

**M O D E L
C R I M I N A L
C O D E**

Discussion Paper

CHAPTER 3

IDENTITY CRIME

MODEL CRIMINAL LAW
OFFICERS' COMMITTEE OF
THE STANDING COMMITTEE
OF ATTORNEYS-GENERAL

April 2007

This Discussion Paper 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.

DISCUSSION PAPER

IDENTITY CRIME

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

April 2007

This Discussion Paper 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 2007

ISBN: 1 921241 14 4

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

Chair

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

Members

New South Wales: Ms Laura Wells
Director
Criminal Law Review Division
Attorney-General's Department

Victoria: Mr Greg Byrne
Director
Criminal Law - Justice Statement
Department of Justice

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

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

Northern Territory: Ms Barbara Tiffin
Senior Policy Lawyer
Legal Policy Division
Department of Justice

Australian Capital Territory: Ms Fiona Gallagher
Criminal Law and Justice Group
Department of Justice and
Community Safety

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

MCLOC Participant

Queensland:

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

Advisers:

Ms Kathryn Ovington
Senior Legal Officer
Criminal Law Branch
Attorney-General's Department

Ms Kim Williams
Senior Legal Officer
Criminal Law Branch
Attorney-Generals' Department

Discussion Paper – Identity Crime

1	Introduction	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?	8
4	Overseas Responses to Identity Crime	10
4.1	United States	10
4.2	United Kingdom	11
4.3	Canada	11
4.4	Europe	11
4.5	South Korea	12
5	Existing Legislative Framework	13
5.1	Model Criminal Code offences of theft, fraud and forgery	13
5.2	Model credit card skimming offence	15
5.3	Specific Identity Crime Offences – South Australia and Queensland	16
5.4	Other offences of possible application	17
5.5	Less serious offences	22
6	Model Identity Crime Offences	24
6.1	Model identity crime offence	25
6.2	On-selling identification information	29
6.3	Possession of equipment to create identification information	29

1 Introduction

(a) Identity crime as a national priority

The issue of identity crime has received considerable media and public attention over the last couple of years. It is an issue of major concern to government agencies, law enforcement, 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, States and Territory Agreement on Terrorism and Multi-Jurisdictional Crime, dated 5 April 2002.

(b) 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 the question of the development of a national Model Criminal Code for Australian jurisdictions on its agenda. In order 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. That Committee was originally known as the Criminal Law Officers Committee, but 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 as the Model Criminal Law Officers Committee to reflect the Committee's 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.

(c) Committee's previous work on related issues

Identity crime is closely related to fraud and fraud-related offences, such as credit card skimming. The Committee has previously reported on the law dealing with these related offences. In December 1995 the Committee released a Final Report on *Chapter 3: Theft, Fraud, Bribery and Related Offences*. The Report contained recommendations for model fraud offences including obtaining property by deception; obtaining a financial advantage by deception; production, use and possession of a false document and possession of a device for making false documents.

Similarly, the Committee has reported on credit card skimming. In April 2003, in response to the growing incidence of credit and debit card fraud in the community, SCAG tasked the Committee with developing model credit card skimming offences. The Committee's final report on credit card skimming² contained a model offence to cover credit card skimming and related offences.

¹ MCCOC 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>.

² MCLOC, *Final report on credit card skimming*, February 2006.

The offence was directed to criminalising the dishonest obtaining or dealing in personal financial information without the consent of the person to whom the information relates. The recommended offence did not attempt to cover all forms of 'identity crime'. The type of information covered by the offence was limited to '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'. The offence did not cover the theft or unauthorised use of other personal identifying information such as a name, address, date of birth, driver's licence number or biometric data.

In July 2004, the Committee sought SCAG's direction on whether model identity theft offences should also be prepared. Ministers agreed that MCCOC should examine the issue of identity theft as a separate item from credit card and debit card skimming offences.

This discussion paper examines the conduct that constitutes identity theft in the context of identity crime more broadly, and the impact of identity crime in Australia. The growth in new technologies and increasing Internet usage in Australia and elsewhere has seen a marked increase in the collection and storage of personal information. This has multiplied the risk that this personal information may be misappropriated and used to commit fraud, assist in the commission of terrorism offences and other serious crime.

At present, Australian criminal laws do not fully address the range of conduct that can be attributed to the misappropriation and wrongful use of identity information. While a number of jurisdictions in Australia have offences that can be used to prosecute some conduct associated with identity crime, to date only South Australia and Queensland have enacted offences specifically targeting identity theft.

