FIGHTING IDENTITY CRIME

JOHN FARRAR*

Identity crime is on the increase in most jurisdictions and is a matter of concern to governments and financial institutions as well as victims.[1] In a 2003 study the cost of identity fraud to Australia in 2001-2 was estimated to be $1.1 billion.[2] Only 38% was identified as direct losses. The majority of costs related to resources to combat identity crime.[3] In the United Kingdom the Home Office estimated that for 2007 the cost was £1.2 billion or £25 for every adult in Britain.[4] The subject raises interesting conceptual questions as well as the practical problems of legislating, investigating and prosecuting these types of offences. The techniques of identity crime are well known yet surprisingly little work has been done on profiling this type of fraudster although there is general agreement that identity crime is now being perpetrated by organized crime which is operating on an international basis.[5]

Identity crime also raises technical questions of encryption and other security systems to combat cybercrime. In view of the ingenuity that goes into this type of crime, encryption and security systems constantly need revision. The social costs of

* Emeritus Professor of Law, Bond University, and Professor of Corporate Governance and Joint Director of the New Zealand Governance Centre at the University of Auckland.

1 See generally Martin Biegelman, *Identity Theft Handbook – Detection, Prevention and Security*, (John Wiley & Sons Inc 2009). In the USA, identity fraud is described as growing at a rate of 30% per annum with losses estimated at US$8 billion by 2005 (Supreme Court of the State of Florida, 2002). See also G Main and B Robson, *Scoping Identity Fraud* AG's Department Canberra, 2001; R Lozusic, *Fraud and Identity Theft*, NSW Parliamentary Library Research Service Briefing paper No 8/03; Nicolee Dixon, *Identity Fraud* Queensland Parliamentary Library, Research Brief No. 2005/03; C J Hoofnagle, 'Identity theft: Making the Known Unknowns Known' (2007) 21 Harvard Journal of Law and Technology 97; OECD, Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP (2007)3/FINAL; *Identity Fraud in Canada*, July 2007 (http://www.rcmp-grc.gc.ca/pubs/ci-rc/if-fi/index-eng.htm); The President's Identity Theft Task Force, *Combating Identity Theft – A Strategic Plan*, 2007.

2 S Cuganesan and D. Lacey, *Identity Fraud in Australia – An Evaluation of its Nature, Cost and Extent*, SIRCA, Sydney 2003, 114.

3 Ibid Chapter 5.

4 Identity-Theft UK, *Cost of Identity Fraud to the UK Economy 2006-7*.

5 Kim-Kwang Raymong Choo and R G Smith 'Criminal Exploitation of On-line Systems by Organised Crime Groups' (2008) 3 *Asian Criminology* 37.

all of this are large and increasing every day. Identity crime therefore presents a challenge for law enforcement in every jurisdiction.

The concept of identity and proof of identity[6]

The concept of identity is an aspect of human personality and has developed as a specialist area in psychology in recent years and has even generated its own specialist literature. Early legal systems did not have much of a problem with identity because the population was largely static and it was enough that people were known by their first name. Surnames later developed by reference to kinship, locality or occupation. Increased mobility together with the development of credit cards and electronic banking has now massively increased the problems of proof of identity. Identity is linked with citizenship and licences as well as access to credit.

Recently some countries have installed encryption devices in passports. In the case of the United Kingdom not only has this been done but also separate identity cards have been issued with similar encryption devices. In Canada and the USA work has been done on driver's licences which now include a lot of personal data and these are used for cross border identification purposes. In most countries the majority of people have Eftpos and credit cards with pin numbers which have been the subject of abuse and identity crime.

Terminology

The Australasian Centre for Policing Research, *Standardisation of definitions of identity crime terms: a step towards consistency* has the following definitions:[7]

Identity Crime

- Offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime

Identity Fraud

- The gaining of money, goods, services or other benefits through the use of a false identity

Identity Theft

- The theft of a pre-existing identity

Techniques of identity crime

There are a number of techniques used in identity crime. These include:[8]

6 Cuganesan and Lacey, above n 2, Ch 2.

7 Report Series No 15.3, March 2006.

- Dumpster diving,
- Wallet theft,
- Mail interception and scams,
- Skimming,
- Proof of identity replication,
- Phishing,
- Vishing,
- Pharming, and
- Spear phishing.

