Speech presented by Adam Graycar,Director,
Australian Institute of Criminology:

"Identity-related fraud: risks and remedies"

in Hobart, Perth, Adelaide, Melbourne & Brisbane,
April & May 2002

AUSTRALIAN INSTITUTE OF CRIMINOLOGY

Identity-related Fraud: Risks and Remedies

Text of talk given in
Hobart, Perth, Adelaide, Melbourne & Brisbane

April & May 2002

Adam Graycar

Director
Australian Institute of Criminology
GPO Box 2944, Canberra 2601
phone: 02 6260 9205
fax: 02 6260 9278
e-mail: adam.graycar@aic.gov.au

Identity-related Fraud: Risks and Remedies
Adam Graycar

In the tearoom at the Australian Institute of Criminology there is a cartoon on the noticeboard, and it has a picture of a dog sitting at the keyboard of a computer, and he says to another dog sitting nearby “you know, on the internet, nobody knows you’re a dog”

Knowing who people are is pretty fundamental to the way we live our lives and do our business, and the faking of identity is a much bigger issue than most people think.

When Ned Kelly did his stuff he and his gang wore armour, not only to protect them from bullets, but also to disguise their identities. Pirates on the high seas sometimes flew the flag of another innocent ship in order to approach their victim without alerting them to their true identity and purpose.

These were the old fashioned equivalents of false identity. In the case of economic crime, the objective is to withdraw cash or purchase goods or obtain a line of credit, and then be unable to be located by the creditors or the police, or obtain government benefits or services. The key strategy involved is to pretend to be someone else or to incur liabilities in an entirely fictitious name.

There are also significant identity fraud experiences in the movement of people across borders, both for humanitarian and terrorist activities

TYPES OF FALSE IDENTITY

Some people steal somebody else’s identity, and others create false identities.

Identities can be stolen or created using legitimate or forged documents. Legitimate documents might be stolen from a living or deceased person, while forged documents might involve changed names or variations of real names.

Forged documents can be created to support a fictitious identity - a fictitious name, or a misappropriated real name, date of birth, personal details etc can be forged onto documents. The technologies that allow us to do wonderful desktop publishing allow villains to create illegal documents that look convincingly real.

Names are interesting - people change their names for all sorts of reasons, use maiden names or married names, use their mother’s maiden name instead of their father’s name, and do all of the above inconsistently. One of my daughters uses my name, the other her mother’s, my wife uses her maiden name, and her sister her mother’s maiden name - and we are a simple family not in the business of defrauding anyone! With an increasing non-European immigrant community we find ourselves with decisions about the order of Asian names, or the proliferation of names like Chan, Ngyuen, Mohammed, Abdul etc. This is not to mention the fact that in the Melbourne *White Pages* there are 2,351 Smiths and 1,094 Nguyens (*Age* 22 June 2001).

And, of course, there are many cases where people appear who have no documents at all, and about whom judgements have to be made.

At the benefit concert in New York to raise money for families of the emergency services victims killed in the World Trade Centre attacks, the legendary British rock group The Who brought the audience to their feet with a rousing rendition of their classic song “Who are you”. At the time however, neither the band nor the audience, were aware of just how significant was the timing of this song. Even as it was played, the FBI were busy with the added burden of a new and rapidly escalating economic crime directly related to the New York tragedy.

Within days of the appearance of lists of those missing – or presumed missing – in the rubble of Manhattan, hundreds of millions of dollars of goods and services were being illegally obtained by people who had adopted the identities of the victims. Such was the outpouring of public sympathy that people were literally able to walk in off the street into government offices, shops and banks, report that their usual documentation was lost in the rubble and on the production of the flimsiest of identification, obtain documentation like real driver’s licences, which in turn were then used to obtain other genuine documents.

From here, it was only a short step to illegally obtaining goods and services, such as opening up lines of credit large enough to drive away in brand new and expensive cars. False identity was also an issue on September 11 in that nobody knew for a long time who it was who was flying those planes, how they got into the country etc etc.

This example is grotesque under the circumstances but it highlights in graphic detail a problem of identity theft.

Here in Australia a young man was recently sentenced in the County Court of Victoria to five years’ imprisonment, and ordered to pay the Commonwealth government about half a million dollars as a result of an identity fraud scam. Over a period of 26 months, this man had engaged in a systematic campaign of deception in which he had made use of over 40 names other than his own, had registered fictitious businesses and companies, and opened numerous bank accounts giving false names and false addresses. He obtained almost half a million dollars from various banks and merchants as well as from the Commonwealth government.

