

## Identity Related Crime – A Rapidly Growing Problem

*“But he that filches from me my good name/ Robs me of that which not enriches him/ And makes me poor indeed.”  
Shakespeare, Othello, act iii. Sc. 3.*

**By Shane Ringin MBA. BA. - General Manager Pro Active Strategies**

### Profile

Shane Ringin, is the General Manager of Pro Active Strategies, a consultancy resource to businesses in various areas, including Loss Prevention.

Shane was a member of the Victoria Police Force for over 20 years, with a great deal of that time dedicated to high level investigation of Corporate crime and identity related crime, in the Major Fraud Group, National Crime Authority, and as the Officer in Charge of the Victoria Police DNA squad.

Shane is considered an international expert in regards to identity crime and biometrics, and has completed tertiary studies in the UK in Commercial crime and Terrorism, as part of a British consulate award, as well as studying identity crime internationally through a Churchill Fellowship award.

Shane’s interest in identity related crime manifested itself, whilst evaluating the future criminal trends that threatened the stability of the community, as part of the development of the Crime Department’s input into the Victoria Police Force 10 year plan.

In his role as General Manager of Pro Active Strategies, he sees many incidents of identity related crime that affect both individuals and organisations.

### Identity

The basis of our existence within society is individualised through our unique identities. This consists of three types; Biometric identity, Attributable identity & Biographical identity.

Biometric identity is the most accurate method of identifying an individual and utilises physiological or behavioural characteristics to determine and verify identity. There are many different options, which include, but are not limited to; the scanning of one or more of an individual’s finger, face, voice, iris, retina, hand, signature, keystrokes or DNA.

The advantage of utilising a biometric is that it has a high degree of accuracy, with the disadvantage being that it can be intrusive and there are currently a number of technology issues with implementation and utilisation.

Attributed identity consists of those identifiers that are attributed to us by virtue of our birth, i.e., given name, date of birth, place of birth, parent’s name and mother’s maiden name.

Biographical identity is the identifiers that we collect as we progress through society. They are many and varied and include education, qualifications, references, where you live(d), what you do and previous interaction with institutions; i.e., banks, credit unions, utilities and government agencies, etc.

This rich tapestry of identity information tells the world who we are, and enables us, to a point, to validate and verify who we are.

For individuals, it's the core of our existence -- to be carefully guarded, with access carefully controlled.

For businesses and organisations, it's at the heart of their ability to know their customers and members and reach them in ways that bring value to both the organisation and the customer.

### **Identity related crime**

Identity related crimes, are those which involve the manufacture of a non-existent identity (including the concealment of true identity), or the theft or unauthorised use of another's' identity, in order to facilitate a crime.

Identity related crime is far reaching, and has been the common factor criminals have used to facilitate a diverse range of crimes, including large scale organised frauds against financial institutions, terrorism, voter registration fraud, the obtaining of government benefits and licences.

We may have the perception that identity related crime couldn't touch us, however in reality, it is the crime factor to which every individual and business is most exposed.

In the private sector, we rely on verification of identity to allow us to perform all kinds of transactions and business activities, from the giving of credit, to the employment of staff, whereas the government utilises our identity to fairly and correctly distribute entitlements.

At the core of our exposure to identity related crime, is our reliance on the security and validity of the identity documents that we use to prove who we, and others are, when conducting any number of transactions.

A major issue confronting law enforcement agencies, financial institutions, and business in Australia, is the utilisation of the 100-point identification verification procedure by criminals to facilitate their criminal activity, by creating false identities, or assuming another persons identity. The 100-point identification system was developed to minimise corrupt money laundering and taxation avoidance within the finance industry. The 100-point identification system requires a cash dealer to verify an account holder's identity by the production of certain primary and secondary documents. A certain point score weights these documents, and the total of the documents produced must equal or better 100 points.

A primary identity document is a document primarily intended to confer identity, and includes passports, birth certificates and citizenship certificates. A secondary identity document is used to support identity but is not in itself intended to confer identity, and can include nearly 40 various documents, including a drivers' licence, student ID card, Medicare & credit cards and utility invoices. The major flaw in the 100 point

system is that the majority of documents required for proving identity can be counterfeited, forged or fraudulently obtained, with this compounded by the fact that most people cannot identify what a drivers licence or other identity document from another country or state 'should' look like.

