## Key points

- Emerging technologies such as smart cards, electronic cash and the Internet have been heralded as the next step in the evolution of money laundering. Australian and international law enforcement agencies have however, found little evidence that these new technologies are being used in this way.
- Legislation and law enforcement capabilities need to be developed to deal with emerging technologies that can be used to launder money.
- The techniques used to launder money in 1999–2000 were much the same as those used in previous years. There is, however, a change in how the methods are being used to avoid detection.
- Concern about the use of alternative remittance and underground banking systems is growing. Australia is an attractive 'host' country for these systems because of factors such as the multiplicity of ethnic backgrounds represented in the population, the nation's developed status, and its advanced financial sector.
- If the effectiveness of asset confiscation in Australia is to be measured, national uniform guidelines for statistical recording of asset confiscation are necessary.
- A greater awareness of the importance of following the money trail in the investigation of illicit drug activity has led to a more holistic approach to the investigation of illicit drug offences: financial investigators are now an integral part of multi-skilled teams investigating such offences.

## Introduction

Cash and illicit drugs are inextricably linked. From the time cash is generated through a 'street deal', the proceeds move through the chain—from dealer to trafficker to manufacturer and/or importer. The profit motive is part of each step in the process. But storing cash is an unsafe way of storing wealth, so at some point the cash is converted into something else, often in a bid to disguise the origin of the cash so the proceeds can be enjoyed or used to fund further illicit drug activity.

Law enforcement is becoming increasingly mindful that the proceeds of drug offences present investigators with a 'window of opportunity' to follow the money trail and so identify offenders, who may have been difficult to identify using traditional investigative techniques.

The importance of successfully investigating and prosecuting money launderers lies in the fact that not only are the proceeds identified and the criminals prevented from enjoying the benefits of their crime, but also to prevent criminals from using the funds to commit further crimes.

It is vital that, once they have been identified, the proceeds of crime be confiscated. This attacks the profit motive; it also has an important disruptive effect on the criminal environment, preventing criminals from using the proceeds to commit further crimes.

This chapter covers three important aspects of illicit drugs and money as experienced by law enforcement agencies in 1999–2000:

- Australian and international drug-related money-laundering trends, including the impact of emerging technologies;
- asset forfeiture connected with drug-related offences;
- initiatives in the financial investigation of drug-related offences.

Much of the material presented is based on questionnaire responses from all police jurisdictions, the National Crime Authority, the New South Wales Crime Commission, AUSTRAC (the Australian Transaction and Reports Analysis Centre), the Commonwealth Director of Public Prosecutions and a number of State public prosecutions offices.

## Money-laundering trends

In broad terms, 'money laundering' means knowingly dealing with the proceeds of a crime. Although there are myriad definitions, the most relevant and concise, from an Australian perspective, is that proffered in section 81(3) of the Commonwealth *Proceeds of Crime Act 1987*:

A person shall be taken to engage in money laundering if, and only if:

- the person engages, directly or indirectly, in a transaction that involves money, or other property, that is proceeds of crime; or
- the person receives, possesses, conceals, disposes of or brings into Australia any money, or other property, that is proceeds of crime and the person knows, or ought reasonably to know, that the money or other property is derived or realised, directly or indirectly, from some form of unlawful activity.

There are no reliable figures for how much illicit drug money is being laundered in Australia or globally. The amounts quoted are merely an estimate of the problem. A 1995 study estimated that $3500 million of illicit money was generated in Australia and laundered here or sent elsewhere (Walker 1995). Michel Camdessus, the former Managing Director of the International Monetary Fund, stated in 1998 that 2 to 5 per cent of global gross domestic product would probably be a consensus range for money laundering worldwide. In the 2000 report of the Financial Action Task Force on Money Laundering, most member countries stated narcotics were their single largest source of criminal proceeds.

### Emerging technologies

The electronic world's impact on the way we live and work cannot be underestimated. E-commerce—the purchase of goods and services via electronic means—will be worth A$1.6 trillion in the Asia–Pacific region by 2004 (DCITA 2000). Half of Australia's adults will be Internet users by 2001 (Gosnell 2000).

> The exponential growth of this technology, the increase in its capacity and accessibility, and the decrease in its costs have brought about revolutionary changes in commerce, communications, entertainment, and education. Along with this greater capacity, however, comes greater vulnerability. (Grabosky 2000, p.3)

This growth in the use of new technologies affects law enforcement.

One of the potential advantages of e-commerce for money laundering is the anonymity it offers. The Internet, smart cards and electronic cash, all allow a degree of anonymity and opportunities to operate outside the regulated financial sector.

Australian law enforcement agencies primarily base their anti–money laundering activities on being able to trace—using the AUSTRAC reporting system—financial transactions flowing through third-party involvement of financial institutions and other cash dealers (as defined in the Commonwealth's *Financial Transaction Reports Act 1988*).

The greatest challenge to law enforcement lies in e-commerce starting to operate outside the national banking and financial sector. If funds leave the regulated financial system, they basically disappear (Shepherd 1999).

#### *Smart cards*

Smart cards, or stored-value cards, are credit card–sized devices capable of storing digital information through microchip technology. A smart card can be used to hold electronic cash; it is generally inserted into a terminal, where it comes into contact with a read–write mechanism, allowing information to pass between the card and the terminal.

There are various kinds of smart cards. Some have detailed and complete audit trails because funds transfers are effected through recognised financial institutions. Others—such as the UK Mondex system—can have limited audit trails.

This is the problem for law enforcement. Removing the audit trail through operating outside the financial system provides anonymity for the money launderer. Transactions using this technology are as untraceable as cash transactions.