He started by going to a Westpac branch and opening a bank account in a false name. This is a criminal offence that carries a maximum term of 2 years’ imprisonment. He arrived at the bank armed with a birth certificate and a student identification card in another person’s name that he had created at home using a personal computer, scanner, and laser printer. They were very high quality counterfeit documents. He had his 100 points as required by the *Financial Transactions Reports Act* (1988).

Almost two weeks later, he used the same documents to open a Commonwealth Bank account. In both cases he gave his mailing address as a newsagency post office box which the banks were happy to accept.

In one week he opened 42 new accounts with the Commonwealth Bank and the ANZ using false birth certificates and student identification cards and again gave a post office box at a newsagency as his address. He had so much ID it wasn't funny, and he was easily able to register companies as well.

He then registered a business name "TGE Plumbing" with the Consumer and Business Affairs Office in Melbourne (as it is now called), giving one of the false names he had created as the proprietor of the business. He then opened a cheque account with Westpac in this business name.

He was now ready to commit his crimes. I won't go through the lot, but it involved churning fake cheques, withdrawing money from ATMs, obtaining sales tax refunds which were paid into the various company and business bank accounts, as well as Medicare benefits in his various names. It would take me ages to go through all the details.

Mostly he created identities, and obtained benefits in the name of non-existent people. Some crooks also use real identities to scam various systems.

Let's look at the big picture and the context.

In Australia there are 400,000 to 500,000 new Australian residents per annum (births, permanent new arrivals and long-term visitors)

Last year:

- The Australian Electoral Commission processed 2.46 million enrolment forms and amendments, with more than 12.5 million Australians registered to vote.
- The Australian Taxation Office issued about 500,000 tax file numbers
- Centrelink processed 4.4 million new claims or re-grants of benefits
- The Department of Foreign Affairs and Trade issued 1.4 million passports
- The Health Insurance Commission issued 3.97 million new or updated Medicare cards, covering 7.344 million people

And that is only some of the Commonwealth activity - the states issue drivers licences, which are used for ID (though that is not their main purpose), but we know that not all drivers licences are what they purport to be. Same with birth certificates -

- The NSW Registrar of Births, Deaths and Marriages did a trial verifying birth certificates used with Westpac to open bank accounts. It found that 13% of birth certificates presented during the experimental period were not an exact match with the records held by the issuing authority.
- In surveys of computer crime and security conducted by the Victoria Police (and others) in 1999, 19% of the organisations surveyed thought that identity-related fraud would have an impact on their organisation over the next five years.

But its happening now, and has been for ages:

In 1997, for example, two former Health Insurance Commission employees were convicted of defrauding the Commonwealth by creating false provider accounts and making illegal claims to the combined value of more than $45,000

Misuse of identity is also a problem for the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) There was a recent report on a special market for people who want to migrate to Australia without having their names on any official list. The prospective immigrant pays a syndicate around $100,000. The syndicate works for months or even years establishing a new identity for the person in Australia. The person then flies to Australia using either false documents or documents belonging to someone else, and assumes life under their new name. A different person leaves the country on the same documents, so that there is no record of the person who came to Australia still being here.

On 25 September 2001, a financial consultant contracted to the Department of Finance and Administration was convicted of defrauding the Commonwealth by transferring $8,735,692 electronically to private companies in which he held an interest. He did this by logging on to the Department’s computer network using another person’s name and password. He also was able to obscure an audit trail by the use of other employees’ logon codes and passwords. He was sentenced in the ACT Supreme Court to 7½ years imprisonment.

From 1990 to 1994, an accountant submitted tax returns containing either false group certificates or false statements of earnings under six names, with most of the returns also claiming false business losses. He set up separate bank accounts to process tax cheques received under these false names and defrauded the tax office of $558,668. He was sentenced to 6 years’ imprisonment.

About one quarter of reported frauds to the AFP involve the assumption of false identities.

Looking overseas, in April last year in Tijuana, Mexico, two armed robbers ambushed a delivery van in order to steal 6,000 identity cards that were being delivered to consulates in Mexico. The cards would allow entry into the United States and are estimated to be worth more than US$1 million on the black market.

I could rattle off more Centrelink cases, banking cases, immigration cases, the market in fake University degrees etc, as well as cases of phantom beds in nursing homes occupied by non-existent patients and serviced by non-existent staff.