In addition there are different kinds of hacking to overcome encryption and other security devices.

We talk briefly about each of these.

Dumpster diving involves searching through other people's trash. Whenever personal or commercial documents are included in trash there is a potential problem which can only be solved by shredding. Of particular concern recently has been crime syndicates getting access to documents relating to account of superannuation fund members and initiating fund rollovers to fake self managed superannuation funds.[9]

Wallet theft and theft or misappropriation of credit cards is common, particularly in third world countries. It is important not to let credit cards out of one's sight in restaurants and shops in some parts of the world where the instance of this kind of crime is common.

Mail interception is also a risk, particularly in apartment blocks.

Scams involving emails purporting to be from banks are increasingly common.

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is usually done by a dishonest employees and there are various ways of doing it. Another form of skimming is where a device is inserted into an automated teller machine which reads the magnetic strip as the user passes their card

---

8 See Biegelman above n 1,Chapter 3; J Stickley, *The Truth About Identity Theft*, Pearson Education, Inc, 2009, Parts I and II; T Cullen, *The Wall Street Journal Complete Identity Theft Guidebook*, Three Rivers Press, NY 2007, 40-2.

9 See 'Sophisticated super fund identity fraud on the rise', *The Australian*, Wealth, May 19 2010.

through it. These devices are often used with a camera to read the user's pin at the machine.

Proof of identity replication essentially is forgery of a document.

Sometimes this is done by adaptation of a legitimate proof of identity document. Sometimes it is done by the manufacture of a false document, sometimes in the name of another live or dead person. T C Boyle's novel, *Talk Talk*[10] is a graphic illustration of the problems this can cause. The novel is about a lady who is chronically deaf and has great difficulty proving her identity when someone else steals it.

Phishing takes the form of bogus emails purporting to be sent by banks or credit card companies and the object is to gain access to confidential information.

Vishing is the practice of using analogue phones or voiceover to steal identities and often persuading the victim when he or she is averting identity theft whereas in fact the opposite is happening. The telephone caller purports to be a bank or credit card company.

Pharming is a hacker's attack aiming to re-direct website tracking to another bogus website.

Spear phishing is tracking a specific victim instead of setting an all purpose trap. Again it often takes the form of a personalized approach purporting to come from a specific institution.

Obviously *hacking* can take a variety of forms but the main danger is the cracking of encryption and other security systems. Some of the latest concerns are the possibility of organized crime infiltrating legitimate organizations to achieve this.

In addition there are techniques which are used with ATM's and credit cards.[11] Shoulder surfing is performed at ATM machines where another person is using the machine and the fraudster strategically positions himself or herself so that they can observe the customers PIN code. Skimming is a more elaborate technique which involves a small electronic device which the fraudster installs on the card slot on ATM's or petrol pumps. The device is equipped with a magnetic reader capable of scanning credit cards or EFTPOS cards. Skimmers are hard to detect. Increasing elaborate technique is used with EFTPOS. EFTPOS machines are stolen from stores then modified and equipped with skimming devices. The machines are then replaced without the staff noticing the switch.

---

10 Viking, New York 2006.

11 Erlend Roysum, 'Identity Crime: Techniques, Trends, Consequences and Legal Responses', unpublished LLM paper, Bond University, 2010.

Jurisdictions with specific identity crime offences

In Australia, South Australia, Queensland, Victoria, New South Wales and Western Australia have specific offences relating to identity crime.

In South Australia, Part 5A of the *Criminal Law Consolidation Act 1935* contains provisions about assumptions of a false identity. Section 144B provides that 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,

(iii) makes a false pretence to which this section applies.

Section 144B(2) provides that a person who assumes a false identity is caught even though the person acts with the consent of the person whose identity is falsely assumed.

Section 144B(3) provides that a person who makes a false pretence to which the section applies intending to commit or falsify 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.

Under s 144A serious criminal offence means an indictable offence or an offence prescribed by regulation.

Section 144C deals with misuse of personal identification information and this applies irrespective of whether the person whose information is used is living or dead or consents to the use.

Section 144D deals with prohibited material in connection with identity crime.

Section 144F makes it clear that this part does not apply to misrepresentations by persons under the age of 18 for the purpose of obtaining alcohol or tobacco. This is dealt with separately.

A new s 408D of the Queensland Criminal Code 1899 deals with obtaining or dealing with identification information.