#### *Electronic cash*

Electronic cash, or e-cash, involves 'coins' that can be used to buy goods and services on the Internet. To obtain the e-cash, the system operator requires the customer to deposit funds into a personal bank account. The customer can then request a transfer from the bank account into the e-cash system, which generates and validates the coins for use on the Internet. Only one bank in Australia offers this service at present and, as noted in the *Australian Illicit Drug Report 1998–99*, total anonymity is not possible because of the reliance on the third-party financial institution.

#### *The Internet*

Internet banking has been introduced in Australia. Initially, the service was restricted to transferring funds between accounts and viewing records of past transactions. Now, however, a number of banks offer the ability to open new accounts and pay credit card and other bills. Again, the involvement of the third-party financial institution means that it is not possible to remain anonymous.

An emerging trend noted in 1999–2000 in Australia is increased use of the Internet to buy shares. Shares are bought using share brokers—even on the Internet—so the transactions remain within the regulated financial sector. But using the Internet in this way means there is no face-to-face contact between the customer and the service provider: such an environment reduces the risk that suspicious behaviour will be noticed and reported (OSCA 2000).

It is generally accepted that use of the Internet has not given rise to new methods of money laundering; the Net is, however, quicker and more diverse and it distances users from third-party involvement and regulatory oversight. The basics of money laundering remain the same whether they occur in virtual or real time: money must be placed, layered and then integrated (Lynch 1999). As UK solicitor and money-laundering expert Nigel Morris-Cotterill (1999) notes, however, money laundering sends messages, which may be messages about how to hide, move or invest money. The Internet allows for extremely rapid exchange of messages. Reputable Internet service providers keep detailed customer files, but free e-mail services allow the input of little or even false information in the creation of accounts, making tracing virtually impossible (Lynch 1999).

Transparency and detection capabilities are a concern for law enforcement because of the encryption and other security technologies available to the general population. Encryption involves manipulating messages so that unwanted persons cannot view the contents. Were it adopted by criminal syndicates, it would allow them to communicate undetected or with sufficient lead-time to frustrate investigations (Nicholl 1999).

The Internet also provides a wealth of information on topics such as tax havens and 'how to' guides to money laundering.

The Internet also offers opportunities to buy high-quality false identification. In terms of money laundering, the result of all this ID-related activity is further opportunities for criminals to create false identities for laundering funds, increasing the complexity of investigations of such offences.

Smart cards, electronic cash and the Internet have been heralded as the next step in the evolution of money laundering. From the perspective of law enforcement in Australia, however, the available evidence suggests there has been minimal reliance on these new technologies to facilitate money laundering. This is consistent with international experience. The Financial Action Task Force on Money Laundering announced in 1998 that new technology systems—albeit in a phase of steady development and even rapid expansion—were showing little innovation relative to money laundering. Since then, there appears to have been no movement on this position: for 1999–2000, the Task Force stated that no money-laundering techniques using Internet on-line banking have been identified (Financial Action Task Force on Money Laundering 2000).

On the other hand, it is argued that organised crime groups have in fact been using new technologies such as the Internet and encryption, but that law enforcement agencies are yet to identify or prosecute this activity (National Crime Authority 2000). Legislative and law enforcement capabilities need to be developed to deal with emerging technologies that could be used to launder money, using either new methods or known methods via a different means. In Australia, research work to prepare for this transition is well under way. The Heads of Commonwealth Operational Law Enforcement Agencies Action Group into Electronic Commerce has produced a number of reports, one of them assessing the technical implications of electronic commerce for law enforcement and revenue agencies. In addition, the recently formed Commissioners' Electronic Crime Steering Committee has done considerable work in evaluating Australasia's capacity to respond to future challenges in the area of electronic crime and is developing a draft Australasian Law Enforcement Electronic Crime Strategy.

The 1990s saw the globalisation of crime through manipulation of the international financial system (Pinner 1996). Combined with emerging technologies, this has created a rapidly changing criminal environment, one that calls for greater vigilance on the part of law enforcement and highlights the continuing need to identify the possible risks posed by the introduction of new technologies.

### The international situation

The Financial Action Task Force on Money Laundering, which was established at the G7 economic summit in Paris in 1989, is an intergovernmental body charged with developing and promoting policies, through international cooperation, to combat money laundering. The policies aim to prevent the proceeds of crime from being used in future criminal activity and from affecting legitimate economic activity. The Task Force has 29 member countries—including the major financial powers in Europe and North and South America—and representatives of two international organisations, the European Commission and the Gulf Co-operation Commission.

Numerous other international organisations are also involved in the fight against money laundering, among them:

- the Caribbean Financial Action Task Force;
- the Asia–Pacific Group on Money Laundering;
- the Council of Europe;
- the Commonwealth Secretariat;

- the United Nations Office for Drug Control and Crime Prevention.

The establishment of these international organisations reflects the global significance of money laundering and an awareness of the need for international cooperation. Another organisation is the Egmont Group—a consortium of financial intelligence units that was established in 1995—of which Australia, represented by AUSTRAC, is a member. The Group's purpose is to encourage the establishment of further financial intelligence units and the exchange of financial intelligence between countries.

In February 2000 the Task Force listed 25 criteria, for use in identifying rules and practices that impede international cooperation in the fight against money laundering. In June 2000 the Task Force released a list of countries that had breached any of the 25 criteria. The purpose was to encourage adherence through dialogue and through the Task Force's provision of technical assistance. The Task Force did, however, state that it would consider taking action against countries that remained uncooperative.