To address the lack of a specific offence in most jurisdictions, MCLOC has developed model offences. These model offences attempt to proscribe a very broad range of conduct that constitutes identity crime. In addition, MCLOC has suggested that model provisions in this area should include some avenue for victims of identity crime to obtain court certification.

MCLOC encourages interested people or organisations to provide their views on any aspect of this discussion paper. These comments will be used to assist MCLOC in preparing its final report.

Comments should be sent to:

The MCLOC Secretariat
Criminal Justice Division
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

Fax: 02 6250 5918
Email address: criminal.law@ag.gov.au

2 What is Identity Crime?

2.1 Identity and identification

At a basic level, the possession of an identity is inseparable from an individual's sense of self and individuality.³ Identity can be defined by how your identity is established, for example by identifiers including:

- (a) physical or biometric identifiers – from photos to iris scans, fingerprints and voice prints
- (b) written identifiers – such as drivers licences and passports, and
- (c) 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.⁴ The United Kingdom Cabinet Office in a 2002 report⁵ referred to attributed and biographical elements of 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 social interaction with society, from documents such as

- (a) electoral registers
- (b) marital certificates
- (c) education or technical qualifications, and
- (d) 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.⁶

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

³ 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, p 1.

⁴ SIRCA report, p 1.

⁵ United Kingdom Cabinet Office, *Identity Fraud: A Study*, Economic and Domestic Secretariat, London; available online at: <http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf>

⁶ 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, his mother's and wife's maiden names to commit tax fraud.⁷

Fraud rings that use fictitious identities often reuse and rearrange the same names over and over. A report by the US 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'.⁸

It has been estimated that over 88% of all identity fraud in the USA involve fictitious or synthetic identities.⁹

2.4 Impact of identity crime

Identity crime can have a number of different 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.¹⁰

For a business or organisation, the indirect financial damage can be to its reputation or the opportunity cost resulting from foregoing benefit generating activities to counter identity crime.¹¹

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 types of crime.¹²

⁷ United Kingdom Cabinet Office, *Identity Fraud: A Study*, Economic and Domestic Secretariat, London; available online at: <http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf>

⁸ ID Analytics, 'Creation of a fictitious identity or manipulation of one's own identity', available at <<http://www.business.mcmaster.ca/IDTDefinition/defining/fictitious.htm>>

⁹ ID Analytics, *US National Fraud Ring Analysis*, <<http://www.idanalytics.com/whitepapers/index.html>>

¹⁰ 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

¹¹ SIRCA report, see n 3 above, p 43.

¹² *Identity Fraud in Australia: An evaluation of its nature, cost and extent*, Suresh Cuganesan and David Lacey, SIRCA, September 2003

(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,¹³ for example the suffering caused to a family following the theft of a deceased stillborn baby's identity, 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 are committing 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.¹⁴

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.¹⁵

Identity crime encompasses 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

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, emails are sent to individuals pretending to be from a bank, directing the person to a fake website designed to look like the bank's 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.

¹³ 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.

¹⁴ François Paget, *Identity Theft White Paper*, <www.mcafee.com>, January 2007.

¹⁵ SIRCA report, p 8.

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) On-selling information

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. 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 listings of personal identification information which is then on-sold to other crime groups. However, on-selling information may also involve the legitimate acquisition of personal identification information. The original person or group of people may have no criminal intent, but sells the information on to a group that 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 and comprises all of the governmental regulatory agencies and departments in Australia and New Zealand who have responsibilities for consumer protection. The Taskforce recently launched a campaign (SCAMS TARGET YOU - Protect Yourself) to raise awareness about scams and fraud prevention.

(c) Traditional techniques

Techniques that are used for obtaining 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).

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)>

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

Identity crime can be difficult to detect as it can involve the use of lawful processes, eg a change of name by deed poll.¹⁸ However, the Committee notes that identities can also be adapted for lawful purposes, eg the lawful use by women of their maiden and married names.

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 Australasian Centre for Policing Research has proposed²⁰ a uniform set of definitions along the following lines, based on the current use within Australasian policing.