Under s 408D(1) a person who obtains or deals with identification information for the purpose of committing or facilitating the commission of an indictable offence commits a misdemeanour.

The Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General in its final Report on Identity Crime of March 2008 [12] recommended the creation of the following model offences:

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

The text of the model provisions is set out in the Appendix.

The Victorian provisions which are now sections 192A – 192E of the *Crimes Act 1958* are substantially based on the Model Criminal Code proposals are set out in the Appendix. Section 192A sets out definitions. Section 192B deals with making, using or supplying identification information. Section 192C deals with possession of identification information. Section 192D deals with possession of equipment to make identification documentation and s 192E states that it is not an offence to attempt to commit an identity crime offence.

New South Wales has recently introduced similar provisions in ss 192I-192M which impose a penalty of up to 10 years for dealing with identification information. This is double the model provision. Two private member's bills were introduced into the Western Australian Parliament, one based on the Queensland provisions and the other on the south Australian provisions. These ultimately did not proceed but the Government introduced the Criminal Code Amendment (Identity Crime) Bill 2009 based on the model provisions. This was enacted as the *Criminal Code Amendment (Identity Crime) Act 2010*.

There is a need for uniform laws based on the model provisions in all the states and territories as was recognised by Standing Committee of Attorney General. In 2002 the Police Commissioners Conference agreed to develop a national policing strategy on identity crime and this is in the program of the Australian Crime Commission.

The recent *Commonwealth Law and Justice Legislation Amendment (Identity Crimes and other Measures) Act* 2011 amends the *Criminal Code Act* 1995 by adding a new Part 5 to provide for identity crime offences substantially following the model provisions.

The Commonwealth Crimes Legislation Amendment (*Telecommunications Offences and Other Measures) Act (No 2) 2004* prohibits credit card skimming and internet banking fraud, including phishing. The *Cybercrime Act 2001* deals with serious

[12] Final Report on Identity Crime, March 2008. <www.agd.gov.au>.

computer offences and the *Financial Transaction Reports Act 1988* makes it an offence to open an account in a false name by tendering a false identification document.

Tasmania, Australian Capital Territory and the Northern Territory all have legislation that deals with computer offences and general provisions that might be used to prosecute some identity crime.

New Zealand has a number of sections in the *Crimes Act 1961* relating to fraudulent use of identity to obtain a benefit. Amendments in 2003 updated provisions relating to computer crime. These are:

- accessing a computer system and dishonestly or by deception obtaining a financial benefit or causing loss (new s 305ZE(1))
- accessing a computer system with intent to obtain a benefit or cause loss (new s 305ZE(2))
- damaging or interfering with a computer system with intent to cause serious damage (new s 305ZF(1)(a))
- recklessly damaging or interfering with a computer system knowing that serious damage is likely to result (new s 305ZF(2)(a)).

These sections focus on property rather than identity crime as such. They nevertheless are capable of being used for identity crime offences.

Canada and the United States have provisions which apply to identity crimes. Section 403 of the Canadian *Criminal Code* deals with impersonation with intent and new offences of obtaining identity information to use dishonestly, trafficking and unlawful possession of government issued identity documents were introduced in 2010. The United States *Identity Theft and Restitution Act of 2008* deals with cyber crime and supplements the *Identity Theft and Assumption Deterrence Act 1998* and state legislation.

United Kingdom Legislation – a different approach

The *Fraud Act 2006* created a new offence of fraud that can be committed in three ways: by making a false representation, by failing to disclose information, or by abuse of position.

In addition, the *Identity Cards Act 2006* contains provisions relating to possession, control and use of false identity documents.

Profiling fraudsters

As far as I am aware there has been no detailed research on profiling identity fraudsters in Australia and New Zealand. However, there has been useful work done

