IDENTITY FRAUD
THE CAMOUFLAGE OF CHOICE:
CONTROLLING THE CHAMELEON

Master of Arts (Criminal Intelligence)
Charles Sturt University
Faculty of Arts
20th June 2007

Student: Bernadette Beard

Graduate Diploma of Criminal Intelligence
Graduate Certificate in Applied Police Management
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATEMENT OF ORIGINALITY</td>
<td>4</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>5</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>6</td>
</tr>
<tr>
<td>LIST OF GRAPHS AND TABLES</td>
<td>9</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>10</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>10</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>12</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>12</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>15</td>
</tr>
<tr>
<td>HISTORICAL OVERVIEW</td>
<td>15</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>20</td>
</tr>
<tr>
<td>CRIMINAL METHODOLOGY</td>
<td>20</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>25</td>
</tr>
<tr>
<td>COST AND MAGNITUDE</td>
<td>25</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>43</td>
</tr>
<tr>
<td>VICTIM ASSISTANCE AND PREVENTION</td>
<td>43</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>60</td>
</tr>
<tr>
<td>FACILITATION OF TERRORISM</td>
<td>60</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>67</td>
</tr>
<tr>
<td>IDENTITY DOCUMENTS</td>
<td>67</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>83</td>
</tr>
<tr>
<td>BIOMETRICS</td>
<td>83</td>
</tr>
<tr>
<td>CHAPTER 10</td>
<td>101</td>
</tr>
</tbody>
</table>
STATEMENT OF ORIGINALITY

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgement is made in the dissertation. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged.

I agree that this dissertation be accessible for the purpose of study and research in accordance with the normal conditions established by the Executive Director, Library Services or nominee, for the care, loan and reproduction of dissertation.

Bernadette Beard
ACKNOWLEDGEMENTS

Many thanks to Patrick Walsh, my subject Coordinator for your guidance and assistance throughout the completion of this dissertation.

In appreciation of the understanding and patience of my husband who has supported me throughout this period. Without your assistance diverting the attention of our twin babies, I would still be completing this dissertation.
ABSTRACT

Identity crime is one of the most insidious developments of fraud, both as a stand alone activity and in its ability to facilitate other high level criminal activities such as drug trafficking, people smuggling, money laundering and terrorism. The first step in identifying the risk of identity crime to the Australian community is to quantify the extent of the problem. There exists a substantial inadequacy in measuring and understanding the scope, extent and fiscal cost of identity fraud within this country.

This paper is a qualitative research and analysis of a significant breadth of published and unpublished literature including documents, reports and a myriad of inter-related pieces of legislation relating to the issues of identity crime, being both the 'stealing' of a person's identity and the creation of a fictitious identity. In addition, a comparative approach was adopted to examine international trends in identify fraud in order to gauge Australia's progress in dealing with these issues compared to other countries such as the UK, US, and Western European countries with similar cultural and economic values. The author also relied on industry expertise in the subject matter, as a senior police officer responsible for the management of criminal intelligence analysis of fraud within New South Wales.
Only once the true extent and nature of identity crime in Australia is fully comprehended can the most appropriate treatment options, such as biometric identifiers, facial recognition technology, or the introduction of identity cards be thoughtfully considered. As such, it would be prudent for the implementation of a centralised national database on incidents of identity crime. The collection of this information would assist to facilitate an in-depth analysis as to the magnitude of identity crime in Australia.

Other recommendations arising from this paper include: the promotion of victim hardening strategies by government and private sector organisations, the creation of a central register of stolen documents, promoting the sharing of data between law enforcement and government agencies, improving the initial authentication of an individual identity when issuing documents and a standardised legislative approach to identity crime through nationally consistent Commonwealth and State legislation.

The lack of reliable quantitative data available may arguably be the result of a history of governments, and their respective departments, not comprehending the significance of identity theft and identity fraud, resulting in a failure to proactively pursue strategic interdiction policies aimed towards elevating the notion of identity as a major personal and national security imperative.
Now however, there is enough national and international evidence to suggest that this is no longer the case. The establishment of a Commonwealth Government led Commission of Inquiry into the prevalence of identity fraud within Australia, is required in order to facilitate appropriate solutions that balance security, accuracy, privacy, technology and penalty so as to proactively combat this serious organised criminal activity.
LIST OF GRAPHS AND TABLES

Graph 1 - Use of False Identities in Serious Fraud Cases.......................... 29

Graph 2 - Number Of Multiple Identities Used by Offenders..................... 30

Table 2 Types of Non Monetary Harm as Reported to the FTC

(November 1999 to September 2001)................................................................ 49

Table 3 Summary of GAO’s Interviews of Victims........................................... 50

Table 4: List of 25 Countries having suffered most from terrorist attacks since 1986 ........................................................................................................... 62
Identity crime is one of the most pervasive developments of fraud. It encompasses both identity theft, whereby the identity of an individual is ‘stolen’ and subsequently assumed by another, and identity fraud which involves either the creation of a totally fictitious identity or using a combination of ‘real’ and fictitious identifiers to ultimately partake in an illegal activity with the aim of remaining undetected.

It is the enabling abilities of identity crime to facilitate other high level criminal activities such as drug trafficking, people smuggling, money laundering and terrorism that is cause for significant concern, particularly when one considers the ever increasing prevalence of identity crime.

As noted earlier, this paper is a qualitative research and analysis of a significant breadth of published and unpublished literature including documents, reports and a myriad of inter-related pieces of legislation relating to the issues of identity crime, being both the ‘stealing’ of a person’s identity and the creation of a fictitious identity. This paper will focus on the following areas as they relate to identity crime;
- The History of Identity Crime
- Criminal Methodology
- Cost and Magnitude
- Victim Assistance and Prevention
- Facilitation of Terrorism
- Identity Documents
- Biometrics
- Legislative Analysis

In addressing these areas, an overview of identity crime in Australia and its implications will be ascertained, highlighting issues requiring further Government and Non-Government intervention.
Chapter 2

METHODOLOGY

This research project has two key objectives:

1. To provide an overview of identity fraud in Australia and its implications;

2. To identify areas for further intervention in order to counter identity fraud.

A qualitative historical approach using content analysis was, under the circumstances, considered the most appropriate research design to address the above two research objectives. Two key strategies were selected for the qualitative design for the study. Firstly, a content analysis of the relevant literature and of legislation was considered to effectively identify key issues. Secondly, a comparative approach was adopted to examine international trends in identify fraud in order to gauge Australia's progress in dealing with these issues compared to other countries such as the UK, US, and Western European countries.

Other research approaches were considered initially for example a quantitative study that may have included surveys or structured interviews of industry professionals working within both the private and public sectors. This approach would have been useful in gaining greater understanding of the current extent of identity fraud. There exists a substantial inadequacy in measuring and understanding the scope, extent and fiscal cost of identity fraud within this country.
At the commencement of this paper, numerous inquiries were conducted with industry representatives within both the private and public sectors. However, it quickly became apparent that legislative restrictions and private sector reluctance to divulge commercially sensitive quantitative data would be an impediment to establishing a quantitative research based model to estimate the cost of identity fraud to the Australian community.

Therefore, a qualitative, historical research model was adopted in order to describe, contextualise and analyse the broad gambit of identity fraud history, methodology, counter-measures and the legal framework. Given the lack of current and reliable data, this model was also identified as the most appropriate, so that clear linkages between methodology, fraud counter-measures and the impact of the Australian legal framework could be fully explored and conclusions developed. Additionally, the researcher’s desire to analyse differences in legislation in Australia and internationally was more appropriately addressed using a qualitative content analytical approach.

In designing this research approach, the author is aware that document analysis does have its limitations. The literature contains potentially a diverse range of biases. Firstly, there are the biases of the sources. Identity fraud is a sensitive issue and it is possible, particularly in the case of private sector sources that the extent of it or how it is described can be different from public sector agencies, particularly in the government sector. Secondly, there are the author’s own biases as a researcher and as a police officer working in the area of identity fraud. Such author based biases could include a bias toward law enforcement initiatives at the
expense of traditional societal freedoms, or a preponderance toward more serious penalties for those convicted of crimes. To reduce the impact of bias the author used a wide range of sources to analyse similar issues and this resulted in the author being able to provide some balanced perspectives on how to best counter identity fraud in the future.

In summary, given that there is a paucity of reliable quantitative data derived from public and private sector inquiries into identity fraud in Australia, the author conducted a qualitative research and analysis of a significant breadth of published and unpublished literature including documents, reports and a myriad of inter-related pieces of legislation into the subject matter. The author also relied on industry expertise in the subject matter, as a senior police officer responsible for the management of criminal intelligence analysis of fraud within New South Wales.

The Australian culture, political and economic psyche, is particularly vigorous and often vocal in preventing the sharing of an individuals’ private information both between government agencies and government and non-government agencies. Bearing this in mind, the author predominantly focused research towards other democracies that hold similar cultural and economic values. The conclusions and recommendations emanating from this paper are the result of that research and analysis process.
Chapter 3

HISTORICAL OVERVIEW

Identity crime is not a new phenomenon. The use of false identities throughout history is both extensive and interesting. Attempting to assume the identity of the Son of God was not beyond some, whilst rightful heirs to thrones have also been contested. A classic example is the thirty or so individuals who claimed to be Dauphine Louis, son of Louis XVI, after his father the King died. It is believed that the ‘real’ Dauphine Louis died in prison during the French Revolution, however these nefarious self-proclaimed individuals declared that they (proclaiming to be Dauphine Louis) had escaped from prison. One of these individuals was of Negro appearance with ‘frizzy hair’. (Caslon Analytics n.d)

On his death bed in 1584, the first Czar of Russia, Ivan IV or Ivan the Terrible appointed Boris Godunov as his successor and guardian to his sons. It is believed that the murder of one of these sons, Dimitri was attributed to Godunov to ensure his continued rule. Ironically in 1604 an impostor claiming to be Dimitri rallied support and easily invaded Russia,’ re-claiming’ the throne. (Caslon Analytics n.d)

The activities of individuals who perpetrate identity fraud have also been immortalised in film on numerous occasions. For example, the film ‘Catch Me If You Can’ released in 2002 depicts the life of Frank Abagnale who posed as a lawyer, doctor and airline pilot. He spent $500,000 on clothes, hotels and meals
and defrauded banks of another two million dollars. He served five years in US, French and Swedish gaols and now lectures at the FBI Academy in Quantico Virginia on Fraud Prevention.

A further example, is the French Villager Martin Guerre case which is the basis of the film The Man In the Iron Mask. Guerre disappeared after going to war and returned in 1556. He was hard working, and more popular, however property disputes led to claims that he was an impostor. These allegations were subsequently substantiated when a one legged man entered the court claiming that he was the real Martin Guerre. The penalty for identity fraud in this case was public execution. (Caslon Analytics n.d)

Whilst these examples are interesting, the significant implications and consequences of identity crime is not isolated to those worthy of celluloid infamy or of noble blood. Identity crime significantly impacts upon the economy, business and law enforcement. However, it is the effect that identity crime has at the grass roots level upon the individual who has had their identity stolen that must be acknowledged.

Identity crime generally and identity theft particularly can have devastating consequences to the victim. In the short term this may result in countless hours spent closing bank accounts and opening new ones, convincing financial institutions that unauthorised transactions have taken place. The longer term effects can be far reaching. An erroneously acquired bad credit rating may result
in the denial of loans and rental property applications, the inability to connect utilities and even the prospect of being arrested for crimes not perpetrated by the victim, but rather the person who assumed their identity.

As illustrated, crime has been around since the first human interactions. A common thread entwined through modern crime is the improvements to technologies used and exploited by the criminals themselves. Criminals are able to perpetrate crimes on a much wider scale than in the past, duplicating records, establishing fictitious identities and ‘stealing’ the personal information of legitimate citizens.

Whilst the traditional ‘con artist’ has plied his/her trade for centuries, such people spent considerable time in establishing a persona. Today, anybody with a personal computer, scanner, printer and/or card-reader can successfully fabricate a false identity.

The convergence of computing and communications technologies has dramatically changed the nature of most facets of our society. In particular, technology improvements, have not only greatly influenced contemporary business and corporate activities, but has also facilitated one of the most sinister of criminal activities, terrorism. Business transactions, which are often the cornerstone of supporting ones identification have, in many instances, become faceless activities, with the need for face to face interaction often eliminated. Additionally, the traditional boundaries both in the corporate and criminal world, such as national
orders, have been removed through technological advances such as the internet.

The benefits of improved technologies are immense. However, like most things, it has come at a price.

Historically, a business customer would attend the business location and undertake business activities in person. Both the business representative and customer would openly see each other, thereby reducing the likelihood of fraudulent activity. Should some criminal activity occur, either side of the transaction could provide police with intimate knowledge of the other to assist in identifying and prosecuting the offender. However, technology improvements coupled with the increasingly faceless nature of business and corporate society has eliminated the physical ability to identify participants to a transaction. This has meant the need to properly and thoroughly identify a person, such as a customer, is now of paramount importance.

The same technologies that have provided so many benefits to governments and corporate society have also created enormous opportunities for criminals. Criminals can now communicate in secret, disguise their identities and manipulate electronic systems to obtain a desired outcome (usually financial gain) illegally. For example, email accounts can be set up with no verification of identity in addition to the use of internet cafes by individuals to further hamper being identified. The use of false identities and documentation is not limited to the perceived white collar crime of fraud, but plays a significant role in both the funding and actualisation of terrorist activities.
On the 11th September 2001, nineteen terrorists hijacked four planes and crashed two of them into the twin towers of the World Trade Centre. (The 9/11 Commission Report). Two of these terrorists were Abdul Alomari and Ahmed Saleh Alghamdi. In addition to their involvement in these terrorist acts, these two terrorists were also involved in identity fraud. Alomari and Alghamdi had obtained false documentation indicating that they had Virginia residences. These documents were used by them to board two of the ill fated planes. In addition, five of the nineteen terrorists had also acquired Virginia residency documents, whilst another five had obtained false social security numbers. Incidentally, Alomari and Alghamdi did not assume an existing persons’ identity, they used their own names on their documentation, however adopted false identifiers with regard to their addresses and other documentation (The 9/11 Commission Report).
Chapter 4

CRIMINAL METHODOLOGY

Obtaining personal information of individuals to steal their identity is achieved by criminals utilising both low and high tech means. These methods vary from the age old crime of 'pick pocketing' to technologically advanced methods of utilising computer viruses to elicit information. Other methodology includes:

- 'Dumpster Diving' - simply the process of rummaging through residential or business garbage for personal information. Pieces of information are collected until there is enough to create an identity. These pieces may be details from envelopes, receipts, credit card slips with details still visible, old driver's licences and credit/debit cards.

- 'Stealing Mail' - An unsecured letter box is an invitation to an identity thief. Again, vital pieces of information are obtained that either individually or collaboratively can be used to create an identity. In addition, there are some reported instances of criminals arranging a re-direction of the victim's mail to a new address. Subsequently increasing the lag time between offence and detection.
> ‘Shoulder Surfing’ – this occurs when an individual literally stands behind or beside the victim when they are transacting at an Automatic Teller Machine (ATM) an EFTPOS transaction or conducting telephone banking. The intention being to obtain either the victims’ Personal Identification Number (PIN) by viewing it as it is entered in the keypad of an ATM or a telephone pad, or by listening as the victim supplies details over the telephone phone to book a hotel room or purchase a product.

