SENATE LEGAL AND CONSTITUTIONAL LEGISLATION COMMITTEE
ATTORNEY-GENERAL'S DEPARTMENT

Output 2.1

Question No. 49

Senator Ludwig asked the following question at the hearing on 24 May 2006:

In relation to national identity security strategy:

a) Who are the members of the Security Steering Committee?

b) Who are the members of the Commonwealth reference group on identity security?

c) In relation to the Commonwealth reference group on identity security – have they been working on or have they provided any documents, more broadly dealing with security that:

(i) have been published or;

(ii) that can be provided to the committee in terms of their work?

d) Did the five-point framework outlined by Mr Jordana last year originate from the Commonwealth reference group on identity security?

The answer to the honourable senator's question is as follows:

a) The National Identity Security Coordination Group is chaired by Mr Miles Jordana, Deputy Secretary, National Security and Justice, Attorney-General's Department. Members of the group are as follows:

State	Agency	Name
	Attorney-General's Department (Commonwealth)	Mr Miles Jordana
	Attorney-General's Department (Commonwealth)	Dr Dianne Heriot
	AUSTRAC	Ms Liz Atkins
	Department of Foreign Affairs and Trade	Mr Bob Nash
	AGIMO	Ms Robyn Fleming
	Department of the Prime Minister and Cabinet	Ms Rebecca Irwin
	Office of the Privacy Commissioner	Ms Karen Curtis
	Council of Australasian Registrars of Birth, Deaths and Marriages	Ms Helen Trihas
	Austroads	Mr Michael Bushby
ACT	Department of Justice and Community Safety	Mr Brett Phillips
NSW	Cabinet Office	Ms Leigh Sanderson
NSW	Attorney-General's Department (NSW)	Mr Laurie Glanfield
VIC	Department of Premier & Cabinet	Ms Jane Treadwell
QLD	Department of Premier & Cabinet	Mr Tony Keys
SA	Department of Premier & Cabinet	Mr Adam Graycar
SA	South Australian Police	Superintendent Tony Rankine
WA	Department of Premier & Cabinet	Dr John Phillimore

NT	Department of Justice	Mr Robert Bradshaw
TAS	Department of Premier & Cabinet	Ms Michele Mason

b) The Commonwealth Reference Group on Identity Security is chaired by Mr Miles Jordana, Deputy Secretary, National Security and Justice, Attorney-General's Department. Members of the group are representatives from the following agencies:

Attorney-General's Department	Department of Education, Science and Training
AUSTRAC	Department of Employment and Workplace Relations
Australian Communications and Media Authority	Department of Family and Community Services and Indigenous Affairs
Australian Crime Commission	Department of Finance and Administration
Australian Electoral Commission	Department of Foreign Affairs and Trade
Australian Federal Police	Department of Health and Ageing
Australian Government Information Management Office	Department of Human Services
Australian Secret Intelligence Organisation	Department of Immigration and Multicultural Affairs
Australian Taxation Office	Department of Industry, Tourism and Resources
Australian Securities and Investments Commission	Department of Prime Minister and Cabinet
Centrelink	Department of Transport and Regional Services
Commonwealth Scientific and Industrial Research Organisation	Department of Treasury
Customs	Department of Veteran Affairs
Department of Communications, Information Technology, and the Arts	Office of the Federal Privacy Commissioner
Department of Defence	Medicare Australia

c)(i)(ii)The Commonwealth reference group on identity security has not published any documentation regarding the work it has undertaken. However, the following reports are publicly available:

- ***Scoping Identity Fraud*** – an abridged version of a report on Identity Fraud Risks in Commonwealth Agencies (Attorney-General’s Department, September 2001). Attached as hard copy.

- ***Identity Fraud in Australia*** – An evaluation of its Nature, Cost and Extent (SIRCA, September 2003) available at: www.austrac.gov.au/publications/index.htm

d) The five-point framework outlined by Mr Jordana reflects the Australian Government announcement, on 14 April 2005, of the development of a national identity security strategy to combat identity theft and the fraudulent use of stolen and assumed identities as a matter of national priority.

ATTORNEY-GENERAL'S DEPARTMENT

SCOPING IDENTITY FRAUD

AN ABRIDGED VERSION OF A REPORT ON
IDENTITY FRAUD RISKS IN
COMMONWEALTH AGENCIES

by

GEOFF MAIN PSM
BRETT ROBSON

September 2001
Canberra

Preface to the Abridged Version

This paper is an abridged version of a more substantial document entitled:
"*Who Goes There? – A Study on the Management of Identity Fraud Risks*".

The report was the result of a scoping study undertaken by the authors for the Attorney-General's Department and was completed in August 2001. The study examined the Proof of Identity risks facing key Commonwealth agencies and developed options to improve personal identification practices and to prevent and detect identity fraud.

The study was allocated a "Protected" classification because of the sensitive nature of the material presented and discussed. Distribution of the report was restricted to those participating Commonwealth agencies.

Identity fraud represents a growing area of risk for all Commonwealth agencies and the community in general. In the interests of raising the overall level of awareness of the risks associated with false identification this document has been prepared for distribution to interested organisations who were not part of the study.

September 2001

TABLE OF CONTENTS

CHAPTER 1: Introduction

CHAPTER 2: A Framework for Considering False Identity Risks

CHAPTER 3: Some Options for Greater Consistency in POI Controls

CHAPTER 6: Recommendations

CHAPTER 7: Unique Personal Identifiers – An Overview

LIST OF FIGURES

INTRODUCTION

PERSONAL IDENTIFICATION

It is generally accepted within the Australian community that in order to receive a range of benefits and services an individual must first identify themselves to the organisation with which they wish to do business. Most organisations, whether in the government or private sector, have established personal identification and authentication procedures which a new client must satisfy to prove they are who they say they are.

The requirement to prove identity is ongoing as the Australian population grows, new organisations evolve and individuals move their business from one organisation to another. An indication of the dynamics associated with quantifying the population of Australia is depicted in Figure 1. The diagram portrays the inflows and outflows of categories of people which interact to drive the growth in the number of residents. Addition of the numbers in the individual categories shows a total population flow for 1999-2000 of more than 16 million people.

Based on Australian Bureau of Statistics (ABS) population statistics 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.

Some sense of the volume of personal identification checks required can be gauged by considering the operations of selected Commonwealth agencies. Last year, the Australian Electoral Commission processed 2.46 million enrolment forms and amendments, the Australian Taxation Office 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. The total number of registrations performed by these four agencies is huge but would represent a minor proportion of proof of identity transactions completed by all Commonwealth, State, Local Government and commercial organisations.

