

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

Discussion Paper

CHAPTER 3

**CREDIT CARD
SKIMMING OFFENCES**

March 2004

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

**MODEL CRIMINAL CODE
OFFICERS
COMMITTEE OF THE
STANDING COMMITTEE OF
ATTORNEYS-GENERAL**

DISCUSSION PAPER
MODEL CRIMINAL CODE
CHAPTER 3
CREDIT CARD
SKIMMING OFFENCES

Model Criminal Code Officers Committee of the
Standing Committee of Attorneys-General

MARCH 2004

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

ISBN 0 642 21147 7

Preface

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 (CLOC), but, in November 1993, the name was changed to the Model Criminal Code Officers Committee (MCCOC) in order to reflect the principal remit of the Committee directly.

The first formal meeting of the Committee took place in May 1991. In July 1992, the Committee released a discussion draft of the general principles of criminal responsibility. After a great deal of public consultation, the Committee delivered a Final Report to SCAG which was released in December 1992. With the exception of the general principles relating to intoxicated defendants, the recommendations in that Final Report formed the basis for the Commonwealth Criminal Code Bill, 1994, which was passed by the Commonwealth Parliament in March, 1995.

In 1994, both the Commonwealth Government and the State and Territory Premiers’ Leaders Forum endorsed the Model Criminal Code project as one of national significance.

In December 1995 MCCOC released its Final Report titled Theft, Fraud, Bribery and Related Offences. MCCOC has since released discussion papers on Non Fatal Offences Against the Person in August 1996 (report September 1998), Sexual Offences in November 1996 (report, June 1999), Contamination of Goods Offences in May 1997 (report March 1998), Serious Drug Offences in June 1997 (report October 1998), Administration of Justice Offences in July 1997 (report June 1998), Model Domestic Violence Laws in November 1997 (report April 1999), Serious Drug Offences in Commonwealth Jurisdiction in December 1997, Slavery Offences in April 1998 (report November 1998), Fatal Offences in June 1998, Model Forensic Procedures Bill and the Proposed National DNA Database in May 1999 (report February 2000), Damage and Computer Offences in January 2000 (report January 2001), and Issue Estoppel, Double Jeopardy and Prosecution Appeals against Acquittals in November 2003.

This discussion paper deals with new offences to address credit card skimming and includes a model credit card skimming offence for proposed inclusion in the fraud provisions of the Model Criminal Code.

Credit card skimming has recently emerged as a significant law enforcement challenge for Australia. The availability of sophisticated ‘skimming’ devices and increasingly widespread use of electronic, telephone and Internet banking

have contributed to the growing incidence of credit and debit card fraud. At the SCAG meeting in April 2003, SCAG tasked MCCOC with developing model credit card skimming offences.

This discussion paper examines the scope of the skimming problem and outlines the processes used to identify and capture personal credit and debit card data. Australian laws do not at present fully address credit and debit card skimming. A range of existing Commonwealth, State and Territory fraud and forgery offences cover many of the activities related to credit and debit card skimming. However, they do not comprehensively capture the act of skimming the data or possession of the skimmed data. At present, law enforcement agencies in Australia are generally unable to act against the skimming activity until a further offence has been committed.

While a number of overseas jurisdictions have criminalised credit card skimming, to date South Australia is the only jurisdiction in Australia to do so. The *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA) addresses credit card skimming as a form of identity theft. While MCCOC has prepared a model offence which specifically deals with credit card skimming, this discussion paper also considers the alternative option of criminalising credit card skimming as part of broader provisions on the topic of identity theft.

As with its previous publications, MCCOC has attempted to produce a document which is comprehensive, concise and capable of being understood by the general public as well as those who have some legal expertise.

The Committee encourages interested people and groups to provide their views on any aspect of this discussion paper. These comments will be used to assist MCCOC in preparing its final report.

This discussion paper was written by Margaret Joseph of the Commonwealth Attorney-General's Department. Initial research was completed by Ben Batros of the Commonwealth Attorney-General's Department.

Comments should be sent to:

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

COMMITTEE MEMBERS

Chairperson

His Honour Justice Rod Howie QC
Supreme Court of New South Wales

Members

New South Wales:

Mr Lloyd Babb
Criminal Law Review Division
Attorney-General's Department

Victoria:

Mr Greg Byrne
Manager
Legislation & Policy
Department of Justice

Western Australia:

Mr George Tannin SC
Crown Counsel
Crown Solicitor's Office

South Australia:

Mr Matthew Goode
Attorney-General's Department

Tasmania:

Ms Lisa Hutton
Director, Legislation Development & Review
Department of Justice

Northern Territory:

Ms Rosslyn Chenoweth
Policy Division
Department of Justice

Australian Capital Territory:

Ms Nicole Mayo
Criminal Law and Justice Group
Legislation and Policy Branch
Department of Justice and Community Safety

Australian Government:

Mr Geoff McDonald
Assistant Secretary
Criminal Law Branch
Attorney-General's Department

Advisers:

Ms Margaret Joseph
Senior Legal Officer
Criminal Law Branch
Attorney-General's Department

Mr Ian Leader-Elliott (Consultant)
Faculty of Law
University of Adelaide

Part 1:—What is credit card skimming?

What is the scale of the problem?

Credit card fraud is estimated to have cost the Australian economy approximately \$100 to \$120 million in 2002, up from \$50 to \$70 million in 2001.¹ Globally, credit card fraud is thought to cost approximately \$US3 billion each year.² In Australia, credit card “skimming” is estimated to account for approximately 50% of these losses, up from 10% towards the end of 2001.³

As the owner of the credit card is rarely liable for the fraudulent transactions, the true victims of credit card skimming and related fraud are the banks, financial institution and/or credit card companies. Ultimately the community pays through high banking costs. The owner of the credit card can still also suffer from adverse credit profiles, the inconvenience of identifying the fraudulent transactions and replacing the stolen cards and information and, on occasion, getting stranded away from home without any money.⁴

What is “skimming” - how does it happen?

Credit card skimming is generally considered to be the process by which legitimate credit card data is illicitly captured or copied, usually by electronic means. A range of activities can constitute, or are closely related to, credit card skimming.

Although the term “credit card skimming” is often used, many of these activities are not limited to credit cards - “skimming” card details at ATMs or EFTPOS terminals, or intercepting data transmitted from EFTPOS terminals, can be used to target debit cards as well. It is possible that in the future, as the use of “stored value” cards increases, these cards may also be susceptible to “skimming” or similar activities. The term “credit and debit card skimming” covers the skimming of both credit and debit card details, including the skimming of card details at ATMs or EFTPOS terminals.

1 “Credit card fraudsters hit tourist spots”, Tanya Moore, *The Courier Mail*, 17 May 2003 (accessed at <http://www.couriermail.news.com.au> on 17 June 2003); “Credit skim flicks for a dirty game in the cards”, Ian Hamilton, *The Weekend Australian*, Business News p. 25.

2 “Let no one skim your card”, Jennifer Sexton, *The Australian*, 22 November 2002, p. 12.

3 “Posting cards too risky; warn police”, Kirsty Needham, *Sydney Morning Herald*, 27 November 2002, p. 3; “Credit skim flicks for a dirty game in the cards”, Ian Hamilton, *The Weekend Australian*, Business News p. 25. According to VISA International, skimming of card details accounts for 50% of credit card fraud, lost or stolen cards account for 20%, stealing card details from discarded receipts or statements or insecure electronic transactions account for 20%, stealing new credit cards from mailboxes accounts for 7% and fraudulent applications using false identities account for 3%.