> ‘Card skimming’ involves literally ‘skimming’ information from the black stripe on the back of a credit/debit card. A device may be attached to an ATM and invariably a camera is also attached within a panel on the ATM or is disguised as advertising. (As illustrated a pin hole allows the offender to record or remotely monitor the victim entering their personal identification number (PIN)). In combination the offender now has all the information required to not only create a cloned card, but also access cash through the use of the PIN.

Alternatively, the data contained in the black stripe of a debit/credit card can also be retrieved through the use of a hand held device, such a device may be carried
on the belt of a retail sales person or a waiter in a restaurant, who will discreetly swipe the card without the customers knowledge.

- 'Card Cloning' – the information obtained utilising the above method is then transferred to a ‘new’ plastic card that has been embossed with the victims details. Criminals are becoming increasingly adept at avoiding law enforcement detection by creating ‘back up’ identity documents in the same name as the false credit card.

- ‘Phishing’ - Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although law enforcement authorities have received some reports of telephone contact being used in a number of instances.

- ‘Trojan Attacks’ - a Trojan Horse is a program that unlike a virus, contains or installs a malicious program while under the guise of being something else. Trojans are also known to create a ‘backdoor’ on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Compared to phishing, Trojan attacks allow the criminal greater access to personal identity information including passwords and account details.
The more technically minded criminal may hack into computer systems to obtain employee, patient, client information or place ‘trojans’ or key logging software on computer systems to capture personal information. Such computer programs (Trojans) allow the criminal to then review all data stored on the computer periodically to ensure accurate and timely theft of information, including identity details of victims.

**Usage**

It is obvious that individuals partake in identity crime for the purposes of concealment. A fraudulent driver’s licence is rarely used because the individual cannot pass a driving test. It may be used by a disqualified driver to evade detection by law enforcement, though often will be used as one form of identification for other transactions, such as opening bank accounts, applying for credit or other loans. The assuming of a false identity will facilitate a number of activities including:

- Money laundering;
- Tax evasion;
- Obtaining employment using falsified documentation in support of non-existent qualifications;
- Assist an illegal immigrant who is avoiding deportation;
- People smuggling through the use of false travel documents;
- Obtaining restricted items or privileges.
The use of fraudulent credit cards in the name of a stolen identity allows criminals to purchase ‘big ticket’ items that can be easily and quickly re-sold for cash. In lieu of creating a fictitious credit card the criminal has the ability to open a ‘legitimate’ credit account in the victim’s name or apply for a loan to purchase, for example, a portable asset such as a luxury motor vehicle. With a stolen identity the criminal can also empty the legitimate bank accounts of the victim by writing cheques or making withdrawals with the ‘copied’ identity, however there is generally a limited time frame that the criminal has in which to act before being detected. Whilst internet banking, for example, has opened opportunities for criminals, it also allows victims to review accounts daily and thereby detect fraudulent or irregular activity in their accounts.
Chapter 5

COST AND MAGNITUDE

There is paucity of accurate data concerning both cost and magnitude of identity related crime in both Australia and globally. The cost and magnitude of identity crime is not easily quantifiable. A number of factors have contributed to the uncertainty associated with accurately analysing the identity crime landscape.

Invariably identity crime is a facilitator for other criminal activity. In New South Wales it is the ‘other’ criminal activity which is captured for statistical purposes for the simple reason that there is no ‘stand alone’ offence of assuming a persons’ identity. Whilst a National Identity Fraud Register has been established by Australian Crime Commission, the collection methods of this register are less than ideal. Information on identity crime is collected from State law enforcement agencies in an adhoc fashion, often due to the limited ability of individual agencies to retrieve the required statistics.

In addition, there is no centralised process to assist the commercial sector in reporting, if only for intelligence purposes, the incidents of fraudulent documentation. This coupled with perceived restrictions of the Privacy and Personal Information Protection Act 1998 has further thwarted the collection of accurate statistics in regards to the prevalence of identity crime.
Unfortunately, an accurate estimate of identity crime will only occur when national uniformity is achieved regarding the offence of assuming/creating a false identity. However, in the interim a number of public and private sector agencies have attempted to quantify this pervasive criminal activity:

**Australian Bureau of Statistics**

According to the Australian Bureau of Statistics, (1996) it is estimated that the number of births, permanent new arrivals and long-term visitors will result in 400,000 to 500,000 new Australian residents per annum over the next few years. Each of these people will be required to prove their identity to a multitude of government and commercial organisations if they wish to utilise the services being offered.

The volume of personal identification checks required on a day to day basis can be gauged by assessing the operations of selected government agencies. In 2000, the Australian Electoral Commission processed 2.46 million enrolment forms and amendments, the Australian Taxation Office (ATO) issued about 500,000 tax file numbers, Centrelink processed 4.4 million new claims or re-grants and the Department of Foreign Affairs and Trade issued 1.4 million passports. (Main and Robson, 2001). Whilst these figures would have exponentially increased since, they only represent a small percentage of the millions of proof of identity transactions conducted within commercial organisations.
The Federal House of Representatives Standing Committee on Economics, Finance and Public Administration

The Federal House of Representatives Standing Committee on Economics, Finance and Public Administration conducted a review of the Australian National Audit Office (ANAO) Report No. 37 1998-99 on the Management of Tax File numbers in 2000 entitled, ‘Numbers on the Run’. The ANAO report found that there were 3.2 million more tax file numbers than the number of Australians at the time. The review highlighted the issue of identity crime. Indications of the extent of the problem noted by the committee included: ‘the estimate would be that approximately 25 per cent of reported frauds to the AFP involve the assumption of false identities’; that ‘identity kits’ consisting of a set of fabricated documents for a false identity are ‘increasing in availability, particularly due to the ability of modern technology to generate forged documents of very high quality’; ‘that identity documents of various types are available for the payment of money – either forged documents or genuine documents which have been stolen and otherwise dealt with’, including via the Internet; that in a pilot conducted by Westpac and the NSW Registry of Births, Deaths and Marriages of a Certificate Validation Service, that in ‘the particular instances where a birth certificate was tabled to the bank as part of the identification documentation, some 13 per cent were found to be false’; Centrelink detected ‘about $12 million worth of fraud from identity’ in 1999; and The National Crime Authority’s (NCA) concern about the ease ‘with which false identities may be established and used to facilitate organised criminal activity’. In addition, the committee was “concerned at the lack of figures available on the extent and cost of identity fraud”. (pg. 87)
Of interest in the original report were comments made by Mr. Woods from the Australian Bankers Association. He highlighted the interdependence between sectors for identification documents stating that their research on the types of documents produced by customers or potential customers of financial institutions identified that at least 75% of all identity documents were government authority issued.

Similarly, Commonwealth agencies are heavily dependent on State and private sector issued documents for Proof of Identity. According to the ANAO Report ‘Numbers on the Run’ referred to earlier, the ATO provided statistical data on current usage of identity documents for new ‘registrants. This data showed that the ATO uses bank account statements for 11 per cent of registrants and an Australian or overseas birth certificate in 20 per cent of cases; similarly for New South Wales Centrelink registrations, 16 per cent involved a credit card as Proof of Identity, 15 per cent a driver’s licence and 8 per cent a birth certificate.

Such interdependence highlights the need for a holistic approach to addressing the issue of identity crime. Various agencies have argued that the documents they produce, for example a drivers licence, are not intended as a form of identity but rather a licensing or entitlement card. However, the fact that they are being used and integrated into the 100 point identification system requires those agencies to implement security measures to address counterfeiting and to ensure the integrity of the document.
**AIC / PRICE WATERHOUSE COOPERS SERIOUS FRAUD STUDY (2003)**

The Australian Institute of Criminology and PricewaterhouseCoopers conducted a study of 155 serious fraud cases prosecuted in Australia and New Zealand in 1998 and 1999. The study identified that 24%, almost one quarter of the cases, used a fictitious identity, whilst stolen identities were used in 13% of cases. Fifty-four of the cases (36%) involved the misuse of identity. Information on the use of false identities was available in 152 of the files.

**Graph 1 - Use of False Identities in Serious Fraud Cases**

*Australian Institute of Criminology and PricewaterhouseCoopers (2003)*

The use and availability of false identities has increased exponentially with greater accessibility and improvements to technology that assists in the replication of proof of identity documents. This correlates with the rule of Moore’s Law which estimates that the power and ability of computers doubles every 2 years. (Moore’s Law, 2006)
It is the use of multiple identities by offenders that is of greatest concern. Information relating to the number of false or identities used by offenders was gleaned from forty-seven cases.

**Graph 2 - Number Of Multiple Identities Used by Offenders**

*Australian Institute of Criminology and PricewaterhouseCoopers (2003)*

It was ascertained that the majority of cases examined used one or two false names or identities, however one case identified an offender using 16 different names and identities. This example illustrates the vigilance required when collecting and collating statistical data, for example only collecting information on the number of ‘identity fraud’ offenders without considering the number of identities these offenders used would clearly minimise the apparent magnitude of the problem.
**THE KPMG FRAUD SURVEY 2004**

The KPMG Fraud Survey 2004 outlines the magnitude of fraud amongst organisations within Australia and New Zealand. The questionnaire, sought information about fraud incidents during the period April 2002 to March 2004, with a total of 491 respondents. The major findings with regard to identity fraud included that:

- Nine percent of respondents had been the victim of identity fraud during the survey period;

- Within the financial services sector, services obtained by false documentation (including fraudulent loans), credit card fraud and cheque forgery accounted for 72 percent of total external party losses.

- Within retail, the most costly form of external party fraud was services obtained by false documentation (at 94 percent) while for the economy generally (excluding retail and financial services sectors), false invoicing was the most costly form of fraud, accounting for more than 81 percent of losses by value.

Of particular concern in their findings was evidence that only 63 percent of major frauds were reported to police. Organisations quoted “lack of evidence, concern about adverse publicity” and “concern about the resources required to prepare the complaint” as their main reasons for not reporting the matter to the police.
2006 Australian Computer Crime and Security Survey

The Australian High Tech Crime Centre (AHTCC), the Australian Federal Police, all State Law Enforcement Agencies and AUSCERT (who is the national computer emergency response team for Australia based at the University of Queensland) collaborated in producing the 2006 Australian Computer Crime and Security Survey. This survey represents the findings from a broad cross section of Australian industry, including both public and private sector organisations. The survey analyses computer network attacks, computer crime and access misuse in Australia in the last 12 months.

The findings of particular significance to identity crime included:

- In the 12 month period from April 2005 to March 2006 AusCERT handled over 2,000 online ID theft incidents involving hosts used to support Phishing and Trojan attacks. This represents a 27% increase compared to the previous 12 month period.

- Increasingly, online ID theft attacks have utilised rootkits or trojans with rootkit-like functionality, which makes detection by the computer user unlikely and their removal (if detected), extremely difficult.

- The average loss relating to online identity fraud is about $27,000
- Whilst only 5% of respondents attributed losses associated with online identity theft, the average monetary value has increased by 58%.

- There is a continuing prevalence of Trojan attacks that seek to steal Internet banking and other passwords, personal information and any form data from SSL-protected sessions as well as a steady growth in phishing attacks.

Whilst the increased use of the internet to facilitate business transactions has many rewards such as improved efficiency and convenience there are also negative consequences including increased vulnerability, potentially higher victim impact and possible international ramifications.

The subsequent cost of identity crime in an era of interactive, interdependent computer technology has increased. Prior to the internet era the ability of an offender to infiltrate business systems and steal customer data was limited. The business owner must now address the issue of ‘computer hacking’ in the same way as they would lock the door of their premises, both vigilantly and regularly. There are associated costs related to a compromised computer system including; replacing or upgrading computer hardware and software, re-entering compromised or lost data coupled with the additional man hours required to complete the task. In addition, consideration may need to be given to restoring any damage to business reputation not only through addressing the original security breach but
ensuring that public confidence is restored by incurring further costs associated with advertising the fact.

Criminal activity, and in particular identity crime, is not encumbered by geographical distance or borders. Whilst this paper does not attempt to explore in depth the issue of identity crime on an international basis it is important to acknowledge the magnitude and cost of identity crime in other countries with similar jurisdictional structures. Hence, in this paper, we will examine cost estimates supplied by the United Kingdom’s Home Office.

The Home Office Identity Fraud Steering Committee estimates that identity fraud cost the economy of the United Kingdom £1.7 billion over the past three years. (Cabinet Office, United Kingdom 2002). Whilst the table below is quite detailed it is one of the most recent publicly available documents that breaks down the cost of identity crime.
Table 1: Estimate of the Cost of Identity Fraud to the UK Economy

<table>
<thead>
<tr>
<th>DEPARTMENT OR ORGANISATION</th>
<th>COST</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association of British Insurers</td>
<td>£22m</td>
<td>A number of insurers (representing approx 36% of the industry) estimated that their financial loss in 2003 due to identity fraud was £7.9m, which translates to £22m for the industry as a whole.</td>
</tr>
<tr>
<td>APACS, the UK payments association</td>
<td>£504.8m</td>
<td>Losses resulting from plastic cards being used by criminals pretending to be the rightful owner or by criminals using a fictitious identity. This figure comprises: (i) Counterfeit (skimmed/cloned) cards £129.7m (ii) Cards lost or stolen £114.4m (iii) Card not present £150.8m (iv) Mail non-receipt £72.9m (v) Fraudulent applications £13.1m (vi) Account takeover £23.8m</td>
</tr>
<tr>
<td>Audit Commission</td>
<td>£15m</td>
<td>Audit Commission not included in 2002 Study.</td>
</tr>
<tr>
<td>Source</td>
<td>Estimate</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>British Bankers' Association</td>
<td>Estimate of loss to pension schemes due to identity fraud (extrapolated from Audit Commission National Fraud Initiative figures).</td>
<td>The BBA does not collect statistics on identity fraud. Figures from its members for card fraud are included in the APACS figures.</td>
</tr>
<tr>
<td>Building Societies' Association</td>
<td>£3.1m</td>
<td>A number of building societies representing just over 50% of the industry responded to a survey and estimated their financial loss due to ID fraud. The BSA extrapolated figures for the sector as a whole and estimate that this translates to approximately £3.1m losses due to ID fraud over the past year.</td>
</tr>
<tr>
<td>CIFAS – The UK's Fraud Prevention Service</td>
<td>£2.3m</td>
<td>This represents the cost of identity fraud to the retail sector. CIFAS figures have only been included with respect to the retail sector. This avoids double-counting on contributions made by other sectors directly.</td>
</tr>
<tr>
<td>Department for Constitutional Affairs</td>
<td>£29.9m</td>
<td>Unpaid fines due to “tracking” problems - this is due to a number of reasons including false information being provided to the Police.</td>
</tr>
</tbody>
</table>
Unpaid fines due to identity problems – i.e. many people issued with fines do not turn up at courts to verify their alleged name and address. Given this, courts find it difficult to enforce the payment of a fine because they are not certain the identity on the fine is a true identity (many fines get issued to fictitious identities or identities with inaccurate spellings).