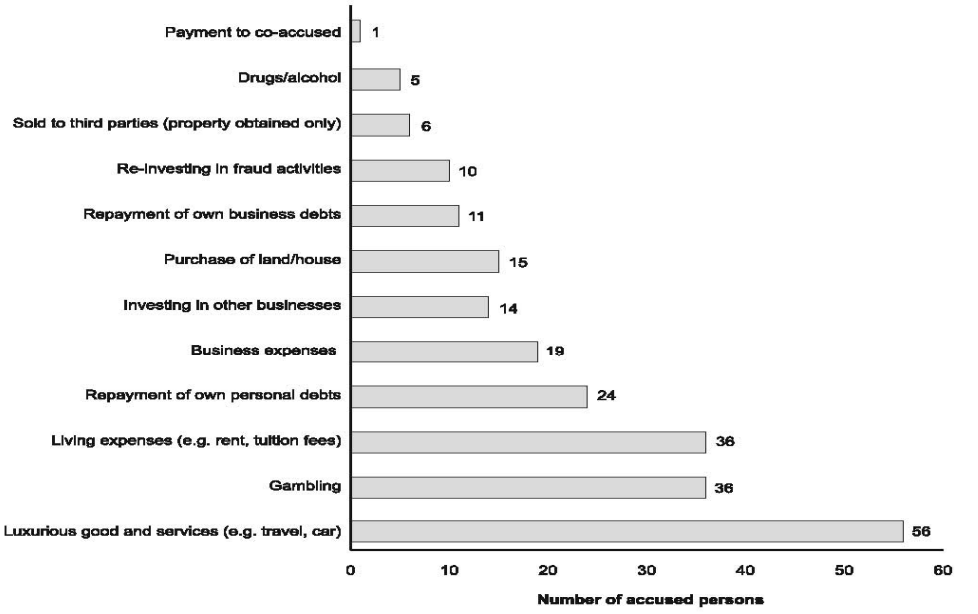
by the Australian Institute of Criminology and PricewaterhouseCoopers on Serious Fraud in Australia and New Zealand in 2003.[13] This revealed the following details:

General serious fraudster characteristics

The accused had a mean age in their early 40s – 42 for females, 43 for males. One fifth were female. Two thirds were born in Australia or New Zealand. Relatively high proportion had completed secondary education or had an undergraduate tertiary degree. A high proportion were at top management level. A high proportion stood in a professional relationship with their victim. A number had a previous criminal record (44%) and 27% had fraud offences.

Motivations

The following is a figure showing the primary motivation of the accused:



Note: In some files offenders spent the proceeds of their crimes in multiple ways. Information was available for 167 of the 208 accused persons.
Source: Australian Institute of Criminology and PricewaterhouseCoopers, Serious Fraud in Australia and New Zealand, 2003 [computer file]

Note: Information on motivation was available for 148 of the 208 accused persons. Numbers indicated on bars are values (number of accused persons), not percentages.

Source: Australian Institute of Criminology and PricewaterhouseCoopers, *Serious Fraud in Australia and New Zealand*, 2003 (computer file).

13 *Serious Fraud in Australia and New Zealand*, 2003.

Profiling identity fraudsters

The question is whether these profiles fit identity fraudsters. Recent Australian research[14] classifies them into:

- organized crime
- sophisticated individuals
- opportunist individuals
- an agent of the victim.

The Australian Institute of Criminology research did not focus on the role of organized crime but did contain examples of individuals and agents of the victim. The research was of a more generic nature. In the USA there is some evidence that organised crime is turning to identity crime instead of drug related offences because it is as lucrative and much safer.[15]

Sophisticated individuals who commit identity theft will often be employees of a bank or other institution. Likewise, opportunist individuals can fall under the second and third categories without necessarily being an employee or agent.

Another aspect which requires more research is the use of websites like Face Book as a means of identity crime victimizing young people. A surprising amount of personal information is provided on these sites which are accessible not only to young people but by any other potential identity fraudster.

US research[16] indicates that the defining characteristic of identity thieves is that they are 'opportunists'. A distinction is drawn between low frequency offenders and high frequency offenders. Low frequency offenders consist of 'crisis responders' and 'opportunity takers'. Crisis responders engage in crime in response to some type of crisis.

Opportunity takers take advantage of some specific criminal opportunity. High frequency offenders consist of 'opportunity seekers' and 'stereotypical criminals'. Opportunity seekers include dumpster drivers and scammers. Stereotypical criminals

---

14 R Jamieson, G Stephens, D Winchester; Rodger Jamieson, Greg Stephens, Donald Winchester, a Model to Classify Perpetrators of Identity Fraud and their Attack Channels in 'An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts', Pacific Asia Conference on Information Systems (PACIS) PACIS 2007 Proceedings, University of New South Wales.

