
Mr David Hawker MP
Chairman
The House of Representatives Standing Committee on
Economics Finance and Public Administration
Parliament House
Canberra ACT

9 March 2000

Inquiry into Tax File Number: Submission

Dear Mr Hawker,

The following information is furnished in response to your invitation to me to make a submission to the inquiry being conducted into the Tax File Number ('TFN') system.

I am currently employed by PricewaterhouseCoopers as a Manager, Fraud & Investigations. PricewaterhouseCoopers provides professional services to the biggest corporations in Australia. We undertake inquiries on behalf of our clients in matters of fraud, credit card and payroll fraud and software piracy. Many of these investigations have as their basis the fraudulent use of documents of identification.

PricewaterhouseCoopers fraud investigators have uncovered a number of examples of frauds which have their genesis in false identification. Some examples include :

- A senior executive in a Local Council obtained employment, in part by providing a false referee, false tertiary qualifications and a changed identity, following a conviction for fraud in a previous organisation.
- A number of payroll frauds have been committed as a result of offenders, with payroll supervision responsibilities, creating bank accounts in fictitious names and channelling unauthorised payments to those accounts.
- A telecommunications employee, with responsibility for providing goods to offshore sections of the company, created a false forwarding/customs agent and paid money to that organisation for alleged services. False bank accounts were opened and the money was syphoned off to support his lavish lifestyle.

The ease with which these offenders created fictitious identities and opened bank accounts is disturbing.

Between July 1994 and November 1999, I was a Detective attached to the New South Wales Police Service Commercial Crime Agency ('CCA'), where among other matters, we investigated many instances of identity fraud and counterfeiting of identity documentation.

I will briefly set out three matters involving fraudulent and counterfeit documents of identification that I investigated whilst attached to the CCA. I will then highlight some possible improvements and recommendations to minimise future occurrences of these types of fraud. The three instances were :

- An offender who falsely made application to the New South Wales Registry of Births, Deaths & Marriages for Birth Certificates in deceased childrens' names. Details of this inquiry are attached at **Annexure A**
- An offender who utilised high quality computer equipment to generate personalities to obtain credit, then fraudulently obtain additional computer equipment. Details of this inquiry are attached at **Annexure B**
- An offender, who generated twelve identities and defrauded financial institutions in excess of \$5 million. Of this, \$1 million was laundered out of Australia to Greece and has never been recovered. Details of this inquiry are attached at **Annexure C**.

The examples as set out in the attached Annexures illustrate the ease in which many organised fraud offenders can accumulate false identity documents. Many offenders not only commit state fraud offences but commit numerous Commonwealth crimes, including taxation offences. Some offenders, having accumulated false birth certificates and false driver's licences also apply for and obtain TFNs. Although taxation documents do not have photographs of the holders of the items, it is a particularly powerful piece of identification for offenders. This is because it is believed that the Australian Taxation Office does not issue TFNs easily and mere possession of a TFN is a strong document of identification.

The offences for which the above offenders were charged and convicted were relatively minor compared to similar legislation in the United States of America. In October 1998, the Identity Theft and Assumption Deterrence Act was enacted in the United States. A reading of the section relating to offences, sets out the seriousness in which United States legislators consider identity theft and fraud. Under Section 1036 :-

- (b) *Whoever in interstate or foreign commerce, or through the use of a communication facility, knowingly, with intent to defraud, and in order to receive payment or any other thing of value the aggregate value of which is equal to or greater than \$1,000 –*
- (1) *receives, acquires, obtains, purchases, sells, transfers, traffics in, or steals, or attempts to receive, acquire, obtain, purchase, sell, transfer, traffic in, or steal, or otherwise causes or solicits another to do the same, any personal identifier, identification device, personal*

information or data, or other document or means of identification of any entity or person;

(2) possesses or uses, or attempts to possess or use, or otherwise causes or solicits another to do the same, any personal identifier, identification device, personal information or data, or other document or means of identification of any entity or person; or

*(3) assumes, adopts, takes, acquires, or uses, or attempts to assume, adopt, take, acquire, or use, or otherwise causes or solicits another to do the same, the **identity** of any entity or person;*

shall be fined under this title, imprisoned not more than 15 years, or both.