<table>
<thead>
<tr>
<th>Department for Work &amp; Pensions</th>
<th>£20m</th>
<th>DWP estimates that £20m-£50m of benefit fraud arises as a result of identity fraud (i.e. claiming benefit in false identities).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver &amp; Vehicle Licensing Agency</td>
<td>£2.5m</td>
<td>Estimated cost of operational activity required to help prevent abuse of the driving licence in identity crime.</td>
</tr>
<tr>
<td>Driving Standards Agency</td>
<td>£1.12m</td>
<td>Estimated costs of ensuring that DSA is satisfied as to the identity of candidates presenting for theory and practical tests. The resultant enforcement activity in preventing and detecting impersonations, ensuring that only those entitled can hold driving licences reducing the ability to commit identity fraud.</td>
</tr>
<tr>
<td>Finance &amp; Leasing Association</td>
<td>£1.4m</td>
<td>FLA not included in 2002 study. This figure relates to identity fraud arising from the provision of motor</td>
</tr>
</tbody>
</table>
It is not possible to determine if the scale of this problem has changed since 2002. The figure from the original study has been included for illustrative purposes to help estimate any comparative changes to the overall cost of identity fraud since 2002.

**HMRC** has identified a number of fraudulent and potentially fraudulent tax credit claims based on false and stolen identities.

Some 6,800 fraudulent claims have been identified based on stolen DWP staff identities, of which 4,100 were fully intercepted by HMRC before any payment. The loss from this fraud is estimated at £2.7 million.

HMRC is currently subjecting around 30,000 potentially fraudulent tax credit claims to detailed investigation including claims based on the stolen DWP staff identities and on stolen Network Rail staff identities. It is too early to estimate the loss from this fraud.

**Child Benefit**

HMRC has experienced a small number of attempts to
defraud the Child Benefit system by the use of false documents. These attempts have been successfully detected and it believes the risk of identity fraud to be minimal.

<table>
<thead>
<tr>
<th>Source</th>
<th>Cost</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Office (Immigration &amp; Nationality Directorate)</td>
<td>£36.2m</td>
<td>Approximate cost to IND of undertaking enforcement activity against individuals who may be involved in some form of identity theft or identity fraud, potentially involving document abuse.</td>
</tr>
<tr>
<td>Local authorities Investigation Officers Group (LAIOG)</td>
<td>£28,564</td>
<td>From an online poll of its members, LAIOG identified that £28,564 was specifically due to identity fraud. However, most LAIOG members contacted stated that as identity fraud was usually part of a larger fraud, it would not necessarily be recorded.</td>
</tr>
<tr>
<td>Money laundering</td>
<td>£385m</td>
<td>The overall size of money laundered in the UK is not known currently but is believed to be substantial. This cannot be attributed to any single organisation. No figures are available currently on the proportion of money laundering that relies on identity fraud. It is not possible to determine if the scale of this problem has changed since 2002. The figure from the original study has been included for illustrative purposes to help estimate any comparative changes to the overall</td>
</tr>
</tbody>
</table>
It is not possible to estimate the overall cost of identity fraud to the Police Service. However, figures show that last year Police Forces in England and Wales spent 15,000 to 20,000 days dealing with bogus callers – a crime that relies heavily on false identities.

Cost of £1.73m is based on Police Forces in England and Wales spending 17,500 days (midpoint of 15,000 – 20,000 days) at a daily cost of £99.19 (made up of £82.19 per day per officer and support costs of £17.00 per day per officer) to deal with bogus callers.

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police Service</td>
<td>£1.73m</td>
<td>It is not possible to estimate the overall cost of identity fraud to the Police Service. However, figures show that last year Police Forces in England and Wales spent 15,000 to 20,000 days dealing with bogus callers – a crime that relies heavily on false identities. Cost of £1.73m is based on Police Forces in England and Wales spending 17,500 days (midpoint of 15,000 – 20,000 days) at a daily cost of £99.19 (made up of £82.19 per day per officer and support costs of £17.00 per day per officer) to deal with bogus callers.</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>£372m</td>
<td>Telecoms not included in 2002 study. The cost of identity-related fraud is a substantial component of the total fraud/revenue loss in the telecoms sector.</td>
</tr>
<tr>
<td>UK Passport Service</td>
<td>£62.8m</td>
<td>The cost to UKPS of measures to counter identity fraud when processing applications for UK passports issued in the UK.</td>
</tr>
<tr>
<td>TOTAL</td>
<td>£1.72bn</td>
<td>cost of identity fraud since 2002.</td>
</tr>
</tbody>
</table>
This table represents the most comprehensive and holistic assessment of the cost of identity fraud. Not only does this assessment attempt to quantify the fiscal implications to business but also it addresses the subsequent cost of man hours as an administrative consequence.

It is an interesting interpretation taken when referencing the cost of identity crime to the Police Service. Initial thoughts when considering the cost of identity crime would tend to focus on the man hours spent attempting to identify offenders of crimes. This survey however, focused the cost on the number of 'bogus' or what New South Wales police would refer to as 'public mischief' calls. This example, further illustrates the difficulty in estimating the true (and thorough) cost of identity crime.

The experiences of the Department of Constitutional Affairs relating to the issuance of fines to individuals using fictitious names may soon be replicated in New South Wales. The introduction of the Criminal Infringement Notice System in 2007 within the NSW Police does not require the mandatory fingerprinting of individuals for certain offences, the onus is on the Police Officer. The individual may simply be issued a fine for the offence and, if paid on time, the offence will not be recorded on the persons' criminal history record. In addition, if false particulars were supplied, without fingerprint verification the fine will remain unpaid and the offender will evade further police detection.
Unfortunately there is limited public information available relating to the survey and methodology used in gathering the statistics used in the previously listed table, and whether in fact confidentiality of information was guaranteed to stakeholders prior to participation. It is envisaged that similarly to the Australian economic environment, private sector reluctance to divulge commercially sensitive quantitative data may have impeded the collection of accurate data. This is demonstrated in part by the absence of contribution by the British Bankers Association, instead deferring to data obtained from the United Kingdom Payments Association (APACS) which clearly only captures identity fraud related to ‘plastic cards’. In addition the response rates for some stakeholders were omitted, such as the Local Authorities Investigations Officers Group (LAIOG), whilst low response rates of others such as the Association of British Insurers (36%) further reduces the accuracy of statistical data. These difficulties however, should not be used as the rationale by opponents to a similar survey within Australia, any information will be advantageous in estimating the extent of the problem.
Chapter 6

VICTIM ASSISTANCE AND PREVENTION

The impact of identity crime to a victim is far reaching. Unlike a burglary, for example, the 'continuation' of the crime can be long term. The victim may not be aware of the offence until they receive a debt collection notice, are declined a line of credit with a financial institution or become aware of a bad credit rating. The effects of the criminal activity upon the individual victim may continue for years through fraudulently opened accounts and credit purchases made by the offender.

To adequately address the issue of victim assistance and prevention, it is imperative to look offshore to those countries who have recognised the serious nature of identity crime, it’s impact and consequences and who have or are in the process of implementing systems to further secure and protect the identity of individuals.

There is no central reporting agency in Australia for victims of identity crime. Initially the victim is required to report the matter to their respective State law enforcement agency, in addition to contacting every financial institution or company they have a current business relationship to advise of the incident. Unfortunately, they must then be prepared to continue this process each time a new financial institution or business contacts them regarding any fraudulently opened accounts or loans opened in their name. Whilst there is no accurate data
in Australia as a reference, research conducted by the United States General Accounting Office (GAO-02-363), estimates a victim spends, on average 175 hours and $100 (not counting legal fees) to fix his/her credit rating.

A number of American insurance companies are now offering an 'Identity Protection Service'. One such example is a United States company Intelius, who offer a range of products including:

- **Identity Reports** - that advise of your "Financial, Public and Professional Identity picture". The report outlines a person's name and addresses assigned to their Social Security Number, their phone connection and utilities status, any enquiries conducted on financial or credit information, current property report and any compromised credit cards.

- **Id Watch** – which provides email notification if there are any changes made associated with the person's Social Security Number, Address, Phone, Property Sales, New Loans etc.

- **Insurance Coverage and Recovery** – this is a plan that assists a person in restoring their identity. It includes assistance in filing reports, sending fraud alerts to credit agencies and covering legal fees. The total coverage is up to $25,000.

The fact that this company offers such a commercially viable service is indicative of how prolific identity crime is in the United States of America.
Whilst identity crime is not new, its proliferation to date has been far greater in other countries, to the extent that a response has been implemented. Australia is not immune to the exponential increase in this activity, and as such, government and law enforcement agencies should become conversant with strategies implemented elsewhere. Contingencies implemented in countries of similar economic and socio-cultural makeup are summarised below:

**United Kingdom**

In the United Kingdom, The Home Office in collaboration with other government departments and private sector organisations has set up the Home Office Identity Fraud Steering Committee. The aim of the committee is to lead a programme to address identity theft and identity fraud.

The Home Office Identity Fraud Steering Committee have listed a number of key successes on its website, www.identity-theft.org.uk, these include:

- Aligning penalties - Many organisations use passports and driving licences to help establish identity. The maximum fine of £2,500 was no longer a credible penalty for fraudulently obtaining a driving licence given the level of fraud that it can be used to perpetrate. The Criminal Justice Act 2003 changed the law to align the penalty for fraudulently obtaining a driving licence with that for fraudulently obtaining a passport and made these offences arrestable. Obtaining either document fraudulently now incurs a
maximum penalty of two years imprisonment.

- New criminal offences - Organised criminals often use false identity documents. The Identity Cards Act 2006 created new criminal offences of being in possession or of 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.

- Developing and sharing good practice – Identity Fraud – The UK Manual was produced and launched in June 2003 it includes examples of known security features from UK passports and driving licences and provides guidance to organisations to help spot forgeries.

- Identity and Passport Service (IPS) initiatives - IPS has deployed a database of lost and stolen passports that is being shared with border authorities and police worldwide to help prevent identity fraud.

- The National Identity Scheme - The Government's decision to introduce a National Identity Scheme was announced in the Queen's Speech on 17 May 2005. The Identity Cards Act 2006 has now passed all of its Parliamentary stages and received Royal Assent on 30 March 2006. The Identity and Passport Service is responsible for introducing a National Identity Scheme that will provide people with a highly-secure means of
protecting their identity. The National Identity Scheme will eventually become compulsory. This means that all UK residents over 16 will need to have an ID card. However, it will not be compulsory to carry the ID card with you. It is expected that the first cards will be issue from 2008/2009.

**Netherlands**

The Netherlands Police maintain a central database of lost or stolen identity documents called the Verification of Identity System (VIS). In 2002 there were over six million documents held on the central database (Cabinet Office, July 2002, p 38). Details of deaths are also recorded to prevent the stealing of a deceased person’s identity.

**United States of America**

In the United States there are three national consumer reporting agencies that have call-in centres for reporting identity fraud or theft; the Federal Trade Commission (FTC), which maintains a database of complaints concerning identity theft; the Social Security Administration and The Office of the Inspector General (SSA/OIG), which operates a hotline to receive allegations of Social Security Number (SSN) misuse and program fraud; and Federal law enforcement agencies—Department of Justice components, Department of the Treasury components, and the Postal Inspection Service—responsible for investigating and prosecuting identity theft related cases.
The Federal Trade Commission in America have a Division of Privacy and Identity Protection, it is the newest of the Bureau’s divisions and oversees issues related to consumer privacy, credit reporting, identity theft, and information security. In addition, the Division educates consumers and businesses about emerging privacy, credit reporting, and information security issues, as well as identity theft prevention and assistance.

The Identity Theft and Assumption Deterrence Act of 1998 was the first piece of federal legislation to deal directly with identity theft. The Act required the Federal Trade Commission (FTC) to establish “procedures to ... log and acknowledge the receipt of complaints by individuals”, as well as educate and assist potential victims. In response, a telephone hotline was established in November 1999 for consumers to report identity theft. In addition victims can receive counseling and advice on what to do if their identity has been stolen. The information gathered from this hotline is maintained in a central database, the Identity Theft Data Clearinghouse. Law Enforcement Agencies who have membership to the Clearinghouse have the ability to access the database to determine whether there are additional victims or information that would be relevant to their current investigations.
The Federal Trade Commission in collaboration with the United States General Accounting Office has illustrated some of the non-financial impacts to victims of Identity Crime.

**Table 2 Types of Non Monetary Harm as Reported to the FTC**
*(November 1999 to September 2001)*

<table>
<thead>
<tr>
<th>Types of Monetary Harm</th>
<th>Number of Complaints</th>
<th>Percent Based on Subtotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denied credit or other financial service</td>
<td>7376</td>
<td>55.2</td>
</tr>
<tr>
<td>Time lost to resolve problems</td>
<td>3489</td>
<td>26.1</td>
</tr>
<tr>
<td>Harassed by debt collector or creditor</td>
<td>2968</td>
<td>22.2</td>
</tr>
<tr>
<td>Criminal investigation, arrest, conviction</td>
<td>1281</td>
<td>9.6</td>
</tr>
<tr>
<td>Civil suit filed or judgement entered</td>
<td>819</td>
<td>6.1</td>
</tr>
<tr>
<td>Denied employment or loss of job</td>
<td>580</td>
<td>4.3</td>
</tr>
<tr>
<td>Other</td>
<td>3780</td>
<td>28.3</td>
</tr>
<tr>
<td>Total</td>
<td>13,357</td>
<td></td>
</tr>
</tbody>
</table>

*Details and percentages do not add up due to victim being subject to more than one type of harm*

*Source: GAO-02-363, 56*
In addition the following table gives a sample of the activities committed by offenders and the subsequent consequences to the victim.