What we have is false identity in funds transfer fraud, revenue fraud, theft, financial services fraud, social security fraud, other Commonwealth benefits, health insurance fraud, general insurance fraud, workers compensation fraud, payroll tax fraud, and lots more things in the future - things we haven’t thought of such as electronic conveyancing.

We know therefore that members of the public, like our con-artists use false identity to obtain benefits illegally. We know that people in trusted positions sometimes do the wrong thing, whether they be professionals like our accountant, or staff members inside banks or the

Health Insurance Commission, or somewhere similar. We know that in the international arena those who smuggle people, launder money and move drugs and arms are into identity fraud in a big way.

In our Australian Institute of Criminology training course on identity fraud, as we look at what it is, how to identify it and develop effectiveness in fraud control, how to develop key prevention strategies, and we also examine some of the forensic indicators of identity fraud, and bring people together to see the whole picture.

But there are also a lot of big questions - bigger than our training course!

- How should government organisations identify people when they issue official documents such as birth certificates, driver's licences, and passports? Is it enough to rely on documentary evidence or should people be interviewed or asked to provide some biometric evidence such as a fingerprint?
- What steps should financial institutions take to verify the documents that people produce when they open accounts? Is the "100 Point System" adequate in the twenty-first century?
- Would a nationally-issued identity document solve the problems of identity-related fraud, or would this just be another document that could be counterfeited and abused by fraudsters?
- Should it be possible to share information on public and private sector databases in order to find counterfeit or altered documents used to verify identity? Should the police maintain a database of identities that have been used for dishonest purposes?
- What is the right balance in terms of ensuring accuracy of identification, business efficiency and cost-effectiveness, and personal liberty?

These are issues that both governments and corporations need to discuss and analyse critically and openly in order to control what is clearly an escalating crime problem.

We can't say we don't have challenging questions to start the day.

Quantifying the Scale of the Problem

In Australia alone we have estimated identity theft to cost in excess of $2 billion per year. This is miniscule compared to the losses in the USA where credit card fraud makes up 50% of identity theft complaints to the Federal Trade Commission, and where ID theft victims either knew or were related to the criminals in 14% of cases reported.

As senior managers you probably have some idea of the dollar value of the losses to your organisations to identity fraud. One of the key facts that we need to know in assessing the scale of the problem of identity-related fraud is how much money is being lost to this type of criminal activity.

Knowing how much has been lost in cases involving fraud has important implications for deciding whether or not to embark on a prosecution, and also for justifying, in terms of Return on Investment, any expenditure associated with taking legal action.

Knowing exactly how much has been lost to an organisation following fraud is also important for the costing of future fraud prevention initiatives.

Sometimes organisations may be unaware of how much they have lost in individual cases and it will only be after the case has been investigated by forensic accountants and the police that the full extent of losses will become apparent.

PREVENTION AND COUNTER MEASURES

It is often said that crime follows opportunity. Whenever there is an opportunity to get some money, obtain a benefit, or have access to something highly desirable, there are opportunities for illegality, and in these areas there is always the need for people to have documents and information that can be used to prove their identity with certainty.

In general, the steps for effective fraud control are

- prevention
- detection
- investigation and prosecution
- reporting of cases
- training and education

To make crime harder to commit there are three general situational strategies that we might ponder in looking at identity fraud,

- Increasing the effort
- Increasing the risk
- Reducing the rewards

I want you to think about whether these strategies are available to you, and how you make sure your staff can respond.

Increasing the effort can be both technological and operational.

The “100 Point System” is an operational means of increasing the effort, although, as we have seen, it is relatively easy to overcome the procedures that have been established.

The problem is that both the primary and secondary documents used to verify identity under this system were not created with the intention that they be used for identification purposes. As a result, they often do not have adequate security features in place which makes them susceptible to counterfeiting and alteration.

Another means of increasing the effort is for documents or cards to be created which can be used to identify people with certainty, and which are designed specifically so as to make them difficult to counterfeit or alter. One example is the plastic money - notes, not cards, that Australia has pioneered. The money you carry in your wallet is a great international innovation.

Unique identifiers could be used to establish identity for all commercial and private transactions or business relationships where it is essential to identify the participants accurately, such as when opening bank accounts or registering for government benefits. As electronic commerce becomes more widely used, the need to identify people to whom encrypted key tokens will be issued, will also become of critical importance.

What is also important from a policy perspective is the need for organisations to be able to verify the legitimacy of documents presented for proof of identity purposes with the issuing agency. For example, an officer of the Health Insurance Commission needs to know that a New South Wales driver’s licence tendered by someone wishing to obtain a Medicare card was in fact issued by the NSW Roads and Traffic Authority to the person in question.