As noted, the Task Force found no new money-laundering methods for 1999–2000 (Financial Action Task Force on Money Laundering 2000). It did find, though, that many of the so-called unsophisticated laundering techniques—such as structuring (dividing large cash deposits into smaller amounts to avoid transaction-reporting requirements) and false-name accounts—continued to be used, even as part of more complex laundering schemes. It also noted a number of other trends:

- currency smuggling across borders, to avoid attention that might be attracted if the funds were deposited into the financial system where the crime was committed;
- structuring through the use of ATMs;
- the continuing use of professionals, in particular securities and commodities brokers, to assist in the money-laundering process;
- the continuing use of real estate as a vehicle for money laundering or a place for investing funds;
- the continuing use of insurance brokers or insurance products to assist with money laundering;
- the continuing use of gambling as a means of money laundering;
- the continuing role of legitimate remittance services in money laundering;
- the continuing role of legal entities and legal relationships (such as trusts) in money-laundering schemes.

Further, the report discussed several other aspects of money laundering: on-line banking, trade-related money laundering and alternative remittance systems.

### *Trade-related money laundering*

The Task Force noted the continuation of an international trend in goods and services being used as a cover for money laundering or as an actual money-laundering mechanism. An example was given of a merchant paying large sums of money for worthless goods. Investigations revealed that the payments were in fact narcotics proceeds and when the goods were received they were either thrown away or sold as junk. The Task Force also noted the importance of customs officials in the detection of trade-related money laundering, given their role in overseeing cross-border trade.

### *Alternative remittance systems*

The Task Force discussed the nature and impact of 'underground money/banking systems'—such as the black market peso exchange, the Indian Hawala system and Chinese and East Asian systems—noting that they play a significant role in the movement of illicit funds for particular groups. The concern for law enforcement is that transactions take place outside regulated financial systems. Further difficulties are posed by the cross-jurisdictional nature of the systems and cultural and linguistic barriers.

The Task Force was pleased by the development of the Asia–Pacific Group on Money Laundering, which in March 1999 established a working party to examine the threat of underground banking and alternative remittance systems. It commented that the use of alternative remittance systems was the most important money-laundering method in the region.

As organised crime becomes globalised and as criminal syndicates are able to exploit the expanding international financial system, Australia becomes more exposed to international money laundering. This is particularly because of Australia's close financial relationship with Asia, where money-laundering controls are less developed. In many cases the money laundered from Australia will pass through banking systems in the Asia–Pacific region (Pinner 1996).

## The Australian situation

As is the case internationally, the 'usual suspects' in the money-laundering armoury were identified in Australia during 1999–2000:

- sending money via electronic funds transfer to bank accounts overseas, particularly in Asia—the amounts sent are often under $10 000 in an attempt to avoid the reporting conditions specified in the Commonwealth's *Financial Transaction Reports Act 1988*;
- smuggling large amounts of undeclared cash offshore—methods include physically carrying the cash out of the country, mail, or sea or air cargo;

- mingling illegitimate funds with legitimate funds, then characterising the total amount as legitimate business income;
- claiming the funds originated from successful gambling;
- placing assets in associates' names or in false names;
- use of trusts and joint names;
- having assets subject to hire-purchase or mortgage arrangements, thus diverting attention (although the funds to pay off the assets in question are invariably illicit).

In relation to underground banking and alternative remittance systems, an Australian perspective was presented at the Asia–Pacific Money Laundering Methods Typologies Workshop in Japan in March 1999. Among other things, the report stated,

> Australia may constitute an attractive 'host' country for alternative remittance and underground banking systems due to such factors as its multicultural population, developed status and advanced financial sector. Its geographical location naturally means that it predominantly hosts systems servicing 'home' countries in the Asian Region. (National Crime Authority 1999, p.3)

The report defined alternative remittance systems as systems that involve a person or people arranging for funds (or value) to be sent or made available overseas on behalf of a third party who does not wish to directly use formal, regulated banking mechanisms. Such systems have strong historical roots in Asian cultures and usually operate within ethnic groupings in Australia; among the systems are the Hawala, Hundi, Fei Ch'ien, Poey Kuan, Chiti and Chop Shop banking. Although largely unregulated, the remittances can be processed through both unregulated informal networks and the regulated financial sector.

The report also raised the question of 'displacement'—in other words, because of the success of Australia's monitoring of financial transactions through the *Financial Transaction Reports Act 1988*, the use of alternative remittance services for money laundering has increased.

A National Crime Authority investigation in 1999 uncovered Vietnamese remittance services in Melbourne. The services were operating from retail shops selling clothes or fabrics and, for a fee, they arranged the transfer of money from Australia to Vietnam and vice versa. The cash was received from customers and sub-agents. Some was banked and some was kept on hand. The money was transferred to Vietnam by telegraphic transfer purchased with cash or a cheque or by telegraphic transfer via trading companies in Hong Kong and Vietnam.

Some emerging trends were identified for 1999–2000:

- stock market manipulation, or share ramping, and generally pumping the proceeds of drug sales into the securities market. The funds used for these transactions are sent offshore to a foreign country, then moved onshore again to buy Australian securities;
- use of e-commerce to buy shares and other marketable securities.

Although much of the same money-laundering techniques were used in 1999–2000 as in previous years, changes in how these techniques are being used are emerging. This includes greater use of non-nationals in the process and an increased incidence of criminal syndicates operating across State and Territory boundaries.

A National Crime Authority investigation in 1999–2000 found that a person suspected of laundering money for a narcotics syndicate was using Chinese nationals in Australia on student visas. The suspect—herself a Chinese student—used fellow students to remit funds overseas via telegraphic transfers in amounts less than $10 000.