- (a) '*Identity crime*' is a generic term with broad scope to describe a wide range of identity-related offences in which a defendant uses a false identity to commit, or facilitate the commission of, a crime.
- (b) '*Identity fraud*' describes the gaining of money, goods, services or other benefits, or the avoidance of obligations, through the use of a false identity. It includes: fraudulently obtaining a financial benefit (eg by credit card skimming), avoidance of taxes or financial loss, and intangible benefits, such as access to citizenship, professional affiliation, and medical services.²¹
- (c) '*Identity theft*' describes the theft or assumption by one person of another person's identity, whether the other person is alive or dead.²² It may also extend to the use of a fictitious identity.²³

¹⁸ ACPR, *Standardisation of definitions of identity crime terms: A step towards consistency*, Report Series No 145.3, March 2006, p 9.

¹⁹ ACPR, *ibid*, p 5.

²⁰ ACPR, *ibid*, p 13.

²¹ 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, p 25.

²² This is consistent with the definition adopted in the National Crime Prevention Program publication, *ID Theft - A kit to prevent and respond to identity theft*, Feb 2004, available online at <http://www.crimeprevention.gov.au/agd/WWW/ncphome.nsf/Page/Information_Kits>

²³ See the definition of 'false identity' in s 144A of the South Australian *Criminal Law Consolidation Act 1935* and proposed s 408D(2) in the Criminal Code and Civil Liability Amendment Bill 2007 (Qld).

3 Extent and Cost of Identity Crime?

Studies have observed that the incidence, extent and cost of identity crime is 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 on individuals by private sector and other organisations which provides opportunities for easier access to personal information.²⁴

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.²⁵

The high cost of identity crime to the Australian economy and the significant impact on victims indicates the seriousness of the problem. The fact that identity crime may often facilitate more serious crimes, such as terrorism and people smuggling, also demonstrates that identity crime is a substantial challenge currently facing the Australian criminal justice system.

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'.²⁶ *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 2001-02.²⁷

²⁴ Lozusic R, *Fraud and Identity Theft*, Briefing Paper 08/2003, 30/05/2003. Available at <<http://www.parliament.nsw.gov.au>>; Suresh Cuganesan and David Lacey *Identity Fraud in Australia: An evaluation of its nature, cost and extent*, SIRCA, September 2003.

²⁵ Unisys Security Index Australia, A Newspoll Survey, December 2006. Available at <<http://www.unisys.com.au>>

²⁶ AIC, "Identity Fraud", *Australian Institute of Criminology Newsletter*, Summer/Autumn 2002, no 17, p 3

²⁷ Securities Industry Research Centre of Asia-Pacific, SIRCA 02-2003 : *Identity Fraud: An evaluation of its nature, cost and extent*, 8 September 2003. 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 US *2007 Identity Fraud Survey Report* found that 8 million adults in the USA (or just under 4% of the adult population) were victims of identity fraud, with a total cost involved of \$US49.3 billion.²⁸

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 study²⁹ 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 6 months, with a loss to the individuals involved estimated at \$US3.2 billion.³⁰

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.³¹ Another UK survey by CIFAS, the UK's Fraud Prevention Service, found that the number of victims of impersonation to be over 67,000 with total cases of identity fraud reported at over 80,000.³² Other research by CIFAS³³ indicates that deceased fraud (or impersonation of deceased persons) is Britain's fastest growing identity theft crime, estimated to cost the UK £250 million a year.

Canada has experienced significant issues 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.³⁴

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

²⁹ Javelin Strategy, *2007 Identity Fraud Survey Report*, <<http://www.javelinstrategy.com/research>>, accessed on 27 February 2007.

³⁰ US Department of Justice Bureau of Justice Statistics, *Identity Theft 2004*, NCJ 212213.

³¹ Home Office Identity Fraud Steering Committee, *Identity Theft, Don't Become a Victim*, <<http://www.identitytheft.org.uk>>

³² CIFAS Online, *2006 Fraud Trends*, <http://www.cifas.org.uk/press_20070130.asp>.

³³ CIFAS, *Deceased Frauds – Research Results – December 2004*, <http://www.cifas.org.uk/reports_deceased_fraud.asp>.

³⁴ Public Safety and Emergency Preparedness Canada, *Report on Identity Theft*, October 2004.

4 Overseas Responses to Identity Crime

Identity crime is a universal problem facing most countries around the globe. In developing a legislative response to the issue, it is helpful to look at the way some other countries have dealt with the problem. Below are some illustrations of how countries have responded to the issue of identity crime. Many countries have data protection laws, which address the improper use of information and which may also apply to identity crime. However, only identity crime specific offences have been included in the below discussion.