15 See G R Newman and M M McNally, 'Identity Theft Literature Review,' National Institute of Justice Focus Group Meeting, Jan 27-8 2005, 26.

16 Ibid 26 et seq.

are the highest frequency offenders and this category spans all types of identity theft and is particularly relevant to the connection of organized crime.

Sentencing identity fraudsters

There is little published information on the sentencing of identity fraudsters but the matter was recently considered by The Court of Criminal Appeal of the Supreme Court of New South Wales in *Stevens v R.*[17] In this case which predated the amendments to include specific offences of identity crime the accused was charged with (1) using a false instrument with intent, (2) possession of a false travel document and (3) obtaining a benefit by deception. The sentencing judge imposed a fixed term of 9 months imprisonment for (1), a non parole period of 1 year and 6 months for (2) and a non parole period of 2 years for (3).

The total sums involved were $402,935. The sentencing judge concluded that 'it is difficult to conceive of a more deliberate and planned course of systematic dishonesty'. The sentence was to denounce the accused's conduct, punish him and deter others. This was upheld on appeal. McClellan CJ at Common Law said, 'Electronic banking has brought many benefits to the community. It is efficient and convenient. It allows individuals and corporations to complete transactions where previously paper would be generated and in many cases physical attendance at bank premises would be required. It is of benefit to the disabled just as it is to business. Electronic banking is already utilised by many people but will inevitably become the almost universal method of conducting financial transactions. However, as the current offences make plain the electronic system is vulnerable to persons intent upon dishonestly exploiting any weakness. That vulnerability may result in a complete loss of confidence in the system if breaches occur. If public confidence in the integrity of the system is to be maintained the courts have an obligation to ensure that when dishonest breaches of its security are identified the offenders are appropriately punished. Both personal and general deterrence are of particular significance in relation to these types of offences'.

Spigelman CJ said, 'The case with which identity crimes can be committed has expanded well beyond the traditional means of stealing mail or eavesdropping to obtain personal data. The new techniques are multifarious and have a facility of execution which is, of itself, such as to require that sentencing for such offences gives considerable weight to general deterrence. These techniques include:

- The theft of personal information from computer databases.

[17] [2009] NSW CCA260 (28 October 2009). For sentencing for hacking the identity of a sewerage pump see *R v Boden* [2002] QCA 164.

- Fake emails purporting to be from trusted organisations such as banks (known as "phishing"), requesting log on details by way of reply.
- Social networking sites and instant messaging and unsolicited emails which encourage persons to divulge personal information.

Although the sentencing regime is likely to be addressed in the near future by legislative change, by the creation of more focussed offences and by an increase in maximum penalties, the significance of general deterrence in the exercise of the sentencing discretion will remain a matter to which particular weight must be given'.

The new sections discussed above now create the new offences and impose new penalties two of which are higher than the model code penalties.

Combating identity fraud

Specific technology has been devised to combat identity fraud. This includes:[18]

- tamper proof plastic cards
- tamper proof documents
- firewalls and encryption software
- remote frequency ID chips

Elaborate systems have been developed to attempt to combat identity crime. These include cryptography and computer security as well as identification and/or authentication. Cryptography has been described by one writer as a 'shadowy protective entity – something like Batman – kind of menacing but on the side of justice, and endowed with mystic powers'.[19] It is often thought of in terms of acronyms which accomplish various security tasks. These represent protocols for digital content protection and use different algorisms. Computer security often involves digital signature schemes. Identification and authentication traditionally used passwords, but increasingly biometrics is being used. A third solution is access tokens. It has been said 'as technology becomes more complicated, society's experts become more specialized. And in almost every area, those with the expertise to build society's infrastructure also have the expertise to destroy it'.[20]

[18] See B Schneier, *Secrets and Lies – Digital Security in a Networked World*, Wiley Publishing, Inc, Indianapolis, 2004

[19] Ibid 85.

[20] Ibid 389.