Traditionally, there is no formal single unique identifier used as such in Australia. The photo drivers licence is widely accepted as a formal identifier, used by individuals to verify identity when passing a cheque or hiring a video, and likewise accepted by organisations when accepting that cheque and hiring out the video.

Drivers licences, passports, credit cards, Medicare cards, and any other documents that we accept as 'Proof of Identity' (POI) documents, are only issued by the authorities for their primary purpose, (ie: to prove the holder is qualified to drive), and are not currently intended to be used primarily as identity documents.

In reality, these documents are relatively easy for criminals to obtain or manufacture, in either a fictitious identity or in an identity takeover of someone with a good credit rating, who won't know they are the victims of an identity theft until the bills start arriving as a result of credit unlawfully obtained utilising their identity.

In May this year, police in NSW arrested the principal of an organised crime syndicate after an operation, which netted 400 fraudulent identities, including drivers licences, firearms licences, security licences, birth certificates, blank credit cards, and rolls of holograms.

Another recent example occurred when the Victoria Police Major Fraud Group received a complaint that four victims, all aged over 55, had their superannuation funds stolen, to the value of \$612,000. The offender assumed the identity of the victims, and then forwarded documentation to the superannuation fund requesting release of the funds. The funds were released with cheques being forwarded to the identity thief. On every occasion the identity documents produced were fraudulent.

Identifiers of businesses as bone fide are also susceptible; as a result of the implementation of the ABN system in 2000, the Australian Taxation Office identified numerous incidences of fraudulent applications. The Australia Securities & Investment Commission has also documented cases of person fraudulently registering themselves as directors of bona fide businesses without authority of those businesses.

Many investigations conducted for organisations by our Loss Prevention division, regarding both internal and external crimes, have involved identity crime.

We have seen situations of staff retaining a customers' credit cards used in an eftpos transaction, or obtaining card details from a previous transaction, and then using them to take over the identity of the customer in obtaining credit and purchasing goods. Other examples include external criminals purchasing from organisations, often via phone or on-line orders, using a legitimate persons identity that they have taken over as a result of gaining access to, or purchasing personal information.

Organisations can be exposed to loss, particularly via on-line transactions where the validation processes in place for the purchasers details or credit card details are inadequate. In July 2002 police from the NSW Computer Crimes Unit arrested a 22 yr old Bankstown man with a hack attack on Optus in December 2001, in which he allegedly obtained 40,000 customer passwords.

## **Employment fraud**

The employment area is showing an alarming increase in incidence of identity crimes, due to the level of competition for jobs, compounded by the relatively low standard of screening regarding references and criminal history of applicants.

The recent New Zealand case involving the gaoling of a television executive, who was employed based on false credentials, emphasises both that people with poor employment histories or criminal convictions, will lie to a prospective employer to secure a job, and that employers will trust details presented on a resume, without verification.

We have seen more organisations using our pre employment screening services, to assist them in obtaining the maximum available information, and verification of identity and background, prior to hiring staff.

We frequently find that applicants we screen for clients have criminal histories, and that resumes involve omissions or lies, designed to portray a poor history as an acceptable one.

And of course the staff who are the subject of the hundreds of internal investigations that we conduct on behalf of organisations every year, potentially go straight back into the labour market, after being dismissed and prosecuted for theft, and subsequently employed by unsuspecting employers.

It is not un-common to discover situations where previous employers listed have been fictitious, with friends being set up to take reference check calls from prospective employers, portraying themselves as a past employer.

The risk of employing a person who does not technically exist, or do not have the skills or experience you think they do, or is pre-disposed to dishonesty, are potentially significant.

If that person has demonstrated dishonesty in someone else's workplace previously, or has been criminally prosecuted for a crime of dishonesty, there's a higher likelihood that they will do the same in your workplace, particularly if they utilise fraudulent identity documents or non disclose previous dishonest behaviour to you.

The time to find out these facts is before you hire.

## **Counting the Cost**

A significant challenge for Australia is to determine the real cost of identity-related crime to our society.

The Federal Attorney Generals Department estimates the cost of identity related crime at \$4 billion dollars annually.