4 “Thieves cash in stolen identities” Anna Fenech, *Sunday Telegraph*, 21 January 2003, Business News p. 94.

Most credit card data is compromised at a point of purchase, without the card-holder's knowledge. The most common form of skimming is where a credit card that is handed over for a legitimate transaction is also run through a small (often hand-held) card reader that stores the information contained on the credit card's magnetic strip. This information can later be re-encoded onto counterfeit credit cards which become exact replicas of the originals.

Skimming in this form is most likely to take place at businesses where the credit card may be out of view of the owner during the transaction, where there are a high volume of credit card transactions, and where supervision is low. Restaurants and petrol stations are considered to be particularly susceptible to skimming, with some industry sources estimating that 75% of card skimming taking place at petrol stations.⁵

Credit card skimming is a growing part of the wider problem of credit card fraud. Some jurisdictions, such as Canada and the USA, consider skimming as a form of identity theft.⁶ There are a range of methods that can and have been used to illicitly obtain credit card data, some of which are closely related to the traditional "skimming" described above.

Sophisticated, small skimming devices have been fitted to ATMs. These devices are covertly fitted over the card slot and designed to look like part of the ATM. The devices record and store the details of all credit and debit cards as they are inserted into the ATM. Because debit cards require a personal identification number (PIN) to operate, the criminals must obtain this by either covertly watching the customer enter their PIN ("shoulder surfing")⁷ or by mounting a pinhole camera to record the customer using the ATM and entering their PIN. This form of skimming received substantial media attention after incidents in late 2002 where groups allegedly stole \$500,000 by fitting such skimmers to ATMs in Sydney and Melbourne.⁸

The telephone or data cables connecting financial institutions and large commercial customers may also provide opportunities for skimming card

5 "Posting cards too risky; warn police", Kirsty Needham, *Sydney Morning Herald*, 27 November 2002, p. 3; "Credit skim flicks for a dirty game in the cards", Ian Hamilton, *The Weekend Australian*, Business News p. 25; "Credit card fraudsters hit tourist spots", Tanya Moore, *The Courier Mail*, 17 May 2003 (accessed at <http://www.couriermail.news.com.au> on 17 June 2003); "Let no one skim your card", Jennifer Sexton, *The Australian*, 22 November 2002, p. 12. Staff at restaurants and independent service stations have reportedly been paid \$200 for every credit card that they "skimmed" - "Don't let credit card skimmers swipe your cash", Anthony Hughes, *Sydney Morning Herald*, 13 November 2002 (accessed at <http://www.smh.com.au> on 17 June 2003).

6 see Public Advisory: Special Report for Consumers on IDENTITY THEFT (Solicitor General of Canada and US Department of Justice) ("Special Report for Consumers of Identity Theft").

7 Special Report for Consumers of Identity Theft; "Credit skim flicks for a dirty game in the cards", Ian Hamilton, *The Weekend Australian*, Business News p. 25.

8 "Posting cards too risky; warn police", Kirsty Needham, *Sydney Morning Herald*, 27 November 2002, p. 3; "Plastic designed to plunder", Kara Lawrence, *Daily Telegraph*, 6 December 2002, p. 25; "Log-on rip-off", Michelle Innis, *Sydney Morning Herald*, 23 April 2003, Supplements p. 6.

details, as these cables carry credit and debit card information for purchases made at EFTPOS terminals. Overseas, in Canada, Malaysia and Europe, highly organised groups have tapped the telephone data cables between a commercial premises (such as a large department store) and their bank. The credit and debit card information is intercepted, copied, and the copy sent to the skimmer who is often located overseas.

There have been incidents reported of physical or electronic “bugs” being downloaded or inserted into ATMs and EFTPOS terminals. These “bugs” capture and store the information and PIN from any debit or credit card that is run through the ATM or EFTPOS terminal and then either transmit these details to the organiser/criminal over the phone lines or allow the details to be downloaded to a laptop computer at a later time.⁹

Skimming by “bugging” an ATM or EFTPOS terminal or by tapping the telephone cables is particularly difficult to detect as the card information is captured during the legitimate use of the card (rather than requiring the card to be swiped a second time), there is no external, physical skimming device that can be detected by an observant customer, and the criminal may not need to come to the site of the skimming to access the skimmed data.

Credit card details can be obtained without the criminals having physical access to the credit card. The Internet has provided a wide range of opportunities for criminals to obtain personal details including credit card details from unsuspecting persons. One common technique is known as “spoofing” - a person receives an email that appears to be from a legitimate business, for example a financial institution or on-line auction site. This email directs the person to the “business” website, where the person is asked to enter personal data including credit card information. Although the website appears to be an official site of a legitimate business, it has no connection with that business but has been established by criminals to record the information that is entered which can then be used for fraudulent purposes.¹⁰ An example of this form of fraud was seen in Australia in April 2003, when fraudulent “mirror” or “ghost” websites for AMP Banking, the Commonwealth Bank of Australia, Westpac and ANZ were established.¹¹ Another “spoofing” attempt, suspected to have originated in Florida, targeted Westpac and ANZ customers in July 2003.¹²

9 “Newly discovered bug ‘skims’ credit card data”, Jay Lyman, *NewsFactor Network*, 22 June 2001 (<http://www.newsfactor.com/perl/story/11494.html>, accessed on 28 May 2003); “Laws to deter ATM thieves”, *Daily Telegraph*, 17 February 2003, p. 5

10 Special Report for Consumers of Identity Theft; “Smart Cards on the way as credit fraud increase”, Karen Dearne, *The Australian*, 20 May 2003, Computer p. 10; “Convenient, but risky”, *Mercury*, 5 May 2003, Business News p. 18. This form of fraud was the subject of an ASIC consumer warning “Fraudulent emails: Watch out - some look surprisingly genuine” (9 April 2003 - <http://www.fido.asic.gov.au>).

11 “Log-on rip-off”, Michelle Innis, *Sydney Morning Herald*, 23 April 2003, Supplements p. 6.

12 “Internet fraudsters hit bank customers”, Garry Barker, *The Age*, 5 July 2003, p. 9.

Credit cards can also be compromised by a number of other, non-electronic means. An increase in incidents of new credit cards being stolen from customers' mailboxes, and a number of attacks on Australia Post drivers to steal bags of letters containing credit cards, prompted the NSW Police to recommend that banks stop posting credit cards and that customers collect cards directly from the bank branches.¹³ There have also been reports overseas of criminals obtaining credit card or bank account details from credit card or bank statements or receipts that have been stolen from mailboxes or discarded (known as "dumpster diving").¹⁴ Overseas (particularly in the USA) there have also been incidents of criminals stealing pre-approved credit card offers from mailboxes.¹⁵

What happens to the "skimmed" data?

The "skimmed" data is generally stored in the skimmer and then transmitted to a computer. The data can then be downloaded onto another magnetic strip, in most cases a counterfeit credit card which becomes an exact copy of the original. However the skimmed credit card data can be downloaded onto any form of media that has a magnetic strip, including a library card, a security card or even a parking ticket.

The counterfeit cards or other media are then used to make fraudulent purchases of goods or to withdraw funds from ATMs. The form of media that the skimmed data is downloaded onto will limit the possible uses - data on a parking ticket is unlikely to be used to purchase goods "over the counter", but could be used in some instances to withdraw cash from ATMs.

It is also possible that the information skimmed from credit cards could be used to purchase goods over the phone or the Internet. This removes the need to forge any counterfeit credit card or create any physical record of the skimmed data.