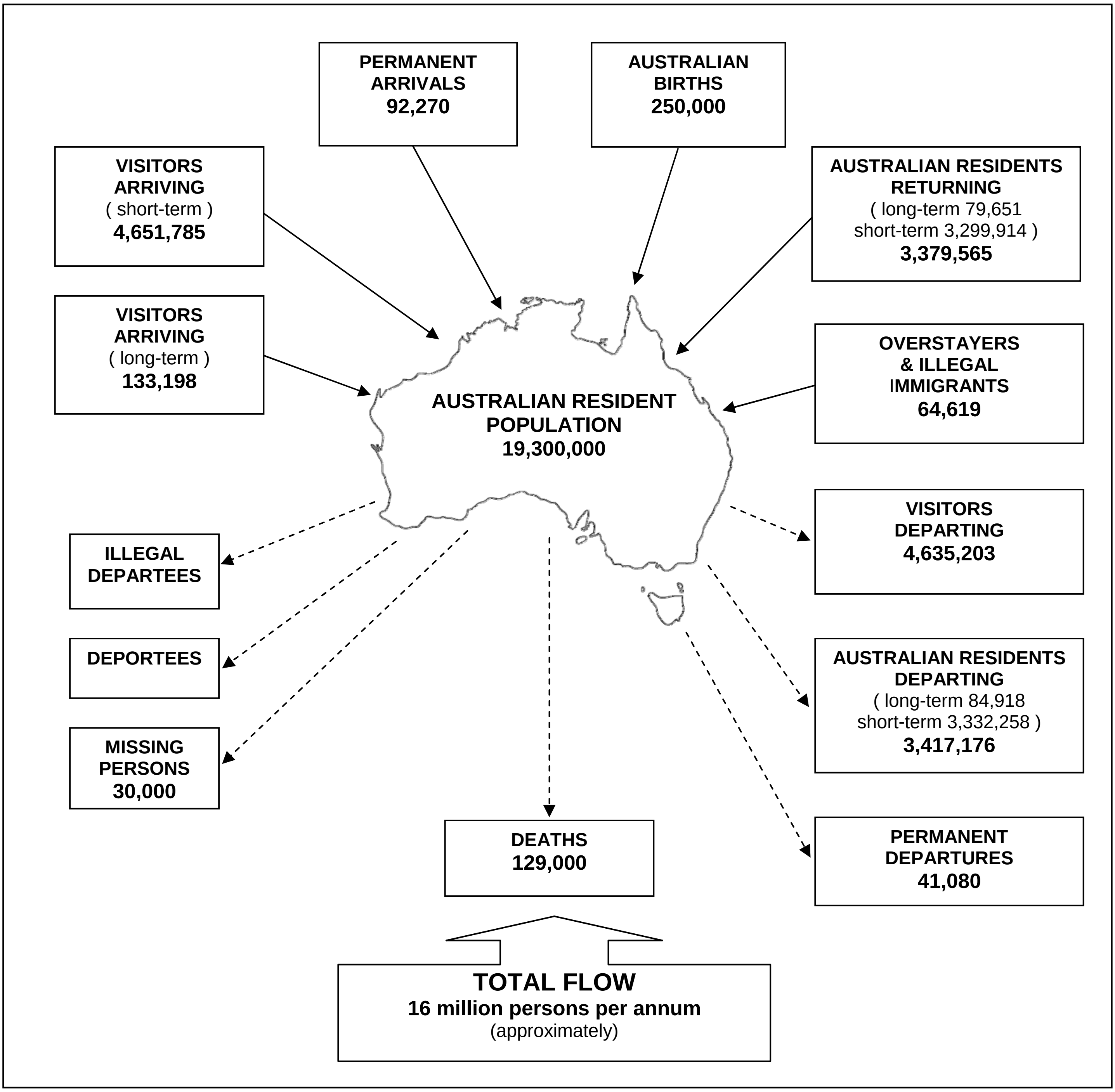
It is imperative that agencies accurately identify the person registering for benefits or services as a vital first step in maintaining confidence and integrity in their operation. Without such confidence organisations will be unsure of their clients’ entitlements to benefits and services and leave themselves vulnerable to fraud.

WHAT IS IDENTITY FRAUD?

Identity Fraud may be defined as an individual falsely representing him or herself as either another person or a fictitious person to an organisation for some benefit. This misrepresentation is supported by fraudulently obtaining or falsely reproducing identity documents.

FIGURE 1

FACTORS IMPACTING THE NUMBER OF AUSTRALIAN RESIDENTS - POPULATION STOCK AND FLOWS 1999-2000[1]


PERMANENT ARRIVALS 92,270
AUSTRALIAN BIRTHS 250,000
VISITORS ARRIVING (short-term) 4,651,785
AUSTRALIAN RESIDENTS RETURNING (long-term 79,651 short-term 3,299,914) 3,379,565
VISITORS ARRIVING (long-term) 133,198
OVERSTAYERS & ILLEGAL IMMIGRANTS 64,619
AUSTRALIAN RESIDENT POPULATION 19,300,000
ILLEGAL DEPARTEES
VISITORS DEPARTING 4,635,203
DEPORTEES
AUSTRALIAN RESIDENTS DEPARTING (long-term 84,918 short-term 3,332,258) 3,417,176
MISSING PERSONS 30,000
DEATHS 129,000
PERMANENT DEPARTURES 41,080
TOTAL FLOW
16 million persons per annum
(approximately)

[1] Sources:
Australian Bureau of Statistics, Population Size and Growth Statistics;
Australian Department of Immigration and Multicultural Affairs, Australian Immigration Statistics 1999-00;
National Missing Persons unit, Missing Person Statistics

In recent years it has become more widely accepted that identity fraud is presenting a growing threat throughout the world and that false identity provides a means of committing a wide range of criminal activity. An Australian Institute of Criminology (AIC) paper entitled *Identity-related Economic Crime* (September 1999) states that:

“The first step in perpetrating many acts of dishonesty is to ensure that any financial reward obtained is unable to be linked with the offender.”

Further, the growing use of technology in conducting business and accessing government services provides an additional means for the offender to preserve anonymity. Thus, we can expect that the incidence of crime associated with identity fraud will continue to grow.

THE IDENTITY FRAUD THREAT

In a paper entitled, *The Criminal Exploitation of Identity* (2000*)*, the Office of Strategic Crime Assessments (OSCA) points out that it is “critical to the functioning of the economy” that stronger systems for proof of identity are developed.

OSCA has identified the existence of significant forces that will amplify the criminal exploitation of identity over the next five years. They conclude that weaknesses in existing systems for managing identity along with changes in technology and business practices will worsen these risks.

Some statistical evidence published in *Numbers on the Run*, a report produced by the House of Representatives Standing Committee on Economics, Finance and Public Administration supports these concerns:

- An estimate that 25% of reported frauds to the Australian Federal Police (AFP) involve the assumption of false identities.
- A pilot of a “certificate validation service” conducted by Westpac and the NSW Registry of Births, Deaths and Marriages found 13% of birth certificates to be false.
- Centrelink detected about $12 million worth of fraud involving false identity in 1999.
- A survey by KPMG of over 1800 of Australia’s largest businesses found some 11.9% of fraud committed by outsiders involved the use of false documents.

For comparative purposes it is useful to look at some summary statistics on fraud in the United States of America. An indication of the potential size of the identity fraud problem in the US can be gauged from an estimate by the Association of Fraud Examiners that US organisations lose 6% of annual revenue to fraud and abuse each year. It is likely that identity fraud comprises a significant component of this as a number of independent analyses in the US have shown that this represents in excess of 90% of all financial crime.

Recently, in a speech made to the US House of Representatives, the Honourable Ron Paul said of identity theft (a particular type of identity fraud), “Just last year, American businesses and consumers lost 25 billion dollars to identity thieves!”[2]. Also, the FBI estimated last year that between 350,000 and half a million instances of identity theft occur in the United States each year[3].

LIKELY COST OF IDENTITY FRAUD IN AUSTRALIA

In considering the costs of identity fraud the *Numbers on the Run* report includes the following point:

“As stated by … the AIC, ‘the figures do not exist’ when it comes to considering the significance and cost of identity related fraud for the Australian government and the community.”

This view has general agreement, in particular it is supported by the Australian National Audit Office, National Crime Authority and AFP who all confirm a lack of national statistics on identity fraud numbers and cost.