4.1 United States

The United States has adopted a series of measures to tackle identity crime. In 1998 the US Congress enacted a new specific criminal offence of identity theft in the *Identity Theft and Assumption Deterrence Act 1998*.³⁵

This identity theft offence, codified at 18 USC 1028(a)(7), prohibits the knowing use, transfer, or possession, without authorization, 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 US federal law or any felony under US state or local law. The penalty for a simple breach is a maximum 5 years' imprisonment and an aggravated offence attracts a penalty of 15 years' imprisonment.³⁶

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

The US 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* also introduced a series of protections for consumers.

- Consumers can obtain a free credit report on request, to help them to monitor their financial information and provide an early alert.
- Consumers can place a fraud alert to flag their account, which requires credit reporting agencies to block potentially fraudulent information on consumer credit reports. 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.
- The Act sets a national standard in the US requiring merchants to truncate account numbers on credit or debit card receipts.

³⁵ PSEPC report, see n 34, p 11

³⁶ The aggravated offence was created by the *Identity Theft Enhancement Penalty Act of 2004*.

- Victims of identity theft can 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.

The federal bank and thrift regulatory agencies have issued the *Guidelines requiring the Proper Disposal of Consumer Information*³⁷ 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

The United Kingdom does not have a specific identity crime offence. However, there have been some recent laws that 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 UK 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.³⁹ In addition, Canada has offences that criminalise activities that are integral to the criminal misuse of personal information.

4.4 Europe

Although it is acknowledged that identity crime is also a problem in Europe, one recent report notes that France, Germany and the Netherlands do not have a specific offence covering identity crime. Consistent with the Canadian situation 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.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 other non-European countries) are members of the Council of Europe Convention on Cybercrime. The Cybercrime Convention, in Article 1, 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.

³⁷ US *Federal Register*, Volume 69, Number 248, Rules and Regulations, Page 77610-7762128, December 28 2004; see <www.fdic.gov>.

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

³⁹ Ibid.

⁴⁰ The Fight Against Identity theft, Katy Owen, Gemma Keats, Martin Gill, June 2006, p 4.

⁴¹ Ibid.

Article 5 deals with system interference and Article 6 deals with misuse of devices that could commit any of the offences in Articles 2 through 5. Article 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 is therefore not required to be enacted at a national level by any of the ratifying countries.

One of the most notable aspects of the Cybercrime Convention is in Chapter 3, which deals with international cooperation. The inclusion of this chapter in the Convention is a recognition that these types of offences do not recognise 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 is going to 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 then place a greater onus on financial institutions to maintain a high level of security to prevent identity theft.⁴³

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

⁴³ Ibid.

5 Existing Legislative Framework

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

5.1 Model Criminal Code offences of theft, fraud and forgery

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

(a) Model Criminal Code theft offences

The phrase 'identity theft' is somewhat of 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 permanently⁴⁶. 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 being able to use that information.

The use of identifying information relating to another person or to a fictional person in order 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 (Going equipped for theft, robbery, burglary or other offences) of the Model Criminal Code 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, see n 17, p 9.

⁴⁶ See for example section 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' 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.

This is a preparatory offence and as such only carries a maximum penalty of 3 years.

(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 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 a false 'document'. The term 'document' is broadly defined 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 of 7 years and 6 months imprisonment is higher than those applicable for theft offences.

(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.

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

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.⁴⁸

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 theft⁴⁹ because of the differences between the two offences.

- (a) **Type of information used** – In credit card skimming, the personal information about a person is that information 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 section 3.3.5(1) of the Model Criminal Code, which defines ‘personal financial information’ to mean ‘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 which 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.

In this regard, section 144A(1)(a) of the *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA) includes in its definition of ‘personal identification information’ a ‘series of numbers or letters (or a combination of both) intended for use as a means of personal identification’.

- (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 which do not have the purpose of obtaining a financial benefit, and do not achieve that result. The sole purpose of some identity theft activity, for example where the activity involves stalking a victim, may be to cause distress and anxiety to the victim or to intimidate the victim. More importantly, identities may be misused for the purpose of smuggling people between borders for the purposes of organised crime or terrorism.

⁴⁸ See the crime of fraud in section 409 of the *Criminal Code Act Compilation Act 1913* (WA).