(c) Whoever is a party to a conspiracy of 2 or more persons to commit an offence described in subsection (b), if any of the parties engages in any conduct in furtherance of the offense, shall be fined in an amount not to exceed the amount of the fine to which that person would be subject for that offense under subsection (b), imprisoned not more than 7.5 years, or both.'

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

One issue highlighted in the attached annexures is the issue and obtaining of birth certificates. These documents are a major segment in the chain of identity documentation. Under the Financial Transactions Reports Act, to open a bank and credit card account, one hundred points of identification must be achieved by the applicant. An individual's birth certificate is worth seventy points, and is therefore a very significant portion of the total. With the apparent ease at which false or counterfeit birth certificates are being obtained, serious consideration should be given to reducing its individual points value.

It is also a concern that not all state Registries of Births Deaths and Marriages are fully computerised. It is apparent that not all the state and territory Registries interface with each other with relevant information. That is, a person registered as deceased in Western Australia, may have been born in New South Wales. A fraudulent application for a Birth Certificate in New South Wales would be issued, as the New South Wales Registry would not know that the applicant was deceased.

However, the New South Wales Registry of Births Deaths and Marriages has taken significant steps in the past two years to limit the issues of birth and death certificates to false applicants. The Registry has trialled an internet verification system whereby organisations are able to enter certain details of a birth certificate – name, date of birth and certificate number – and receive information back either verifying or negating the validity of the information. However, I believe that this system may only be destined for use by

government departments such as the New South Wales Roads and Traffic Authority. This system would be extremely advantageous to the financial and credit card institutions to avoid ongoing problems of false account opening. This in turn could minimise the incidence of false applications for TFNs.

The internet verifications system could also be extended to state and territory driver's licence information. All applications at financial institution for the opening of accounts with the applicant using a driver's licence as the primary document of identification, could be verified using a similar system. This would reduce the incidence of fraudulent interstate driver's licences being used as identification.

All the systems for the issue of birth certificates and driver's licences need to be secured. If the issue of these documents cannot be guaranteed, the fraud control systems for all of the other government departments – Australian Taxation Office, Passports Australia – and private organisations – financial institutions and credit card companies – become superfluous. The apparently excessive issue of TFNs may be in part due to the lackadaisical issue of birth certificates and interstate driver's licences that are at present, unable to be verified.

Perhaps consideration should be given to pursuing systems of biometric identification. The various biometric identification systems of identification available would more significantly assure an individual's identity and assist in minimising the incidence of identity fraud and theft, including the issue of TFNs to false applicants.

I appreciate the opportunity to tender this submission for the inquiry. If you wish to discuss any aspects about the submission, please do not hesitate to contact me on (02) 8266-9253.

Yours sincerely

Paul Baker

ANNEXURE A

IDENTITY FRAUD COMMITTED UPON NEW SOUTH WALES REGISTRY OF BIRTHS DEATHS AND MARRIAGES

Between 1995 and 1996, an offender made numerous false applications for Birth Certificates to the New South Wales Registry of Birth Deaths and Marriages ('Registry'). The CCA was notified by the Registry that they had detected a false application for a birth certificate via their postal issue system. Over the ensuing three month investigation, the CCA identified an additional twenty six (26) birth certificates that had been falsely applied for and issued. The offender utilised a basic system of applying for these certificates. He identified deceased children by visiting various cemeteries around New South Wales and subsequently applied for their Death Certificates from the Registry. This document gave the offender sufficient information to apply for the Birth Certificates. All applications were done via post, with minimal documentation supporting the application.

After obtaining the birth certificates, the offender was then able to accumulate various other documents including membership cards to clubs or libraries, Medicare membership and even registration to vote. The offender was then able to open numerous bank accounts at the four major financial institutions. The offender was able to accumulate such an array of false documentation from these organisations, that he effectively created individuals who for all intents and purposes existed.

During the course of the inquiry, we were able to identify some of the 'holders' of these documents, who we believed purchased packages containing these documents from the main offender. These people included :-

- 1 Two Czech nationals who had been in Australia for two months prior to being arrested by the CCA in Kings Cross. Both had the birth certificates, bank account documentation, library membership and Medicare membership in false names that had been created by the main offender. Both men were charged with fraud offences and deported to Europe, where they were wanted in Prague, Czech Republic for firearm and economic offences.
- 2 Another Australian offender with a criminal history for drug trafficking was found to have obtained a false Australian Passport and was travelling through South East Asia. He was able to obtain this passport due to the false documentation he purchased from the main offender.
- 3 A third offender, with a criminal history for drug trafficking, was located in Eastern Europe, also travelling on a false Australian Passport. After the Australian Federal Police forwarded information on behalf of the CCA to local authorities, this person was arrested and charged with possession of the false passport.