**Table 3 Summary of GAO'S Interviews of Victims**

<table>
<thead>
<tr>
<th>Victim</th>
<th>Activities committed in victim’s name</th>
<th>Non monetary harm</th>
<th>Monetary harm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>• Opened 12 to 18 charge accounts</td>
<td>• Harassed by collection agency</td>
<td>• Out of pocket expenses ($100 to $200)</td>
</tr>
<tr>
<td></td>
<td>• Obtained housing</td>
<td>• Reappearance of charges after they had been removed</td>
<td>• Lost job &amp; wages ($6000)</td>
</tr>
<tr>
<td></td>
<td>• Obtained utility service</td>
<td>• Time (200 hours over 10 months) to clear name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Obtained fraudulent identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Opened cell phone account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>• Attempted to open charge account</td>
<td>• Time (400 hours over 4 to 6 weeks) to clear name</td>
<td>• Out of pocket expenses (less than $20)</td>
</tr>
<tr>
<td></td>
<td>• Made charges on existing account</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 3. | • Obtained charge accounts  
• Obtained housing  
• Purchased car  
• Wrote bad checks  
• Obtained employment and owed back taxes | • Time (3 months over 6 years) to clear name  
• Difficulty in obtaining credit  
• Harassed by collection agencies | • Out of pocket expenses ($20)  
• Could not claim tax refund ($1000) |
|---|---|---|
| 4. | • Opened charge account  
• Attempted to obtain car loan  
• Wrote bad checks  
• Obtained fraudulent identification  
• Opened cell phone account | • Time (between 150 to 200 hours over 6 weeks) to clear name | • Out of pocket expenses ($20-30) |
<p>| 5. | • Violated traffic laws | • Arrest warrant | • Could not claim |</p>
<table>
<thead>
<tr>
<th>(3 speeding tickets)</th>
<th>issued for speeding tickets</th>
<th>IRS tax refund ($814)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Opened charge accounts</td>
<td>• Time (hundreds of hours over last 6 years) to clear name</td>
<td></td>
</tr>
<tr>
<td>• Wrote bad checks</td>
<td>• Went to court to contest tickets</td>
<td></td>
</tr>
<tr>
<td>• Obtained employment</td>
<td>• Difficulty in obtaining credit</td>
<td></td>
</tr>
<tr>
<td>• Filed tax return</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>• Obtained utility services</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>• Obtained fraudulent identifications</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>• Attended college classes</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

<p>| 6. | • | • | • |
| --- | • | • | • |
| • Opened 10 charge accounts | • Harassed by retailers over bad checks | • Purse was stolen | |
| • Wrote bad checks | • Time (missed 3 days work in 2 months) | • Out of pocket expenses ($20) | |
| • Made fraudulent identification | • Lower productivity at | | |
| • Used existing credit accounts | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th>7.</th>
<th>8.</th>
<th>9.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Opened 20 charge accounts</td>
<td>- Difficulty obtaining credit</td>
<td>- Out of pocket expenses (several hundred dollars)</td>
</tr>
<tr>
<td></td>
<td>- Difficulty purchasing car</td>
<td>- Time (48 hours over 2.5 years) to clear name</td>
<td>- Time (30 hours over 1.5 years) to clear name</td>
</tr>
<tr>
<td></td>
<td>- Car searched for drugs at police station</td>
<td>- Car searched for drugs at police station</td>
<td>- Lost job and wages ($2500)</td>
</tr>
<tr>
<td></td>
<td>- Filed for income tax refunds</td>
<td>- Filed for income tax refunds</td>
<td>- Obtained fraudulent identification</td>
</tr>
<tr>
<td></td>
<td>- Arrested 3 times in victims name</td>
<td>- Obtained fraudulent identification</td>
<td>- Opened bank</td>
</tr>
<tr>
<td></td>
<td>- Difficulty in obtaining credit</td>
<td>- Opened bank</td>
<td>- Lost job and wages ($2500)</td>
</tr>
<tr>
<td></td>
<td>- Out of pocket expenses (several hundred dollars)</td>
<td>- Out of pocket expenses (several hundred dollars)</td>
<td>- Out of pocket</td>
</tr>
</tbody>
</table>

53
<table>
<thead>
<tr>
<th>Account</th>
<th>Difficulty in obtaining employment</th>
<th>10.</th>
<th>Difficulty in obtaining credit</th>
<th>Out of pocket expenses ($59)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Purchased car</td>
<td></td>
<td>Evicted 3 times from housing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained prescription medication</td>
<td></td>
<td>Obtained fraudulent identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained employment and later fired</td>
<td></td>
<td>Opened multiple charge accounts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received unemployment benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Evicted 3 times from housing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained fraudulent identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opened multiple charge accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained prescription medication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained employment and later fired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received unemployment benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained fraudulent identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opened multiple charge accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained prescription medication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained employment and later fired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received unemployment benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained fraudulent identification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opened multiple charge accounts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained prescription medication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained employment and later fired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Received unemployment benefits</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Obtained fraudulent identification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Australian Consumers Association, CHOICE have listed a number of steps on their website (CHOICE.COM.AU) as guidance if you become a victim of identity fraud. If your identity has been stolen you may only find out months later when you discover a credit card bill is outstanding or when you’re denied credit because of a default on your credit report.

**Prevention**

_'An ounce of prevention is worth a pound of cure' - this ancient proverb first recorded in Latin, Henry De Bracton’s De LEGIBUS (c. 1240) is certainly pertinent to Identity Crime._

The effort and time, not to mention frustration associated with re-establishing one’s credit rating and good name cannot be understated. In Australia, as yet we do not have a central database or agency to assist victims of identity crime. As such there is invariably a duplication of effort required of the victim to convince financial institutions, and other government and non-government agencies of their plight.
Actions one can take to avoid becoming a victim of identity crime include:

- **Provide only necessary information about yourself.** Sometimes businesses request large amounts of information they don't need.

- **Read the privacy policy** before providing information to any business to ensure you understand how protected your data will be.

- **Choose passwords that are difficult to guess.** Use a combination of letters and numbers. Change passwords from time to time.

- **Use a number of different passwords** for different kinds of transactions/accounts.

- **Limit the amount of credit you have in accounts.** Consider using a separate credit card account with a low credit limit for online transactions and when overseas.

- **Thoroughly check account statements.**

- **Don't leave personal documents in your car glove box** such as registration papers.

- **Only carry personal documents with you if you really need them** to minimise the damage if your wallet gets stolen.

- **Securely store personal information** at home.
➢ **Destroy personal information** such as bills and account statements by tearing, cutting up or shredding before throwing them away.

➢ **Lock your letterbox.**

➢ **Check you've received all expected bills and statements.** A missing letter could indicate a thief took it from your letterbox or changed your billing address.

➢ **Collect your new credit card and cheque books in person** rather than by mail - ask your bank. If that's not possible watch out for them and contact your bank if they haven't arrived when expected.

➢ **Order a copy of your credit report about once a year,** check it and ask the credit reference agency to correct any mistakes. Credit reference agencies should provide you with a free credit report in a reasonable time (10 working days); most also offer an express service for a fee.

Baycorp also offers a credit monitoring service for a fee that notifies you whenever a credit provider accesses your report. Include your full name, date of birth, driver's licence number, current/previous addresses, phone number, your current/previous employers and the credit provider you most recently applied to and contact “Baycorp Advantage’ PO Box 964. North Sydney.
Diligence in implementing the above checklist will certainly reduce the chances of becoming a victim; however the following incidents are indicators that a form of identity crime may have occurred:

- Non receipt of bills or mail;

- Receipt of credit card accounts that you have not applied for;

- Repossession of an unknown vehicle;

- Being contacted by debt collected for unknown goods or services;

- Being denied credit for no apparent reason, or connection to utilities;

- Being contacted by police for alleged offences you did not commit.

Prevention is not only the concern of the individual. Financial institutions and other organisations are also researching and implementing prevention strategies to combat this criminal activity.

One such strategy is the introduction of ‘chip and pin’ technology. The United Kingdom has target hardened ‘points of compromise’ through the implementation of this technology. The ‘chip and pin’ card has a Personal Identification Number
(PIN) securely encrypted within a chip inside the card. The consumer must enter their PIN to make a transaction. A similar PIN system in France has seen an 80 per cent reduction in fraud since its introduction over 10 years ago. *(Chip and Pin 2006)*

The implementation of chip and pin technology to the United Kingdom in 2005 has seen a reduction of nearly £60m in counterfeit and fraud on lost and stolen cards when compared to 2004. The PIN is securely encrypted (held in a secure memory) within the chip, meaning that it is extremely difficult and time consuming for a criminal to access the PIN if your card is stolen, and they would be likely to destroy the card in the process. *(Chip and Pin 2006)*. As the chip and PIN programme is a worldwide initiative it is envisaged that commensurate results will be experienced when the technology is fully implemented in Australia.

It is the enabling abilities of identity crime to facilitate other high level criminal activities such as drug trafficking, people smuggling, money laundering and terrorism that is cause for significant concern. As discussed earlier, the use of false identities and documentation is not limited to the perceived white collar crime of fraud. Information gleaned through United States Congressional Hearings and Sentencing Commissions highlight the significant role that identity fraud plays in both the funding and actualisation of terrorist activities.
Chapter 7

FACILITATION OF TERRORISM

In February 1993, an explosion at the World Trade Centre Complex in New York City killed six people and injured approximately one thousand others. According to a report by the United States Department of Justice’s Office of the Inspector General (Report No: I-99-10, 1999):

“One of the conspirators in the World Trade Center bombing entered the country on a photo-substituted Swedish passport in September 1992. The suspect used a Swedish passport 'expecting to pass unchallenged through the INS inspection area at New York's Kennedy Airport—since an individual bearing a valid Swedish passport does not even need a visa to enter the United States.' When the terrorist arrived at John F. Kennedy International Airport (JFK), an INS inspector suspected that the passport had been altered. A search of his luggage revealed instructional materials for making bombs; the subject was detained and sentenced to six months’ imprisonment for passport fraud. In March 1994 he was convicted for his role in the World Trade Center bombing and sentenced to 240 years in prison and a $500,000 fine.”

A United States Sentencing Commission report (1999), also relating to this incident noted that, “The World Trade Center defendant used, and was in possession of, numerous false identification documents, such as photographs, bank documents, medical histories, and education records from which numerous false identities could have been created.”
An FBI representative at a February 2002 congressional hearing stated

"Terrorist financing methods range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been utilized by terrorists and terrorist groups. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, ... bulk cash smuggling, identity theft, credit card fraud, and other criminal operations such as illegal drug trafficking." (Lormel, 2002).

This was a contributing factor to the FBI beginning criminal financial investigations focusing on fraud schemes with a possible nexus to terrorist financing.

The organisation Privacy International in their report 'Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism', (2004, pg 5) refer to a list of 25 countries assessed by the Israel Based International Policy Institute for Counter-terrorism as having suffered most from terrorist attacks since 1986.

Privacy International acknowledge that the list is biased, highlighting that Sudan is not mentioned despite the US cruise missile attack in 1998, however they drew the following conclusion:

'Eighty per cent of these countries have long-standing identity card systems, a third of which contain a biometric such as a fingerprint. While it is impossible to claim that terrorist incidents have been thwarted as a result of an ID card, the above data establishes that the cards are unable to eliminate terrorist incidents.' (Privacy International, 2004, pg.6)
Table 4: List of 25 Countries having suffered most from terrorist attacks since 1986

<table>
<thead>
<tr>
<th>Country</th>
<th>No. of attacks</th>
<th>Deaths</th>
<th>Identity Card</th>
<th>Biometric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Afghanistan</td>
<td>4</td>
<td>34</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Algeria</td>
<td>41</td>
<td>280</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Argentina</td>
<td>2</td>
<td>129</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>5</td>
<td>49</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Cambodia</td>
<td>8</td>
<td>37</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Colombia</td>
<td>90</td>
<td>400</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Egypt</td>
<td>22</td>
<td>115</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>France</td>
<td>31</td>
<td>37</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>India</td>
<td>46</td>
<td>520</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Indonesia</td>
<td>14</td>
<td>250</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Israel</td>
<td>227</td>
<td>-</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Kenya</td>
<td>3</td>
<td>267</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>
The issue as to whether an identity card will thwart terrorism assumes that all terrorists are 'aliens' to the country being targeted. Privacy International asserts
that 'it is impossible to claim that terrorist incidents have been thwarted'. Whilst the above data may establish that identity cards do not eliminate terrorism the unknown factor is whether they have minimised the incidents.

The Beslan School Massacre which occurred on 1st September 2004 killed 331 people, with Chechen rebels initially taking more than 1000 people hostage. The rebels had crossed heavily-policed territory to reach Beslan. Jeremy Page, a Moscow Correspondent of The Times said: "Relatives of victims blame both local and federal authorities for allowing hostage takers to get across the borders." Investigations since the Massacre have failed to determine how the rebels passed through these borders, however identify fraud has not been discounted.

Opponents of identity card systems refute claims that such a scheme will assist in fighting terrorism through the identification of individuals using multiple or single false identities. Privacy International in their report Mistaken Identity (2004) asserts that a biometric identity system assumes the following circumstances:

- The target terrorists will be entitled to an identity card;
- The target terrorists will apply for an identity card;
- Target terrorists who are entitled and motivated to apply will do so using their true identity;
- Measures will be in place to detect suspected persons who are living in the UK without an identity card;
- Data matching systems will reveal information that relates to a suspect.
As illustrated, there is an argument that limiting the abilities of individuals to participate in identity fraud will not prevent terrorism. This may be true, as a suicide bomber will invariably seek to have their identity known once they commit such an act, to further what they believe will be adulation from similarly minded individuals. However, limiting identity fraud will inhibit the ability of individuals and organisations to fund terrorism through false bank accounts and money laundering schemes. The use of a fictitious identity provides an opportunity for terrorists to travel freely without triggering name-based watch lists utilised by law enforcement and federal agencies.

According to Lormel, (2001) terrorism is funded by traditional fraud schemes such as credit card fraud, identity theft and insurance fraud. The ability of terrorists and their supporters to open bank accounts or obtain credit cards in fictitious names, coupled with the utilisation of the internet for added anonymity adds to the appeal of this methodology. In his testimony before the U.S. House Committee on Financial Services (3 October 2001) Dennis Lormel stated, “Cutting off the financial lifeblood of the individuals and organizations responsible for the September 11 acts of terrorism is a vital step in dismantling the organization and preventing future terrorist acts.”

On the 1<sup>st</sup> October 2001, Mr John Pistole, Assistant Director Counter Terrorism, FBI commented on the use of fraudulent documentation and the implications to homeland security before the U.S House Select Committee on Homeland Security.
Investigations and interviews of detainees highlighted a number of instances of the use of fraudulent documents and false identities related to terrorism matters.

➤ The use of stolen credit cards and fictitious sales scams by an Al-Qa’ida terrorist cell in Spain to make purchases for the cell. The use of false passport and travel documents to open bank accounts to facilitate money transfers for the mujahadin movement. In addition to the use of stolen telephone and credit cards to conduct anonymous communications back to Pakistan, Afghanistan, Lebanon and other countries.

➤ A Pakistani who was a guard and doctor for the Taliban was arrested at John F Kennedy Airport for attempting to enter the United States on a forged passport.

➤ An Iraqi who was arrested in Turkey after attempting to enter the country using a false Moroccan passport, purchased for $150 in US currency.

➤ A detainee of Yemeni extraction who acquired a false Yemeni passport and was able to get a Pakistani visa.

Mr. Pistole stated in his testimony that whilst these individuals may not themselves be terrorists, proceeds from their fraud schemes were directly or indirectly used to fund terrorist activities or groups. (Pistole, 2003)
Chapter 8

IDENTITY DOCUMENTS

The non-government organisation ‘Privacy International’ asserts that approximately one hundred countries have official compulsory national identity cards that are used for a variety of purposes. In 1985 the Australian government proposed legislation introducing a national identity card. The benefits of the card were then espoused to be the combating of welfare and taxation fraud. The system was to include a register to facilitate the sharing of information about individuals. There was a lot of opposition to the proposal by both the opposition and the community. In 1987, a joint sitting of parliament failed to pass the legislation due to a technical flaw with regard to the constitution.