Technologically the effort can be increased by a range of passwords, PINs, and unique identifiers for people to gain access to that which they should be able to gain access. Technology is moving quickly on that front. There are down sides, as well - I often can’t get into websites because I simply can’t remember which of my many log on names or PINs goes with that account.

There are also biometric identifiers (such as fingerprints or retinal images) which are being used when individuals first make contact with organisations and are now being used by a range of public and private sector organisations including hospitals, banks, and retail stores. However, these only confirm that the person is the person who first made the contact (and who may have stolen or assumed another identity!)

Increasing the risk involves your organisations setting in place procedures for detecting people who do the wrong thing, and the consequences if they are caught - and I won’t spend any time on that now. The only point I want to make here is that there are significant data matching opportunities, but at the same time significant privacy considerations - and this is going to be a lulu of a debate!!

Reducing the rewards involves a range of legislative responses and organisational activities. Russell Smith has documented these in some detail including the use of increased penalties and the confiscation of assets. In the United States, federal legislation now makes identity theft a crime with penalties of up to 15 years’ imprisonment and a maximum fine of US$250,000.

This is not the occasion, however, to do a long and ponderous analysis of all the issues. These will be unfolded over time. A significant part of our work at the Australian Institute of Criminology in developing crime prevention specialists in the public and private sectors is alerting government and business at all levels to the very real risks to which they are being exposed under current practice. We also run training courses in this area, such is our level of concern at this burgeoning type of economic crime. Part of the problem is that people do not appreciate how easy it is to commit this type of crime, given access to modern technology.,

The steps which can be taken to prevent identity-related fraud depend upon a range of considerations. These are:

- the likelihood that the risk will be realised;
- the cost of the countermeasures;
- the effectiveness of the technologies used;
- the user-friendliness of systems;
- privacy concerns if data-matching is contemplated; and
- possible negative consequences on the behaviour of users.

It might be possible to prevent all forms of identity-related fraud but the solutions may simply be too costly, unwieldy, and authoritarian to be acceptable.

Technology will provide some of the solutions but these need to be supported by a simple and effective legal regime to ensure that instances of abuse can be prosecuted and that individual privacy is safeguarded.

What is of critical importance, however, is for people to be made aware of the risks of identity-related fraud and how to protect themselves.

Taking action after a crime has been committed is difficult, costly and often impractical. Commercial and personal reputations are often hard to repair and offenders often impossible to find.

What I wanted to do today was to introduce you to the concept of identity-related fraud and to let you know about some of the work we at the AIC are doing on it. Russell Smith and his team have been examining the area, they have published on the issues and ramifications, and preventive and counteractive mechanisms. The AIC’s Learning and Knowledge Development Unit is turning a lot of their material into materials focussing on awareness of identity-related fraud and risk assessment.

By your being here, you know that keeping up-to-date on the new risks of identity-related fraud is essential for senior executives, as new vulnerabilities are created all the time, and previous crime prevention solutions are overcome by more knowledgeable offenders.

The Way Forward

To conclude, I would like to leave you with three observations on how we should respond to identity-related fraud in the future.

- *The first concerns awareness-raising of the nature and extent of the risks involved.*

There is now considerable information available about the nature of these risks and how to avoid them. People need to be taught how to protect themselves and how to avoid situations of high risk. Managers need to make sure that their staff are adequately trained in detecting possible acts of deception and in dealing with them effectively. And, of course, effective risk assessment procedures need to be in place.

- *The second involves making effective use of existing strategies*.

Many of the solutions to identity-related fraud already exist. People, however, have neglected to make full use of them in order to simplify their business and personal lives. Sometimes we are too busy to change computer access passwords or to pick up the phone to check with a referee about a new employee. Our staff might think it unnecessary to call an issuing authority to confirm the validity of a document that someone has produced.

- *Finally, there is the need to develop and use new technologies*.

New technological solutions such as public key systems, biometrics and data-matching are being developed all the time. Although the cost of some may be large, resources need to be given to such R&D and, most importantly, any new solutions should be properly evaluated in order to test their effectiveness. Assessments also need to be made of the potential social and privacy implications which the use of some new technologies entails. The importance of these concerns should not be under-estimated.

As in all areas of fraud control, keeping one step ahead of criminals is an on-going task that requires time, commitment, and resources. We are not an operational agency, but we work closely and harmoniously with those organisations that are, and we are always happy to look at blending our knowledge and skills with yours.