The main offender was ultimately arrested in a violent scuffle in a suburban bank where a female New South Wales Police detective was stabbed in the throat and held hostage. He was charged with attempted Murder, Kidnapping and numerous fraud matters. He is currently in custody and awaiting trial.

ANNEXURE B

IDENTITY FRAUD COMMITTED UTILISING HIGH QUALITY COMPUTER EQUIPMENT

In 1997, the CCA received information from a registered informant that an associate of his was making false applications for credit cards and generating massive debts on them. The victims in these matters included American Express, Visa Card International, Mastercard and GE Capital incorporating Grace Bros credit card and David Jones credit card. Additionally, the offender was allegedly counterfeiting birth certificates and driver's licences to support his false applications.

After extensive surveillance, the offender was located in commercial premises in inner western Sydney. On execution of a search warrant, in excess of \$100,000 in packaged software and \$500,000 in high quality computer and scanning equipment was seized. All the equipment – hardware and software – was purchased on falsely obtained credit cards. He was in possession of over one hundred bank account cards and credit cards, some of which were stolen, but most obtained through fraudulent application. The computers were analysed and found to contain templates of documents of identification – birth certificates, driver's licences, sales tax exemption forms, telephone bills and electricity bills.

Further analysis of the offender's purchasing procedures found that he conducted all of his purchases over the telephone, supplying credit card details of his fraudulently obtained cards, and facsimiling requests to computer companies, including fraudulent sales tax exemption forms complete with fictitious numbers. It was apparent that the offender was minimising the cost of his fraudulent purchases by obtaining this property utilising the sales tax exempt forms.

The offender was arrested and charged in September 1996, and refused bail due to the extent of his fraud and his ability to create fictitious identities. He was granted bail in November 1996 and subsequently disappeared. Extensive surveillance again located him in a small unit in western Sydney. He was part way through compiling a similar computer set up for which he was originally arrested. He was again arrested, and eventually pleaded guilty to numerous counts of fraud, and sentenced to six years imprisonment, with a non-parole period of three years. He is due for release just before the Sydney 2000 Olympic Games.

ANNEXURE C

IDENTITY FRAUD COMMITTED UPON VARIOUS FINANCIAL INSTITUTIONS

Between 1996 and 1998, an offender was involved in a scheme which involved creating twelve (12) false identities. He was able to produce these false identities by utilising high quality computer equipment and scanners, creating fraudulent birth certificates and Northern Territory Driver's Licences. He then opened numerous bank accounts in these various names, with most of the identities having multiple accounts.

In his correct name, the offender purchased small one bedroom units in the inner Sydney city area for between \$100,000 and \$130,000. Over the ensuing three years, he sold these units amongst the various false names. On each sale, he would inflate the value of the unit, and obtain loans from the banks not exceeding 80% of the alleged value of the units. (The financial institutions would not send an officer out to inspect the units if the loan was less than 80% of the total value of the property). To support his loan applications, the offender counterfeited numerous pay slips and Australian Taxation Office Group Certificates from fictitious employers.

The offender used other false names to pose as a conveyancer for his false identity. Blank letterheads for these conveyancers were found at his home when the CCA executed a search warrant.

In most cases, the purchased units were leased and the mortgage payments would be financed from the rent and other monies fraudulently obtained for the false identity by reproducing the same fraud on other banks with other units.

At a later stage, the units would be sold to another of his false identities and on receipt of the monies on settlement, would be directed by the offender's pseudonym to be made payable to his other identities. In total, the financial institutions (of which there were three institutions but multiple branches) lost in excess of \$5 million. At least \$1 million was laundered into Greek and Cypriot bank accounts in his and his wife's names and has never been recovered.

The offender was subsequently arrested and charged in May 1998. He appeared in the Sydney District Court in January 2000, and after pleading guilty was sentenced to six years imprisonment, with a non-parole period of four years.

This matter in particular highlighted distinct flaws in the fraud controls maintained by major financial institutions. The offender effectively utilised these flaws to achieve his fraudulent goals.