A New South Wales Police Service investigation in 1999–2000 revealed the existence of a highly organised Malaysian syndicate using Malaysian tourists to launder stolen and altered cheques. The tourists were brought to Australia and shown how to open bank accounts in their real names. Once the accounts were opened, the ATM cards and PINs were handed to organisers within the syndicate. Stolen and altered cheques were then deposited into many of the accounts.

A good example of criminal syndicates operating across State boundaries is a recent joint investigation by the Australian Federal Police and the Australian Customs Service, which resulted in the seizure of 225 kilograms of cocaine at Coffs Harbour, New South Wales. Although the importation was predominantly organised overseas and in New South Wales, investigations revealed that money laundering for the syndicate occurred in Adelaide, South Australia. Federal agents commented that basing the money-laundering activities in a jurisdiction other than the one where the importation was occurring was a deliberate attempt to make law enforcement detection and investigation more difficult.

Information from the National Crime Authority shows the increasing incidence of importing cartels—importing cocaine in particular—using a 'Chinese wall' structure. This involves those members of the syndicate who are laundering the profits being completely segregated from those dealing with the importation and distribution of the narcotics.

## Asset confiscation

Once it has been confirmed that particular assets are the proceeds of illicit drug activity and other criminal offences, the next step is to restrain and confiscate. Asset confiscation in Australia aims at confiscating not only the proceeds of crime but also assets used in the commission of serious offences.

Criminals are involved in illicit drugs for profit, and asset confiscation attacks criminality through the profit motive. Removing unlawful assets also:

- assists in the fight against money laundering;
- inspires confidence in the criminal justice system;
- deters people from crime by reducing the anticipated returns;
- generally improves crime detection (Performance and Innovation Unit 2000).

All Australian jurisdictions have enacted legislation dealing with confiscation of the proceeds of crime.

### The effectiveness of confiscation legislation

From a national perspective, it is difficult to determine the effectiveness of confiscation legislation because there are no national reporting standards. Statistical data on asset confiscation are not uniform and differ from jurisdiction to jurisdiction. In some jurisdictions it is difficult to differentiate the confiscation information corresponding to crime types, such as illicit drug activity.

Seizure, restraint and confiscation activities are generally reported quantitatively—in terms of the number of orders and the value of property. Such data are helpful, but the assumptions that underlie the figures are often unreported or unavailable.

Confiscation legislation in Australia is the subject of review. A number of jurisdictions have reviewed and amended their legislation, but in the Commonwealth, Queensland, Tasmania, the Australian Capital Territory and the Northern Territory the legislative scheme continues substantially as originally enacted (Australian Law Reform Commission 1999).

Law enforcement agencies play an extremely important part in the review process: by making submissions and presenting case studies, they can direct legislators' attention to possible inadequacies in current legislation.

The following is an overview of amendments or proposed amendments to asset confiscation legislation during 1999–2000.

#### *Commonwealth*

The Commonwealth *Proceeds of Crime Act 1987* allows the confiscation of criminal proceeds only if the person or people who generated the proceeds have been convicted of an indictable Commonwealth criminal offence. In its 1999 report *Confiscation that Counts*, the Australian Law Reform Commission made a large number of recommendations for reform of the *Proceeds of Crime Act*, principal among them that:

- the Commonwealth introduce civil forfeiture legislation modelled on the scheme in the New South Wales *Criminal Assets Recovery Act 1990*;
- strong statutory measures be introduced to prevent the unreasonable dissipation of restrained assets for legal expenses.

The Attorney-General's Department subsequently established a working group of representatives of Commonwealth agencies to consider the Commission's recommendations and to draft proposals for their implementation.

#### *New South Wales*

The New South Wales Attorney-General is conducting a review of the New South Wales *Confiscation of Proceeds of Crime Act 1989*. Although not a legislative change, there has been a change in relation to how the Act is administered. Previously, police authority to initiate proceedings under the Act rested with the Commissioner: to improve the efficiency of the Act, this authority has now been delegated to police commanders and police prosecuting services.

#### *Western Australia*

On 24 June 2000 the *Criminal Property Confiscation Bill* was introduced into Western Australia's Legislative Assembly. Among the features of the Bill are:

- the confiscation of unexplained wealth, where the person has wealth beyond what he or she might legally have acquired;
- confiscation of all property owned, effectively controlled or given away by a declared drug trafficker;
- confiscation of the value of property used in the commission of a relevant offence where the particular property is not available for confiscation.

Further parliamentary debate of the Bill is due to take place.

### *The Northern Territory*

No legislative changes were made in 1999–2000 to the Northern Territory's *Crimes (Forfeiture of Proceeds) Act 1988*. The Act is, however, being reviewed by a working party comprising representatives of the Northern Territory Police, the Northern Territory Office of the Director of Public Prosecutions and the Northern Territory Attorney-General's Department to determine what legislative changes are required to improve its effectiveness.

## Other matters

### *Conviction- versus non–conviction based confiscation*

The debate about conviction-based confiscation and non–conviction based confiscation is currently occupying legislators in a number of Australian jurisdictions, as evidenced by the proposed amendments to Commonwealth and Western Australian legislation. Apart from legislation in New South Wales and Victoria and a narrow range of provisions in the Commonwealth's *Customs Act 1901*, all legislation dealing with confiscation of the proceeds of crime in Australia is conviction-based. This means the legislation requires that criminal activity be proved beyond reasonable doubt before assets are forfeited. With non–conviction based legislation, the trigger for forfeiture is proof to the civil standard of the balance of probabilities that the person has committed a serious offence.

