Economic crime investigations can't be done in isolation

John Lawler, the AFP's General Manager for Eastern Operations, presented the opening speech of the Insurance and Corporate Fraud Conference, held in Sydney in early October. Hosted by 'The Investigator' magazine, participants came from the government and private sector.

In his address to the conference Mr Lawler related the role of the Commonwealth of Australia in the fight against economic crime, as undertaken by Australian Federal Police. He examined new strategies being employed by the AFP to counter the challenges imposed on law enforcement by the "pervasive and emerging illicit activity that is economic crime".

Mr Lawler addressed key fraud investigation areas, including partnerships, better intelligence management tools and strategies, the use of evidence in the context of technology and recent legislative change.

John Lawler
General Manager
Eastern Operations

The value of establishing strong partnerships in the investigation of economic crime cannot be understated and it is well recognised that as fraud investigators, we operate in an environment where it is not possible for the AFP, law enforcement or any organisation to pursue investigations in isolation.

The increasing complexity of criminal activity together with the level of expertise required to investigate such matters will require the pooling of resources to achieve an effective outcome.

The AFP continues to embrace opportunities to develop collaborative links

A recent example of an effective partnership involved the investigation of copyright offences in the software industry by the Trade Mark Investigation Service (TMIS) and Microsoft.

TMIS

Trade Mark Investigation Services (TMIS) is a Brisbane- based firm of corporate enquiry agents specialising in investigations throughout Australasia and the Pacific Rim.
Ken Taylor, a former Australian Federal Police officer and a member of the Royal Hong Kong Police Force (1976 – 1989) founded the company in 1991 quickly finding a niche in Australia where his investigation skills and knowledge of Asian Culture and language could be used.

with its domestic and international law enforcement partners, as well as a range of academic and industry bodies. The AFP's international relationships are predominantly engaged through our Overseas Liaison Network, through which it has 34 representatives in 22 countries. In addition, the effective functioning of the Law Enforcement Cooperation Program has enabled valuable opportunities for networking and confidence building, including the implementation of law enforcement personnel exchanges with a large number of Australia's near neighbours.

In the AFP we have witnessed the national focus shift from talking to 'our clients' to talking with 'our customers'. We have established dedicated teams charged with ensuring that we are more responsive to our customers and are seeking innovative solutions to resourcing issues.

One such initiative is the out-posting of federal agents to key customers, particularly those agencies involved in major fraud investigations, on either a full cost recovery basis or a secondment arrangement. These placements have proved to be enormously successful in building capacity and leveraging respective expertise.

Efforts have been made via information seminars to engage both the public and the private sector in identifying the capacity of the AFP in respect to the investigation and prevention of economic crime. Importantly, the seminars provide an effective means of gathering together private investigational bodies with government agencies enabling any resourcing gaps to be met.

A recent example of an effective partnership involved the investigation of copyright offences in the software industry by the Trade Mark Investigation Service (TMIS) and Microsoft.

The AFP has much to offer in these types of investigations, including a specific and powerful knowledge of the Commonwealth Crimes Act. However, computer companies such as Microsoft are able to offer much in terms of expertise, equipment and meeting the costs in what can be an extensive and time consuming investigation.

The cooperative arrangements in this case resulted in benefits for the AFP and its customers; the AFP was able to increase its knowledge in relation to commercial expertise and computer forensics while TMIS and Microsoft, learnt much about police procedure, especially in relation to continuity of evidence.

Of course in these types of cases there will always be potential for conflict regarding the needs of the police and the needs of the customers, however, the parallel civil and criminal proceedings in this case demonstrates as to how those interests may be pursued in harmony.

Crime management strategies

The AFP has moved into a business-planning environment with a focus on outcomes and outputs. One of our key performance measures is 'how well did we disrupt the criminal environment'.

A component of the new AFP Business Planning Framework is the Crime Management Strategies. Crime management involves identifying and prioritising high impact problems confronting the jurisdiction and dealing with them in a holistic manner. Crime management recognises that criminal groups can be involved in a range of offences involving various illicit commodities and illegal activities.

Crime Management Strategies are used to support the AFP's business planning cycle and are a means of integrating intelligence, operational activity and policy development under each crime type. There are seven broad

Crime Management Strategies that are aligned with the 26 crime types in the range of work undertaken by the AFP. The strategies are designed to provide a funnel for collecting information and intelligence. Economic Crime is one of those strategies.

Each Crime Management Strategy has enabling functions that determine the organisations needs in particular areas, including Science and Technology and International activity.

The Economic Crime-Crime Management Strategy focuses on information collection and intelligence gathering and analysis. This means ensuring that the AFP has a good understanding of the economic crime environment and then places itself and its customers in a strategic position to deal with the issues. Some of the enabling functions include the more focused use of strategic partnerships with other agencies and better-managed use of client services and out-posted officers.

Intelligence gathering

Intelligence gathering is particularly important given the internationalisation of economic crime, the explosion in the use of technology, including the Internet and the growing impact and sophistication of organised crime in this area of criminality.

Traditionally, economic crime has been dealt with in an insular manner, with each fraud investigated and prosecuted on its own, with little attention given to its relevance and importance in the wider context. As the environment is changing however, there is a recognition that intelligence is becoming more important as a proactive tool in reducing the economic crime problem.

The AFP's Fraud Control Policy and Guidelines of the Commonwealth, now in final draft, places a significant emphasis on intelligence and has shifted the responsibility for the management of internal fraud to respective CEOs of Commonwealth agencies. There is also provision for a Fraud Trend Information Network where members of Commonwealth departments will be required to meet on a regular basis and discuss fraud trends and emerging threats.