Most of the skimmed credit card details are transmitted overseas to be stored onto counterfeit credit cards. Indications are that the details from most cards skimmed in Australia are sent overseas, where counterfeit credit card "factories" have been found. The counterfeit credit cards are used to purchase

13 "Posting cards too risky; warn police", Kirsty Needham, *Sydney Morning Herald*, 27 November 2002, p. 3.

14 A Taiwanese man arrested in Melbourne in 2002 with 103 forged credit cards, which were alleged to have been used in frauds totaling more than \$500,000, is thought to have obtained most of the credit card details by "dumpster raids" and stealing documents from letter boxes. "Name theft a \$100bn industry", Garry Barker, *Sydney Morning Herald*, 7 July 2003, Business News p. 28.

15 Special Report for Consumers of Identity Theft; "Fraud alert: losing your good name in the post", Kirsty Needham, *Sydney Morning Herald*, 24 May 2003, p. 13; "Convenient, but risky", *Mercury*, 5 May 2003, Business News p. 18

goods in the region, or are sold to tourists for their use while abroad.¹⁶ By transmitting the data overseas and committing the fraud in another country, the skimmers increase the time that the counterfeit cards can be used for (as it can take longer for foreign vendors to report, and for the credit card companies to process, international purchases) and also inhibit the investigation of their activities by Australian authorities.

While most of the credit card data is transmitted overseas, the number of counterfeit credit cards (using skimmed data) being used in Australia is rising. There are indications that the data on many of these counterfeit cards has not been skimmed in Australia, but has been skimmed overseas and the counterfeit cards are being used by foreign tourists in Australia.¹⁷

What equipment do “skimmers” use?

Card skimming requires a device (a skimmer) that will read and capture the data contained on the magnetic stripe of a credit or debit card, store that data (often storing data from a number of swiped cards)¹⁸ and then allow it to be accessed or reproduced later.

The most common skimmers are reprogrammed magnetic strip readers. Battery powered magnetic strip readers that are the size of a cigarette packet are commercially available in Australia and have a wide range of legitimate uses. These commercially available magnetic stripe readers can be reprogrammed to act as skimmers, although this requires a degree of technical sophistication.¹⁹

Hand-held, portable skimmers have been found in Australia that are no larger than a pager, however there are reports that even smaller skimmers, the size of a book of matches, have been found overseas. These more sophisticated skimmers appear to be designed as skimmers rather than modified commercial magnetic stripe readers.

Where criminals target ATMs, they use a very fine magnetic strip reader that is set into a plastic “sleeve”. This custom made “sleeve” is fitted over the slot that the credit or debit card is inserted into, and is designed to look like part of the ATM. The skimmer will record and store the details of each card that is inserted into the ATM, until the organisers remove the skimmer and extract the data.

16 “Don’t let credit card skimmers swipe your cash”, Anthony Hughes, *Sydney Morning Herald*, 13 November 2002 (accessed at <http://www.smh.com.au> on 17 June 2003); “Credit skim flicks for a dirty game in the cards”, Ian Hamilton, *The Weekend Australian*, Business News p. 25.

17 “Credit skim flicks for a dirty game in the cards”, Ian Hamilton, *The Weekend Australian*, Business News p. 25.

18 Skimmers found in Adelaide were designed to store details of up to 40 cards. “Thieves with a new calling card”, Lee Jeloseck, *Adelaide Advertiser*, 23 November 2002, p. 36.

19 “Laws to deter ATM thieves”, *Daily Telegraph*, 17 February 2003, p. 5.

Once the card details have been skimmed, the person or group will require equipment to access the data stored in the skimmer and to either re-store this data onto another magnetic strip (on a counterfeit credit card) or to transmit the data overseas.

Part 2:—Existing laws relating to “skimming”

Difficulties in combating skimming

Credit and debit card skimming has emerged as a significant law enforcement issue as a result of rapidly changing technology. There are already a wide range of modalities of skimming and related activities. With further technological developments, it is almost certain that new forms of skimming will emerge. The potential for rapidly changing modes of criminal activity poses a significant challenge in drafting offences that will not become “outdated” as the technology and activities develop.

Even existing modes of skimming are likely to pose challenges for enforcement of current laws. The credit card owner is often not aware that any crime has been committed until the fraudulent purchases either show up on their credit card statement or exceed their credit limit. Where the credit card data is sent overseas and used to commit fraud abroad, the time taken to detect the offence can be even longer due to the time required for the credit card companies and/or financial institutions to process overseas transactions. Making the fraudulent purchases overseas can also further complicate enforcement of existing offences.

Relationship between skimming and existing offences

While a range of existing offences will cover many of the activities related to credit and debit card skimming, it is unlikely that any of these comprehensively cover the act of skimming itself. The application of ordinary criminal offences such as fraud and forgery to acts related to credit card skimming is aided by the definition of “document” in most jurisdictions. In most jurisdictions, “document” has been defined to include magnetic records, such as computer discs, and will include the information contained on the magnetic strip of a credit card. Forgery offences criminalise forging of such a “document”.

There is currently no law prohibiting importation of a skimming device. Magnetic strip readers are imported into Australia for a wide range of legitimate purposes under a number of import classes. Skimming devices are very closely related to legitimate magnetic strip readers, indeed some skimmers have been converted from magnetic strip readers. Prohibiting the import of skimming devices would be administratively complicated and difficult to enforce efficiently, and would not prevent the domestic manufacture of skimming devices or the conversion of legitimate magnetic strip readers into skimming devices in Australia. While the import (or export) of skimming devices is not prohibited, it is prohibited to import or export counterfeit credit, debit or charge cards.²⁰

²⁰ Unless permission is granted in writing by the Minister, for example where the counterfeit cards are required for training purposes. Regulation 4T of the *Customs (Prohibited Imports) Regulations 1956* and regulation 13D of the *Customs (Prohibited Exports) Regulations 1958*.

While no law specifically prohibits possession of a skimming device, s. 16.7 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, amongst other offences, obtaining property by deception. This is a preparatory offence, which is committed well before an attempt to commit the principal offence (theft, robbery, burglary or other related offences) has occurred. This section could be used to prosecute possession of a skimming device in some circumstances, however it may be difficult to prove the required intent that the device be used in connection with fraud.²¹ While this section does not extend to possession of the device intending to use it in connection with forgery, s. 19.6 of the Model Criminal Code criminalises making or possessing a device for making a false document.²²

The creation of a counterfeit credit card using skimmed data is likely to be covered by existing Commonwealth, State and Territory forgery offences. A counterfeit credit card made using skimmed data will be a false document for the purposes of s. 19.2 of the Model Criminal Code. Persons who manufacture such a counterfeit credit card will be guilty of making a false document (s. 19.3) provided that they did so intending that a person would dishonestly use the counterfeit credit card to obtain a gain. This will apply in almost all cases (except, for example, if counterfeit credit cards were being manufactured for the purpose of training exercises). The offences of using or possessing a false document (ss. 19.4 and 19.5) could also apply in many cases.

Section 19.6 of the Model Criminal Code goes further, and criminalises possession of a device for making false documents. This provision will cover the possession of blank credit cards,²³ and it is likely that a skimmer will also be considered to be a device “designed or adapted for the making of a false document”. The offence requires that the accused knows “that the device is so designed or adapted”. If the prosecution is also able to prove an intent that the device be used by the accused or another person to commit forgery, then the penalty is substantially more severe.