The New South Wales *Criminal Assets Recovery Act 1990* introduced a non–conviction based civil forfeiture regime that is directed at people rather than assets. The legislation is administered by the New South Wales Crime Commission. A restraining order can be obtained to prevent a person from dealing with his or her property if the New South Wales Supreme Court is satisfied that there are reasonable grounds to suspect that the person has been engaged in a serious crime-related activity. Such a restraining order can also be obtained if there are reasonable grounds to suspect that the property derives from 'serious crime'. If the restraining order is to be preserved, an assets forfeiture order must be applied for within 48 hours of the making of the restraining order. The Court must make an assets forfeiture order if it finds, on the balance of probabilities, that the person whose suspected activity that forms the basis of the restraining order was, at any time in the previous six years, engaged in serious criminal activity. (For drug-related activity, this involves an indictable quantity of a prohibited drug.) Under this legislation, the onus is on the suspect to prove the property was not illegally acquired.

The legislation also allows for application before the New South Wales Supreme Court of a proceeds assessment order. This requires a person to pay an amount assessed as the value of proceeds derived from illegal activity for up to the previous six years. The amount is assessed by the Court. Again, the Court's finding is based on the balance of probabilities. In making the assessment of benefits, the Court is assisted by a rebuttable presumption that the amount of all the defendant's expenditure in the six-year period was proceeds derived from illegal activity.

In Victoria, under the *Confiscation Act 1997* civil forfeiture offences apply only to offences of drug cultivation or trafficking when the quantity of the drug involved amounts of a commercial quantity. An applicant for a civil forfeiture order must prove, on the balance of probabilities, that the defendant committed the offence. The matter may be proved irrespective of whether the defendant has been tried and, if tried, acquitted of the substantive offence in the criminal trial.

Amendments in 1979 to the Commonwealth's *Customs Act 1901* allow for civil proceedings to be initiated by seeking an order that a person pay a pecuniary penalty to the Commonwealth in respect of funds obtained from narcotics dealings. The definition of 'narcotics dealings' includes selling or dealing narcotics that were imported into Australia. If satisfied, on the balance of probabilities, that a person has engaged in the alleged activities, the court must make an assessment of the value of benefits derived by the person and order the person to pay a pecuniary penalty of the assessed value. The action can be brought irrespective of the person being convicted of an offence or even if no proceedings for an offence have been instituted. The provisions have, however, had minimal use because of the need to show that a person derived money from a specific, provable act. If narcotics are seized before they are sold, there is usually no income from the offence and therefore nothing to recover (Australian Law Reform Commission 1999).

Proponents of non-conviction based schemes argue that these schemes are more effective in depriving criminals of their ill-gotten gains. There have been numerous cases where the evidence was inadequate to secure a conviction, although the available material pointed strongly to involvement in criminal activity and consequent unjust enrichment (Australian Law Reform Commission 1999).

Proponents of non-conviction based schemes also argue that these schemes are more disruptive to criminal activity. It is argued that by being more effective in removing assets from the criminal system, they prevent criminals from enjoying the proceeds of their criminal activity and from using the assets to commit further crime. When introducing the criminal assets recovery legislation, the then Premier of New South Wales, the Hon. Nick Greiner MP, argued,

> 'It is not only the profits of a discrete transaction but the proceeds of a life of crime that will be confiscated' (Australian Law Reform Commission 1999, p.69).

### *Legal expenses*

Another area of confiscation legislation that has been the subject of some debate is the question of access to restrained assets for legal expenses. What is at issue is the use of lawfully restrained assets to fund a legal defence, resulting in the assets being completely used up.

In its submission to the Australian Law Reform Commission's 1999 review of the Commonwealth *Proceeds of Crime Act 1987*, the New South Wales Police Service argued that the release of criminally derived assets to finance a legal defence is '… abhorrent where there is clear evidence that property is the direct proceeds of crime'. In contrast, the Legal Aid and Family Service submitted, 'The presumption of innocence implies that the "tainted" assets are only "tainted" if the defendant is found guilty'.

In weighing up these contrasting viewpoints, the Australian Law Reform Commission concluded:

> The proposition that restrained assets should be able to be made available to fund a defence to the very proceedings that would, in the event of a finding against the defendant, lead to the forfeiture or possible forfeiture of that property cannot, in the view of the Commission, be sustained.

The Victorian *Confiscation Act 1997* makes provision for payment of the reasonable living and business expenses of a person whose property is restrained. It does, however, prohibit the payment of legal expenses out of restrained property. The Court may order Victoria Legal Aid to provide legal aid for the accused.

The Queensland *Crimes (Confiscation) Act 1989* and the New South Wales *Criminal Assets Recovery Act 1990* have provisions that prohibit access to property to fund a legal defence if the property was acquired as a result of the particular criminal activity or, in the case of the New South Wales legislation, acquired as a result of any illegal activity (Australian Law Reform Commission 1999).

### The Victorian approach

Proponents of national reporting standards for confiscation outputs argue that the development of such standards for confiscation outputs must be supported through the development of a centralised database, which would be used to manage the collection and dissemination of information to interested parties, both nationally and internationally. It is argued that such an exchange of information would increase the effectiveness of confiscation activity in Australia.

A logical extension of consistent reporting standards is uniformity of Commonwealth and State and Territory legislation. In its 1999 review of the Commonwealth *Proceeds of Crime Act 1987*, the Australian Law Reform Commission listed a number of advantages offered by uniform legislation, among them:

- advantages to investigators and prosecutors, particularly in dealing with multi-jurisdiction organised crime;
- greater capacity to establish joint investigation teams;
- minimising costs;
- more effective use of court time;
- more effective protection of the rights of innocent parties;
- greater capacity for private enterprise to develop compliance programs;
- minimising the financial costs of compliance.

Uniform legislation would also eliminate the problems associated with differing reporting standards. But, although in theory the benefits are clear, in practical terms a highly committed, coordinated national political response would be necessary if uniform legislation were to be implemented.