⁴⁹ 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 State or Territory to enact an offence which specifically criminalises 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 (Identity Theft) Amendment Act, 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 – s 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 also amended the *Criminal Law (Sentencing) Act 1988* by providing for the issue of a certificate, on application by the victim of the offence, where a court convicts a person for 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 section 408D 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 is fictitious, and
- (c) whether or not the entity consents to the use of the identification information.

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 SA Identity Theft Act) to cover the situations of a person under 18 using a fake ID to gain entry to premises, or to buy alcohol or tobacco. However, as section 408D requires an intent to commit, or facilitate the commission of, an indictable offence, this conduct would not be captured as using a fake ID to gain entry to premises or to buy alcohol or tobacco is a summary offence.

5.4 Other offences of possible application

Some of the existing offences under Commonwealth, State and Territory laws that could apply to identity crime are outlined below. Many of these offences are longstanding and well-established, for example, those relating to fraud or impersonation. This is not an exhaustive list but rather an illustration of the kinds of offences with possible application.

(a) Commonwealth

The *Criminal Code Act 1995* 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 above. 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* goes some way to address 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) which could be used to prosecute identity crime include:

- inducing persons to enter into certain arrangements by misleading statements (s 185A), maximum penalty of 5 years' imprisonment
- personating 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, and
- obtaining money by deception (s 178BA), by false or misleading statements or false pretences (s 179), maximum penalty of 5 years' imprisonment.
- false or misleading information (s 307B), maximum penalty of 2 years' imprisonment.
- unauthorised access, modification or impairment with intent to commit serious indictable offence (s 308C) carries a penalty the same as 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 carry a maximum penalty of 10 years' imprisonment
- possession of data with intent to commit serious computer offence (s 308F) and producing, supplying or obtaining data with intent to commit serious computer offence (s 308G) both carry a penalty of 3 years' imprisonment.
- unauthorised access to or modification of restricted data held in computer (s 308H) and unauthorised impairment of data held in computer disk, credit card or other device (s 308I) are both summary offences with a maximum penalty of 2 years' imprisonment.

(c) Victoria

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

- making false statements (s 247), maximum penalty of 5 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 10 years' imprisonment, and
- fraudulently inducing persons to invest money, maximum penalty 15 years' imprisonment.

Under the Victorian *Qualifications Authority Act 2000*, impersonation carries a maximum penalty of 60 penalty units or 12 months' imprisonment.

(d) Queensland

Section 408C of the Criminal Code is cast in broad terms. It applies to a person who dishonestly obtains property, 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 5 years' imprisonment or 10 years' imprisonment in certain circumstances.⁵⁰

The term 'property' is widely defined in section 4 of the Code. However it is further extended by section 408C (3) 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 will apply to much conduct covered by Queensland's proposed identity crime provision, and may also include on-selling identification information. However, unlike the new section 408D offence, which requires proof of intent to commit an indictable offence, the section 408C offence requires the prosecution to prove dishonesty.

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

- computer hacking and misuse (s 408E), penalty range of 2 to 10 years' imprisonment
- forgery and uttering (s 488), maximum penalty 3 years' imprisonment to life depending on what the thing forged purports to be
- attempts to procure unauthorised status (s 502), maximum penalty 3 years' imprisonment
- instruments and materials for forgery (s 510), maximum penalty 14 years' imprisonment, and
- personation in general (s 514), maximum penalty 3 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) which could be used to prosecute identity crime include:

- fraud (s 409), maximum penalty 7 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 2 years' imprisonment or \$8,000
- procuring or claiming unauthorised status (s 488), maximum penalty 3 years' imprisonment

⁵⁰ For example, where the property or yield to the offender is of a value of \$5,000 or more, employee/employer relationship, director/company relationship.

- personation of a person with the intent to defraud any person (s 510), imprisonment for 3 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 20 years' imprisonment.

(f) South Australia

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

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

Section 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 2 years.

(g) Tasmania

In Tasmania, the more serious offences in the *Criminal Code 1924* (Tas) which 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 a separate maximum penalty, with the exception of murder, the Tasmanian Criminal Code provides an overall maximum term of imprisonment of 21 years and leaves it to the courts to place the various crimes into different categories of gravity.

(h) Australian Capital Territory

In the ACT, the more serious offences in the *Criminal Code 2002* (ACT) which 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 5 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 5 years and/or \$50,000 [money value of 500 penalty units], 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 1 year imprisonment, while general dishonesty carries a maximum penalty of 5 years' imprisonment.