At the same time in June 1985, seven European Union (EU) countries signed a treaty to remove all internal border check points; this became known as the Schengen Agreement, named after a town in Luxembourg where the first agreements were signed. Prior to the agreement citizens of Western European countries could travel across neighbouring borders by showing their national identity card or passport, whilst nationals of some other countries were required to present separate visas for each country they were visiting. The result was an increase in traffic congestion, delays at border checks which inevitably cost both time and money to both visitors and commerce. Whilst these two events may
seem to be contradictory with regard to freedom of movement, the Schengen Agreement was introduced to create consistency. (Schengen Visa, 2003)

The Schengen Agreement created uniformed rules as to the issuance of the Schengen Visa. Visitors who are non-European Union (EU), non-European Economic Area (EEA) citizens, staying less than three months are required to satisfy a number of conditions including the purpose and conditions of their stay, their means of subsistence and obviously a passport or travel document which entitles the person to cross the border. The need for a separate visa for all the (Schengen) European countries has subsequently been eliminated.

A total of twenty six countries, including all European Union States excluding the Republic of Ireland and the United Kingdom have signed the agreement. The fifteen countries who have implemented the Agreement are: Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Italy, Greece, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Norway and Iceland. The latter two being external to the European Union.

Central to the Schengen Agreement is the Schengen Information System (SIS), which is a centralised information system that allows member states to share information relating to individuals and vehicles of interest. On 27th May 2005 the Schengen III Agreement was signed by seven countries (Austria, Belgium, France, Germany, Luxembourg, Netherlands, and Spain) which may enable a greater
exchange of information to include all biometric data such as fingerprints and DNA. (Schengen Visa 2003)

The changes in the landscape of national security since the proposed Australia Card and the original Schengen Information System in 1985 are considerable. In the aftermath of the terrorist attacks of 11th September, 2001, many countries have fast tracked plans for the adoption of a new passport standard that will increase the security of travel documents in line with time frames stipulated by the US when Congress passed The Patriot Act in 2002.

As a result of The Patriot Act, 2002 in combination with the Enhanced Border Security and Visa Entry Reform Act 2002, the International Civil Aviation Organization (ICAO) formulated the standard for the 'e-passport' in May 2003, stating

"By October 26, 2004, in order for a country to remain eligible for participation in the visa waiver program its government must certify that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and which incorporate biometric and authentication identifiers that satisfy the standards of the International Civil Aviation Organization" (ICAO, 2006).

There are 27 countries in the visa-waiver programme that are now required to have a biometric in place by October 2006 if they are to facilitate visa-free travel to the US. Specifically, the standard specifies that all e-Passports are to contain a
“photo” of the traveller in jpeg image format. This is a digital image format compatible with facial recognition technology.

The European Union regulations go further than that of the US stipulating two sets of biometric data – ‘fingerprint in interoperable formats’ and facial scans. The E-Passport issued by the US will combine face recognition and contactless chip technology. The chip will contain the same information as recorded on traditional passports: name, date of birth, gender, place of birth, dates of passport issuance and expiration, passport number, and photo image of the bearer. The passport will also contain an anti-skimming device to increase security. It is anticipated that E-passports will become an important tool in preventing individuals using multiple identities. (*E Passports, Uses and Initiatives, 2005*)

As illustrated various legislations, agreements and policies have shaped the current status of identity authentication internationally. This in combination with historical significance of identity documents, economic wealth, and embracement of technology has determined the importance or otherwise that a country places upon an identity.

The following illustrates a sample of countries who have implemented a form of identity card (*List of Identity Cards by Country, 2006*)

**France**

France has had a national identity card since 1940. The card was compulsory for anyone over the age of 16. A central record was also instituted; from 1942 French
people of Jewish religion had the word "Jew" added to their card in red, which helped authorities identify 76,000 people for deportation as part of the Holocaust. In 1955 a revised non-compulsory card was introduced and the central records abandoned. The card included a photograph, surname, given name, date and place of birth and incurred a fee upon renewal. In 1995 the cards became machine-readable and in 1998 they were issued free of charge.

The current French national identity card (Carte nationale d'identité sécurisée or CNIS) is an official non-compulsory identity document. It is a laminated plastic card bearing the owners photograph, name and address.

In addition to the card, the owner is required to supply a fingerprint which is stored in paper format. Access to the fingerprint is only permitted by a judge under specific circumstances. A central database holds the information contained on the identity cards, however strict laws prevent the dissemination of this information or the linking of the records to any other database. The cards may be used to verify identity or can be used for travel within the European Union in lieu of a passport. The cards are widely accepted when opening bank accounts.

As the identity card is not compulsory laws were changed to enable individuals to use any official and certified document (even if expired) issued by a public administration to verify identity. Law enforcement can also accept photocopies as proof of identity provided that the original is presented within two weeks. This is an 'interesting' clause, if the individual is using a forged photocopy and then fails
to present the original within two weeks, where do the law enforcement officers locate the person?

Recently the French Government proposed a 'secure electronic national identity card', to be implemented from around 2007. The proposal was for a credit card style identity card containing a fingerprint and photograph on a chip, which would be recorded on a central database. This proposal was opposed by human rights groups and the national authority and regulator on computing systems and databases, the Commission nationale de l'informatique et des libertés, (CNIL). Another non-compulsory card is being discussed.

**Germany**

Compulsory registration of individuals was introduced under the Reich Registration Law of 1938, and identity cards were introduced in 1950. It is not compulsory to carry the German identity card the, "Personalausweis", however it is compulsory to prove your identity to police if requested. (List of Identity cards by country, 2006)

The card contains name, date and place of birth, nationality, address, height, eye colour, date of expiration, signature and photo. Upon change of address authorities must be notified within one week, addresses are not considered personal information. Addresses are changed by putting a sticker on the old address, similar to a New South Wales driver's licence. There is no central database of identity card information.
Sweden

Sweden introduced a national identity card containing biometric data on the 1st October 2005, however it is not compulsory and does not replace previous paper based identity documents. The new identity card will facilitate travel within the Schengen region and also complies with the ICAO standards. The card has a contactless chip containing a digital picture of the cardholder and a traditional chip that will allow it to be used to access e-government services in the future.

Sweden also has a national population register, whereby everyone is issued with a personal number at birth which was previously used for many official transactions. The information contained within the register is not protected; anyone can look up the personal details of another. Whilst the national population register is widely accepted there has been opposition on grounds of individual rights to a linkage between the new identity card and the population register. Consequently the new card is not linked to the register and information is stored in the chip on the card.

Spain

It is compulsory to carry the Documento Nacional De Identidad (DNI) from 14 years of age at all times. It may be issued earlier to facilitate travel to European countries, and is often photocopied by private and public organisations. Credit card purchases cannot be made without showing this identification. It is to be replaced by Electronic DNI, similar in size to a credit card it will contain an embedded microchip that will store the cardholders personal data in electronic
format, a certified digital signature, and two biometric identifiers (facial image and fingerprint scans).

Brazil

Brazilians have used identity cards since the beginning of the 20th century. Also compulsory, the Brazilian identity card must be carried at all times. The card includes a photograph, full name, parents name, national status, thumb print and serial number.

Each state in Brazil is allowed to print its own identity card, however the layout for each must be identical. In Rio De Janeiro the cards are fully digitised which allow information contained within the card to be verified against its owner off-line.

The bar code on the card encodes a colour photograph, a signature, two fingerprints and other information. The technology was developed in 2000 to improve the security of the Brazilian identity card.

In compliance with E-passport regulations, the Brazilian passport will contain signature, photograph and ten rolled fingerprints. The passport contents and identity verification will be read electronically as the fingerprints and facial images will be available for automatic recognition.
United Kingdom
The introduction of a National Identity Scheme was announced in the Queens Speech on 17 May 2005. The scheme will eventually become compulsory, requiring all UK residents over 16 to have an identity card, however it will not be compulsory to carry the card. It is expected that the first cards will be issued from 2008/2009.

The identity card will include the cardholders name, date of birth and address, referred to by The Home Office as a 'biographical footprint'. This information will be cross checked with other databases such as National Insurance or driving licence records. The identity card will look similar to a credit card, however it will also contain a chip that contains your biographical footprint, an Identity Registration Number (printed on the card) and biometric data. In addition the card will also be enabled with a Personal Identification Number determined by the cardholder.

To minimise the chance of forgery the cardholder's details are verified by using the 'identity verification service' which will confirm the details contained on the card with those held on the National Identity Register. Basically the Identity Verification Service operates on the basis of confirming only the information that is required, for example, proof of age, work visa status, criminal record checks etc. All organisations need to be accredited to use the system and cardholder consent must be obtained to conduct a verification.
It is interesting to note that one of the nominated advantages to an Identity Card and Register by The Home Office is the use of information by police and security services to use the National Identity Register to compare fingerprints found at a crime scene that do not match existing police records. (Identity and Passport Service, UK. n.d.). The use of biometrics in this arena has the potential to provide investigative leads to unsolved serious crimes such as murder, rape and terrorist incidents.

**Israel**

The use of biometrics in identity documents is no better illustrated than in Israel where biometrics have been used extensively for several years. The border crossings from Israel to the Gaza Strip and West Bank are controlled by gates through which authorised Palestinians may enter. Thousands of Palestinians pass through these gates every day to work in Israel, at peak periods more than 15,000 people an hour pass through the gates, each person must have an identity card which is issued by the Israeli Military. There is a photograph printed on the identity card. A digital version is then stored on the smart card chip of the card which also contains biometric data of the cardholder’s fingerprints, facial geometry and hand geometry. (Jewish Virtual Library, 1999)

**Australia**

There is currently no official identity document in Australia, however in the financial sector, the Financial Transaction Reports Act 1988 (Cth) regulates the manner in which identity is established when an account with a financial
institution is opened. This process is the benchmark that many other sectors use to establish identity. The points based system is created under the Financial Transactions Reports Regulations 1990 (Cth). Documents submitted as proof of identity are each assigned a value depending upon their level of security and importance. To open an account with a financial institution a total of 100 points are required.

Under the Regulation documents are classified as either Primary or Secondary documentation with the following points allocated to each: Primary documents (which are allocated 70 points) include a current passport, birth certificate and a certificate of citizenship. Secondary documents include a drivers licence (40 points), public employee or student ID card (40 points), credit card (25 points), Medicare card (25 points) and local council rates notice (25 points).

The legislation creates various offences for breaching these regulations. It is an offence to open an account in a false name or to disclose only one of two names by which a person is known. This carries a maximum penalty of 2 years imprisonment (s. 24 Financial Transactions Reports Act 1988 (Cth). It is also an offence to knowingly or recklessly make a false or misleading statement in advising a financial institution of a change of name. This carries a maximum penalty of 4 years imprisonment (s. 21A Financial Transactions Reports Act 1988 (Cth).

The 100 points system is far from infallible. The ability of offenders to submit forged or altered documents is dependent only upon the quality of the document.
The system relies solely on the ability of the employee to verify the authenticity of documents. There is no system or process in place to facilitate verification by the issuing agency to confirm the details supplied.

On 26th April, 2006 the government announced that it had ‘decided to proceed in principle with a new access card for health and welfare services, though it ruled out introducing a compulsory national ID card.’ (Media Release, Prime Minister, 26 April 2006).
According to the Government the purpose of the proposed card is to assist people in obtaining Government benefits in a “convenient and reliable” way, with a primary function to minimise fraud and misuse of public funds.

The access card will have the cardholder’s name, a digital photograph, their signature and card number. In addition a microchip within the card will store a photograph, date of birth, address and details of children or dependents. The proposed card will be designed to facilitate the voluntary inclusion of additional information including emergency contact details, allergies, health alerts, chronic illnesses, immunisation information and organ donor status.

Information contained within the card will also be held within a database, the Secure Customer Registration System (SCRS). The Government at this stage has only stated that information contained within the database will only be available to authorised persons”. (Media Release, Prime Minister, 26 April 2006). Additional information relating to the card is limited. The technological architecture of the proposed access card has not been released, subsequently impeding public debate
and limiting analysis of the system relating to security of information contained within the SCRS.

The website of the Department of Human Services, www.humanservices.gov.au supports the use of the proposed access card as a proof of identity document outside of those interactions with the Department of Veterans' Affairs, Medicare and Centrelink, (being the agencies for which the access card is to be designed), however the Government has publicly asserted that the access card is not an identity card.

The cost of establishing the access card is $1.09 billion over four years. An independent assessment by KPMG has found that the access card will, improve efficiency, reduce identity fraud and fraud against Government health services which is estimated to result in a cost saving of $3 billion over ten years. In the KPMG Assessment, the Australian Bankers Association estimated an identity card system would cost their members over one hundred million dollars over ten years. Total private sector compliance costs were estimated at around one billion dollars annually. The official figure for the Australia card was $820 million over seven years. The revised estimate including private sector and compliance costs, together with other factors, would amount to several times this figure. (KPMG, 2004)

Claims that an access card or even an identity card will reduce identity fraud should be considered carefully. The quintessence of a secure system would include a tamper proof card that could not be replicated and a centralised database, which
would be imperative to authenticate an identity card that is impenetrable to criminals.

Opponents of the proposed 'access card' cite 'function creep' as one of the vehicles that will transform the original proposal into a national identity card. One such group is the Electronic Frontiers Australia Inc., a non-profit national organisation representing the online freedom and rights of Internet users, who have grave concerns about privacy and security in relation to such proposals and considers the roll out of smart cards by government as having an extremely high potential to result in the equivalent of an Australia Card, whether or not that is the government's intention at the outset. This potential arises from a combination of factors including the ease with which smart cards can be used for two-way communication with a centralised database and their assertion that smart card technology is designed to facilitate function creep. (Electronic Frontiers Australia, 2007)

At the Australia Card Summit in June 2005, the then Attorney-General, The Honourable Phillip Ruddock M.P rejected the idea of a national identity Card stating it 'could increase the risk of fraud because only one document would need to be counterfeited to establish identity.' This statement is in keeping with the Governments' announcement referred to earlier regarding the introduction of an access card as opposed to a national identity card.
In light of those countries who have fully embraced the concept of an ‘identity card’, such as Israel and those who are still assessing the pros and cons, such as Australia, one must acknowledge that the creation of one card in lieu of existing multiple proof of identity documents, creates a trophy of sorts to any criminally minded person to attempt to access such data. In reality, efforts are then centred on ‘hacking’ into one database and replicating one card. Even without technical skill, there is always the ability of criminals to infiltrate and corrupt the ‘holders of the key’ being those people ‘authorised’ to access information.

The damage to the individual who has their identity stolen when their community relies solely on one ‘identity card’ is magnified to that of a diversified identity authentication system. The benefits of an identity card must be weighed against the dangers associated with the issuance of a fraudulently obtained card and the consequences to, not only the victim of the stolen identity, but the community as a whole.

The inclusion of a biometric identifier has been touted as the solution to combating identity fraud. In theory, its inclusion will eliminate the use of multiple identities by individuals; however not necessarily eliminate the ability to steal another's identity who has not yet registered for such a system.

In May 2002, a Japanese cryptographer, Tsutomu Matsumoto, used gelatine to take a mould from a live finger which was used to fool fingerprint sensors. More remarkably was the experiment he conducted that involved the use of superglue to
replicate fingerprints from a glass. The superglue was then photographed with a digital camera; the contrast of the fingerprint image was then improved using a readily available software system, Photoshop and printed onto transparency sheets. Matsumoto then used a photo-sensitive print circuit board (available in hobby stores) and the fingerprint transparency to etch the fingerprint into copper, making it three-dimensional. This was then transposed onto a gelatin finger as explained earlier. Both methods fooled fingerprint sensors 80% of the time. (Schneier, 2002). This example of subverting biometric security systems and recent legislative amendments in the United States and Europe requiring the inclusion of a biometric identifier in passports leads to the question of biometric reliability.
Governments and businesses are increasingly turning to technologies to improve their ability to positively identify users of their services. Whilst ‘smart cards’ and ‘personal identification codes’ have become widely used, more recent technological applications include the use/inclusion of personal ‘biometric’ data to assist in establishing identity.