Similarly, the use of a counterfeit credit card based on skimmed data to purchase goods in Australia or obtain any other financial advantage is likely to constitute fraud under existing Commonwealth, State and Territory offences. In developing the fraud offences in the Model Criminal Code, MCCOC specifically provided for fraud being perpetrated on computers or

21 MCCOC makes it clear that the prosecution must prove that the person intended to use the article for theft or a related offence. However MCCOC notes that “Where it can be shown that an article is made or adapted for [a relevant offence] that will be evidence from which inferences can be drawn that the defendant has the article for that purpose.” *MCCOC Final Report on Chapter 3 - Theft, Fraud, Bribery and Related Offences* (Dec 1995), p. 103.

22 See below. See also s. 474 of the *WA Criminal Code*, discussed below.

23 *MCCOC Final Report on Chapter 3 - Theft, Fraud, Bribery and Related Offences* (Dec 1995), p. 249.

machines. Section 17.1(b) of the MCC is also designed to catch a person who dishonestly uses another person's credit card to obtain money from an ATM.²⁴ This would obviously also extend to catch a person who uses a counterfeit copy of another person's credit or debit card to obtain money from an ATM.

In developing the fraud offences in the Model Criminal Code, MCCOC recognised that there were potential difficulties in using conventional fraud offences for some instances of credit card fraud. These difficulties arise in cases where a person presents a credit card that they are not authorised to use (for example, because it is stolen or because its authority has been revoked). Arguments have been put that the deception (that the person is entitled to use the credit card) does not cause the merchant to hand over the goods because the merchant knows that they will be paid by the credit card company regardless of whether the person producing the card is authorised to do so.²⁵ These arguments are likely to carry less weight in cases of credit card skimming, as it is less likely that a merchant would hand over the goods if they knew that the card was counterfeit. Therefore the deception (the representation that the credit card is a valid credit card that the person producing it is authorised to use) is more likely to have caused the merchant to hand over the goods.

However these general offences do not cover the act of skimming the data, the possession of skimmed data or the possession of a skimming device. The key weakness in these offences is that law enforcement agencies cannot act against the skimming until a further offence has been committed. This poses particular problems given that much of the data that is skimmed in Australia is sent overseas, and that the crimes of forgery and fraud are likely to be committed outside of Australia.

If the act of forgery or fraud is committed in Australia, then the person who skimmed the data is likely to be guilty of aiding and abetting the commission of that offence. However the aiding and abetting provisions are not well suited for combating credit card skimming as they require the authorities to wait for the principal offence to be committed - they can only be used to prosecute the skimming after the skimmed data has been used to commit forgery or fraud. In some cases, the organiser of the credit card skimming may care little whether the skimmer is prosecuted once they have reaped the benefit of the skimmed data through its fraudulent use. Further, State and Territory aiding and abetting provisions are unlikely to be able to be used to prosecute the act of skimming where the fraud or forgery is committed

24 MCCOC Final Report on Chapter 3 - Theft, Fraud, Bribery and Related Offences (Dec 1995), p. 139.

25 These arguments and the counter-arguments are set out in MCCOC Final Report on Chapter 3 - Theft, Fraud, Bribery and Related Offences (Dec 1995), pp. 139-41.

overseas, especially as there may be difficulties in proving the commission of the ultimate offence and the necessary link between the acts of the skimmer and the commission of that offence in such cases.

Attempted fraud or forgery does not require the principal offence to be committed. But skimming of credit card data is unlikely to constitute attempted forgery or fraud as the act of skimming credit card data is unlikely to be more than preparatory to the commission of fraud or forgery.²⁶ It is also doubtful whether many skimmers would have intention with regard to each physical element of the principal offence, especially in cases where an organised group pays employees of service stations or other high-risk industries to skim cards and the group then commits the fraud or forgery. While the employee who skimmed the credit cards may be reckless regarding the use of the data, recklessness is not sufficient in cases of attempt. Where the principal offence is to be committed overseas, and would not be an offence against any Australian law, this poses further problems for prosecuting attempts in Australia.

Where such organised groups are involved in skimming the conspiracy to commit fraud, or the specific offence of conspiracy to defraud, are likely to apply. The use of a specific conspiracy to defraud offence would simplify the prosecution of such offences. The Model Criminal Code conspiracy to defraud offence requires only dishonesty, rather than also deception,²⁷ and can be based on an intention only to obtain a gain, rather than requiring proof of intention to cause a loss. Conspiracy will be made out in many cases where there is an agreement by the skimmer and at least one other person and each party intended that forgery or fraud would be committed pursuant to the agreement. While the act of skimming is unlikely to constitute an act which is more than merely preparatory for the purposes of attempt, it will constitute an “overt act” for the purposes of conspiracy. The difficulty in using conspiracy to defraud in skimming cases is that it requires proof of the agreement, and it will not always catch individual operators.

In addition to the general fraud and forgery offences that could be applied to some instances of skimming and related activities (either directly or through various principles of extended liability) other specific offences may apply to certain instances of credit card skimming.

If skimming is perpetrated by interception of credit and debit card information from data cables between a commercial premises and a financial institution, then this is likely to constitute an offence under the *Telecommunications (Interception) Act 1979 (Cth)* or Part VIIB of the *Crimes Act 1914 (Cth)* (telecommunications offences).

26 LBC *Laws of Australia* cites the case of *R v Lobreau* (1988) 67 CR(3d) 74 (CA Alta), where making an impression of an ignition key was not sufficient to constitute attempted stealing.

27 MCCOC has expressed concerns over the application of fraud offences to credit card fraud due to possible problems with proving that the deception caused the gain or loss - see note 25 above.

Section 7(1) of the *Telecommunications (Interception) Act* prohibits any person from intercepting, or enabling any person to intercept, any communication passing over a telecommunications system. Section 105 makes contravention of section 7(1) an offence punishable by imprisonment for up to 2 years.

Section 85ZK of the *Crimes Act* makes it an offence to connect equipment to a telecommunications network with the intention of using it in relation to an offence against Commonwealth, State or Territory law. Therefore to connect equipment to a telecommunications network to intercept credit card information intending to use that information to commit forgery or fraud would be an offence. Section 85ZKB prohibits the possession of devices that a person knows can be used to enable a person to intercept communications passing over a telecommunication system. The maximum penalty for each of these offences is imprisonment for 5 years.

Whether these offences apply will largely depend on the nature of the data cable or network from which the data was intercepted or “skimmed” - the offences will only apply where the cable constituted part of a telecommunications system or telecommunications network.²⁸

In contrast, the existing computer offences (Model Criminal Code Part 4.2; Commonwealth Criminal Code Part 10.7) do not extend to most internet-based skimming techniques such as “spoofing”, as the fraud is committed through computers rather than by unauthorised access to or modification of legitimate computer data.

The need for a skimming offence

It has been suggested that Australia is lagging behind the big credit card markets in the region, Japan, South Korea, Taiwan and Malaysia, in adopting chip-based “smart cards” (to replace magnetic strips). As chip-based cards

28 s. 5 of the *Telecommunications (Interception) Act 1979* defines:

telecommunications network means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication.

telecommunications service warrant means a warrant issued or to be issued under section 9, 11A, 45, 46 or 48.

telecommunications system means:

(a) a telecommunications network that is within Australia; or

(b) a telecommunications network that is partly within Australia, but only to the extent that the network is within Australia;

and includes equipment, a line or other facility that is connected to such a network and is within Australia.

are considered much less susceptible to skimming and related fraud, some analysts fear that skimming could continue to increase in Australia as Australia is seen as an easy target.²⁹

Even if Australia does introduce “smart cards”, while such technological advances may make skimming more difficult, it may be a solution that is vulnerable to more sophisticated advances in skimming technology and techniques. New skimming techniques (such as tapping telephone or inserting a bug into an EFTPOS terminal to obtain data without a second “swipe” of the card) have been seen overseas, and further modes of activity are likely to emerge in the future.