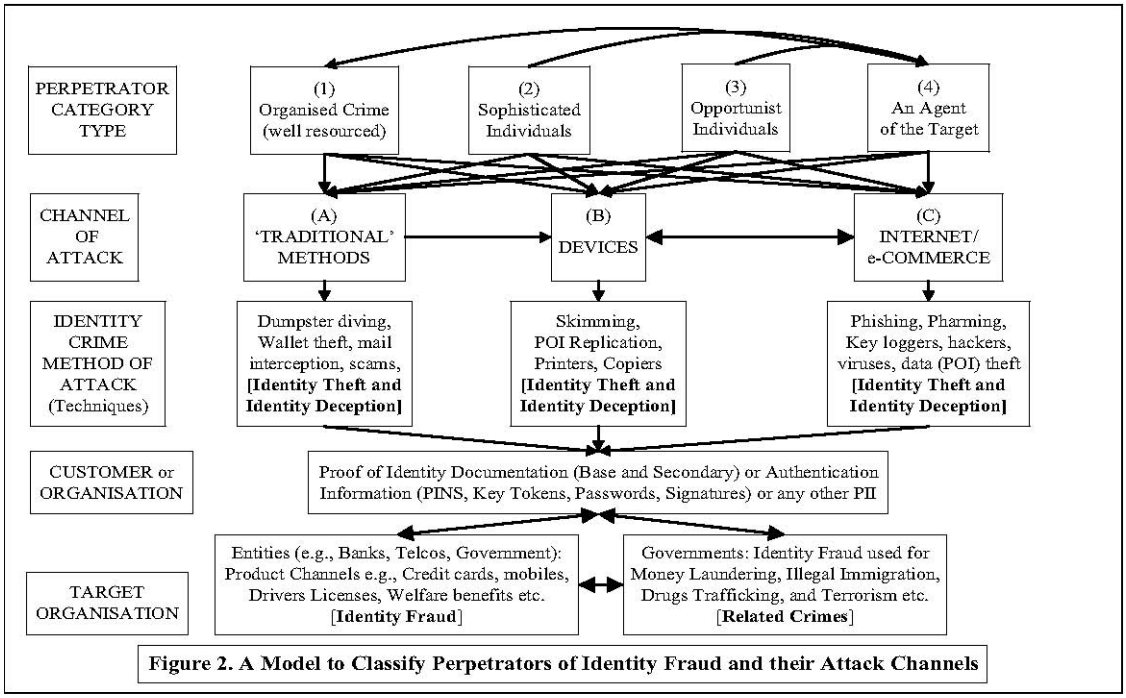


Figure 2. A Model to Classify Perpetrators of Identity Fraud and their Attack Channels

Figure 2. A Model to Classify Perpetrators of Identity Fraud and their Attack Channels.[21]

Conclusion

Identity crime is on the increase, is costly and is difficult to combat. It is difficult to draft legislation which covers all aspects of identity crime and difficult to investigate its perpetration. We have seen how some jurisdictions have attempted to legislate specific provisions whereas others deal with it by general provisions. There is a need for uniform laws with adequate penalties which reflect the seriousness of this kind of offence. Little detailed research has been done on profiling identity crime specifically and more needs to be done to investigate offenders and their connection with organized crime. In the meantime, there is plenty of work for experts to devise protective security systems. This problem will not go away.

---

[21] Rodger Jamieson, Greg Stephens, Donald Winchester, a Model to Classify Perpetrators of Identity Fraud and their Attack Channels in 'An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts', Pacific Asia Conference on Information Systems (PACIS) PACIS 2007 Proceedings, University of New South Wales.

APPENDIX

RECOMMENDED MODEL IDENTITY CRIME OFFENCES

3.3.6 Identity fraud

(1) Definitions.

In this section:

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

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

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

a) a name or address,

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

c) a driver licence or driver licence number,

d) a passport or passport number,

e) biometric data,

f) a voice print,

g) a credit or debit card, its number, or data stored or encrypted on it,

h) a financial account number, user name or password,

i) a digital signature,

j) a series of numbers or letters (or both) intended for use as a means of personal identification,

k) an ABN.

l) (Based on Section 408D of the Criminal Code (Qld)).

(2) Dealing in identification information.

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

Maximum penalty: Imprisonment for 5 years.

(3) Possession of identification information.

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

Maximum penalty: Imprisonment for 3 years.

Possession of equipment used to make identification documentation

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

Maximum penalty: Imprisonment for 3 years.

(This is based on s 144D(3) of the *Criminal Law Consolidation Act 1935* (SA)).

(5) This section applies:

a) to a person who intends to commit, or facilitate the commission of, an offence even if committing the offence concerned is impossible or the offence concerned is to be committed at a later time, and

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

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

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