Victoria has already adopted a more strategic approach by establishing the Asset Confiscation Office, which became operational on 1 January 1998 as a business unit forming part of the Enforcement Management Division of the Department of Justice.

A 1994 review of the Victorian confiscation program had found, among other things, a lack of coordination in confiscation activities across investigation, prosecution and enforcement. Part of the Asset Confiscation Office's task is to promote a 'whole of government' approach to confiscation schemes established by Victorian legislation, through coordination between law enforcement, the Victorian Office of Public Prosecutions and the Victorian Government.

## Initiatives in the financial investigation of illicit drug offences

Law enforcement agencies are becoming increasingly aware that financial investigation can prove to be the drug offenders' 'Achilles heel'. Often it is connections made through financial transactions that lead to the location of assets that establish the identity of offenders involved in illicit drug activity. The assets can be in the form of proceeds of the crimes committed or funds being used to commit further crimes.

In investigating the funding of illicit drug activity, law enforcement agencies are taking a proactive approach to preventing illicit drugs from reaching the streets of Australia. Such an approach is not a new idea: in 1984 the report of the Royal Commission on the Activities of the Federated Ship Painters and Dockers Union noted:

> 'It should be clear from the contents of this section of my Report that, to assist the containment of illegal drug trafficking in Australia, I favour an approach which hits hard at the financial structures built up by the drug traffickers' (Costigan 1984, p. 159).

Money laundering has moved on from the simple depositing of cash in financial institutions. There are two main reasons for this: first, there has been a shift from the traditional banking system to non-bank financial institutions and other avenues such as bullion dealers; second, the layering of transactions and the integration of funds back into the legitimate economy are becoming ever more sophisticated. The consequence for law enforcement is that greater effort is required to investigate the complex flow of funds associated with illicit drug activity (Pinner 1996).

Money laundering is now a global operation, so investigations involve a great deal of asset tracing overseas. Mutual assistance requests are becoming increasingly important. Added to this is the difficulty of conducting inquiries overseas when the investigation is still at the covert stage: this often creates practical difficulties in terms of maintaining the secrecy and security of investigations (Jolliffe 1999).

In relation to taking the next step and confiscating the proceeds of crime, an asset removal program will work only if it is accompanied by greater law enforcement capacity to follow complicated money trails (Performance and Innovation Unit 2000).

New technologies add a further dimension of complexity to investigators' efforts. A technology environment scan conducted by the Australasian Centre for Policing Research identified a number of challenges law enforcement faces when investigating offences involving computer technology:

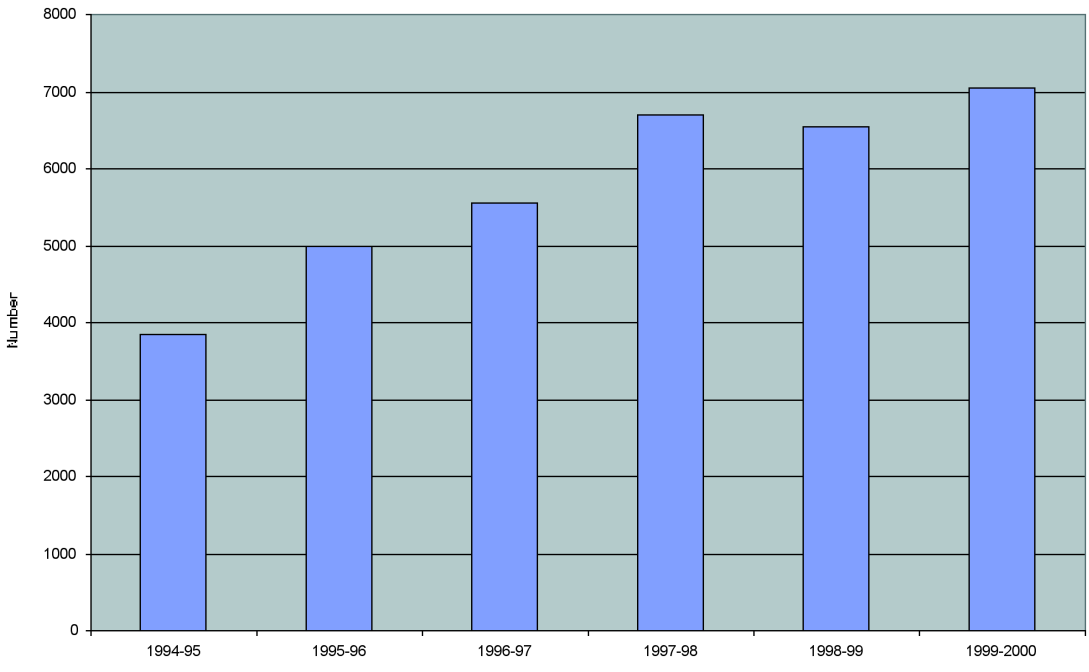
- bridging multi-jurisdictional boundaries;
- retaining and preserving evidence;
- proving identity;
- knowing where to look for evidence;
- responding to crime in 'real time';
- coordinating investigative activities (Rees 2000).

### The Police Commissioners' electronic crime project

In response to these difficulties, Australasian Police Commissioners are developing a law enforcement strategy to deal with electronic crime. During the March 2000 Australasia and the South-West Pacific Region Police Commissioners Conference, the Commissioners expressed concern about the threat posed by electronic crime and stressed the need to develop a strategy to enable prompt, effective policing responses to future challenges.