As discussed above, many of the activities related to credit card skimming are covered by existing offences. However the act of skimming itself is not. A specific credit card skimming offence would allow the act of skimming to be prosecuted without authorities being forced to wait for a further offence, such as forgery or fraud, to be committed. This will also allow prosecution of skimming in Australia where the further offence is committed, or is intended to be committed, outside Australia.

Current skimming offences

A number of jurisdictions in Australia have already developed, or are developing, offences aimed at identity fraud or other specific offences that could be used to target credit card skimming.

In addition to offences of fraud (s. 409) and forgery and uttering (s. 473), the WA Criminal Code contains the offence of preparation for forgery etc. (s. 474):

- (1) Any person who makes, adapts or knowingly has possession of any thing under such circumstances as to give rise to a reasonable suspicion that it has been, or is being, made, adapted or possessed for a purpose that is unlawful under section 473 is guilty of a crime and is liable to imprisonment for 3 years.

Summary conviction penalty: Imprisonment for 18 months or a fine of \$6 000.

While this offence would likely criminalise possession of a skimming device, or adaptation of a commercial magnetic strip reader for the purposes of skimming, it does not criminalise the act of skimming itself. In some

²⁹ “Danger in smart card lag”, Caitlin Fitzsimmons, *The Australian*, 4 March 2003, Computer p. 27; “Smart cards on the way as credit fraud increases”, Karen Dearne, *The Australian*, 20 May 2003, Computer p. 10. VISA International estimates that chip-based “smart cards” would spot about 70% of skimming - “Credit card fraudsters hit tourist spots”, Tanya Moore, *The Courier Mail*, 17 May 2003 (accessed at <http://www.couriermail.news.com.au> on 17 June 2003).

circumstances it may be difficult to prove the required reasonable suspicion that the item is possessed or adapted for the purposes of forgery. There may also be difficulties in using this section if the accused claimed that they did not intend to create a counterfeit credit card or other forged record, but instead had intended to use the credit card data to purchase goods over the phone or Internet (without the need for a physical forged record).

Recent amendments to the *Criminal Law Consolidation Act (SA)* have created offences relating to dishonest dealings with documents and dishonest manipulation of machines.³⁰ New section 140 focuses on the creation, possession and use of false documents. Section 140(6)³¹ criminalises possession of an article for creating a false document or falsifying a document. It is likely that possession of a skimming device would be criminalised by this section.

Section 141³² criminalises a person dishonestly manipulating, or dishonestly taking advantage of a malfunction of, a machine to obtain a benefit or cause a detriment. While this section appears to be more relevant to the use of a counterfeit credit card at an ATM,³³ this section might also be used to prosecute persons who manipulate an ATM or EFTPOS terminal to record the details of each card that is used at the terminal and allow the person to retrieve those details at a later time.

South Australia has introduced identity theft offences which criminalise credit card skimming as a form of identity theft. The South Australian legislation is discussed further in Part 3 of this discussion paper.

The United States and Canada also consider credit card skimming to be a form of identity theft. In their joint *Special Report for Consumers on Identity Theft*, the US Department of Justice and the Solicitor General of Canada define identity theft as where “someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically

30 The amendments were made by the Criminal Law Consolidation (Offences Of Dishonesty) Amendment Act 2002 (SA).

31 **Dishonest dealings with documents**

140. ...

(6) A person who has, in his or her possession, without lawful excuse, any article for creating a false document or for falsifying a document is guilty of an offence.

Maximum penalty: Imprisonment for 2 years.

32 **Dishonest manipulation of machines**

141. (1) A person who dishonestly manipulates a machine in order to-

(a) benefit him/herself or another; or

(b) cause a detriment to another,

is guilty of an offence.

Maximum penalty: Imprisonment for 10 years.

33 In this regard s. 141 is similar in effect to clause 17.1(b) of the Model Criminal Code.

for economic gain.”³⁴ “Skimming” is then listed as one common example of how identity theft occurs, effectively being characterised as stealing the “credit identity” of a person.

In 1998 the US amended Title 18 of the U.S.C., s. 1028 (Fraud and related activity in connection with identification documents and information),³⁵ to create an offence where a person:

“knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law”

The section defined “means of identification” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual”, including a “unique electronic identification number”, which could include credit card information.

Section 1029 (Fraud and related activity in connection with access devices) is also relevant to credit card skimming. The definition of access device³⁶ would encompass credit or debit cards. The section creates offences where a person:

- knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;³⁷
- knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;³⁸ or
- without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of selling information regarding an access device.³⁹

The first of these offences would cover the production, use or trafficking in counterfeit credit cards. The second offence would cover possession of a

34 Special Report for Consumers of Identity Theft

35 The amending law was the *Identity Theft and Assumption Deterrence Act*.

36 s. 1029(e)(1) - “the term ‘access device’ means any **card**, plate, **code**, account number, electronic serial number, mobile identification number, **personal identification number**, or other telecommunications service, equipment, or instrument identifier, or other means of account access **that can be used**, alone or in conjunction with another access device, **to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);**” (emphasis added)

37 s. 1029(a)(1)

38 s. 1029(a)(4)

39 s. 1029(a)(6)(B)

skimmer, if the prosecution was able to prove that the person knew that the device was a skimmer and possessed the skimmer with intent to defraud.⁴⁰ The third offence may cover a person who sold skimmed information to another person (usually for the purpose of creating a counterfeit credit card).

Section 1030 (Fraud and related activity in connection with computers) of the same part of the US Code creates a further offence where a person:

“intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information contained in a financial record of a financial institution, or of a card issuer”.

In addition to the federal laws, various US states also have a wide range of laws relating to identity theft or fraud.⁴¹

In contrast to the US approach of general identity theft offences distinguished by the means of the fraud or theft, Canada has enacted specific offences dealing with theft and forgery of credit cards. The definition of “credit card” in the Canadian Criminal Code includes both credit cards and debit cards issued for use at ATMs and EFTPOS terminals, however it does not appear to include stored value cards.

The key offence provisions in the Canadian Criminal Code are:

s. 342.

Theft, forgery etc., of credit card

- (1) Every person who
 - (a) steals a credit card,
 - (b) forges or falsifies a credit card,
 - (c) possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered
 - (i) by the commission in Canada of an offence, or
 - (ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence, or
 - (d) uses a credit card knowing that it has been revoked or cancelled,

⁴⁰ s. 1029(e)(6) - “the term ‘*device-making equipment*’ means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.” This definition would include a skimmer as a skimmer is equipment designed primarily for making a counterfeit access device (counterfeit credit card).

⁴¹ An index of these laws is contained at <http://www.consumer.gov/idtheft/statelaw.htm>

is guilty of

- (e) an indictable offence and is liable to imprisonment for a term not exceeding ten years, or
- (f) an offence punishable on summary conviction.

...

Unauthorized use of credit card data

- (3) Every person who, fraudulently and without colour of right, possesses, uses, traffics in or permits another person to use credit card data, whether or not authentic, that would enable a person to use a credit card or to obtain the services that are provided by the issuer of a credit card to credit card holders is guilty of
 - (a) an indictable offence and is liable to imprisonment for a term not exceeding ten years; or
 - (b) an offence punishable on summary conviction.
- (4) In this section, “traffic” means, in relation to a credit card or credit card data, to sell, export from or import into Canada, distribute or deal with in any other way.

s. 342.01

Making, having or dealing in instruments for forging or falsifying credit cards

- (1) Every person who, without lawful justification or excuse,
 - (a) makes or repairs,
 - (b) buys or sells,
 - (c) exports from or imports into Canada, or
 - (d) possesses

any instrument, device, apparatus, material or thing that the person knows has been used or knows is adapted or intended for use in forging or falsifying credit cards is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Section 342(1) deals with the creation and use of counterfeit credit cards. While this is more specific than current forgery and fraud offences in Australia (for example it specifically criminalises use of a cancelled or revoked credit card and criminalises possession of a counterfeit credit card), its coverage is similar.