Indeed, the quantification of the economic impact of identity fraud seems to be a common problem confronting a variety of organisations worldwide. All agree however, that the problem is significant, and growing.

An indication of the proportion of financial crime that is related in some way to identity fraud can be gauged from two US studies. The US General Accounting Office (GAO) has reported that for the years from 1995 to 1997 an average of 94% of arrests for financial crime involved identity fraud. Also, the same GAO report indicates that MasterCard International reported “about 96% of the …. total fraud losses involved identity fraud-related categories” in 1997[4].

Further, the AIC estimated in 1996 that the financial and economic costs of crime in Australia were a “minimum of 2.5% of Gross Domestic Product (GDP)”[5]. The analysis contained a breakdown of the costs of crime into its major components and it was calculated that the category of “fraud, forgery and false pretences” accounted for approximately 28% of the cost of all crime. If this figure is taken to represent the best measure of financial crime currently available, and it is agreed that most financial crime is identity related, then it (the figure of 28%) can be used to derive an estimate of the cost of identity-related fraud.

A simplistic attempt is made below to calculate the potential cost of identity fraud in Australia by utilising the AIC statistical analysis as a basis. The equation is:

Cost of identity fraud = Australian GDP ($billion) * Cost of Crime Estimated (%)
* Proportion of Crime which is Identity-related (%).

[2] Identity Theft, Hon. Ron Paul of Texas in the House of Representatives, 13 February 2001

[3] Congressional Press Release, 12 September 2000, www.nationalfraud.com/stats.htm

[4] General Accounting Office, “Identity Fraud: Information on Prevalence, Cost and Internet Impact”, (Briefing Report, 5/1/98, GAO/GGD - 98 – 100BR)

[5] Estimates of the Cost of Crime in Australia in 1996 (No. 72), John Walker, AIC

Australian GDP in 1999/2000 has been calculated by the Australian Bureau of Statistics to be in the order of $632 billion[6].

Application of the equation produces an estimate for the cost of identity-related fraud of in excess of $4 billion per annum. (i.e. 632 * 0.025 * 0.28 = 4.4)

This figure is effectively only an update of the AIC's 1996 estimate of $3 - 3.5 billion for the category of "fraud, forgery and false pretences"[2] but it provides an indication of the minimum likely cost.

A greater knowledge of the type and incidence of identity fraud being perpetrated against the community is required before more accurate quantification of both the size and cost of the problem is possible. Commonwealth agencies could provide a valuable contribution in this area and key agencies are currently examining the feasibility of conducting a joint exercise.

CURRENT WORK ON IDENTITY FRAUD

The *Who Goes There?* report, which forms the basis of this paper, makes particular reference to the studies completed by the House of Representatives Standing Committee on Economics, Finance and Public Administration - *Numbers on the Run*, the Office of Strategic Crime Assessments Occasional Paper - *The Criminal Exploitation of Identity* and the Australian Transaction Reports and Analysis Centre convened Steering Committee paper - *Proof of Identity*.

Also, the Australian Taxation Office (ATO) has over the last two years facilitated workshops between Commonwealth and State agencies on proof of identity issues. This work has been instrumental in raising the awareness of the risks posed by identity fraud and has contributed significantly to greater communication on fraud matters between agencies. A working group formed from these agencies has developed a common approach for assessing proof of identity documents which is currently receiving joint consideration. The working group has also developed a 'hierarchy of solutions' which recognises some fundamental concepts for preventing and detecting false identities and presents them in a diagrammatic form.

The undertakings of the above groups have resulted in a widespread recognition of the level of risk posed by identity fraud and significant analysis of the major issues is continuing on many fronts.

[6] Monthly Economic & Social Indicators 2000-2001, National Income, Expenditure & Product, ABS, Australian Parliament Library website

A FRAMEWORK FOR CONSIDERING

FALSE IDENTITY RISKS

AN OUTLINE OF THE PROPOSED MODEL

No complete framework which disaggregates, identifies and defines the full range of risks associated with false identity, and which in their totality we refer to as Identity Fraud, is available. It is intended that the model proposed here will overcome this deficiency by identifying each of the individual risk components and providing some structure to them. The inter-relationships that exist between these components, and which are sometimes confused, are identified and simplified.

The vulnerability of the current systems used for personal identification is emphatically explained in *The Criminal Exploitation of Identity* (OSCA). At the most fundamental level the limitations of the current systems can be categorised into two components, either involving the identity, or the document. First, there are limitations which relate to ensuring that the personal identification details provided by an individual are truly theirs. Second, there are also those limitations that relate to the veracity of the physical documentation presented as evidence of identity.

It must be concluded then, that without exhaustive checking of identity details, and the documentation provided, an agency cannot be certain if the identity information recorded on a document is accurate, singular and relates to the holder of the document, or even if the document is authentic.

Any specification of the risks associated with identity fraud needs to ensure that both those risks associated with the integrity of the identity and also those which target the integrity of the document, are fully considered. There are a number of discrete risks associated with each group and either, or both groups, are readily manipulated. The result is that a wide variety of methods are available to perpetrate identity fraud, ranging in sophistication and effectiveness.

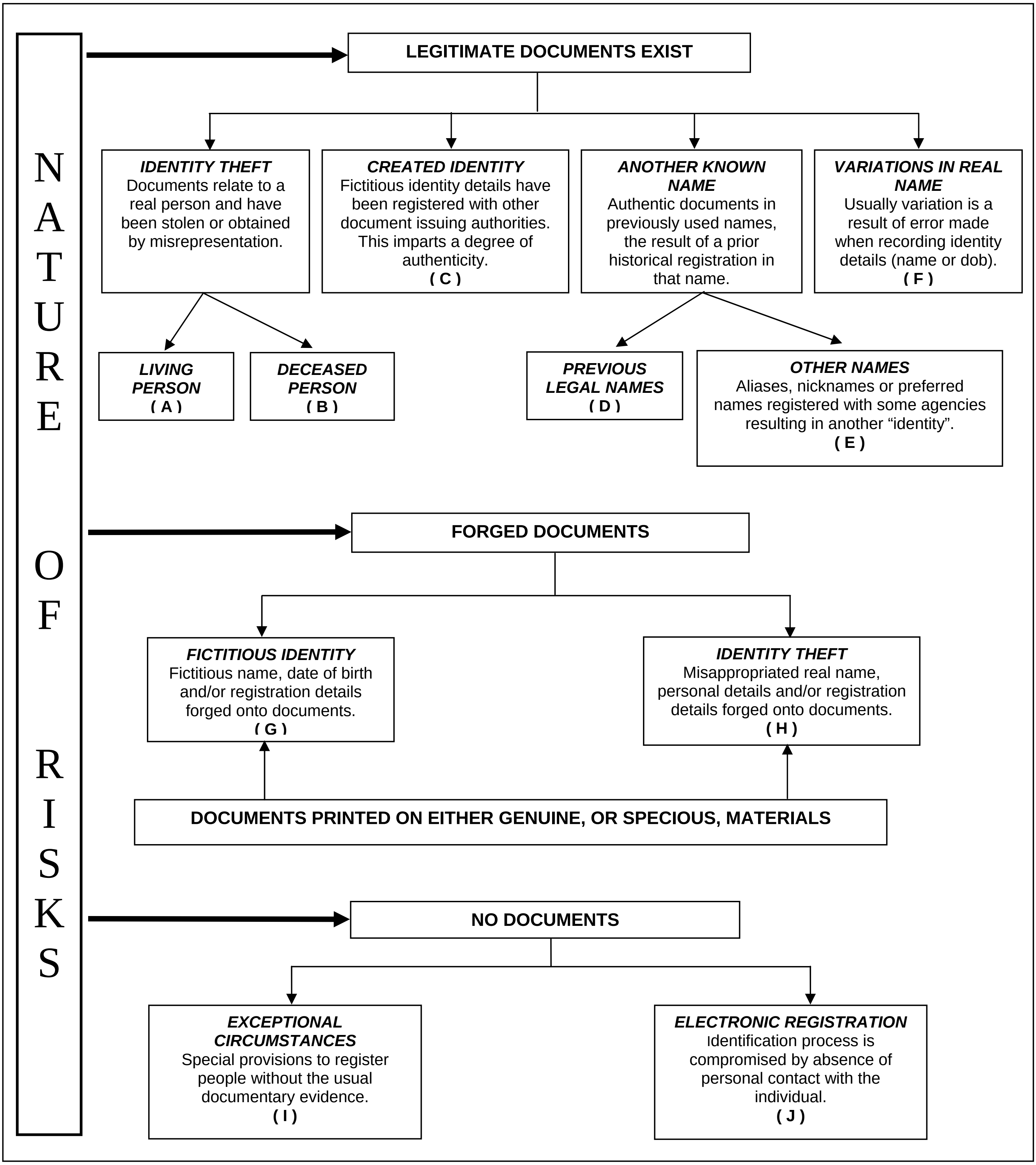
The individual characteristics of each particular risk and its inter-relationships with the other risks have been combined to form a model of the identity fraud problem. The proposed model is explained in the following section and is illustrated in Figure 2.

