(This document has been scanned from the original and may contain some errors.)

19 June 2000

Our reference: NE 4699

NATIONAL
CRIME
AUTHORITY

Ms Melissa Stutsel
Principal Research Officer
House of Representatives Standing Committee on
Economics Finance and Public Administration
Parliament House
CANBERRA ACT 2600

Dear Ms Stutsel

CASE STUDIES: IDENTITY FRAUD FACILITATING CRIMINAL ACTIVITY

As advised in our submission to the Committee the Authority is concerned about identity fraud because it underpins a great deal of organised crime, including organised tax evasion. Further to our submission, and as discussed with Ms Carter, we enclose a number of case studies, which can be referred to in a public document, to assist the Standing Committee in the preparation of its report.

As the Committee is aware, identity fraud includes the creation of false identities which can be used for, but not limited to, establishing bank accounts, falsifying the registration of businesses, and sending money overseas. It is a prevailing and recurring theme identified during National Crime Authority investigations into organised criminality including serious tax evasion, money laundering and associated drug trafficking or other predicate offences under the Swordfish, Blade (South East Asian Organised Crime), Freshnet (Established Criminal Milieu) and Panzer (Outlaw Motorcycle Gangs) Task Forces.

Some false documents and complete identities have been created in Australia, whilst others have originated overseas and used in Australia. There are numerous variations in the use of organised fraud to facilitate financial criminal activity. The creation of a convincing identity through the use of false/forged documentation has been detecting facilitating:

1. Overseas remittances

2. Asset Concealment

NATIONAL OFFICE
GPO Box 5260, Sydney NSW 2001
201 Elizabeth Street
Sydney NSW 2000
Telephone (02) 9373 2100
Facsimile (02) 9373 2599

3. Falsified business structures, proprietors

The advent of technology, e-commerce and non-physical transactions increases opportunities to facilitate criminal activity associated with the use of falsified identities and credentials due to the anonymity it affords users.

1. OVERSEAS REMITTANCES

Sending money overseas using false identification assists in the laundering of money, and tax evasion. To date millions of dollars have been detected being sent overseas with the assistance of falsified sender and receiver details, making it very difficult in some cases to recover the proceeds.

Case Study 1

Investigators identified around $4.6M in unpaid tax on a business' cash earnings. Assumed names of employees, associates, friends and in some cases maiden names and previous married names were used to move structured amounts overseas. Close to $3.7M in unpaid tax has been recovered.

Bank drafts using a false identity for amounts less than $10,000 were also purchased. The drafts were then carried offshore and deposited in accounts.

A deceased relative's identity was also used to obtain a credit card, which was used to obtain a drivers' license and to open bank accounts at three different banks. Although the false name bank accounts were not directly used to transfer money, they may have been used indirectly to establish the transferor as a current bank customer.

Case Study 2

In this case approximately $5.5M, suspected of being laundered money, was detected flowing through Australia, with some funds being moved to apparently false international companies. The NCA understands tax assessments of just under $1 M have been raised with some $200,000 recovered.

False passports and drivers licence were used by international visitors to Australia, on short-term business or student visas, to open bank accounts connected to shelf companies. One passport number was recorded as being associated with four other passports in different names. The identification and bank accounts were in turn used to open a Term Deposit.

The money paid into the Australian banks was from a number of international sources and is believed to be the result of laundering. It remained in these accounts for a short period before being moved offshore.

No tax was paid and the company directors/operators did not declare the money was income. As the fund's origins cannot be identified it is difficult to dispute the money was capital and as such it is not subject to Australian taxation. A joint Australian bank account using identification documentation of a relative who had never entered Australia was also opened. The international inquiries required to determine the authenticity of the signature contribute significantly to investigation time delays and costs.

Case Study 3

A number of different syndicates using very similar modus operandi have been detected by one of the Task Forces. In these operations a number of people have been identified exchanging International Fund Transfer Instructions (IFT1s) using a combination of false and genuine name/addresses to conduct over the counter money transfers. The high level of criminal organisation and the fact the accounts were not used repeatedly, combined with the swiftness of the money being moved in and out of the accounts, inhibited the possibility of further investigations.

In one of these operations it is estimated $4M over two years, in amounts under $10,000, was remitted overseas. The scheme was assisted by the use of false identification and a bank employee's familiarity with banking procedures. It was not possible to identify the ultimate beneficiaries of the remitted funds as they tended to be withdrawn in cash. Funds appear to have been remitted for at least four separate fund suppliers, making it difficult to identify any pattern to the remittances.

An elaborate structuring methodology supported by nine bank accounts has also been detected. Set up in false names the accounts were used to move $3.2M, suspected of being proceeds of criminal activity, to various overseas accounts over six months. The principal remitter, with the assistance of a relative, structured more than $1.46M overseas via Sydney banks using false sender details.

2. ASSET CONCEALMENT

Another way to launder money and avoid or reduce tax liability on criminal proceeds is to invest in assets and conceal the true ownership. This is often carried out by misappropriating the identities of trusted relatives, friends and associates (sometimes acting in collusion). The end result facilitates an avoidance of taxation scrutiny as the properties and businesses are not in the names of persons being investigated. ATO intervention may also be avoided because the properties may be declared as 'gifts' and cannot be confiscated under Proceeds of Crime legislation, however, they may still be subject to a taxation assessment.

Case Study 1

As a result of this investigation a tax assessment for $1.3M has been raised on undeclared income used to acquire substantial assets. It is suspected the money is the proceeds of drug sales. The principal offender is believed to have provided the money to purchase the real estate and assets and along with an associate is:

1. Laundering proceeds of criminal activity by purchasing real estate in false names and in the names of wives, de factos and relatives, placing proceeds of legal and illegal activities into a bank account operated by a trusted associate and concealing cash monies in a safety deposit box in a financial institution.

2. Evading tax by purchasing legitimate businesses but only being listed as an ‘employee' in lieu of the owner/director.

3. FALSIFIED BUSINESS STRUCTURES

The registration of business names using false identities and creating businesses or companies with false proprietors facilitates the commission of a variety of offences from tax fraud and money laundering to fraud against investors.

Case Study 1

Approximately $1.2M of investors' funds were used to fund the lavish lifestyle of the person under investigation. Business associates were used to establish accounts in their names and facilitate the transfer of the investors funds from Australia to international bank accounts. The offender was convicted of willful false promise/pretence and opening and operating false accounts - with eight years imprisonment.

Case Study 2

In this investigation a principal used the cash proceeds of drug trafficking to fund living expenses and purchase expensive assets through an associate who owned a car yard. Other laundering techniques included depositing cheques into a private company and then withdrawing cash, and operating a private company in a relative's name.

CONCLUSION

These cases give some indication of the different types of organised fraud detected during NCA operations. They provide an indication of the magnitude of organised fraud and in particular the significance of identity fraud in facilitating criminal activity. This highlights the need for stricter controls and practices in relation to proofs of identity in such areas as provision of passports and the issue of drivers' licenses. False identities are also used to avoid AUSTRAC's financial reporting regime and hinder efforts to counteract fraud and money laundering. False identities have been used to open bank and business accounts, to deal with the ATO and to move money around the world.

The emerging concern for law enforcement agencies is that this type of activity will be made much easier through the use of the Internet where identities can be disguised and multiple transactions carried, out quickly and without detection.

We trust that the Committee will find these case studies of some assistance in its deliberations.

Yours sincerely

P J Lamb
General Manager Operations

Encls