Sections 342(3) and 342.01, however, deal directly with credit card skimming. The criminalisation of the possession of credit card data (fraudulently and without colour of right) would effectively criminalise the act of credit card skimming once that act had been completed. The criminalisation of possession of any instrument or device knowing that it is adapted or intended for use in forging or falsifying credit cards (s. 342.01(d)) will criminalise the possession of a skimming device. Its scope is similar to 18 U.S.C. s.1029(a)(4) and s. 474 of the WA Criminal Code. Indeed, the Canadian provision is less stringent than the WA provision, as the WA provision only requires “reasonable suspicion” that the device is adapted or possessed for the purposes of forgery whereas the Canadian provision requires proof that the person knows that the device is intended or adapted for use in forging or falsifying credit cards.

Part 3: Creating new skimming offences

Is “skimming” an example of fraud or identity theft?

Given the range of activity that can constitute skimming, or is closely related to skimming, a key challenge in developing offences is identifying precisely what scope of conduct is to be criminalised. The definition of credit card skimming suggested above was “the process by which legitimate credit card data is illicitly captured or copied, usually by electronic means”. However the subsequent examination of activities related to skimming reveals a wider range of activities, including identity theft.

Identity theft (a subset of identity fraud and identity crime) is generally considered to refer to the theft and use of personal identifying information of an actual person, as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of persons either living or dead.⁴²

South Australia has enacted the only legislation to date in Australia which addresses identity theft. The *Criminal Law Consolidation (Identity Theft) Act 2003* (SA) (‘the Identity Theft Act’) (**Appendix A**) has amended the Criminal Law Consolidation Act 1935 (SA) to create new identity theft offences.

The model credit card skimming offence has been drafted for inclusion in Part 3.3 of the Model Criminal Code which deals with Fraud. From one point of view, the activity of credit and debit card skimming is simply another fraud related offence. The additional model offence specifically targeting credit card skimming is required because of the new technologies used to facilitate this type of fraud and because of the essentially preparatory nature of the activity.

However, the Committee has considered the question of whether credit card skimming could be more effectively addressed as an aspect of identity theft. The Identity Theft Act adopts this approach, criminalising credit card skimming as part of broader provisions on the topic of identity theft. The Committee acknowledges that there may be significant advantages in comprehensively dealing with all activities involving the unauthorised use of personal identifying information (including financial information) in a single set of model offences. As an alternative option to the model credit card skimming offence and to encourage public discussion of these issues, the Committee has included the provisions of the Identity Theft Act and a commentary on the provisions at **Appendix A**.

⁴² This definition is adopted in the National Crime Prevention Program publication, *How to prevent and respond to identity theft* (2004), available online at <http://www.crimeprevention.gov.au>

The Identity Theft Act creates a number of offences involving the assumption of a false identity (or falsely pretending to have particular qualification or have, or be entitled to act in, a particular capacity), the use of personal identification information, and the production and possession of prohibited material.

The model credit card skimming offence

The model credit card skimming offence is an attempt to address credit and debit card skimming separately from the broader issue of identity theft although the offence may capture some aspects of identity theft activity.

The model offence criminalises dishonestly obtaining or dealing in 'personal financial information' without the consent of the person to whom the information relates. 'Personal financial information' is defined broadly 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.

One of the most pressing questions for the Committee to address was the appropriate fault element to apply to the model offence, as the model offence is essentially a preparatory offence. In developing the model offence, the Committee weighed the risk of inadvertently criminalising innocent activities (or activities that ought not 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. 'Dishonest' 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.

This offence is designed to capture all credit and debit card skimming activity and can accommodate changes in technology. Firstly, it is not restricted to physical access to a credit or debit card. This offence would apply, for example, where the credit card data is 'skimmed' remotely, including where a data cable is tapped or Internet 'spoofing' takes place. Secondly, the model offence is not limited to electronic skimming or skimming by some technological device, but covers other methods of illicitly obtaining credit card details (for example from discarded bank statements or receipts).

This offence does not criminalise possession of a skimming device. However, it does criminalise dishonest possession of personal financial information. It is difficult to envisage scenarios where there would be an honest or legitimate use of a skimming device to obtain another person's personal financial information without that person's consent. For this reason, a person's possession of any personal financial information obtained using a skimming device is likely to be a dishonest possession.

Adapting the model offence to identity theft

The Committee notes that this model offence also has the potential to be adapted to the identity theft context. If the term ‘personal financial information’ were replaced by ‘personal identification information’ this offence could capture a broad range of identity theft activities.

‘Personal identification information’ could again be defined in broad and technologically neutral terms to mean “information relating to a person that may be used (whether alone or in conjunction with other information) to identify the person.”

If this offence were to be adapted in this way, this offence would criminalise dishonest dealings with ‘personal identification information’ with the absence of the person’s consent.

However, arguably such an offence would not cover all aspects of identity theft activity. For example, it would not cover the situation where a person pretends to be qualified as a doctor and engages in this pretence without the use of another person’s ‘personal identification information.’

The offence of assumption of a false identity in the Identity Theft Act would capture this activity, provided the person pretended to be a doctor intending by doing so to commit, or to facilitate the commission of, a serious criminal offence.

Chapter 3 Theft, fraud, blackmail, forgery, bribery and related offences - continued

Part 3.3 Fraud - continued

3.3.5 Credit card skimming and related offences

(1) In this section:

personal financial information means 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.

(2) A person who dishonestly obtains or deals in personal financial information without the consent of the person to whom it relates is guilty of an offence.

Maximum penalty: imprisonment for 5 years.

(3) For the purposes of this section:

(a) obtaining personal financial information includes possessing or making any such information, and

(b) dealing in personal financial information includes supplying or using any such information.

(4) For the purposes of this section, a person is taken to obtain or deal in personal financial information without the consent of the person to whom it relates if the consent of the person is obtained by any deception.

(5) This section extends to personal financial information relating to a natural person or a body corporate, or to a living or dead person.

Section 14.2 of the Model Criminal Code

Dishonesty

14.2 (1) In this Chapter, “**dishonest**” means dishonest according to the standards of ordinary people and known by the defendant to be dishonest according to the standards of ordinary people.

(2) In a prosecution for an offence, **dishonesty** is a matter for the trier of fact.

Note: Section 15.2 affects the meaning of dishonesty in offences related to theft and section 17.2(3) affects the meaning of dishonesty in the offences of obtaining property or a financial advantage by deception. See also section 9.5 (Claim of right).

Part 3.3. Fraud - continued

3.3.5 Credit card skimming and related offences

3.3.5(1) defines ‘personal financial information’ to cover all 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.

Adopting a definition of ‘personal financial information’ which does not refer to technological devices or the physical credit or debit card ensures that this model offence will not be overtaken by developments in technology.

‘Personal financial information’ extends beyond the physical credit and debit cards to include account numbers or credit card numbers which could be used, for example, to order goods over the telephone or to withdraw money over the counter at a bank from a savings account (in conjunction with falsifying a person’s signature).

‘Personal financial information’ would also include any data captured from a credit or debit card, including information captured by bugging an ATM. In addition, it would include a person’s user identification name or number and password for access to Internet banking services.