(i) Northern Territory

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

- unlawful access to data with the intent to cause harm etc 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 7 years' imprisonment
- unlawful modification of data (s 276C), maximum penalty of 10 years' imprisonment, and
- falsification of registers (s 265), maximum penalty of 7 years' imprisonment.

5.5 *Less serious offences*

There is longstanding law on the use of identity, covering personation, 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.
 - NSW *Parliamentary Electorates and Election Act 1912*, section 66L – False Statements
 - VIC *Electoral Act 2002*, section 148 - False Information
 - QLD *Electoral Act 1992*, section 347 - Impersonation of authorised officer
 - WA *Electoral Act 1907*, section 190 - Electoral offences
 - SA *Electoral Act 1985*, section 69 - Entitlement to vote
 - TAS *Electoral Act 2004*, section 183 - False or misleading statements or declarations
 - ACT *Electoral Act 1992*, section 311 - Electoral papers—unauthorised possession
 - NT *Electoral Act 2004*, section 21 – Entitlement
 - CTH *Electoral Act 1918*, section 339 – Other offences relating to ballot-paper etc
- Offences for representing that one is qualified or registered to work in various trades and professions.
 - NSW *Sheriff Act 2005*, section 9 - Impersonation of sheriff's officers
 - VIC *Gas Industries Act 2001*, section 199 - Impersonation of Inspector
 - QLD *Prostitution Act 1999*, section 283 - False representation that a person is a registered agent
 - WA *Legal Practice Act 2003*, section 129 - Practitioner making false representation to be certificated
 - SA *Fisheries Act 1989*, section 29 - False representation of a Fisheries Officer
 - TAS *Fertilizers Act 1993*, section 18 - Impersonating an Inspector
 - ACT *Criminal Code 2002*, section 360 - Impersonating territory public official
 - NT *Totalisator Licence and Regulation Act 2004*, section 100 - Impersonation of an inspector
 - CTH *Australian Federal Police Act 1979*, section 63A – Personation etc of protective service officers or special protective service officer.
- Offences for impersonating public officers.
 - NSW *Police Act 1990*, section 204 - Impersonation of police officers
 - VIC *Nurses Act 1993*, section 62A - Impersonating a Nurse
 - QLD *Criminal Code*, section 97 – Personating public officers
 - WA *Fire and Emergency Services Authority of Western Australia Act 1998*, section 38C - Impersonation of a member of staff
 - SA *Electricity Act 1996*, section 88 - Impersonation of officials etc
 - TAS *Criminal Code*, section 290 - Personating public officers
 - ACT *Criminal Code*, section 3.8362 - Impersonating police officer
 - NT *Police Admin Act 2006*, section 38C - Impersonation of member of staff section 154
 - CTH *Criminal Code*, section 148.1 – Impersonation of an official by a non-official

- Misuse of particular types of government-issued identification, such as motor vehicle driver's licences.
 - NSW *Road Transport (Driver Licensing) Act 1998*, section 22 - Obtaining drivers licence by false statements
 - VIC *Road Safety Act 1986*, section 71 - Obtaining licence etc. by false statements
 - QLD *Transport Operations (Road Use Management) Act 1995*, section 126 - Fraud and unlawful possession of licences
 - WA *Road Traffic Act 1974*, section 97 - Offences
 - SA *Motor Vehicles Act 1959*, section 96(3) - Falsely representing to be the person on the Licence
 - TAS *Vehicle and Traffic Act 1999*, section 64 - Offences of dishonesty
 - ACT *Road Transport (Driver Licensing) Act 1999*, section 30 - Unlawful possession of licence etc
 - NT *Motor Vehicles Act 1978*, section 11 - Obtaining a permit, licence by misrepresentation
 - CTH *Australian Passports Act 2005*, section 32 – Improper use of or possession of an Australian travel document

6 Model Identity Crime Offences

As outlined in section 5 above, there are many existing offences which already capture some forms of identity crime. However, there are some gaps in the coverage of those offences. Accordingly, the Committee recommends the creation of a general identity crime offence 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 to do so. The Committee considers that there is such a need in the case of on-selling personal identification information and possession of equipment to create personal identification information.

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

- (1) identity crime – which encompasses identity theft and identity fraud
- (2) on-selling identification information, and
- (3) possession of equipment to create identification information.