Biometrics, such as fingerprints, have been used by law enforcement agencies and other limited government agencies for a significant period of time. However, an increasing need to secure government information and services, and the activities of the corporate environment, has seen increased interest in the use of biometric data. As discussed earlier, Governments are also implementing the use of biometric data for border control purposes. Business is seeking to identify acceptable biometric applications for fraud control, particularly in relation to credit cards. Both are seeking the use of biometric data as forms of access control to sensitive and/or restricted areas.

Whilst a great deal of excitement is being generated by the potential of security improvements using biometric data, it is not (and should not be seen as) the panacea for preventing identity fraud and other crime. Many proponents of the
use of biometric data cite privacy concerns, whilst others identify a lack of scientific acceptance of proposed ‘standards’. From a fraud investigation prospective, an increased use of biometric data applications has both positive and negative connotations. Whilst the ability to identify a legitimate person will assist in preventing crime or identifying offenders, what happens when the biometric data of a person is ‘stolen’ or ‘cloned’? Additionally, the legal system within Australia is historically conservative and suspicious of accepting new technologies until they have been thoroughly and scientifically tested.

‘Biometrics’ is an identification system based upon the physiological, biological and/or behavioural aspects of a person. Woodward (2001, p.3) defines biometrics as the “...use of a persons characteristics or personal traits to identify, or verify the claimed identity of that individual”. Biometric indicator systems can provide fast and automatic identification of a person by converting the biometric indicator into a digital form, and then comparing it to information stored on a data-base. In this way, fingerprints, DNA, facial characteristics, voices, eye characteristics, hand geometry and signature dynamics are able to be used to assist in identification and identity authentication.

Biometric technology enables the measurement of particular physical characteristics or behavioural traits to recognise or verify the identity of an individual. There are a number of biometric applications being used or developed, including:

➢ Fingerprints
DNA

Iris and retinal imaging

Face recognition

Hand geometry

Voice recognition

Signature dynamics verification

Russ & Jain (2004, pp.134-135) identify that the use of biometrics applications has four important modules:

Sensor module – which acquires the raw biometric data of an individual

Feature extraction module – which processes the acquired data to extract a feature set that represents the biometric trait

Matching module – in which the extracted feature set is compared against the templates residing in the database through the generation of matching scores

Decision making module – in which the matching scores are used to either validate the user’s claimed identity (verification) or determine identity (identification).”

Grijpink (2001, p.155) suggests that the usefulness of biometric data applications is that it directly links a person to a data record by means of an unchangeable and non-transferable means: “Biometrics derives its significance from the person-related nature of the physical characteristics that serves as the point of recognition. In comparison with the
Biometrics has a wide range of uses. Many of the biometric indicators identified above are being implemented in one form or another in government and private sector environments.

**Fingerprint Technology**

An individual's fingerprint is formed as a foetus and expands uniformly as the body increases in size. Those fingerprints will remain unchanged until death, unless they become seriously altered by injury, scarring or disease. Fingerprint biometric indicators have been used by governments and law enforcement agencies for more than a century. One of the first records of the use of fingerprints as a biometric indicator of identity is in July of 1858 when Sir William Herscel (1833 -1918) a Chief Magistrate in India required a palm print and later fingerprints on the back of contracts. This use of fingerprints was based upon superstition, believing that personal contact with a document made it more binding that just simply signing the document. (Roberts, 2005)

Fingerprint technology has evolved significantly since the early days of ink on paper. Modern technology has allowed fingerprints to be scanned through electronic means. These advances have also allowed the technology to evolve to assist in providing a very accurate and quickly discernable biometric indicator. Unlike comparison of ridges and furrows with ink print impressions, modern
scanning procedures create an image of a fingerprint, then digitise certain feature extractions to provide a unique 'biometric code'. The feature extraction process identifies measurements based on ridges and burrifications (ridge separations). It is this unique digital code which is then stored on the database for future comparison purposes.

Wood (2002, p.47) suggests that, whilst not infallible, fingerprint biometric applications are sufficiently accurate to make them a viable application for broader identification uses; "Whilst this form of biometric is not the most accurate available, the chances of a device making a 'false accept' are extremely low". However, Wood makes one concession regarding the accuracy of this technology and extends that the scanning device can be calibrated to accept a lower number of positive matches of 'feature extraction points'. This lowering of the standard of identification has the potential to increase the likelihood of a false comparison.

The main advantages of the fingerscan/fingerprint biometric application include:

- Non-invasive nature;
- Rapid speed of comparison;
- Cost effective technology;
- Scientific and legal examination/acceptance of accuracy.

Fingerprint technology has become widely accepted within law enforcement and the wider community as a means of positively identifying a person. This general acceptance is well founded with a plethora of scientific research. It is also assisted
by popular use of fingerprint biometrics in novels, movies and other fictional entertainment mediums. The first author accredited with the popularisation of the use of fingerprinting is Mark Twain in his 1883 novel 'Life on the Mississippi', in which a murderer was identified with fingerprint identification.

Australian law enforcement agencies have been using fingerprint matching technology for many decades. In 1986, the National Automated Fingerprint Identification System (NAFIS) was implemented. This system is currently managed by CrimTrac, a Commonwealth government led collaboration of law enforcement agencies from each State and Territory within Australia. The NAFIS database is reported to hold in excess of 2.4 million records and is installed in over 30 locations around Australia (www.crimtrac.gov.au/fingerprints). If a comparison match between a sample and the data-base is identified, a fingerprint examination expert is still required to manually confirm that the comparison is a correct match.

The acceptance of the accuracy and application of fingerprint biometric data by the broader community may also provide the impetus for resistance to its application in private sector applications, such as banking and credit cards. Some privacy advocates suggest that, should government fingerprint records be cross matched with private sector fingerprint records, then personal information (such as a minor criminal conviction decades ago) may be provided to an employer, finance company, insurance company, etc. Whilst suggestion is made that the private sector can solely rely upon taking their own fingerprint biometric data
directly from customers, this information will still ultimately need to be verified (by one method or another) to government records.

**Facial Recognition Technology**

‘Facial Recognition Technology’ is a comparatively new biometric application when compared with fingerprint analysis. Whilst it is true that people have made assessments as to identity through matching a face with that of a person previously seen or known (such as recognising a friend or conducting a police identification parade with a victim of crime), it significantly differs as it applies to the analysis of digitised measurable characteristics, such as distance between the eyes. This is somewhat similar to that of digitised fingerprint biometric analysis. Current applications of facial recognition technology perform the task of identifying a person through their facial features by using geometrical analysis, thermal pattern imaging, line detection or a combination of these applications. Hubble (2002) suggests that the most common application of facial recognition utilises geometrical analysis, measuring distances between facial features and using comparison algorithms to differentiate between digitised database records.

Facial recognition technology is increasingly being considered as a viable, non-intrusive and passive biometric application by law enforcement, governments and the private sector. NSW Police have implemented the 'Phototrac' system to record offender photographs (under controlled conditions) and use those photographs to match against surveillance tapes installed in hotels, banks, etc. The Phototrac system is also currently matching offender photographs with other
offender photographs of similar physical characteristics to improve the integrity of police photographic identification ‘line-ups’. It is reported that NSW Police have in excess of 350,000 photographs available on a data-base (NSW Police Weekly, 2003, Vol 15). Police in Tampa, Florida, reportedly trialled facial recognition technology upon the crowd at a sporting event (NFL Superbowl). Whilst no arrests were made (as it was a trial only), the system used is reported to have identified several persons recorded on the local police offender database. (Pearce, 2004)

Other government agencies, including Australian Customs Service, have been trialling facial recognition biometric technology for border control purposes. This biometric system is one of the systems being considered to meet US Government passport improvement requirements. Similar to other biometric systems, private sector applications may also include credit card verification and banking services identification.

However, Krishnan (2004, p.5) identifies that facial recognition technology is not as effective and acceptable (at this stage) as other biometric applications. Citing results from the U.S. Government “Defence Advanced Research Projects Agency”, during the ‘Face Recognition Vendor Test 2002 (FRVT)’, it is noted that results only included conclusive positive comparison rate of “83% for a database of 800 people, 83% for 1600, and 73% for a data-base of 37,437 people.”
Subsequently, the reported accuracy rates suggest that facial recognition technology has scope for further development before being implemented as a fully automated and stand alone or single use biometric identification/verification system.

**Applications for Biometric Indicators**

Many industries, government agencies and financial institutions have long been grappling with the question of how to confirm identity, "Identifying people with certainty is both a time-consuming and costly activity." (Smith, 2003) The mere possession of an identification card (such as Medicare card), a passport or even a personal identification number (PIN) or password does not confirm or validate a claimed identity.

Those same industries, government agencies, law enforcement agencies and financial institutions have implemented biometric indicator systems to deal with some of their security and business issues. With the exception of biometric access control systems, such as fingerprint door access scanners, it is suggested that the most prevalent use of biometric technology has been the law enforcement sector. Some law enforcement applications of biometric technology includes:

- Identifying criminals through fingerprint matching technologies;
- DNA analysis of convicted and suspected offenders;
- Illegal immigration matters;
- Use of facial recognition technology to assist in identifying suspects.
The storage and use of these biometric indicators by law enforcement agencies are significantly restricted. Police will generally only possess the fingerprint records of criminals and persons employed in specially regulated industries (such as policing, gaming, security and intelligence professions). The breadth of data is therefore limited and does not include the general population. Additionally, the access to use this information is highly restricted to legitimate law enforcement purposes, and biometric data may not be provided to a third party, such as a bank or other private business. In many instances, the biometric information cannot even be provided to other government agencies.

With the increasing need for security in private sector applications, such as banking and financial transactions, businesses are seeking the development and implementation of effective biometric indicators. Such applications may include identity verification using biometrics in credit card applications/usage and personal loans.

Limitations in the use of Biometrics

The ability of both government agencies and the private sector to implement a truly useful biometric identification system is problematic. Both require the collection of identification through current traditional methods before it can be aligned to a sample of biometric data also being provided. In the case of government agencies, unless the provider of that biometric data has previously provided biometric data, such as a convicted criminal having been fingerprinted
(or the person is very well known), it is possible for a fictitious or stolen identity to be provided at the time of providing the biometric. Whilst this could mean that a criminal could legitimise a false or stolen identity through the implementation of a new biometric identification system, it is also acknowledged that it means the individual will be limited to that particular identity whilst remaining within that country/jurisdiction (such as Australia). The only possible solution to this conundrum is for the government to obtain biometric data at birth.

The configuration of the system used will also have a direct bearing on the limitations of the biometric data. Krishnan, (2004) identifies two distinctly different biometric systems:

**One to many comparison** – where a persons’ biometric information is stored on a central database and comparison is made by the person to that database (such as a finger-scan system at a shop linked to a central computer to confirm the identity of a credit card user.

**One to one comparison** – where a person’s biometric information (such as a fingerprint) is stored on a smart card and comparison is made between the person presenting the card and the information contained on it.

The question of centralised or decentralised storage is important. The storage of biometric detail on a ‘smart-card’ (decentralised) in the possession of the person who provided the biometric data allows for the determination as to whether the card holder is entitled to use that card. However, this will not establish whether that person has fraudulently obtained other ‘smart-cards’ using different identity
details (such as with another bank). Opponents of this system argue that if biometric information can be stored on the 'smart-card', then it will only be a matter of time before criminals can clone these cards or manipulate the data within them to change the biometric information to their own (as is the case with current cloning of information on a credit card magnetic strip).

At the other end of the spectrum (centralised), should a person’s biometric detail be stored within a central database, it would allow for an immediate determination as to whether the person has previously registered using a different identity. However, this system may also raise significant privacy and security concerns. Opponents of this system also suggest that, unless significant security measures are developed, it may also be prone to computer hackers who could steal or similarly manipulate the database for criminal purposes.

Apart from the integrity of the initial record or sample of biometric data, limitations in the usefulness to law enforcement and government/private sector applications of biometrics can be categorised into two broad groups:

- Legal Issues
- Privacy Issues

**Legal Issues:**

**Dissemination of government biometric information:** - Government agencies are currently strictly controlled in the collection and/or dissemination of the
personal information of citizens within Australia. The control of this information is by means of legislative process, including Commonwealth, State & Territory privacy laws. In essence, government agencies (including police) cannot disseminate the personal information held on government databases except for legitimate law enforcement purposes and only to prescribed authorities, such as Australian Taxation Office and Workcover. As an example, at present the personal information regarding a driver's licence is stored, both on a government data-base and on a licence in the possession of the person. Should the person provide a driver's licence to a private sector organisation as proof of identity, it is unlikely that the private organisation can be completely satisfied that the licence, and identity of the person, is completely legitimate as they cannot cross reference against the government (RTA) database. Therefore, depending upon whether Commonwealth and/or State governments utilise a centralised, whole-of-government database or implement localised individual systems, the biometric information in the possession of the government may not be disseminated to the private sector organisation under current legislation (except if the localised database also records biometric data on a device such as a smart-card, as a replacement for a driver's licence).

In effect, this means that, irrespective of government awareness of the identity of an individual, private sector organisations may not be in a position to verify or authenticate the identity of a person any more conclusively than present procedures (such as the 100 point identification regime). As a post-script, it is suggested that any move to an integrated private/public sector database or data-
sharing program would drastically increase citizen objection based on privacy concerns.

**Self-Incrimination:** - The judicial system used in Australia relies upon the long established right of an individual against self-incrimination. Legal objection may arise if an individual is not afforded that right during a process to collect biometric data, such as a credit card application. There is currently no legislation or case law in Australia relating to the use of biometric data collected by a private organisation that has subsequently been used in the criminal investigation and prosecution of a person for an offence. For example, if a person must provide a bank with a fingerprint to establish identity to obtain a credit card (and that person has never been fingerprinted by police previously), then has that same person been afforded the right against self-incrimination if the police obtain that fingerprint from the bank database for the purposes of investigating an offence?

**Accuracy/Expert Status:** - The long history of fingerprint analysis within law enforcement has enabled police to formulate and benchmark acceptable standards, upon which expert evidence may be admitted to a Court regarding identification. This process has been relentlessly tested in the Courts to define those acceptable standards. In both Commonwealth and State evidence legislation, the ability to provide ‘expert scientific evidence’ is governed by respective Evidence Acts and requires a strict regime of establishing the level of expertise of the provider of that evidence. Expert status is established with considerations such as training, experience and exposure to the relative field. However, the same rigorous legal
scrutiny has not yet been established for automated biometric applications (including fingerprint and facial recognition). This may affect the ability of government authorities to provide evidence based upon an automated biometric comparison, without resorting to traditional ‘expert’ evidence. Whilst this is not problematic for fingerprint evidence or facial recognition, it may be for other biometric applications such as iris scanning, which has a much more limited depth of scientific and legal scrutiny.