The Electronic Crime Steering Committee was established to help law enforcement agencies ensure the integrity of government and business processes and community safety and security. It has direct responsibility for this critical and urgent matter and is made up of Commissioners Palmer

**Figure 9.1: Suspect transaction reports, 1994–95 to 1999–2000**




**Source: AUSTRAC.**

## Case studies

The following examples provided by AUSTRAC demonstrate the way in which financial information generated by the organisation's systems assisted in illicit drug investigations in 1999–2000.

*Case 1*

Case 1 involved an investigation of a multi-kilogram heroin importation into Australia. The drug was secreted in commercial goods. One person pleaded guilty to possession of the heroin and was sentenced to more than 10 years' imprisonment. Another person was convicted of attempting to possess heroin and sentenced to a similar period. AUSTRAC's assistance was post-operational and began during the second phase of the investigation. Searches of the AUSTRAC database revealed large cash deposits reported through significant cash transaction reports and subsequent telegraphic transfers of funds overseas. Assessments of whether the funds were the proceeds of crime were conducted and the assets of one of the targets were subsequently forfeited.

*Case 2*

Case 2 was initiated by AUSTRAC's automated monitoring systems and brought to the attention of an Australian law enforcement agency. Searches of the AUSTRAC database revealed a number of reports showing cash transactions in Australia and funds being sent overseas. The targets were suspected of being involved in drug trafficking. The AUSTRAC alert facility was then used and all the transactions of the targets were monitored. During the ensuing year a consistent pattern emerged, revealing a series of significant cash transactions and international funds transfers. As the investigation progressed the alert facility continued to generate reports. This information was used to obtain warrants that resulted in a raid and the seizure of amphetamines and cash and a number of arrests. In total, more than 20 charges were laid for offences including drug smuggling, money laundering, and possessing money suspected of being the proceeds of drug deals. The principal in this operation was convicted and received a lengthy prison sentence.

*Case 3*

Case 3 involved suspected narcotic trafficking. The operation was carefully planned—on the basis of detailed analysis of the crime patterns of the individuals concerned—and numerous law enforcement officers conducted simultaneous searches of several houses. More than 20 people were arrested and over 55 charges were laid. Gold, drugs and cash were seized during the house searches. One person was arrested after a search revealed a quantity of heroin following a controlled delivery. The syndicate was alleged to have distributed a large amount of heroin. Subsequently, more than 20 other people were arrested and charged with more than 155 drug-related offences. An amphetamine laboratory was also found and closed down. Property, believed to be acquired with the proceeds of drug-related activity, was also seized. AUSTRAC searches revealed a large amount of financial information. Analysis of this and other information assisted in uncovering the movement of funds and the personal details of a network of targets and their associates.

(Australian Federal Police), Hyde (South Australia) Matthews (Western Australia) and Robinson (New Zealand). The project's charter is as follows:

- to carry out an assessment of current and future, local and global electronic crime environments;
- to evaluate Australasia's capacity to respond to future challenges in the area of electronic crime;
- to initiate action to deal with immediate problems;
- to develop a draft Australasian Law Enforcement Electronic Crime Strategy.

In defining 'electronic crime', the Steering Committee included the concept of electronic money laundering. Although the strategy has not yet been finalised, a number of the principles that have been identified will assist in the effective investigation of e-crime offences:

- developing the capacity within policing to respond effectively and promptly to incidents of electronic crime;
- strategic sharing of scarce resources within policing;
- prompt exchange of tactical and strategic intelligence and information between law enforcement agencies and the wider community.

As new technology accelerates the rate at which crime can be committed, the exchange of intelligence on e-crime needs to become more and more efficient and effective.

### AUSTRAC

AUSTRAC—the Australian Transaction and Reports Analysis Centre—seeks to make a valued contribution towards creating a financial environment that is hostile to money laundering, major crime and tax evasion.

The *Financial Transaction Reports Act* came into effect in 1988 as part of Australia's anti–money laundering program and requires 'cash dealers' to report:

- suspicious transactions (as defined in the Act);
- significant cash transactions of $10 000 or more (or the foreign currency equivalent);
- all international funds-transfer instructions.

AUSTRAC collects, retains, compiles, analyses and disseminates to law enforcement agencies financial intelligence relating to money laundering. Having access to this information gives the agencies an invaluable analytical tool for investigating the financial aspects of illicit drug offences.

There were 7051 suspect transaction reports in 1999–2000. Figure 9.1 shows the number of suspect transaction reports for the period 1994–95 to 1999–2000.

In recent years AUSTRAC has implemented a number of initiatives that have increased law enforcement agencies' capacity to investigate illicit drug syndicates using financial intelligence. The more recent initiatives have been funded under the Prime Minister's National Illicit Drug Strategy. In 1998 AUSTRAC was allocated funds to develop a drug-specific money-laundering detection system designed to expand the organisation's capacity to identify suspicious patterns of financial activity. The TargIT system has been successfully implemented; it has identified financial activity related to some of the larger drug seizures in the past two years.

Up-to-date lists of financial transaction reports relevant to the monitored entities and their associates can be generated immediately and disseminated to relevant law enforcement officers on request. This feature has been available for only a short time but is proving effective. Coordination of investigative opportunities among law enforcement agencies may also occur as a result.

A further allocation of funds under the National Illicit Drug Strategy in 1999 has enabled AUSTRAC to recruit extra support staff, who have been placed in the offices of partner agencies in Brisbane, Sydney and Melbourne. The support staff are primarily responsible for providing training, helping partner agencies with operations and intelligence probes, and generally raising awareness of the benefits of using financial intelligence. Transaction Reports Analysis and Query (TRAQ) system has been well received by all the agencies that have been assisted in this way and, as a result, AUSTRAC has seen a dramatic increase in use of the system. Perhaps more importantly, on-line users in the various agencies have honed their investigative skills.