The model identity crime offence is discussed immediately below. The other specific offences are covered in sections 6.2 and 6.3 below.

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.

Each of the aspects of this offence is described in turn below.

6.1 Model identity crime offence

(a) Capture, use or transfer

Identity crime may occur at various stages of the flow of personal information from one person to another. The offence needs to cover the *capture* of information (or ‘obtaining’ as used in section 408D of the Queensland Criminal Code). It also needs to cover the *use* (or ‘misuse’ as referred to in section 144C of the South Australian Criminal Law Consolidation Act). Finally, it should cover the transfer of information, which may occur separately from the capture or use of that information.

(b) With or without consent

The Committee considers it immaterial whether the person whose identity is used or assumed gives consent to such use or assumption. This will address situations where people collude to commit identity crime.

(c) Personal information

The model identity crime offence should cover the broadest possible range of identification information. Both the Queensland Criminal Code and the South Australian Criminal Law Consolidation Act 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.

The Committee recommends a similar approach.

(d) Belonging to another

The offence should exclude the use of one’s own personal information. This may well constitute criminal conduct in some circumstances but does not come within the scope of identity crime. Instead, the misuse or falsification may fall under other provisions, such as general fraud or forgery provisions.

(e) Alive or dead, real or fictional

As discussed in [2.3] above, the use of fictitious identities can prove just as harmful as the use of true-name identities. Both the Queensland and South Australian provisions cover conduct involving another entity’s identification information where the entity is alive or dead, real or fictitious.

The Committee considers it appropriate to cover the use of fictitious or synthetic identities in the model identity crime offence.

(f) Intent to commit another offence

The model identity crime offence would require proof that an offender captured, used or transferred the personal identification information of another with the intent to commit, or to facilitate the commission of, an indictable or serious offence.

In formulating the model identity crime offence, the Committee considered whether a 'mere' identity crime offence (without intent to commit another offence) was appropriate. However, the Committee was concerned about inadvertently criminalising innocent activities, or activities that should not be subject to criminal sanction. There are situations where the use by one person of another's personal identification information would not be considered to merit criminal sanction, for example:

- a woman who uses a false identity to escape domestic violence
- the use of a dead spouse's name and identification by her surviving spouse where the death certificate has not yet been issued.

In these situations, no harm has been caused to others by the use of another's identification information.

The Committee also considered the situation of an underage teenager using a false identity card to enter a club or to buy alcohol. Although this is a serious matter, the Committee's view is that the correct response is not to imprison the underage teenager but rather to enforce the matter by current means, eg criminalise the supply of alcohol to underage persons. The Committee also notes that the false representation of age already constitutes a summary offence⁵¹ in certain circumstances in some jurisdictions.

On the other hand, the person who produces the false identity cards and supplies them to an underage teenager should be targeted by an identity crime offence. The distinction lies in the fact that this producer of false identity cards intends, or at least is reckless as to the fact, that the cards will be put to an illicit purpose. As discussed above, the use of another's identification information with the intention to commit a further offence such as fraud may involve considerable harm. Some people have had their entire identity assumed by another. In the case of the manufacturer of false identity cards, the cards might well be used ultimately to assist people smuggling or terrorists to unlawfully enter the country.

The Committee has therefore sought to frame the proposed offence to target those cases where the offender intends by capturing, using or transferring the identification information of another to commit another offence.

⁵¹ For example, falsely representing age to be supplied smoking products is a summary offence in Queensland.

Dishonesty

In formulating the model identity crime offence, the Committee considered criminalising the dishonest capture, use or transfer of another's identification information. 'Dishonesty' is defined in section 14.2 of the Model Criminal Code to mean dishonest according to the standards of ordinary people and known by the defendant to be dishonest by the standards of ordinary people.

The model credit card skimming offence refers to dishonesty in criminalising the dishonest obtaining or dealing in personal financial information. However, there are situations where a person involved in credit card skimming may not have known of the proposed use of a device or personal information. The Committee weighed the risk of inadvertently criminalising innocent activities (or activities that ought not to be subject to criminal sanction) with the potential difficulty in proving that a person knew the proposed use of a device or piece of information. The use of the Model Criminal Code fault element of 'dishonesty' is an attempt to balance these two factors.⁵²

By contrast, the Committee considers that it could be onerous for the prosecution to prove that the offender *dishonestly* captured, used or transferred another's personal information. The prosecution would need to prove that the offender used some form of deceit or trickery to capture, use or transfer the information, which may not always be the case. A shopkeeper may obtain a person's drivers' licence number for a specified purpose, such as to process the person's use of a cheque to pay for goods in the shop. However, the shopkeeper may then subsequently form an intent to commit a fraud with the drivers' licence by altering it, or by assuming the other person's identity completely.