**Evidence continuity** – A significant legal principle in the Australian judicial system is the requirement of the prosecuting authority to establish, “beyond reasonable doubt”, all elements of an offence (and on the balance of probabilities for civil proceedings). In this respect, the prosecutorial obligation often includes a necessity to establish the continuity of evidence. This may be particularly difficult in the use of a person’s biometric data that has been collected for private sector purposes of identity/verification. The private sector may not prioritise potentially remote investigation/evidence concerns over commercial concerns, such as customer service and marketing. In essence, a lack of definable continuity of biometric records may render that evidence useless for investigative purposes, should a private sector system be compromised by criminals.

**Privacy Issues**

Privacy concerns have been raised in relation to the introduction and application of biometric identification/verification systems. Those concerns include:
- Surreptitious use of personal biometric information;
- Discrimination of persons as a result of the misuse of biometric information;
- Control over the ‘third-party’ or unauthorised dissemination of biometric information.

Concern may be raised regarding the potential for biometrics to reveal more information than originally intended. This concern is extended to the potential for the misuse of that information by private and public sectors alike. Krishnan (2004, p. 3) notes that

"Voice can reveal emotions and age; face can reveal emotions, race and health; and iris can reveal health. This information, if available to an employer, may result in improper use and could result in decisions based on the "extra" information the biometrics provide. This may result in people from certain groups being targeted, and may result in denial of services and other embarrassing situations."

Rees (et al; 2004, p.4) suggests that one of the more sinister privacy issues regarding the misuse of biometric data is ‘function creep’, whereby the biometric data collected for one specific purpose may subsequently be used for another unintended or unauthorised purpose. An example of ‘function creep’ could include an insurance company that collects biometric information for identification/verification purposes, then uses that information to determine potential health risks for future health insurance purposes. The same principles and concerns apply to the unintended dissemination and use of biometric data by
'third parties', such as law enforcement agencies following the commission, or suspected commission, of an offence.

Gridipink (2001) notes that one of the fundamental pillars of the protection of privacy is that data from one sector cannot automatically be used in another sector. Dependent upon the biometric system and application, it also may be possible for 'smart-card' technology and facial recognition technology to be integrated and misused, whereby remote scanners could correlate 'smart-card' (simply containing a fingerprint) with photographs to surreptitiously establish a more broader profile of a person. Prior to the broad implementation of biometric systems, definitive legislative controls need to be established to regulate the use and misuse of such technology – “Applications with a supra-sectoral character call for explicit public approval because the implications for the protection of privacy could become apparent only gradually and over a wider area than people may initially have anticipated. A regulation by law could supply the necessary approval.” (Gridipink, 2001, p. 4).

Technology has drastically altered the way society carries out business. However, those same technological advances have spawned their own problems, not least of which is 'identity fraud'. The impersonal nature of many business and government transactions makes anonymity in the digital environment somewhat easier. Whilst law enforcement agencies have used fingerprint biometrics for many decades, it is envisaged that broader biometric applications will be increasingly of great significance to the prevention of crime through identity verification and/or authentication. The use of biometric based applications is growing as
governments, corporations and the general public place increasing emphasis on security, including personal identity security, and security from crime/terrorism.

The design and choice of a biometric application involves a large number of implicit choices that will determine the effectiveness of the application, both in terms of security, fraud prevention and the consequences for personal privacy. Biometric technologies that enable the automated verification of identity will be a cornerstone in minimising crime involving stolen or manufactured identities. However, comprehensive accuracy, legal, security and privacy issues need to be examined before the true potential of biometric applications in the government and private sectors can be realised.
Chapter 10

LEGISLATIVE ANALYSIS

Legislation in Australia relevant to identity theft and/or fraud is essentially aimed towards three specific areas.

1. Prohibiting particular activities, such as impersonating a person with some form of legal definition (such as solicitor, police officer or doctor); obtaining a valuable item through impersonation; or the manufacture and presentation of fraudulent documents within an intention to obtain an item, a service or authorisation to conduct some other form of regulated function (such as driving a certain class of motor vehicle).

2. Legislation to assist persons who may become the victims of identity related crimes, such as certain powers to access necessary information.

3. Statutory obligations upon organisations to protect the personal information collected or entrusted to them.

Whilst point 2 is of significant importance, the legislative impact of points 1 and 3 requires a closer analysis. Why? Because any legislative framework to assist
victims of identity theft is very much reliant upon what is specifically proscribed in legislation and regulations pertaining to the 'theft' of identity and the protection of lawfully acquired personal information. Point 1 is also specifically relevant to the prevention of manufactured or fictitious identities.

Prior to examining Australian and international legislation, it is prudent to note that under current Australian legislative parameters, it is legally impossible to 'steal' a person's legitimate identity. Stealing or Larceny can only occur for a tangible object and identity is neither 'tangible' nor an object. It is however possible to fraudulently assume the identity of a natural person, or to purport oneself as being identical to that of another natural person. Naturally, it is also possible to create or manufacture an entirely fictitious identity, or any part thereof (such as merely changing the year of birth in order to increase or decrease age).

**The historical legislative framework in Australia**

"Identity fraud in its own right is a nebulous thing. We ought to be looking at the ultimate crime that is committed, not necessarily the methodology of committing it. That is, if you have defrauded the Commonwealth of a particular sum of money, what ought to be of issue to us is that you have defrauded the Commonwealth of the money, not so much whether you did it by identity fraud, by sticking your hand through a window or by whatever method." (Federal Agent Williamson – Australian Federal Police, ANAO REPORT No. 37)
Because “identity theft is typically not a stand alone crime” (GAO-02-363), criminal law in Australia has predominantly been reactive and very narrowly focussed towards the concept of ‘identity’ as only being a mechanism of the overall deception to obtain certain valuable things, services or restricted authorisations. The idea that ‘identity’ itself may be a valuable commodity, or at the very least a highly specialised criminal tool, does not appear to have been understood or adequately addressed in criminal legislation. A typical example of how the criminal law has been traditionally narrowly focussed in this regard may be viewed in the Western Australian Criminal Code (Section 510):

**Criminal Code (W.A.)**

**Section 510 - Personation in general**

510. Personation in general

_Any person who, with intent to defraud any person, falsely represents himself to be some other person living or dead, is guilty of an offence which unless otherwise stated, is a misdemeanour; and he is liable to imprisonment for 3 years._

_If the representation is that the offender is a person entitled by will or operation of law to any specific property, and he commits the offence with intent to obtain such property, or possession thereof, he is guilty of a crime, and is liable to imprisonment for 14 years._

Similarly, Section 184 of the Crimes Act, 1900 (NSW) creates the offence of Fraudulent Personation.
Crimes Act 1900 (NSW)

Section 184 - *Fraudulent Personation*

*Whosoever falsely personates, or pretends to be, some other person, with intent fraudulently to obtain any property, shall be liable to imprisonment for seven years.*

*Nothing in this section shall prevent any person so personating, or pretending, from being proceeded against in respect of such act, or pretence, under any other enactment or at Common Law.*

Both Section 510 of the Western Australia Criminal Code and Section 184 of the New South Wales Crimes Act are typical of criminal law in all States and Territories within Australia. The legislation has historically been predominantly focussed towards financial fraud related offences. The legislation has a requirement for the prosecution to prove, beyond a reasonable doubt, that the accused person assumed the identity of another person with the 'mens rea' (guilty mind) of an intention to defraud. The use of a stolen or fictitious identity is merely viewed as the vehicle by which another crime, such as financial or credit fraud, may be committed.

*The effect of Births, Deaths & Marriages legislation.*

The subordinate context of identity in Australian criminal legislation may have been facilitated by an acknowledgement that identity of Australian citizens is not absolute. Each State and Territory in Australia has virtually identical legislation regarding changes of name. Particularly, each State and Territory has enshrined in
legislation that a person has a right to change their name either through an amendment to the respective State register or by way of "repute or usage".

**Births, Deaths & Marriages Registration Act 1995 (NSW)**

*Section 32 - Change of name may still be established by repute or usage*

32. Change of name may still be established by repute or usage

*This Part does not prevent a change of name by repute or usage.*

Essentially, the right of citizens to be registered as one identity, yet freely use any number of other identities through "repute or usage" is absolute. The effect of Section 32 of the Births, Deaths & Marriages Act 1995 (NSW) is that there is no legislative requirement for any person to maintain usage of their identity as registered with the respective State or Territory Registrar of Births, Deaths and Marriages. Whilst the insertion of this type of Section may have been an acceptance of the Australian cultural psyche of shortening names (e.g.: Harold to 'Henry', or Catherine to 'Cathy'), it potentially creates a strong legal argument that it may also render inoperable other pieces of legislation which specifically seeks to identify a person – such as requirements in obtaining a driver's licence.

Whilst it is a legally 'grey' area, some pieces of legislation may attempt to limit a person from assuming a new identity, by reason of "repute or usage". One such example is the group of offences prescribed in Section 307 of the Crimes Act 1900.
(NSW). Particularly, Section 307B creates an offence for a person to provide false or misleading information.

Crimes Act 1900 (NSW)

Section 307B - False or misleading information

(1) A person is guilty of an offence if:

(a) the person gives information to another person, and

(b) the person does so knowing that the information:

(i) is false or misleading, or

(ii) omits any matter or thing without which the information is misleading, and

(c) any of the following subparagraphs apply:

(i) the information is given to a public authority,

(ii) the information is given to a person who is exercising or performing any power, authority, duty or function under, or in connection with, a law of the State,

(iii) the information is given in compliance or purported compliance with a law of the State.

Maximum penalty: Imprisonment for 2 years, or a fine of 200 penalty units, or both.

(2) Subsection (1) does not apply as a result of subsection (1) (b) (ii) if the information is not false or misleading in a material particular.

(3) Subsection (1) does not apply as a result of subsection (1) (b) (ii) if the information did not omit any matter or thing without which the information is misleading in a material particular.
(4) Subsection (1) does not apply as a result of subsection (1) (c) (i) if, before the information was given by a person to the public authority, the public authority did not take reasonable steps to inform the person of the existence of the offence against subsection (1).

(5) Subsection (1) does not apply as a result of subsection (1) (c) (ii) if, before the information was given by a person (the "first person") to the person mentioned in that subparagraph (the "second person"), the second person did not take reasonable steps to inform the first person of the existence of the offence against subsection (1).

(6) The burden of establishing a matter referred to in subsection (2), (3), (4) or (5) lies on the accused person.

(7) For the purposes of subsections (4) and (5), it is sufficient if the following form of words is used:

"Giving false or misleading information is a serious offence."

Whilst Section 307B of the Crimes Act 1900 (NSW), and the other group of offences contained within Section 307 of that Act, seek to prosecute persons who may provide false or misleading information, legal uncertainty still remains as to whether a person who provides a name other than the identity registered with the Registrar of Births, Deaths & Marriages (or contained in a passport for a non-citizen) is criminally culpable if that (other) name falls within the parameters of "repute or usage". There is currently a paucity of case law regarding the interaction and effect of the provisions of the Births, Deaths & Marriages Act 1995 (NSW) upon other relevant Acts. However at best, the various pieces of legislation are ambiguous and provide legal uncertainty.
Why is the 'repute and usage' parameter, as reciprocated in 'Births, Deaths & Marriages Register' legislation throughout Australia, potentially so important to the issue of false identity?

➢ It provides a legal mechanism for an argument that people may utilise a name other than that which is contained on the official register of births in this country (or passport information for non-citizens).

➢ It renders ambiguous other legislation aimed at ensuring correct identity details are recorded in registers for restricted activities (such as obtaining a driver's licence).

➢ For the long-term criminally minded, it would provide an avenue for the legitimate establishment of multiple identities, potentially including manufactured identities or the assuming of another person’s identity.

➢ It fails to counter the cultural norms of other countries, such as nations from the Middle East and South American regions, where the use of varying and multiple prefixes is accepted and legitimate, yet which would allow such a person in Australia to obtain multiple identities. Prefixes such as ‘bin’, ‘el’ and ‘al’ contained within and between names are, in some cultures, interchangeable, yet within Australia would enable sufficient difference to legally differentiate a person from others. The reciprocal of that differentiation is that a person could legally obtain multiple forms of identification (such as multiple driver’s licences) with those slight differences. For example, a person may legitimately be known as Mahmoud al salim bin Mohammad. This person could legitimately obtain identification in the names:
The cultural uniqueness of some regions may thereby provide lawful avenue for an individual to obtain multiple forms of identification in at least seven differing name structures. This is not limited to Islamic or nations from the Middle East. Predominantly Christian South American nations often allow individuals to have both names consisting of a first name and family name, in addition to the adoption of a single name (such as well-known soccer identities 'Ronaldhino' and 'Pele'). This single name may have no literary connection with their first name or family name.

- It may provide a longer period of time between the acquiring of documentation containing a false identity to that of detection by law enforcement agencies. This latter point is particularly salient in circumstances where the fraudulent identity has been used for purposes other than fraud related activities (such as establishing bank accounts to transfer monies from Australia for terrorist purposes, or the hiring of a vehicle to be used in connection with a terrorist incident). The linking of
the ‘other (false) identity’ to the person’s true or registered identity may take law enforcement agencies significantly greater time and resources to achieve.

**Penalty Disparity and the use of penalties to discourage false identities**

Another factor of particular note in reviewing identity related legislation is the penalty disparity between criminal legislation and legislation directly relating to licensing & entitlement cards. As identified above, the NSW Crimes Act (Section 307 A-C) provides significant penalty of 2 years or 200 penalty units. At the present time, a penalty unit is equivalent to AUD$110. Therefore, a penalty for providing false or misleading information is 2 years or AUD$22,000 if criminally prosecuted.

However, specific legislation regarding the provision of false or misleading information, such as identity, in the acquisition of a driver’s licence in NSW only attracts a penalty of “20 penalty units” or AUD$2200.

**Road Transport (Driver Licensing) Act 1998 (NSW)**

**Section 22 - Obtaining driver licence by false statements**

(1) A person must not:

(a) by a false statement or any misrepresentation or other dishonest means, obtain or attempt to obtain a driver licence or the renewal of a driver licence, or
(b) without lawful authority or excuse, possess a driver licence obtained or renewed using those means.

Maximum penalty: 20 penalty units.

(2) A driver licence so obtained or renewed is void, and the Authority may alter the driver licence register accordingly.

(3) Subsection (1) does not apply to a driver licence receipt issued by another jurisdiction.

Notwithstanding the ambiguity regarding the use of an identity that is provided by way of "repute or usage", there is little alignment of penalties regarding criminal legislation and that of legislation pertaining specifically to persons fraudulently acquiring licensing or entitlement cards. Common law in Australia dictates that the most appropriate indictment should be pursued, particularly where an indictment is enacted for a specific set of circumstances. In this regard, there is little disincentive for criminals to use fraudulent identity information in acquiring a driver's licence as they would be most likely to receive an insignificant fine.

The issue of penalty parity is particularly poignant in respect to a driver's licence, as this is one of the more significant forms of identification which is also commonly used as the primary identifier in applications for other goods and services (such as bank accounts, passports and restricted goods such as chemicals).
An argument for legal reform in Australia and Overseas

There is growing evidence that the notion of identity theft or illicit identity manufacture as only being 'a vehicle for other crimes' is largely reactive and may be somewhat outdated. Some may view the historical perspective as akin to only prosecuting armed robbers following a robbery and not proactively seeking to legislatively restrict access to firearms before they can be used in a crime.

