipment capable of manufacturing identification information, and
- that the person possessed that equipment being reckless with respect to whether it was used for an unlawful purpose.

The Discussion Paper suggested that the equipment would not need to have actually been used to manufacture identification information for the offence to apply.

The Discussion Paper recommended that the fault element for the offence be recklessness.

The Discussion Paper proposed a penalty of three years for all identity crime offences.

The Committee noted in the Discussion Paper that s 144D(3) of South Australia's Criminal Law Consolidation Act contains a separate offence for the possession of equipment for making identification information, which carries a lesser fault element than those for the offences of assuming a false identity (s 144B) or the misuse of identification information (s 144C). The prosecution is required to prove that the defendant intended to commit, or assist in committing, another offence.

Submissions and commentary

Definition of equipment

A number of stakeholders expressed concern that the term 'equipment' was not defined and made suggestions as to what the term 'equipment' should include.

Victoria Legal Aid suggested that the term 'equipment' was too broad:

For example, any computer, scanner, printer or photocopier could be used to create false identity documents. We suggest it should be limited to specific types of equipment.

The Australian Customs Service suggested that:

The proposed offence for the possession of equipment to create identification information requires further definition. It is not clear if this offence is intended to capture commonly available equipment such as photocopiers, laminators, computers and printers, which are capable of producing high quality identity documentation.

The Australian Federal Police suggested that:

Equipment in the context should include electronic data such as templates on computer equipment, data storage mediums, laminators, printers, card printers, embossers and scanners.

After considering stakeholder comments, the Committee agreed that the offence needed to be further refined, while bearing in mind that most equipment used to make identification information is innocuous (computers, printers, laminators etc), and that many people possess such equipment for lawful purposes.

Forfeiture of equipment

The South Australian Police Force recommended the automatic forfeiture of the device/equipment upon conviction. However, the Committee determined that this is a matter better left to the general provisions on forfeiture of instruments of crime in each jurisdiction.

Broadening the offence

The CDPP suggested:

Part (b) suggests that the information must have been used before the offence is committed. This seems a narrow approach and would mean that the offence would not be made out if the person possessed the equipment being reckless to the fact that the information produced could be used for an unlawful purpose, but where it had not actually been used for such a purpose yet. For this reason, this office raises whether this offence should also cover the situation where the defendant possessed equipment being reckless as to whether the information that was produced by it could be used in the future for an unlawful purpose.

The Committee accepts that equipment does not actually have to be used for an offence to be committed, and this is reflected in paragraph (5) (a) of the draft offence. However, the Committee has proposed a fault element of intention, rather than recklessness, for

the reasons explained below.

Fault element

The Committee has decided that there should be an offence for possession of equipment capable of making identification documentation.

A person who possesses equipment capable of making identification documentation may use that equipment themselves to commit an identity crime offence. Alternatively, they may intend for another person to commit an identity crime offence, and facilitate the commission of that offence by allowing the other person to use the equipment. In either case, there is an appropriate basis for this to be an offence, even if there is no evidence to make out the subsequent identity crime (ie use of the identification document made using the equipment.)

The Committee considered creating two separate possession of equipment offences. The first offence would occur if a person possessed equipment capable of being used to make identification documentation and *intended* to use that equipment themselves to commit an identity crime offence. The second offence involved a person possessing equipment capable of being used to make identification documentation and being *reckless* as to whether the equipment was used by another person to commit an identity crime offence.

However, the Committee was concerned that a fault element of recklessness risked being too broad and might capture circumstances that it was not intended to capture, particularly in light of the fact that most of the equipment used to make identification documentation is itself lawful and legitimate (for example, photocopiers, scanners and laminating machines).

Therefore, the Committee agreed that a fault element of intention was appropriate for the possession of equipment offence. Chapter 2 of the Model Criminal Code provides the following description of intention:

A person has intention with respect to conduct when he or she means to engage in that conduct. A person has intention with respect to a circumstance when he or she believes that it exists or will exist. A person has intention with respect to a result when he or she means to bring it about or is aware that it will occur in the ordinary course of events. (p 22)

Penalty

A number of submissions suggested that the penalty should be 10 years. The Committee considers that 10 years imprisonment is too severe a penalty.