It is intended that this model provide the reference point for the further assessment of risk in this study.

For the model to be a useful tool in this regard it is imperative that it encapsulate all possible means of perpetrating an identity fraud. The complete specification of risk is a prerequisite for evaluating the effectiveness of existing identification systems and, if required, for designing new methodologies and processes to detect and prevent identity fraud.

FIGURE 2

**THE FALSE IDENTITY FRAMEWORK:
A MODEL FOR EXAMINING THE RISKS ASSOCIATED
WITH THE PROOF OF IDENTITY PROCESS**



NATURE OF RISKS

LEGITIMATE DOCUMENTS EXIST

IDENTITY THEFT Documents relate to a real person and have been stolen or obtained by misrepresentation.

LIVING PERSON **(A)**

DECEASED PERSON **(B)**

CREATED IDENTITY Fictitious identity details have been registered with other document issuing authorities. This imparts a degree of authenticity. **(C)**

ANOTHER KNOWN NAME Authentic documents in previously used names, the result of a prior historical registration in that name.

PREVIOUS LEGAL NAMES **(D)**

OTHER NAMES Aliases, nicknames or preferred names registered with some agencies resulting in another “identity”. **(E)**

VARIATIONS IN REAL NAME Usually variation is a result of error made when recording identity details (name or dob). **(F)**

FORGED DOCUMENTS

FICTITIOUS IDENTITY Fictitious name, date of birth and/or registration details forged onto documents. **(G)**

IDENTITY THEFT Misappropriated real name, personal details and/or registration details forged onto documents. **(H)**

DOCUMENTS PRINTED ON EITHER GENUINE, OR SPECIOUS, MATERIALS

NO DOCUMENTS

EXCEPTIONAL CIRCUMSTANCES Special provisions to register people without the usual documentary evidence. **(I)**

ELECTRONIC REGISTRATION Identification process is compromised by absence of personal contact with the individual. **(J)**

EXPLORING THE FALSE IDENTITY MODEL

A variety of methods are available to create a false identity. The range of methods and the inter-relationships which exist between them are depicted in Figure 2. A particular identity fraud may be committed by using one, or a number, of the methods outlined.

The distinguishing features of each identity risk is described below and referenced to Figure 2 by the use of an alphabet character from A to J.

False identity established with legitimate documents

- Theft of another person’s identity details can occur when a fraudster obtains authentic documents belonging to a real individual. The documents may be stolen, or obtained by misrepresentations made to the agencies which issue the documents. The person who has their identity stolen may be either living, or deceased and may be resident in Australia, or overseas. The misappropriated documents can be used for a multitude of fraudulent purposes including opening bank accounts, tax evasion, money laundering or welfare fraud. These frauds are usually more sophisticated in nature, use multiple identities and are relatively difficult to detect. Often research to identify deceased children is undertaken in order to obtain birth certificates to facilitate identification (see Figure 2, A and B).

- Often the starting point in the process of creating a new identity is for a stolen, counterfeit or altered document to be used by the holder to obtain legitimate documents from other agencies. Conversely, a new identity can be created and registered with a particular agency to obtain the initial supporting documentation. The above approaches have been described as the ‘circular path’ to identity creation and are characterised by the exploitation of weaknesses in identification systems to obtain one document which, in turn, is used to obtain others (see Figure 2, C).

- Many individuals are known by more than one name. This might be as simple as a woman having a maiden and married name, or as complex as multiple legal name changes. Some people prefer to be known by another name, or a slight variation of their “correct” name, such as a nickname. Regardless, documents with varying degrees of value have been issued at some time in the past by various agencies in those names. As these documents are legitimate it is very difficult for an agency not to accept the person as genuine (see Figure 2, D and E).

- Minor variations in the recording of a person’s real name can be the source of multiple identities for that individual. These can arise through errors made by agencies when recording identity details at the registration stage, by an individual having a preference for using their second name in place of their first name or by transposition of forenames and surnames. The later can be a particular problem with ‘double’ or composite surnames. Asian names in particular are frequently transposed. The incorrect recording of a date of birth can also lead to the formation of a 'new' identity as another document supporting the existence of an individual with different personal details now exists (see Figure 2, F).

False identity established with forged documents

- Fictitious identities can be given apparent legitimacy by transcribing believable personal details onto official looking documents. The advantage to the fraudster is that the identification processes of those agencies which normally issue the document are bypassed, simplifying the commission of the fraud. The counterfeited documents may be produced on genuine physical media stolen from the appropriate agency complete with document security features. Document identifying details, such as the agency reference number, can be replicated from legitimate documents. Alternatively, the manufactured documents may be very poor copies made on specious material and be readily identified as forgeries. The wide availability of, and familiarity with, computer and scanning technology mean this type of identity fraud is readily committed (see Figure 2, G).

- Identity theft has been mentioned earlier (see Figure 2, A & B) in relation to its commission with legitimate documents. It also occurs when personal identity details belonging to a real person are used on counterfeit documents. If the counterfeit documents themselves are of high quality then the resultant false identity will have a high level legitimacy. That is, the identity can be independently confirmed, as may the identifying features on the forgery (see Figure 2, H).

False identity established with no documents

- Most agencies have provisions to register people who through some 'exceptional circumstance' are unable to obtain documentary evidence to prove their identity. Often the only identification requested by an agency is that the person provides the name of a witness, or referee, to confirm their details. This arrangement, which predominantly exists to assist disadvantaged groups of people, represents an area of enhanced risk of exploitation by persons intent on establishing a false identity (Figure 2, I).

- As agencies re-engineer their business processes to take greater advantage of technological developments there is increasing risk that the client identification process will involve no personal contact. In the absence of appropriate controls, such an environment will facilitate the remote registration of false identities and the associated anonymous nature of the interaction encourage more offenders (see Figure 2, J).