However there are several factors, which make it difficult to accurately quantify the cost and extent of these crimes, including:

- A lack of standardised definition of identity related crimes across the Commonwealth, States and Territories;

- Because identity related crime is an element of many other crimes it is not statistically recorded independently;
- There is no offence for possessing fraudulent identity documents or another person's personal identifying information without intent to use them for dishonest means;
- There is no one organisation responsible for identity related crime;
- Not all identity related crime is reported.

Internationally, identity related crime is recognised as the fastest growing type of crime, with the US Government declaring it the No.1 crime in the US. Identity fraud in the United Kingdom saw a 461% increase in 2000, followed by a 165% increase in 2001, and now a further rise of 55% in the first two months of 2002.

Of particular interest is that the US Federal Trade Commission indicates that **over 50 per cent of all identity theft complaints are related to credit card fraud**, followed by, the establishment of fraudulent phone and utility accounts, bank fraud, and fraudulent loans.

In Australia, the Australian National Audit Office found in 1999 that there were 3.2 million more individual Tax File Number (TFN) registrations than people in Australia counted at the last census and an estimated 185,000 potential duplicate records of individual taxpayers amongst 17.1 million active tax records of such taxpayers.

It is estimated that up to 2 per cent of new customers to private and public organisations in Australia use fraudulent identity documentation.

A trial undertaken by the Westpac Banking Corporation with the NSW Registrar of Births, Deaths and Marriages to verify certificates found that some 13 per cent of birth certificates presented were not an exact match with the records held by the issuing authority, and had been altered, fabricated or forged.

Birth certificates are the classic starting point in the establishment of the circle of identity, as they allow for the building up of other identity documents.

### **Current Issues and Challenges**

With the increasing expansion of e-commerce opportunities for businesses and customers, the Internet poses a unique problem in addressing the issue of identification of subscribers and operators, in that no physical presence is widely available.

Additionally, it is not uncommon for individuals to have numerous identities in an electronic environment (eg email addresses).

The issue is how do individuals and organisations ensure that the people presenting themselves are actually who they say they are, and that the POI documents produced are valid. The accurate identification of persons requesting goods services and benefits from private and public organisations are crucial. Of serious concern, is the use of web hijacking, which involves the takeover of a legitimate organisation's web page, or redirecting users to a fraudulent constructed page through false

pretences, to steal an individual's identity. One recent example involved the emailing of AOL subscribers that their AOL accounts had been recently attacked by a hacker and they were then directed to a web page to fill out personal information (**See figure 1**). The hyperlinks attached to the fraudulent page were linked to legitimate AOL pages that gave the fraudulent page an air of legitimacy. When the source code to the fraudulent web page was reviewed, the following passage was included;

***"I shall not be held responsible for anything from this page/html. This page is a joke and should not be treated seriously. By viewing this page, and by viewing the source code, you agree by these terms. If you work for the fbi, aol, or you want to use this page against me in any way, you cannot use this page, and you cannot use this against me in a court of law. IF you do not agree to these terms you cannot use this page, doing so violates my constitutional rights. Thank you"***

### **Adverse Impact of Identity Related Crime**

Identity related crime impacts on Australian society in ever increasing proportions. Whilst in some instances the costs in terms of economic loss from individual identity frauds are readily quantifiable, the human cost in terms of victimisation and reduced confidence in systems and processes is difficult to determine. Some of the major issues are that identity related crime;

- Whilst conducting interviews with various law enforcement agencies, many police officers spoke of criminals committing crimes and on detection and arrest, utilising stolen assumed identities, resulting in the later arrest of innocent people who had their identity stolen. In South Australia, one young woman had her identity stolen by another female who committed a number of criminal offences, and when arrested used the stolen identity. This young woman now has a significant criminal history recorded against her name and date of birth. Many victims of identity theft in the USA are required to carry their copy of the police report to avoid apprehension and detention for crimes they did not commit.
- Impacts on businesses providing finance & credit to identity thieves and fraudsters. Front line staff of these organisations are not formally trained to detect false or fraudulent POI documents. There has also been an increase in credit facilities offered by retailers who trade outside normal business hours. This can result in restricted access to normal risk management practices and requires screening models to be practical in their application;
- Allows potential opportunities for corruption to develop in agencies issuing identification documents. In April 2002 a long-standing VicRoads employee who issued false licences for payment was imprisoned for one year.
- Is facilitated due to accessible nature of increasingly sophisticated desktop publishing software. The quality of POI documents produced on small home based personal computers, is increasing the difficulty for the untrained eye to detect counterfeit documentation, thereby undermining the due diligence processes of many businesses and organisations;
- Relies on the fact that all electronic based identity systems currently have their initial creation from paper based identity documents. This is particularly problematic to the Internet community.