In this case, again, the distinguishing factor is that the shopkeeper intends to use the identification information to commit another offence.

Intent to commit an indictable or serious offence

In formulating the model offence, the Committee recommends that the prosecution be required to prove that the offender captured, used or transferred the identification information to commit, or to facilitate the commission of, an *indictable* or *serious offence*. This is the approach taken by Queensland and South Australia. Queensland's offence in subsection 408D(1) of the Criminal Code requires proof that the conduct was for the purpose of committing, or facilitating the commission of, an indictable offence. South Australia's Criminal Law Consolidation Act, in sections 144B (assumption of a false identity) and 144C (misuse of personal identification information) requires proof of intent to commit, or facilitate the commission of, a serious criminal offence. The term 'serious criminal offence' is defined to mean an indictable offence, or an offence prescribed by regulation for the purposes of this definition.

Another approach would be to require proof of intent to commit, or facilitate the commission of, *any other* offence. This is the approach taken in section 144D of South Australia's Criminal Law Consolidation Act.

⁵² MCLOC, *Final Report on Credit Card Skimming*, Feb 2006, at <http://www.ag.gov.au/www/agd/agd.nsf/Page/Model_criminal_code>.

In the case of the offence of the production and possession of prohibited material, section 144D(1) requires proof of the defendant's intent to use the material, or to enable another person to use the material, for a criminal purpose.

However, the Committee was concerned that this formulation would pick up the case of the underage teenager who falsely represents age, which is a summary offence in some jurisdictions.⁵³

The Committee notes that the terms 'indictable' or 'serious' offence differ between jurisdictions. Alternatively, the model identity crime offence could refer to the offence by reference to a certain period of imprisonment (for example, an offence punishable by 2 years' imprisonment).

(g) Penalty

The model identity crime offence is a preparatory offence, which requires the 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 3 years' imprisonment. This penalty is commensurate with the maximum penalties attaching to both the Queensland and South Australian identity theft provisions.

An alternative approach would be to set the maximum penalty at 5 years' imprisonment as with the model credit card skimming offence.

(h) Certificates following conviction

Identity crime can cause damage to a person's credit rating, the creation of a criminal record in the person's name, and countless time and effort 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.

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 section 408D of the 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, eg for 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 used by the victim.

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

⁵³ For example, falsely representing age to be supplied smoking products is a summary offence in Queensland.

Other options

The Committee considers that 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.

6.2 On-selling identification information

The model identity crime offence will not always capture on-selling personal information cases where one person captures the personal information of another and then sends that data on to a third person, who in turn uses it with intent to commit an offence. The first person in this scenario may have no intent for the information to be used for the intent which the second person has in mind.

For this reason, the Committee recommends a separate, specific offence of on-selling another's identification information data, where the offender is *reckless* as to the use to which the information is put. While the first person may not be aware of the precise use to which the identity information is ultimately put, he or she will be aware that there is a risk the information will be used unlawfully. In proceeding to on-sell the identification information while aware of this risk, the offender is reckless as to the fact the information may be used unlawfully.

To convict a person of the offence of on-selling identification information the prosecution would have 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.

6.3 Possession of equipment to create identification information

The possession of equipment for manufacturing identification information (eg a machine for making false identity cards) will not always be captured by the model identity crime offence, for similar reasons as on-selling personal information. The person who manufactures the identity cards may not be aware of the purpose for which the other person intends to use the identity cards, let alone intend that the cards be used for that purpose. However, while the first person may not be aware of the precise use to which the identity information is ultimately put, he or she will be aware that there is a risk the information will be used unlawfully. In possessing equipment to make identification information, the offender is reckless with respect to the information being used unlawfully.

For this reason, the Committee recommends 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.

To convict a person of the offence of the possession of equipment to manufacture identification information, the prosecution would have to prove:

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

The Committee notes that subsection 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.

The Committee seeks comment on any aspect of the Discussion Paper and in particular:

- (1) the scope and framing of the proposed identity crime offences
- (2) the proposed maximum penalties attaching to those offences, and
- (3) the proposed certificate following conviction.