Given that the 'equipment possession' offence is in essence a preparatory offence, the Committee considers that a maximum penalty of three years imprisonment is appropriate.

Conclusion

On the basis of submissions and further consideration, the following changes have been made to the recommended offence since the release of the Discussion Paper:

- the offence is subject to a maximum penalty of three years
- the offence occurs when a person possesses equipment capable of being used

to make identification documentation and either intends to use the equipment to commit an identity crime offence, or intends that the equipment will be used by anyone else to commit an identity crime offence

- identification documentation is defined, and
- the provision includes the statement that it applies whether or not the equipment is actually used by any person to commit an offence.

6.5 Certificate may be issued by Local Court in relation to victim of identity crime

Suggested additional provision for inclusion in the criminal procedure law of the relevant jurisdiction (adjustments will have to be made to reflect the manner in which Magistrates Courts are described in the relevant jurisdiction.)

Certificate may be issued by Local Court in relation to victim of identity crime.

- (1) In this section, **victim** of an alleged offence under section 3.3.6, means a person whose identification information is the subject of an offence.
- (2) The Local Court may issue a certificate under this section if satisfied, on the balance of probabilities, that an offence against section 3.3.6 has been committed and that the certificate may assist with any problems the offence has caused in relation to the victim's personal or business affairs.
- (3) The certificate is to:
 - (a) identify the victim of the offence, and
 - (b) describe the manner in which identification information relating to the victim was used to commit the offence.
- (4) The certificate may contain such other information as the Court considers appropriate.
- (5) The certificate is not to identify the perpetrator or any alleged perpetrator of the offence.
- (6) The Court may issue a certificate under this section whether or not:
 - (a) the perpetrator of the offence is identifiable, or
 - (b) any criminal proceedings have been or can be taken against a person in respect of the offence, or are pending.
- (7) The Court may issue a certificate under this section on the Court's own initiative or on application by the victim of the offence.
- (8) The certificate is not admissible in any criminal proceedings in relation to the offence.

Discussion Paper

Identity crime can cause damage to a person's credit rating, the creation of a criminal record in the person's name, and tremendous expenditure of time and effort restoring records of transactions or credit history. For example, a victim may not become aware that identity crime has occurred until he or she is called upon by defrauded creditors to make good on defaulted loan payments.

In these situations, it would be useful for the victim of identity crime to obtain a certificate showing that the transactions and/or criminal conduct were in fact carried out by another person purporting to be the victim. The certificate could contain details of the offence, the

name of the victim and any other matters the court considers relevant. This is the approach taken in the *Criminal Law (Sentencing) Act 1988* (SA). Queensland has adopted a similar approach in s 408D of the Queensland *Criminal Code*. This provision allows for the issue of a court certificate to a victim of identity crime, which may be issued at the court's own initiative or on application by either the victim or the prosecutor.

The certificate in both of these jurisdictions is not a remedy. It does not compel others to take restorative action—for example, it does not compel financial institutions to reinstate a person's credit rating. Rather, the certificate provides a means to present the outcome of a court's decision in a way that may be readily used by the victim to ensure the outcome of the legal proceeding.

The Committee notes that such a certificate is itself identification information, which would be protected from misuse by the model identity crime offence.

The Committee also raised the question whether it may be helpful to allow for certificates to be issued even where a case has not resulted in a conviction. For example:

- a defendant may be acquitted but a court could find on the balance of probabilities that a person's identity has been used by a person, or
- the offender cannot be identified but there is sufficient proof to satisfy a court that the person's identity has been misused.

Submissions and commentary

Several submissions supported the recommendation that certificates be issued even where no conviction has occurred.