## Compromised Credit Rating

The ability to obtain credit or finance for a multitude of requirements relies significantly on an individual's credit rating. This credit rating is developed over many years and involves obtaining, maintaining and repaying loans and credit facilities, as well as ensuring any debt occurred to organisations is repaid within the terms agreed. All this credit information is maintained in the databases of credit reference organisations, such as Baycorp Advantage, or Dun & Bradstreet. When an identity thief steals someones identity, they gain access to the credit rating that is attached to that identity. If the criminal obtains credit or finance utilising the stolen identity, the legitimate owner of the identity may incur a negative credit history that impacts on their future ability to obtain finance.

As there is no offence for possessing fraudulent identity documents, or another person's personal identifying information, without intent to use them for dishonest means, there is no avenue for a person who has had their identity stolen to achieve any redress through the criminal justice system. Currently, the victim of identity related crime is classified by Australian law enforcement agencies as the entity that lost property or was exposed to potential loss (such as the bank in the case of credit cards). This leaves the rightful owner of the stolen identity with potentially costly civil remedies to restore one's credit rating and recover their identity

## Protecting Your Identity

Currently, it is very difficult to protect your identity to the point where it will never be compromised. There are a number of steps that individuals can do to minimise the opportunity for a criminal to target them for identity theft. They are;

- Check your bank and credit card statements and phone accounts carefully. If there are any suspicious or unauthorised transactions report them to the provider immediately.
- Be aware of the tricks the thieves use to get information. Do not share your information with anyone that does not satisfy you of his or her bona fides, particularly direct marketers via the telephone. Beware of emails asking you to confirm your password or account number.
- When in doubt, shred. Never throw out anything that contains your personal information into the rubbish, including junk mail that is personally addressed to you. Criminals obtain that information by rummaging through your rubbish, which is known as 'dumpster diving'.
- Protect your important identity data. Do not leave it lying around the house or on personal computers without being password protected. Remember that not all identity thieves are strangers. Recent US studies reveal that up to 10% of victims knew the offender. The identity thief may be a friend, business colleague, family member or neighbour.
- Contact Baycorp Advantage on [www.baycorpadvantage.com.au](http://www.baycorpadvantage.com.au) or call (02) 9464 6000 and review your credit file. Baycorp also offer a subscription service, My Credit Alert, which immediately notifies you of any changes to your credit file, which would identify any unauthorised transactions.

## Conclusion

An individual's right to privacy is one of the benefits available to all members of Australian society.

A cornerstone of that privacy is a person's identity and that unique identity should be protected by individuals, and by any organisation entrusted with the personal details of an individual. It is becoming increasingly difficult to preserve personal privacy without using biometrics. Biometrics does not compromise privacy. They are designed to provide the user with total control over who has access to their information, supported by a clear audit trail recording all access to that information. Australians need to ask themselves; would they prefer to retain the current system, with your attributable and biographical identity information, including name, address, date of birth, etc available to anyone who has their PIN, password or 'hacked' customer records; or a system that prevents a record from being penetrated unless it is unlocked through biometric verification?

Although the Australian people rejected the concept of the 'Australia Card', when it was first proposed in the mid 1980's, various government agencies currently hold the information that was proposed to be held via this card, including a biometric, being the digital photograph on some states drivers licences. State and Federal governments are currently examining the options for the implementation of a single, whole of government identifier, which may include a biometric. It is time to raise the bar against identity criminals and offer all Australians a legitimate, dynamic and secure identification system that will minimise fraud and protect identity.

*Shane Ringin can be contacted at [www.proactivestrategies.com.au](http://www.proactivestrategies.com.au) or – 1300 13 30 73, and will be available at the Retail Business Technology exhibition in Melbourne, 28-30 August, at the Pro Active Strategies stand - G27.*