3.3.5(2) criminalises dishonestly dealing with personal financial information without the consent of the person to whom it relates. The fault element of ‘dishonesty’ is described in section 14.2 of Chapter 3 of the Model Criminal Code. ‘Dishonest’ means dishonest according to the standards of ordinary people and known by the defendant to be dishonest by the standards of ordinary people.

For the purposes of the offence in 3.3.5(2), it does not matter whether the information is to be used to manufacture counterfeit credit cards, to obtain money from ATMs, to purchase goods over the phone or internet or for any other fraudulent purpose - the details of this final use do not change the nature of the act of dishonestly dealing in the personal financial information without the consent of the person to whom it relates.

Once again, it is important to note that this offence can accommodate changes in technology as it focuses on criminalising the dishonest dealing in personal financial information and does not refer to the specific means by which that information is obtained.

A maximum penalty of 5 years imprisonment is the recommended penalty.

Chapter 3 Theft, fraud, blackmail, forgery, bribery and related offences - continued

Part 3.3 Fraud - continued

3.3.5 Credit card skimming and related offences

(1) In this section:

personal financial information means 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.

(2) A person who dishonestly obtains or deals in personal financial information without the consent of the person to whom it relates is guilty of an offence.

Maximum penalty: imprisonment for 5 years.

(3) For the purposes of this section:

(a) obtaining personal financial information includes possessing or making any such information, and

(b) dealing in personal financial information includes supplying or using any such information.

(4) For the purposes of this section, a person is taken to obtain or deal in personal financial information without the consent of the person to whom it relates if the consent of the person is obtained by any deception.

(5) This section extends to personal financial information relating to a natural person or a body corporate, or to a living or dead person.

Section 14.2 of the Model Criminal Code

Dishonesty

14.2 (1) In this Chapter, “**dishonest**” means dishonest according to the standards of ordinary people and known by the defendant to be dishonest according to the standards of ordinary people.

(2) In a prosecution for an offence, **dishonesty** is a matter for the trier of fact.

Note: Section 15.2 affects the meaning of dishonesty in offences related to theft and section 17.2(3) affects the meaning of dishonesty in the offences of obtaining property or a financial advantage by deception. See also section 9.5 (Claim of right).

3.3.5(3) clarifies that ‘obtaining’ personal financial information include possessing or making any such information, and ‘dealing’ in personal financial information includes supplying or using any such information.

In criminalising both obtaining and dealing in personal financial information without the consent of the person to whom it relates, the model offences cover the situation where the victim consented to a first person obtaining his or her personal financial information but did not consent to the subsequent supply of that information by the first person to a second person.

3.3.5(4) provides that a person obtains or deals in personal financial information without the consent of the person to whom it relates if the consent of the person is obtained by any deception.

This provision is particularly relevant to the problem of ‘mirror’ or ‘ghost’ bank websites and ‘spoofing’. This provision would cover, for example, the scenario where a person acquires another person’s password and user identification name for Internet banking by sending an email request for the details which purports to be an email from the other person’s bank.

Section 17.1 of the Model Criminal Code would apply to section 3.3.5(4).

This section defines ‘deception’ broadly as any deception, by words or other conduct, as to fact or law. ‘Deception’ includes a deception as to the intentions of the person using the deception or any other person, and 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.

For example, section 3.3.5(4) would cover the situation where the victim consented to his or her personal financial information being stored on a secure computer system and that information was obtained by a person who was unauthorised to have access to that computer system.

3.3.5(5) clarifies that these offences cover personal financial information relating to both an individual and a body corporate. It also extends the coverage of the offences to personal identification information of a dead person. For example, this offence would apply where a person, knowing of the death of a second person, intercepted the delivery of an ATM card and password to the person, and then used that data to access funds in the deceased person’s savings account.

Appendix A

South Australia

Criminal Law Consolidation (Identity Theft) Amendment Act 2003

An Act to amend the *Criminal Law Consolidation Act 1935* and to make a related amendment to the *Criminal Law (Sentencing) Act 1988*.

Contents

Part 1-Preliminary

- 1 Short title
- 2 Commencement
- 3 Amendment provisions

Part 2-Amendment of Criminal Law Consolidation Act 1935

- 4 Insertion of Part 5A

Schedule 1-Related amendment

The Parliament of South Australia enacts as follows:

Part 1-Preliminary

- 1 Short title
This Act may be cited as the *Criminal Law Consolidation (Identity Theft) Amendment Act 2003*.
- 2 Commencement
This Act will come into operation on a day to be fixed by proclamation.
- 3 Amendment provisions
In this Act, a provision under a heading referring to the amendment of a specified Act amends the Act so specified.

Part 2-Amendment of Criminal Law Consolidation Act 1935

4 Insertion of Part 5A

After Part 5 insert:

Part 5A-Identity theft

144A Interpretation

In this Part-

criminal purpose means the purpose of committing, or facilitating the commission of, an offence;

digital signature means encrypted electronic or computer data intended for the exclusive use of a particular person as a means of identifying himself or herself as the sender of an electronic communication;

electronic communication means a communication transmitted in the form of electronic or computer data;

false identity a person assumes a false identity if the person pretends to be, or passes himself or herself off as, some other person;

The other person may be-

- (a) living or dead;
- (b) real or fictional;
- (c) natural or corporate.

personal identification information a person's personal identification information is information used to identify the person, and includes

- (a) in the case of a natural person-
 - (i) information about the person such as his or her name, address, date or place of birth, marital status, relatives and so on;
 - (ii) the person's driver's licence or driver's licence number;
 - (iii) the person's passport or passport number;
 - (iv) biometric data relating to the person;
 - (v) the person's voice print;
 - (vi) the person's credit or debit card, its number, and data stored or encrypted on it;

The *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA) inserted Part 5A into the *Criminal Law Consolidation Act 1935* (SA) ('the Act') creating a number of offences involving the assumption of a false identity (or falsely pretending to have particular qualification or have, or be entitled to act in, a particular capacity), the use of personal identification information, and the production and possession of prohibited material.

Appendix A

- (vii) any means commonly used by the person to identify himself or herself (including a digital signature);
- (viii) a series of numbers or letters (or a combination of both) intended for use as a means of personal identification;
- (b) in the case of a body corporate-
 - (i) its name;
 - (ii) its ABN;
 - (iii) the number of any bank account established in the body corporate's name or of any credit card issued to the body corporate;

prohibited material means anything (including personal identification information) that enables a person to assume a false identity or to exercise a right of ownership that belongs to someone else to funds, credit, information or any other financial or non-financial benefit;

serious criminal offence means-

- (a) an indictable offence; or
- (b) an offence prescribed by regulation for the purposes of this definition;

voice print means computer data recording the unique characteristics of a person's voice.

144B False identity etc

- (1) A person who-
 - (a) assumes a false identity; or
 - (b) falsely pretends-
 - (i) to have particular qualifications; or
 - (ii) to have, or to be entitled to act in, a particular capacity,
- makes a false pretence to which this section applies.
- (2) A person who assumes a false identity makes a false pretence to which this section applies even though the person acts with the consent of the person whose identity is falsely assumed.

Section 144A of the Act defines key terms including ‘false identity’ ‘personal identification information’ and ‘prohibited material’.

A person assumes a false identity if the person pretends to be, or passes himself or herself off as, some other person, regardless of whether that other person is living or dead, real or fictional, or an individual or body corporate.