TRAQ offers a wide variety of functions for law enforcement agencies. In varying degrees, users can obtain information reported to AUSTRAC as significant cash transactions, international currency transfers, international funds transfer instructions and suspect transactions.

### The Profits of Crime Case Studies Desk

August 1999 saw the launch of the Profits of Crime Case Studies Desk, which uses Intranet technology provided through the ABCI's Australian Law Enforcement Intelligence Net—ALEIN—to share between Australian law enforcement agencies, information on money-laundering and tax-evasion methods and investigative techniques. The National Crime Authority developed this initiative and agreed to take responsibility for its management, in anticipation of the benefits that would flow from pooling law enforcement knowledge in these areas.

The information provided by the Desk is operationally focused. Its main element is a dynamic store of case studies—contributed by law enforcement agencies—of completed and continuing investigations, allegations and intelligence probes. Importantly, the case studies offer detailed descriptions of known or suspected methods used by the targets in a particular matter to deal with the suspected proceeds of crime and/or to evade tax or other revenue collection. It provides a focus for officers wanting to learn from each other's experience of issues such as financial investigation.

### The Swordfish Task Force

The Swordfish Task Force attacks the financial profits of serious and organised criminal activity such as drug trafficking through a coordinated, multi-agency approach. The National Crime Authority, the Australian Taxation Office, the Australian Federal Police, State police services, AUSTRAC, the Australian Customs Service and other law enforcement agencies work cooperatively to investigate offences, disrupt criminal activity and confiscate the proceeds of crime.

### Other initiatives

There have been a number of other initiatives in the financial investigation of illicit drug offences.

Training in asset confiscation legislation and procedures has been provided to Victoria Police officers involved in general policing and has been incorporated in the training of supervisors, field investigators and detectives. Victoria Police also plan to introduce a practice of seconding members from general policing to the Asset Recovery Squad for three months at a time.

A cornerstone of the National Illicit Drug Strategy was the formation of intelligence-driven strike teams of Australian Federal Police investigators, analysts and support staff. As a result of this initiative, since 1999 the Australian Federal Police has recruited six specialist financial analysts, who are deployed throughout the country and are attached to mobile strike teams as an integral part of the teams' investigative work.

New South Wales Police Service Crime Agencies have increased their use of analysts 'in the field'; which they consider improves their ability to gather financial information in the investigation of illicit drug offences. The Service has also amended its *Police Service Handbook* in relation to the forfeiture of criminal assets. The amendment effectively requires police investigating all serious criminal activity—which includes drug offences—to consider the potential for confiscating the assets an offender has acquired by using money derived from crime as well as items used to commit the crime. The amendment also places responsibility on the Asset Confiscation Unit at Crime Agencies to review reported investigations and arrests and refer appropriate cases to the New South Wales Crime Commission, the Director of Public Prosecutions, or police court and legal services for the purpose of initiating confiscation proceedings.

These initiatives reflect a more holistic approach to the investigation of illicit drug offences. In the past, the financial aspect of an investigation was often separate from the main investigation: now financial investigators are an integral part of multi-skilled teams investigating such offences.

## References


Australian Law Reform Commission 1999, *Confiscation that Counts: a review of the Proceeds of Crime Act 1987*, Report no. 87, ALRC, Sydney.

Costigan, QC 1984, *Royal Commission on the Activities of the Federated Ship Painters and Dockers Union: final report*, vol. 5, Australian Government Public Service, Canberra.

DCITA (Department of Communications, Information Technology and the Arts) 2000, *Government Online: the Commonwealth Government's strategy*, DCITA, Canberra.

Financial Action Task Force on Money Laundering 2000, 'Report on Money Laundering Typologies 1999–2000', Financial Action Task Force on Money Laundering, Paris.

Gosnell, P 2000, 'Chamber's ecommerce bid', *Melbourne Sun*, 3 May, p. 52.

Grabosky, P 2000, *Computer Crime: a criminological overview*, Australian Institute of Criminology, Canberra.

Jolliffe, J 1999, *Money Laundering Prosecutions in Australia*, publisher, Sydney.

Lynch, L 1999, 'Welcome to the Cyber Laundry', *Platypus Magazine*, October.

Morris-Cotterill, N 1999, 'Use and Abuse of the Internet in Fraud and Money Laundering', Paper presented at conference 'Cyberspace: crime, criminal justice and the Internet', College of Ripon and York St John, York, England, 29–30 March.

National Crime Authority 1999, 'Underground Banking and Alternative Remittance Systems', *Australia Jurisdiction Report*, Report presented at the second Asia–Pacific Money Laundering Methods Typologies Workshop, Tokyo, 2–3 March.

National Crime Authority 2000, *The NCA and Cybercrime*, Scoping paper, National Crime Authority, Sydney, June.

Nicholl, J 1999, *Encryption—issues for law enforcement*, National Crime Authority, Sydney.

OSCA 2000, *The Criminal Exploitation of Identity*, Publication no. 2/00, Office of Strategic Crime Assessments, Canberra.

Pinner, G 1996, *Money Laundering: the state of play*, AUSTRAC, Sydney.

Performance and Innovation Unit 2000, *Recovering the Proceeds of Crime: a Performance and Innovation Unit report*, Cabinet Office, London.

Sandhu, H 2000, 'The Global Detection and Deterrence of Money Laundering', *Journal of Money Laundering Control*, vol. l3, no. 4.

Shepherd, D 1999, *E-commerce and the Impact upon Policing*, NSW Police Service Commercial Crime Agency, Sydney.

Walker, J 1995, *Estimates of the Extent of Money Laundering in and through Australia*, AUSTRAC, Sydney.