IDENTIFICATION VERSUS AUTHENTICATION

So far only the vulnerabilities associated with the personal identification process have been examined – that is, only the systems used in identifying and registering a new customer. These processes are employed at first contact with a new applicant who seeks to register for the services provided by the agency. It is necessary that the correct identification of a new customer be considered by all agencies as an essential component of the first time registration process for identity fraud to be minimised.

In any subsequent contact between the new customer and the service provider it is not expected that identity will be proved on each occasion. Rather, it is only necessary that the person verify that they are the same individual who originally proved their identity to the agency. This process will be referred to as authentication.

Accurate authentication is necessary to ensure the person that an agency deals with is indeed the same person who originally registered for the service. Authentication may be conducted in a variety of ways and the degree of verification required will usually depend on the value of the service. A variety of authentication means are used including paper-based (e.g. sighting the original documents again, signature checks), knowledge-based (e.g. provision of little known personal details), electronic identifiers (e.g. passwords, digital certificates) and biometric processes.

In addition to the types of fraud described earlier, identity fraud can also occur where authentication procedures breakdown, thereby enabling a legitimate identity, correctly registered, to be stolen, or 'hijacked' for a period of time sufficient to commit fraud. The generality of this type of fraud is covered in the false identity model as 'identity theft' (see Figure 2, A). The difference between a fraud committed at the authentication stage is that the offender does not need to register the stolen identity, the record already exists. The personal identifiers which provide the authentication necessary to access the owner's record are stolen, or obtained by misrepresentation. By gaining access to these identifiers the offender is able to impersonate the owner and conduct business as them.

In summary, identity fraud can occur at either registration or at any time later if authentication processes are compromised. The identification process (first time registration) is vulnerable to the creation of false identities based on either 'real' or fictitious identities, genuine or forged documents, or a combination of these factors. Where identity fraud occurs after registration it involves the 'hijacking' of a genuine record and is a particular type of identity theft involving the circumvention of controls to authenticate the customer.

SOME OPTIONS FOR GREATER CONSISTENCY IN POI CONTROLS

SUMMARY OF REGISTRATION AND CONFIRMATION PROCESSES

Commonwealth agencies undertake a variety of measures to ensure the person they are dealing with is ‘who they say they are’. Proof of identity processes used by most agencies involve a combination of ‘front-door’ controls that are invoked during initial contact with the applicant and ‘back-office’ checks conducted at a later time.

The methods adopted by agencies to accept and confirm a person’s identity are outlined below.

FIGURE 3

SUMMARY OF REGISTRATION AND CONFIRMATION PROCESSES EMPLOYED

FRONT DOOR REGISTRATION PROCESS
Weighting of documents into categories
Declaration by another person
Index & search engines utilised
Correlation to family members
Check Identity against ‘warning’ flags
Recording or storage of Proof Of Identity

POST REGISTRATION CONFIRMATION
Validation of documents with issuer
Confirm Identity to public sources
Confirm details with referee
Address verified with 3rd party
Internal file matching
TFN or ABN validation

Some Commonwealth agencies employ a wider range of the listed control mechanisms than others and the strength with which particular controls are implemented by a specific agency may also differ.

The proposals for improving the ‘front-door’ processes centre around the main components of the registration process. The actions propose that agencies:

- agree on a set of acceptable identity documents,
- standardise their confirmation processes,
- exchange appropriate identity information and
- ensure the high integrity of the personal identity information they manage.

It is not suggested that the introduction of these controls will solve the problem of identity fraud but rather that their implementation represents good practice which will result in more efficient Commonwealth processes, reduce the extent of identity fraud and provide a foundation on which to build further controls.

An inherent weakness occurs when customers with inadequate or no Proof of Identity (POI) seek delivery of a service. Exercising provisions to cater for these individuals can allow the customer to avoid the usual controls associated with the identification process. Therefore, it is essential that the use of such provisions should be restricted to exceptional cases only and not become the standard approach for registering a substantial proportion of customers.

Even when agencies implement a comprehensive suite of personal identification and confirmation processes, significant deficiencies will remain in the ability of those processes to identify identity fraud.

The particular limitations of 'front-door' controls show it is necessary that additional techniques be developed to ensure that identity fraud in its totality is addressed in the most structured and complete manner.

Further methods for preventing identity fraud are needed and these will build on the strong controls inherent in the registration process.

VALIDATION OF DOCUMENTS

By and large, the personal identification processes employed by Commonwealth agencies are based on the provision of identifying documents by the applicant. A weakness of these processes is that the provenance of the documents is difficult to substantiate with any certainty. The wide availability and simplicity of desktop publishing technology has increased the ability of a much greater proportion of the community to produce very good reproductions of genuine documents. As a result the capacity of an agency to identify forged documents presented as POI has greatly diminished. Therefore, it is becoming increasingly important that an agency be able to verify a document's details with the issuing organisation as an assurance that the information it contains is accurate.

Document validation reduces the need to train customer service staff to visually appraise a document for particular security features and decide on its genuineness. This advantage plus the enhanced integrity of its customer register helps an organisation offset any direct costs associated with validating POI documents.

The ability to validate the accuracy of details recorded on identity documents presented to an agency will add significantly to the robustness of the confirmation process. Although document validation will not prevent all false identity fraud, when incorporated with other controls it will provide a substantial impediment to the registration of false identities using forged, or altered, documents.

Document validation is a direct control that specifically targets the risk of fictitious identities and assists agencies to ensure they are detected prior to registration. It is usual for fraud of this type to be supported by the manufacture of counterfeit identity documents. Such fraud would be prevented if agencies accepted only those documents able to be electronically checked with the issuing authority.

DATA-MATCHING

Data-matching is a technique that can target some particular risk areas that other methods cannot. It is particularly relevant and powerful when it is used in a complementary manner with the methods suggested earlier to improve front-door personal identification and confirmation processes, including document validation. A rigorous and systematic approach to personal identification using a range of 'front-door' controls coupled with confirmation via an electronic document validation service will prevent many types of identity fraud. Even so some false identity fraud will be immune to this raft of controls.

Data-matching can assist in two ways:

- by targeting the residual and more difficult to detect fraud as it occurs, thereby complementing the aforementioned controls and
- as an efficient and effective means of detecting a wider range of identity fraud of an historical nature which has remained undetected to date.

A cross-agency data-matching exercise that verifies the existence of matching identity records provides an agency with a greater assurance that its customers are legitimate. Conversely, the absence of records from the files of organisations where a registration would reasonably be expected to exist casts an element of doubt on the legitimacy of the identity. Such an outcome could indicate a possible fictitious identity and prompt wider investigations to be undertaken to ensure the identity is genuine.

In the context of identity validation, cross-agency data-matching provides a means of enhancing the degree of confidence an organisation has that the person they are dealing with is legitimate. This is particularly important if other means of confirmation are unavailable, although of course, the mere existence of a matching identity record on an external database is not sufficient to ensure the identity is genuine.

PRIVACY CONSIDERATIONS

The protection of an individual’s privacy is an important and complex issue that must be considered in any response to the problem of identity fraud.

The misappropriation of an individual’s identity is a gross invasion of privacy that has few parallels. Therefore, addressing the problem of identity fraud is important from a privacy perspective.

Effective solutions to combat identity fraud require a coordinated whole of government approach. It is likely that any coordinated approach adopted will necessarily involve some measures that are inherently privacy invasive.