‘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. ‘Personal identification information’ is specifically defined to include ‘the person’s credit or debit card, its number, and data stored or encrypted on it.’ In relation to 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 broad definition of ‘personal identification information’ again raises the question of whether the concept of identity theft should have any application to credit card skimming. It is arguable that the definition of ‘personal identification information’ fails to distinguish between fundamental aspects of a person’s identity (such as a person’s name, date of birth and biometric data) and other information used to identify a person. Information such as a person’s name, date of birth and fingerprints clearly constitute key aspects of a person’s identity. However, it is much more problematic to describe information (such as a password) which identifies a person for the purpose of the person accessing his or her funds as an aspect of the person’s identity.

Another argument for distinguishing credit card skimming from identity theft relates to the purpose or motive of the person engaging in the activity. 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, especially where the activity involves stalking the victim, may be to cause distress and anxiety to the victim or to intimidate the victim.

Section 144A defines ‘prohibited material’ as anything (including personal identification information) that enables a person to assume a false identity or to exercise a right of ownership that belongs to someone else to funds, credit, information or any other financial or non-financial benefit.

Appendix A

- (3) A person who makes a false pretence to which this section applies intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence is guilty of an offence and liable to the penalty appropriate to an attempt to commit the serious criminal offence.

144C Misuse of personal identification information

- (1) A person who makes use of another person's personal identification information intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence, is guilty of an offence and liable to the penalty appropriate to an attempt to commit the serious criminal offence.
- (2) This section applies irrespective of whether the person whose personal identification information is used-
 - (a) is living or dead; or
 - (b) consents to the use of the personal identification information.

144D Prohibited material

- (1) A person who
 - (a) produces prohibited material; or
 - (b) has possession of prohibited material,intending to use the material, or to enable another person to use the material, for a criminal purpose is guilty of an offence.
Maximum penalty: Imprisonment for 3 years.
- (2) A person who sells (or offers for sale) or gives (or offers to give) prohibited material to another person, knowing that the other person is likely to use the material for a criminal purpose is guilty of an offence.
Maximum penalty: Imprisonment for 3 years.
- (3) A person who is in possession of equipment for making prohibited material intending to use it to commit an offence against this section is guilty of an offence.
Maximum penalty: Imprisonment for 3 years.

144E Attempt offence excluded

A person cannot be convicted of an attempt to commit an offence against this Part.

Section 144B makes it an offence for a person to assume a false identity (or falsely pretend to have particular qualification or have, or be entitled to act in, a particular capacity), intending by doing so to commit, or to facilitate the commission of, a serious offence.

Section 144C makes it an offence for a person to make use another person's personal identification information, intending by doing so to commit, or to facilitate the commission of, a serious offence.

The offences in sections 144B and 144C criminalise aspects of identity theft as preparatory to the commission of another 'serious criminal offence' (either by the person who commits the identity theft or by another person). In recognition of the preparatory nature of these offences, the penalty applicable to each is "the penalty appropriate to an attempt to commit the serious criminal offence".

While these offences cover a broad range of identity theft activities preparatory to the commission of a serious offence, it is arguable that the complex fault element of 'intention to commit or facilitate the commission of a serious offence' will make it difficult to secure convictions for these offences. The Committee has adopted the fault element of 'dishonesty' in drafting the model credit card skimming offence in an attempt to avoid the problems associated with proving a person's intention to commit a further offence such as fraud or forgery.

In criminalising aspects of identity theft, the offences in sections 144B and 144C of the Act also cover aspects of credit card skimming. Assumption of a false identity is likely to cover a person who presents a counterfeit credit card with the intention of committing a fraud. Making use of another person's personal identification information is a broader concept, and would cover conduct earlier in the process. It is likely to cover the creation of a counterfeit credit card, and the selling (or possibly transmission of) skimmed credit card data. It is open to question whether skimming of credit card data would constitute "makes use of", however it is unlikely that mere possession of skimmed data would qualify. In each case, it must be proved that the making use of the data was done intending to commit or facilitate the commission of a serious offence.

Even if the offence of misuse of personal identification information does not cover skimming data or possession of skimmed data, these aspects are criminalised by section 144D which creates offences relating to prohibited material.

Section 144D(1) criminalises production or possession of prohibited material where the person intends to use (or enable another person to use) that material for a criminal purpose. Given the broad definition of 'prohibited material', this offence would covers both skimming of credit card data and possession of skimmed data where the intent for that data to be used for a criminal purpose can be proved.

Appendix A

144F Application of Part

This Part does not apply-

- (a) to misrepresentation by a person under the age of 18 years for the purpose of-
 - (i) obtaining alcohol, tobacco or any other product not lawfully available to persons under the age of 18; or
 - (ii) gaining entry to premises to which access is not ordinarily allowed to persons under the age of 18; or
- (b) to any thing done by a person under that age to facilitate such a misrepresentation.

Schedule 1-Related amendment

Part 1-Preliminary

1 Amendment provisions

In this Schedule, a provision under a heading referring to the amendment of a specified Act amends the Act so specified.

Part 2-Amendment of Criminal Law (Sentencing) Act 1988

2 Insertion of section 54

After section 53 insert:

54-Certificate for victims of *identity theft*

- (1) A court that finds a person guilty of an offence involving
 - (a) the assumption of another person's identity; or
 - (b) the use of another person's personal identification information,may, on application by a victim of the offence, issue a certificate under subsection (2).
- (2) The certificate is to give details of
 - (a) the offence; and
 - (b) the name of the victim; and
 - (c) any other matters considered by the court to be relevant.
- (3) In this section

personal identification information has the same meaning as in Part 5A of the Criminal Law Consolidation Act 1935;

victim means a person whose identity has been assumed, or personal identification information has been used, without the person's consent, in connection with the commission of the offence.

Section 144D(2) criminalises selling or giving prohibited material to another person, knowing that the other person is likely to use the material for a criminal purpose. This provision may prove useful in combating organised skimming groups, where (for example) service station employees are paid for each credit card that they skim - although they may have no intent regarding the final use of the data, a court may be able to infer that, when handing over the credit card data to the organiser of the skimming, they knew that it was likely that the skimmed data would be used for a criminal purpose.

Section 144D(3) criminalises possession of equipment for making prohibited material, intending to use it to commit an offence against sections 144D(1) or (2). A skimming device would be equipment for making prohibited material. This section therefore criminalises possession of any skimming device (or other magnetic reader) if the prosecution can prove intent to use that device to skim, possess or sell credit card data contrary to sections 144D(1) or (2).

In contrast to the “preparatory” nature of the offences in sections 144B and 144C, each of these offences in section 144D are discrete and carry a maximum penalty of imprisonment for 3 years.

Section 144E provides that a person cannot be convicted of an attempt to commit an offence against Part 5A of the Act. This provision appears to be a consequence of adopting the more complex fault element of ‘intention to commit a serious offence’.

Some may be concerned that this provision displaces the law of attempt. In contrast, section 11.1 of the Model Criminal Code would apply to the model credit card skimming offence. This section provides that a person who attempts to commit an offence is guilty of the offence of attempting to commit that offence and is punishable as if the offence attempted had been committed.

Section 144F clarifies that Part 5A does not apply to misrepresentations by a person under the age of 18 for the purpose of obtaining alcohol, tobacco or any other product not lawfully available to persons under that age. It also does not apply to a misrepresentation by a person under the age of 18 for the purpose of gaining entry to premises to which access is not ordinarily allowed to persons under that age.

The *Criminal Law Consolidation (Identity Theft) Amendment Act 2003* (SA) also amended Part 7 (‘Restitution and Compensation’) of 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 for an offence involving the assumption of another person’s identity or the use of another person’s personal identification information. This certificate contains details of the offence, the name of the victim and any other matters the court considers relevant.