The speed at which criminal activity may now be committed, with the use of progressive technologies, may establish a legitimate necessity for governments to proactively proscribe legislative remedies. Additionally, identity 'theft' and identity 'manufacture' is no longer the sole domain of financial fraud related activities. Stolen or otherwise false identification may also be used to procure or facilitate the acquisition of items that are prohibited to the general community, such as ammonia nitrate based fertilisers.

Assumed or manufactured identities may also mask the true identity of a purchaser of various non-restricted items, such as hexamine, hydrochloric acid, chlorine, castor beans or any other legitimate and innocuous substances that may ultimately be used in the manufacture and detonation of an improvised explosive device, poison or used for another terrorism related purpose.

Recognition of the importance of identity as a legal issue in its own right has seen some legislative reform in Australia. For example, the South Australia's
Criminal Law Consolidation (Identity Theft) Amendment Act 2004 specifically concerns identity theft. It provides that assuming a false identity of another person - living or dead, real or fictional, natural or corporate - makes a 'false pretence', even if the person acts with the consent of the person whose identity is falsely assumed. Making a false pretence with the intention of committing or facilitating the commission of a serious criminal offence is in itself an offence, whether or not that crime occurs. The 2004 Act also encompasses production or possession of material (including personal identification information) that enables a person to assume a false identity.

Criminal Law Consolidation Act 1935 (S.A.)

Section 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.

(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.
Whilst the provisions of the South Australian offences relating to false or assumed identities may not completely nullify arguments emanating from the ‘repute or usage’ provisions of the respective State Births, Deaths & Marriages Acts (or the cultural use of prefixes), it is nonetheless recognition that an identity is itself a commodity that requires closer legislative scrutiny and protection. It is also recognition that the fraudulent use of an identity (whether assumed or manufactured) is not restricted to financial fraudulent activity.

Recognition of this phenomenon and the impact of technology on identity as an issue in its own right have seen some other countries create legislation prohibiting the manufacture or possession of stolen or fraudulent identification as an offence. Such legislation is seen to be a preventative measure before a person then uses that stolen/fraudulent identity to commit a crime. For example, the USA has enacted the ‘Identity Theft and Assumption Deterrence Act, 1998’, which focuses specifically on identity fraud, in recognition of the growth of such offences at different levels of government. Essentially, ‘Identity Theft and Assumption Deterrence Act, 1998’ (U.S.) establishes, as a Federal offence, the assumption of another persons’ identity. The Act also provides significant penalty (both imprisonment and financial penalty) –

“This Act makes the theft of personal information with the intent to commit an unlawful act a federal crime in the United States of America, with penalties up to fifteen years imprisonment and a maximum fine of $250,000. This Act treats the issue of
identity theft and fraud more significantly than current Australian state legislation".

(ANAO REPORT No. 37)

The United Kingdom has also established the Identity Cards Act 2006, which seeks to establish the production and use of a national identity card system noted earlier. Irrespective of the arguments for and against the introduction of such a national identity mechanism, the legislation also treats the notion of identity as that of a substantive issue. Additionally, the legislation creates two categories of offences for the acquisition, possession and use of fraudulent identity documents:

1. The possession of an identity document or document making equipment with an intention to use it for the purpose of establishing registrable facts.

2. The possession of an identity document or document making equipment without lawful excuse.

Identity Cards Act 2006

Section 25 - Possession of false identity documents etc.

(1) It is an offence for a person with the requisite intention to have in his possession or under his control-

(a) an identity document that is false and that he knows or believes to be false;

(b) an identity document that was improperly obtained and that he knows or believes to have been improperly obtained; or

(c) an identity document that relates to someone else.

(2) The requisite intention for the purposes of subsection (1) is-
(a) the intention of using the document for establishing registrable facts about himself;
or

(b) the intention of allowing or inducing another to use it for establishing, ascertaining or verifying registrable facts about himself or about any other person (with the exception, in the case of a document within paragraph (e) of that subsection, of the individual to whom it relates).

(3) It is an offence for a person with the requisite intention to make, or to have in his possession or under his control-

(a) any apparatus which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents; or

(b) any article or material which, to his knowledge, is or has been specially designed or adapted to be used in the making of false identity documents.

(4) The requisite intention for the purposes of subsection (3) is the intention-

(a) that he or another will make a false identity document; and

(b) that the document will be used by somebody for establishing, ascertaining or verifying registrable facts about a person.

(5) It is an offence for a person to have in his possession or under his control, without reasonable excuse-

(a) an identity document that is false;

(b) an identity document that was improperly obtained;

(c) an identity document that relates to someone else; or
(d) any apparatus, article or material which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents or to be used in the making of such documents.

(6) A person guilty of an offence under subsection (1) or (3) shall be liable, on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine, or to both.

(7) A person guilty of an offence under subsection (5) shall be liable:

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction in England and Wales, to imprisonment for a term not exceeding twelve months or to a fine not exceeding the statutory maximum, or to both;

(c) on summary conviction in Scotland or Northern Ireland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both;

The relevant legislation contained within the United Kingdom Identity Cards Act 2006 has a slight and unique difference to legislation in Australia concerning the possession of false identification documents. Whilst Australian legislation, such as Section 302 – Crimes Act 1900 (NSW) prohibits the custody of a false instrument (such as an identity document), it requires the prosecution to prove an intention to use that false instrument in order that a person may:

(a) ... accept the instrument as genuine, and
(b) because of that acceptance, to do or not do some act to that other person’s, or to another person’s, prejudice.

Whilst subsections 1-3 of Section 25 of the Identity Cards Act 2005 (UK) has similar ‘intention’ requirements, it additionally has a parameter to prosecute a person in possession of a false identification document “without reasonable excuse” (Section 25, subsection 5). This allows the prosecution of a person who is found in possession of a false document, without requiring the prosecution to prove an ‘intention’.

At the furthest end of the identity card spectrum is the example instituted in the Republic of South Africa, which has also enacted provisions prohibiting the creation of a false identity or the assumption of another person’s identity in the Identification Act 1997 (R.S.A.). A penalty of five years imprisonment is prescribed in Chapter 4, Section 18, which prohibits any person from:

- Providing false particulars in the identification register or on an identification card;
- Possessing an identity card of another person;
- Asserting any incorrect information on an identity card as being correct.

In addition to a requirement for all nationals over the age of sixteen years to obtain and carry an identity card, the Government of the Republic of South Africa has included a biometric identifier on both a central database and the identity card. The biometric identifier used in this instance is a fingerprint. The recording of biometric data, both on the card and a centralised data-base, may assist in limiting
instances of identity fraud - particularly by the novice criminal. Whilst it may not completely eliminate identity theft or fraud, such a dual biometric checking mechanism may ultimately be required to enhance the security of the information. However, just like the 100 point identity system used in Australia, the accuracy of stored identity information is limited by the initial data supplied. The implementation of such a system in Australia would also require major amendments to Australian privacy legislation to ensure private sector organisations could compare data embedded in an identity card microchip with information contained within a government centralised database.
Chapter 11

CONCLUSION

"You have no clue who I am, and I could give you my fingerprint and you still wouldn't know who I am...Right now, your best information that I am who I say I am is what I know."

(Wayman; 2003)

This thesis sought to provide an overview of identity fraud in Australia, its implications and to identify areas for further intervention in order to combat identity fraud. A content analysis of the relevant literature was conducted to identify key issues resulting in a comparison of international trends to gauge Australia’s performance with other countries of similar economic and socio-cultural makeup such as the United States, Western European Countries and the United Kingdom. The results have been the exploration of linkages between methodology, identity fraud counter measures and the ability of the Australian legal framework and government policy in addressing one of the most pervasive of criminal activities, identity fraud.

Countering identity theft and identity fraud will require an overarching strategy to make the issue of documents used as evidence of identity and the issue of unique identifying numbers more secure. This will assist authorities to counter the use of counterfeit and stolen documents and to detect and prosecute criminals engaged in identity crime. Significant results in combating identity crime will not be realised...
by tackling just one of these areas. Whilst identity crime may never be completely eliminated, there is much that can be done to significantly increase the difficulty for the organised criminal or the opportunist. Tightening the processes used for the issue of documents commonly used as evidence of identity (such as passport and driving licences) could make identity crime significantly harder to commit. A more thorough checking of identity at point of use would be both possible and desirable. Additionally, the collaboration of counter-fraud activity, both within government and between government and the private sector, can also make identity crimes easier to detect and to punish.

There exists a disturbing lack of reliable quantitative data regarding the scope, extent and cost of identity theft and identity fraud within Australia. This lack of knowledge may arguably be the result of a history of governments, and their respective departments, not comprehending the significance of theft and identity fraud. The result of this has been a failure to proactively pursue strategic interdiction policies aimed towards elevating the notion of identity as a major personal and national security imperative.

The first step in identifying the risk of identity crime to the Australian community is to quantify the extent of the problem. Only once the true extent and nature of identity crime in Australia is fully comprehended can the most appropriate treatment options, such as biometric identifiers, facial recognition technology, or the introduction of identity cards be thoughtfully considered. As such, it would be prudent for the implementation of a centralised national database on incidents of
identity crime. The collection of this information would assist to facilitate an in-depth analysis as to the magnitude of identity crime in Australia. Further research into the facilitation of other criminal activities through identity crime would also be beneficial. However, given the extensive research conducted internationally, particularly the United Kingdom Home Office Identity Fraud Steering Committee, which has comprehensively identified significant fiscal consequences of identity crime in the U.K., it is also highly probable that identity crime is a major financial burden in Australia. Additionally, it must be understood that identity crime may also be a facilitator for non-financial, yet arguably more devastating crimes such as terrorism offences.

However, such research should not only inwardly focus upon the extent and cost of identity crime to Australia, but also outwardly focus upon international counter-crime initiatives. It would be prudent for such research to identify best practice in other countries with similar economic, political and cultural values. Issues such as appropriate levels of information sharing intra-government and government to private sector; how the right to privacy has been balanced or otherwise with the right to safety of others; information security, technology and legislative remedy to victims would all be highly relevant.

Additionally, further comprehensive research should encompass the use of identity cards in other international jurisdictions in order to identify the strengths and weaknesses of their systems and processes. Whilst some countries use identity cards as part of their counter-identity crime strategies, an identity card is only as
secure as the processes used to issue it and the safeguards employed against its counterfeiting and theft.

The issue of identity cards must therefore be analysed in conjunction with that of the accuracy and effectiveness of biometric identifiers. The concept of a biometric marker on key documents used as evidence of identity ostensibly has many attractions. However, with the exception of fingerprint analysis, biometric technology has yet to be proven on any sizeable population and the introduction of a technologically secure system would carry significant risks and costs to the entire community. In this regard, biometrics in isolation should not be viewed as the panacea for identity crime issues. Unless the true identity of a person has already been established through other conventional methods, providing biometric data may merely legitimise a false identity. Although, it is also acknowledged that the provision of biometric data in a centrally-controlled government system would limit the number of times that a person could fraudulently legitimise a false identity to just one instance.

Ultimately, there are a number of cost effective strategies that may be employed to either reduce the incidence of identity crime, or to limit the effect of such crimes upon both individual victims and the wider community:

- Promotion of victim hardening strategies by government and private sector organisations, such as banks and post-offices providing a document shredder for customer use within their premises.
- A central register of stolen documents (such as passports, driving licences and credit cards) would reduce the value of such goods in the market. The central register would also assist individual victims of such crimes to amend government and private databases to reflect their status as a victim (such as driving records, credit reference agency records and bank records).

- Promoting the sharing of data between law enforcement and government agencies, such as the RTA and Health Insurance Commission. The current notion that individual government agencies remain strictly autonomous, and do not share or verify information between them, is arguably a failure of government as a whole in combating identity crime.

- Improving the initial authentication of an individual identity when issuing documents, particularly those endorsed as part of the 100 point system (such as a drivers’ licence). This could include allowing a limited ability for financial institutions to authenticate identity documents with Statutory Authorities (such as a bank verifying the legitimacy of a drivers’ licence with the RTA before opening an account).

- Nationally consistent Commonwealth and State legislation to provide a more standardised legislative approach to identity crime. Such enhancements could include a more precise definition of identity for government issued identifier documents (such as restricting identity to that
which is registered with Births, Deaths & Marriages or passport if a foreign national); the establishment of an offence to possess a document containing a false identity without a lawful excuse; and parity alignment of penalties between various pieces of legislation to reflect the seriousness of identity crime.

Whilst the paucity of information pertaining to the current levels of identity-related crime in Australia may currently prevent informed decisions regarding how the issue could best be prevented, there is sufficient national and international evidence to suggest that identity crime is increasingly becoming a major crime problem. The community should be rightly outraged at the lack of reliable quantitative data into the extent and cost identity theft and fraud. It is therefore incumbent upon all who require personal identifiers in connection with their activities to seek the establishment of a Commonwealth Government led Commission of Inquiry into the prevalence of identity fraud within Australia, in order to facilitate appropriate solutions that balance security, accuracy, privacy, technology and penalty so as to proactively combat this insidious and serious organised criminal activity.
REFERENCES


Australasian Centre for Policing Research, (2002). Identity Crimes Scoping Paper
Australasian Centre for Policing Research, Adelaide.


Australasian Institute of Criminology and Pricewaterhouse Coopers (2003). *Serious Fraud in Australia and New Zealand*, Research and Public Policy Series No. 48, Australian Institute of Criminology and Pricewaterhouse Coopers, Canberra.


E-Passports Uses, Limitations and Impact on Simplifying Passenger Travel Initiatives (2005)
Retrieved 20th November 2005 from


General Accounting Office GAO-02-766 (June 2002). Identity Theft: Greater Awareness and Use of Existing Data are Needed. Retrieved 1st September 2006 from


Iyer, V. (2005). Beslan Massacre 'could have been prevented'; Retrieved on 12th September 2006 from http://www.timesonline.co.uk/article/0,,13509-1961489,00.html


Krishnan, K. (2004), 'Developing a police perspective and exploring the use of biometrics and other emerging technologies as an investigative tool in identity crimes.' Australasian Centre for Policing Research, Australia.

KPMG Fraud Survey (2004)

Lormel, D. Chief, Financial Crimes Section, FBI, Statement for the Record before
the Subcommittee on Oversight and Investigations, House Committee on
Financial Services (Feb. 12, 2002). Retrieved 20th July 2006 from

Lormel, D., Chief, Financial Crimes Section, FBI, Testimony before the House
Committee on Financial Service (October 3, 2001) Cutting off the Financial Lifeline
of Terrorists. Retrieved on 17th May 2007 from
http://www.fbi.gov/congress/congress01/lormel100301.htm

Research Service, Retrieved on 1st May 2006 from:
searchBF082003

Moore's Law, 2006 Retrieved:1st May 2006 from


Rees, A. (2000). Technology environment scan; Australasian Centre for Policing Research, Australia


LEGISLATION


Identity Theft & Assumption Deterrence Act 1998 (United States of America)

Retrieved on 12th March 2007 from www.austlii.edu.au