The rights of individuals in relation to the handling of their personal information by Government agencies and private sector organisations are recognised by law in Australia. Solutions to the problem of identity fraud must take into account the legal framework, the Government’s overall privacy policy direction and any relevant international obligations.

Privacy law in Australia was developed in the late 1980’s in response to concerns about the collection and use of personal information by the Government. As technology has advanced and created new ways for commercial value to be extracted from personal information, concerns have broadened to encompass private sector activities. This is evidenced by increased consumer concern about the use of personal information collected through electronic commerce. Government and private sector entities around the world are working to develop means of providing individuals with greater control over their personal information to facilitate the growth of electronic commerce.

There is a range of privacy legislation and policies in Australia relating to the protection of personal information. Personal information is defined in the *Privacy Act 1988* (Cwlth) as

> “information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.”

The personal information collected by an agency to identify an individual obviously falls within this definition.

The relevant laws and policies at the Commonwealth level include:

- The *Privacy Act 1988* (the Privacy Act) prescribes the manner in which Commonwealth and ACT government agencies may handle personal information. It contains eleven Information Privacy Principles which govern the collection, use, disclosure, storage and security of personal information. It also gives individuals access and correction rights in respect of personal information relating to them. The Act establishes the Office of the Federal Privacy Commissioner to oversee the implementation of the Information Privacy Principles and investigate complaints relating to privacy breaches. The practical operation of the Information Privacy

Principles is further explained in guidelines published by the Federal Privacy Commissioner.

- The *Privacy Amendment (Private Sector) Act 2000* amends the Privacy Act from 21 December 2001. As of that date many private sector organisations will be required to collect and handle personal information in accordance with ten National Privacy Principles. The principles contain obligations that are similar to those that apply to the Commonwealth public sector. In addition, the National Privacy Principles provide individuals with the right to interact with private sector organisations anonymously if to do so is lawful and practicable. The principles also restrict the use by private sector organisations of identifiers assigned by Commonwealth agencies. The practical operation of the National Privacy Principles is further explained in guidelines published by the Federal Privacy Commissioner.

- The Tax File Number Guidelines issued by the Federal Privacy Commissioner pursuant to section 17 of the Privacy Act have the force of law and prevent the use of the TFN as a national identification system and limit the circumstances in which the TFN may be used as an identifier.

- Agencies conducting data-matching exercises that do not make use of the TFN, need to consider the guidelines issued by the Privacy Commissioner – *The use of data matching in Commonwealth Administration.*

- The *Data-Matching Program (Assistance and Tax) Act 1990* regulates the use of the TFN in comparing personal information held by particular Commonwealth agencies. Personal information from welfare agencies is supplied to the Data Matching Agency and compared to taxpayer information to detect inappropriate payments. The Act contains a number of technical controls and fairness provisions that are overseen by the Federal Privacy Commissioner.

- The Medicare and Pharmaceutical Benefits Programs privacy guidelines, issued under the *National Health Act 1953,* provides standards which apply to the management of information about an individual's claims under these programs.

In addition to privacy law and policies at the Commonwealth level, a number of States and Territories have developed or are considering developing legislative or administrative regimes to regulate the collection and handling of personal information by their public sector agencies. For example, there is the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Information Privacy Act 2000* (Vic). In addition, the ACT and Victoria have specific health information privacy legislation – the *Health Records (Privacy and Access) Act 1997* (ACT) and the *Health Records Act 2000* (Vic).

As the focus of this paper is combating identity fraud at a national level, the Information Privacy Principles are the most relevant to the recommendations made in Chapter 6.

The Information Privacy Principles contain provisions that arguably support efforts to protect a person’s identity. For example, the Information Privacy Principles require that personal information is accurate, up to date, complete and held securely. They provide individuals with the ability to find out what information is held about them by Government agencies and to correct it if it is not up to date or complete or is misleading. They also require that each agency only collects information that is relevant to their lawful functions and activities and place limits on the use of that information within the agency or its disclosure outside the agency.

In the identity fraud context problems arise when the personal information that an agency holds about an individual is fraudulent or defective in some way. In such cases the restriction on the disclosure of personal information to another agency inhibits the detection of identity fraud by preventing agencies from cooperating in relation to the verification and authentication process. The restrictions can also prevent agencies from taking pro-active measures to minimise the incidence of identity fraud.

Governments have a responsibility to protect citizens from becoming a victim of identity fraud. An effective means of doing so in Australia would be to standardise the processes surrounding identification and authentication. However, some measures to address identity fraud, while aimed at protecting the individual from the consequences of identity fraud, may be viewed as inconsistent with the individual’s privacy rights. For example, centralisation of data matching in a single Commonwealth agency or the use of a single national identifier could raise such concerns.

The measures to combat identity fraud canvassed in this paper must be considered in this context. Any measures need to be designed so as to minimise the reality and perception of privacy invasion by government and private sector organisations. This will require consideration of limitations and safeguards as appropriate to balance the interests of individuals as embodied in privacy legislation with the broader public interests of the particular measure under consideration.

CRIMINAL OFFENCES

New fraud, forgery, false and misleading statement and impersonation offences in the *Criminal Code Act 1995* cover a wide range of conduct involving deception and misrepresentation as to identity and use of false identity documents. The new offences are also designed to address developments in technology such as automatic teller machines, automated electronic funds transfers, credit cards and smart cards.

The offences include:

- obtaining property or a financial advantage by deception,
- dishonestly obtaining a gain from or causing a loss to the Commonwealth,
- false and misleading statements in applications and false and misleading information,
- impersonation of an official by a non-official and impersonation of an official by another official,
- forgery,
- using a forged document,
- possession of a forged document and
- falsification of documents.

The existing fraud, forgery and computer offences offer extensive coverage of conduct involving use of a false identity. A general false identity offence which applied more broadly than these offences would inevitably catch harmless conduct such as the use of a false name in an internet chat room or on the phone without any culpability. It would not be appropriate to make such conduct subject to a term of imprisonment. Some have suggested a general offence which required proof of an unlawful purpose might be appropriate, but it would not take the matter much further. Apart from the unacceptability of the term ‘unlawfulness’ because it is imprecise, it would seem that if an unlawful purpose under the criminal law could be proved, it would be better to charge the person with the principal offence.

Specialised false identity offences would be appropriate in areas in which the scope of the offence is such that the conduct is unlikely to be harmless, for example, the use of a false name in opening or operating a bank account (*Financial Transaction Reports Act 1988*, s24). An alternative to a series of special offences would be to create a ‘list’ offence. An example of this is section 136.1 of the *Criminal Code* (false and misleading statements in applications) which includes a list of documents which are ‘applications’ covered by the offence. The offence could prohibit using a false identity in a range of specified circumstances. There would be many Commonwealth processes which would not need to be listed because they would be covered by the new false or misleading statement and information offences (ss 136.1 – 137.2, *Criminal Code*). Constructing an appropriate list of circumstances where such an offence is both needed and appropriate would also be a good way of testing the extent to which there is a legal ‘gap’ in this area and whether a common penalty would be appropriate. The use of a false name to open or operate a bank account offence carries a maximum penalty of 2 years imprisonment.

RECOMMENDATIONS

THE CURRENT SITUATION

This chapter presents a number of strategies that Commonwealth agencies might consider in combating identity fraud. In applying any of these measures due recognition needs to be given to balancing individual privacy and civil liberties against broader community interests. This may require the implementation of additional safeguards to ensure individuals' privacy is protected.