A number of submissions also recommended that the certificate be available before a court hearing occurs. The Australian Taxation Office said:

Requiring the conviction of an offender before a victim certificate can be issued, is likely to render the certificate of little use to the victim because conviction may not be achieved until many months (or even years) after the offence.

The Australian Customs Service suggested a Director of Public Prosecutions be able to issue a certificate without it being tied to court proceedings.

The Committee considers that the victim should be able to obtain a certificate from the court regardless of whether criminal court proceedings against an alleged offender are pursued. In addition, a certificate should also be available when a court is satisfied on the balance of probabilities that the person is a victim of identity crime at the end of or in the course of a criminal trial for the identity crime offence (the court can be the trial court).

Conclusion

The Committee recommends that victim certificates be able to be issued by a court (including a trial court) when the court is satisfied on the balance of probabilities that the

person was a victim of identity crime. Courts should be able to issue such certificates at the end or in the course of a criminal trial.

A victim should also be able to apply to a Local Court to obtain a certificate, independently of a prosecution. In light of this view, the Committee also wants to ensure that the rights of an accused person are adequately protected.

The Committee considers that the certificate should not be admissible in any criminal proceedings in relation to the offence for which it was issued, but may be admissible in criminal proceedings more generally, subject to the applicable rules of evidence.

The Committee is conscious that implementation of this provision depends on the arrangements and resourcing in each jurisdiction for summary court proceedings, and notes that not all jurisdictions may wish to implement this provision.

7 On-selling identification information

Discussion Paper

The Discussion Paper recommended an offence for on-selling identification information:

To convict a person of that offence of on-selling identification information the prosecution would have needed to prove:

- (a) that the person obtained the personal identification information belonging to another person—whether the person to whom the information relates is alive or dead, real or fictional—and then sold that information on to a third person, and
- (b) that the person on-sold the information being reckless with respect to the information being used by the third person to commit an offence.

Submissions and commentary

After the following stakeholder recommendations the Committee decided instead to include 'supply' in the offence of making or dealing in identification information.

Supply

The New South Wales Police Force suggested that:

'supply' would be a preferable term than 'on-sell', as it could include a broader range of circumstances.

This suggestion was adopted. 'Dealing' is defined to include 'supply'.

Mules

The Australian Bankers' Association raised the issue of 'mules.' One 'mule' could give the identification information to another 'mule' who then gives it to the person who commits an offence. The first 'mule' should be able to be prosecuted for their actions, even though the second 'mule' to whom the first mule gave the identification information did not commit an offence. This would be captured by the model offence for making or dealing in identification information, because the offence would apply if a person supplied information to another person, intending to facilitate the commission of an indictable offence.

Conclusion

The Committee does not recommend a separate on-selling provision. The Committee believes that this behaviour is better captured by including 'supply' in the offence for making and dealing in identification information.

Appendix A Submissions received on the Identity Crime Discussion Paper

Submissions are available in full at:

<http://www.ag.gov.au/www/agd/agd.nsf/Page/Modelcriminalcode_IdentityCrimeDiscussionPaper>.

1	Tasmanian Department of Police and Emergency Management
2	Northern Territory Police Force
3	Victoria Legal Aid
4	Australian Customs Service
5	Privacy New South Wales
6	Office of the Privacy Commissioner
7	Commonwealth Director of Public Prosecutions
8	New South Wales Department of Public Prosecutions
9	Australian Bankers' Association
10	South Australian Police
11	Consulvest Australia Pty Ltd
12	Microsoft
13	New South Wales Council for Civil Liberties
14	Australian Taxation Office
15	Denise Lofthouse (former law enforcement officer)
16	Queensland Police
17	Human Rights and Equal Opportunity Commission
18	Information Law Branch of the Australian Attorney-General's Department
19	Anonymous submission
20	Australian Finance Conference
21	Abacus—the association for mutual building societies and credit unions
22	Australian Federal Police
23	CHOICE
24	New South Wales Police Force
25	Queensland Council for Civil Liberties
26	Victoria Police