In the absence of a reliable register of the members of the Australian community that would provide the means for each of us to establish our identity, the various organisations in our society who are required to identify their customers have developed alternate means of ensuring an individual is correctly identified.

Generally these arrangements have been implemented independently and in a piecemeal fashion by both government and private sector organisations and are inadequate in meeting our society's needs to identify, register and protect the identity of its citizens.

There is widespread agreement by all organisations that identity fraud already presents a significant problem that is likely to grow further. The lack of statistics on the incidence and cost of identity-related fraud makes the total cost to the community impossible to accurately quantify. Without reliable estimates of the overall cost it becomes more difficult to convince decision-makers that urgent attention is required. It is, therefore, of fundamental importance that research be initiated which will allow the calculation of accurate estimates of the costs of identity fraud and the benefits to be gained from implementing enhanced preventative controls.

> **Recommendation 1:**
>
> **Undertake a random sample survey to conclusively check the identities of persons registered with key Commonwealth agencies. This will provide an improved understanding of nature of identity fraud, the extent it impacts the Commonwealth, the effectiveness of existing controls and how it can be eliminated.**

~

The "Who Goes There?" report introduced a suite of measures that could be implemented in a harmonised fashion to strengthen agencies vetting procedures and give the community increased protection from identity fraud. The options developed in the paper which are considered to represent the most practical means of preventing identity fraud are summarised below. They are listed in sequence, beginning with those considered to be immediately achievable and progressing to those that are more complex and strategic.

IMMEDIATELY ACHIEVABLE

Some agencies pay insufficient attention to the accurate identification and registration of their customers. Personal identification procedures can often be viewed by staff as unnecessary, time-consuming or of inconvenience to the customer and are willingly circumvented. Also, in addition to these impediments, many organisations recognise a plethora of documents as acceptable for a person to prove their identity.

Such policies may bring advantages in customer service but do not enhance the certainty that should be associated with customer identification. Many documents considered acceptable are sourced from registers with little, or no, integrity and formal recognition of them results in a recursive discrediting of other agencies' registers. Over time such policies lead to decreased integrity in all organisation's identity registers.

A united approach is needed by agencies as they attempt to improve the efficacy of their personal identification systems and databases as the resultant overall quality of these systems will only be as good as the weakest link. Recommendations to prevent the ongoing collection of false or inaccurate identity data and remove any existing data of this type are outlined below.

Recommendation 2:

Commonwealth agencies agree on a set of identifying documents of higher integrity, issued by a limited number of reputable institutions, which are the only documents acceptable for personal identification.

~

If a person is unable to provide the required POI documents an agency should habitually invoke exhaustive procedures to establish the authenticity of the nominated identity leaving no doubt as to its genuineness. The additional cost to agencies of applying these procedures, plus the greater scrutiny of the individual, should insure these measures are used only in truly exceptional circumstances and are not regarded as standard procedure.

Significant weaknesses currently exist in the manner some agencies deal with persons with no, or unacceptable, POI. The creation and registration of false identities with these organisations is simplified due to the absence of sufficient checks. The registering agency itself may suffer no material loss from the deficient process but the enhanced credibility engendered by the legitimate, but false name identifying documents issued as a result of that registration allows others to be defrauded.

Recommendation 3:

Standard and more rigorous procedures be developed by Commonwealth agencies for dealing with applicants who supply no, or unacceptable, identity documents.

~

The strict enforcement of stronger POI requirements will provide agencies with the identity and document details necessary to conduct more rigorous verification checks.

In turn the confidence, of organisations and the community alike, in the registers held by the agencies will be enhanced. It is necessary that the key data items sourced from the documents provided are retained and faithfully and exactly recorded on the identity registers. This will assist in the elimination of duplicate records and also reduce the collection of inaccurate and inconsistent identity data that can abet the commission of fraud.

Recommendation 4:

The identifying data items on documents provided as POI should be regarded as key personal identifying data and be retained and stored on agency databases for subsequent checking.

~

It is important that organisations registering new customers ensure no previous record exists for that customer. The existence of duplicate, or multiple records for the customer in the same, or similar names, is very common and is the predominant cause of the occurrence of excess records. The availability of computerised mechanisms to conduct timely and thorough searches of the customer register to compare against the particulars of the new customer (often referred to as indexing) will prevent most duplicate registrations from occurring. This will be especially the case if document data items are retained and checked as per Recommendation 4.

Most agencies currently perform some indexing checks at registration but it is generally acknowledged that significant numbers of duplicate records still exist on agencies' databases. This means that current practices can be improved.

Recommendation 5:

Agencies make available powerful online computerised searching facilities to allow staff registering new applications to ensure no previous records exist for that customer.

~

In the course of their daily operations Commonwealth agencies often receive information from a variety of sources on lost or stolen documents, and false identities. The information is provided by members of the public, law enforcement bodies, other government departments and through an agency's own operational staff and fraud control activities. Whilst an individual agency may make effective use of the information to correct any existing problems it is usual that this information is neither distributed to other agencies nor retained for use in ongoing registration processes. It is therefore necessary that other agencies receive timely advice of potential identity fraud so they can quickly minimise abuse and put mechanisms in place to prevent any use of the associated documents or identities.

Recommendation 6:

Development of a common database containing the details of lost or stolen document details and false identities be considered. The database would allow agencies to ensure new customers are not presenting documents known to be stolen or attempting to register a false name that has been previously detected.

~

A critical factor in preventing identity fraud is the constant commitment by agencies to ensure the identity information they hold on their customers is of the highest integrity. A necessary milestone in achieving this is to 'clean' agency databases of redundant records to ensure there is only one customer registration recorded for each identity. In addition to eliminating these multiple records, which may occur in the same name, a similar name or alternate names, it is also necessary to improve data quality by correcting any inaccurate or inconsistent details held for a person.

Recommendation 7:

Commonwealth agencies that retain a register of personal identity details ensure the integrity of their customer data is improved by eliminating multiple registrations for the same customer.

~

A further aspect of cleansing identity registers is to ensure the records of customers who have died are removed from the database, or marked as deceased. Some agencies conduct data-matching exercises with the Registry of Births, Deaths and Marriages (BDM) National Fact of Death data to complement their own death notification procedures and to provide an assurance that deceased customers are known and their records have been updated. This work could be conducted on a more regular and systemic basis by Commonwealth agencies to ensure all agencies are aware of the information, appropriate action is taken and records are updated in a coordinated manner. The inclusion of historical death data with the information received on more recent deaths, and matching it on a regular and ongoing basis will assist in preventing theft of deceased persons' identities.

Recommendation 8:

Commonwealth agencies make greater and more coordinated use of the BDM National Fact of Death data to improve the quality of their registers and assist in the prevention of identity theft.

~

MEDIUM-TERM STRATEGIES

The two immediately preceding recommendations have examined some methods for cleansing identity details recorded on databases. In particular, ways in which excess records (whether they are duplicate, redundant, same or similar name) can be identified and corrected were outlined.

A further measure, which complements and enhances the integrity of the clean-up process, is needed to identify those false identities that bear no resemblance to the true name. These identities may be based on fictitious details, or result from name changes, including legal changes. Regardless, it is necessary to identify them so cases of fraud can be dealt with and any alternate names linked to the true identity.

Data-matching across agencies will enable a more thorough process in erasing a range of false identity types and will assist in the detection of identity fraud in fictitious names.

Recommendation 9:

Commonwealth agencies undertake greater cross-agency data-matching to cleanse their databases and detect fictitious identity fraud.

~

The detection and elimination of excess and fraudulent records from agency databases as a means of ‘cleansing’ them and creating registers of higher integrity is half of the solution. The other half is preventing false identities from being registered in the first place. The maintenance of database records of high integrity is a continuous process requiring strict adherence to the personal identification and registration processes outlined in this report.

To support these processes and to provide a high level of assurance that a new customer is using a genuine identity, agencies need immediate confirmation that the details recorded on the POI documents provided by customers are legitimate. The ability to validate POI documents gives staff greater confidence the identity is authentic and provides a means of maintaining a register of high integrity.

Recommendation 10:

Commonwealth agencies consider the development of an electronic gateway to each other’s identity records to allow the real-time verification of document and identity particulars.

Recommendation 11:

Consideration be given by Commonwealth agencies to the development of an on-line gateway for mutual use in confirming particular State Government documents such as birth certificates (including documented change of name) and drivers licences.

The above recommendations are not sufficient, alone, to generate the essential discouragement necessary to deter the more adroit and sophisticated use of false identities. In particular, they do not effectively address the eradication of identity fraud built around the use of more complex fictitious identities and the aspect of identity theft. The community is becoming more vulnerable in these areas due to the increasing use of false identities to acquire anonymity and of particular concern is the exponential growth being experienced overseas in identity theft.

Recommendation 12:

Consideration be given to the formation of a Commonwealth Identity Data Agency. Its responsibilities could include:

- **undertaking defined data-matching initiatives to prevent more complex identity fraud and**
- **the administration, or development, of identity validation mechanisms for use by Agencies.**

~

The implementation of any of the preceding recommendations, either singularly or in combinations, would go some way towards improving the accuracy of personal identification, eliminating and preventing some elements of identity fraud.

However, more can be achieved by introducing the recommendations in their totality. Introduced as a package, the recommendations are complementary in addressing much of the identity fraud risk spectrum. Also, the inter-related processes will reinforce each other, providing a means of rectifying identity inconsistencies and detecting particular fraud types whilst simultaneously strengthening our ability to prevent the commission of new offences.

The advantages are significant. Substantial inroads can be made in preventing opportunistic identity fraud, cleansing databases of duplicate, multiple and excess records and detecting much of the fictitious identity fraud currently in existence.

UNIQUE PERSONAL IDENTIFIERS – AN OVERVIEW

A SINGLE IDENTIFYING NUMBER – ADVANTAGES AND DISADVANTAGES

The concept of identifying every Australian resident by a single identifying number is an option which has been previously rejected by the Senate but has nonetheless continued to generate discussion. It is probable the implementation of such a scheme would require the following features:

- The creation of a central register containing the distinguishing identity data for each member of the Australian resident population.
- An associated unique identifying code for each person.
- The allocation of a multi-purpose identification token to each registered person.
- An obligation on the owner to present it to authorised agencies to access specified services.
- The requirement that an organisation request the token as POI for registering new customers and for ongoing authentication.
- The sharing and comparison of data by authorised agencies.
- It may be necessary for those Agencies that continue to issue POI documents and identifiers to guarantee their validity.

A single government client service number which would allow residents to ‘seamlessly’ interact with Government agencies would have a number of advantages to both agencies and individuals. Many of the problems which confront agencies in determining an appropriate set of high integrity POI documents and subsequent confirmation of the authenticity of identities would be substantially reduced. Likewise, individuals would benefit from being less inconvenienced and confused by differing POI requirements and be able to more readily identify themselves when registering for government services.

However, the risks attached to placing total reliance on one identifier are high. The accuracy of the associated central register would need to be unassailable in order to ensure the community’s confidence and trust in the register. To gain and maintain this trust there exists a critical requirement that identification be totally accurate at registration. The importance of this requirement cannot be overstated as the enrolment and ongoing maintenance processes associated with ensuring the register is of the highest integrity would present significant difficulties. It is likely the responsibility for administering these processes would need to rest with a special body.

A major weakness of a central register occurs if it is compromised causing doubts to arise as to the accuracy of its records. The resultant risks posed to the community are then more serious and extensive than would occur with flaws in a single agency's register. This is because of the enhanced status of the single identifying number and its role as the sole identification required by agencies and its widespread adoption by the community. The concern in the USA over misuse of the Social Security Number (SSN) demonstrates the problems which arise when control over the use of a single identifier is lost.[7]

Particular risks confronting the integrity of the register are:

- registering a fictitious identity and issuing an identifier,
- issuing the identifier to a real person who has stolen another's identity,
- compromising the identifier (someone is able to hijack the identifier), and
- the associated denial of service to the real person when this is detected.

The centralised database register would need protection by an extremely high level of security to prevent unauthorised access or corruption of data. Similarly, the personal identifying token itself would require shielding by appropriate security features to prevent use by someone else.

It is possible that the technology chosen for the personal identifying token in such a scenario would be biometrically based.

BIOMETRIC IDENTIFIERS – POSSIBLE PITFALLS

Much has been written about the ability of biometric type identifiers to eliminate the difficulties associated with personal identification. In fact, it seems that the biometric solution is often regarded as a panacea for controlling all POI risks. Unfortunately, this is not the case as the plethora of biometric "identifiers" currently in use can do little more than ensure the individual undertaking a transaction is the same person who originally registered with the organisation. This process is referred to as authentication and was outlined in Chapter 2.

The process of accurately identifying and registering a person – identification – is quite different and is, by and large, not solved by utilising a biometric process.

Establishing a person's 'true' identity at the time of registration or enrolment must be achieved by means external to any biometric system and will usually require documentation of some kind. After a person's identity has been proven it may be appropriate to allocate a biometric token to enable future transactions between the individual and that organisation. It is of course critical that any organisation which issues biometric authenticating tokens has processes in place that ensure an individual is accurately identified. Otherwise the integrity of the registers will be compromised by registrations in false or stolen identities.

[7] Statement of Honorable James G. Huse, Inspector General, Social Security Administration. Testimony Before the Subcommittee on Social Security of the House Committee on Ways and Means. Hearing on Protecting Privacy and Preventing Misuse of Social Security Numbers, May 22, 2001 <http://waysandmeans.house.gov/secsec/107cong/5-22-01/5-22huse.html>

To gain public confidence in biometric processes it may be necessary for an organisation which is responsible for issuing biometric authenticating tokens to gain special accreditation. Alternatively, a specific agency, tasked with the responsibility of personal identification and allocation of a biometric certificate, might need to be established.

Fundamental to the development of new identification and authentication systems is the community's right to expect that personal data is protected and transactions are secure.

Whilst this is the case with any personal information, it is particularly so for a person's biometric data because biometric features, such as a fingerprint pattern or DNA, are one of the characteristics that makes a person unique. People are likely to feel particularly uncomfortable entrusting this information to others, no matter what guarantees are given about privacy and security. As the stored biometric information is a data stream of combinations of zeros and ones, like other personal information such as credit card details and addresses, it can be stolen from computer databases and used to impersonate the owner.

A disadvantage of using biometric characteristics as a means of authentication is that they are irrevocable. Non-biometric authentication systems, such as a password, allow access keys to be revoked if they have been compromised. As the biometric key is tied inextricably to a particular person disabling it to prevent its use by a thief will also mean it can no longer be used by the owner.

Arguments for considering both a single identifying number to provide the means of personally identifying individuals, and any associated biometrically-based identifying token must be able to satisfy the community's demands for the utmost accuracy, security and reliability.