The National Fraud Desk (on the ABCI Alien System) is used by law enforcement to provide non-specific details on relevant fraud committed within each jurisdiction, to advise of fraud alerts and to ensure that they remain appraised of national fraud trends.

Two areas that require a specific Intelligence focus are counterfeit credit cards and identity fraud.

Counterfeit credit cards

Counterfeit credit cards have become an international problem. Over the past five years their prevalence has increased and the widespread use of the cards has created significant fraud problems. On September 9, 1999, the *Customs (Prohibited Imports) Regulation (1956)* and *Customs (Prohibited Exports) Regulation (1958)* were amended to prohibit the importation or exportation of counterfeit credit, debit and charge cards. The AFP now has responsibility for investigating the importation of these cards. Trends have also been identified that relate to the importation of credit card embossing machines.

Investigations have revealed that there are a number of international groups that have targeted Australia in counterfeit credit card fraud. Intelligence is being used in the fight against credit card fraud through the use of an international computer database under the coordination of Interpol. This database allows for the linking of independent investigations by means of technical examination of the credit/payment cards.

Counterfeit credit cards have become an international problem. Over the past five years their prevalence has increased and the widespread use of the cards has created significant fraud problems.

Forensic personnel attached to both credit card companies and to law enforcement agencies may conduct this technical examination. Information gathered by investigational personnel, such as the issuer details, card name and programs, can also be added to the system. The computer-based system is fully searchable for both forensic characteristics and non-forensic (intelligence) information, such as the card name, card program, and issuer, allowing for maximum usage of the database information. The database can provide a valuable international link in intelligence in credit card fraud.

In most cases, acquiring the false identity in itself does not constitute a criminal offence and there are several websites that provide 'novelty' ID cards on line.

Identity fraud

Identity fraud is commonplace in Australia and most parts of the world. We have witnessed it expand beyond the stereotype fraud to include the full range of criminal activity. False identities are a fundamental tool of organised criminal groups, be they involved in terrorism, people smuggling or narcotic importations.

False identities can be obtained in a number of ways by 'manufacturing' an entirely new identity. Another mechanism is to assume real identities, which are 'stolen' from individuals who may be living or deceased. Another term now frequently used is "identity theft" to describe this group.

Enough identity documents to provide a person with the 100 points required by many financial institutions can be produced in the home using office equipment or even at the local library using equipment freely available and seldom traceable. Surprisingly, in most cases, acquiring the false identity in itself does not constitute a criminal offence and it is generally a preliminary step to perpetrating or concealing a crime.

No-one appears to be immune from identify and credit card fraud. A case in point being that last year, golfing celebrity Tiger Woods had his identity stolen by Anthony Taylor of Sacramento. Taylor obtained loans and purchased goods to the amount of $17,000 on Woods' credit card.

Of ongoing concern is intelligence coming to light that government instrumentalities that deal with identity documents are being targeted by organised criminal groups. The corrupt internal activities of persons targeted by these groups often leads to the production of multiple, high-quality, backstopped, fraudulent identities.

Evidence and technology

The future direction in e-commerce will produce changes to evidence in its type and gathering. Evidence in fraud and e-commerce in the past typically has been paper based. Today many frauds are committed via computer and over the Internet without leaving any traditional evidence of wrongdoing as we know it. This creates a whole new set of challenges for those in our industry.

By way of example; a 29-year-old contract accountant at the Department of Administrative Services misappropriated $8.725 million from the department's account. He first transferred $6 million from the department's trust account into another company trust account and the later transferred a further $2.275 million to a related company.

The second transaction was discovered during an audit later in the year, however, the $6 million transaction was not discovered until one month later. It was only after the offender had been dismissed by DOFA for spending too much time being a manager of a Western Australian Mining Company, that DOFA made the discovery of the missing millions. Had he been able to reconcile the books himself he may well have gone undetected.

From an investigational perspective, the fraudster traditionally leaves a trail of documentary evidence. Fraudulent acts may be proven by forensic methods such as handwriting or fingerprint analysis. Likewise, inferences may be drawn from possession of relevant documents and assumptions of false identities may be proven by the location of original documents and forensic proof of

modification. Finally, electronic payments may be proven through the systematic and methodical process of bank account reconstruction. Thus, the presence of physical evidence continues to stand as an invaluable tool to any fraud investigator.

The Commonwealth Government has a commitment to Government-online, which is an initiative to make all services provided by the Government available on the internet, including where appropriate the application for benefits and payments of services. Such a system will call for a change in the way the AFP investigates crime against the Commonwealth Government. The potential for fraud is significant given, for example, that Centrelink alone has 400 Customer Service Offices around the country making payments of approximately $50 billion per year on behalf of government agencies.

The move for the AFP will be towards developing a detailed knowledge of relevant government systems, developing intelligence in relation to new payment options and the training and education of investigators in departmental computer and fraud detection systems. This training will be an essential and vital component of any successful strategy to combat emerging economic crime. The Crime Management strategy referred to earlier addressed this issue under professional competencies.

Additionally, in the absence of complete paper trails, the internal audit reports and computer product represent an integral component of any fraud investigation.

Emerging technologies have the opportunity to frustrate and or enhance our investigational capacities. The AFP is investing heavily in its business, through capital expenditure on science and technology. We have a highly regarded forensic capability that is recognised worldwide, supported by a high level executive focus in this area. As a result three key groups, the Science and Technology Advisory Group, the Information Technology Advisory Group and the Science and Technology Steering Committee, drive our progress in this area.

Among the work being conducted that is directly related to Economic Crime is:

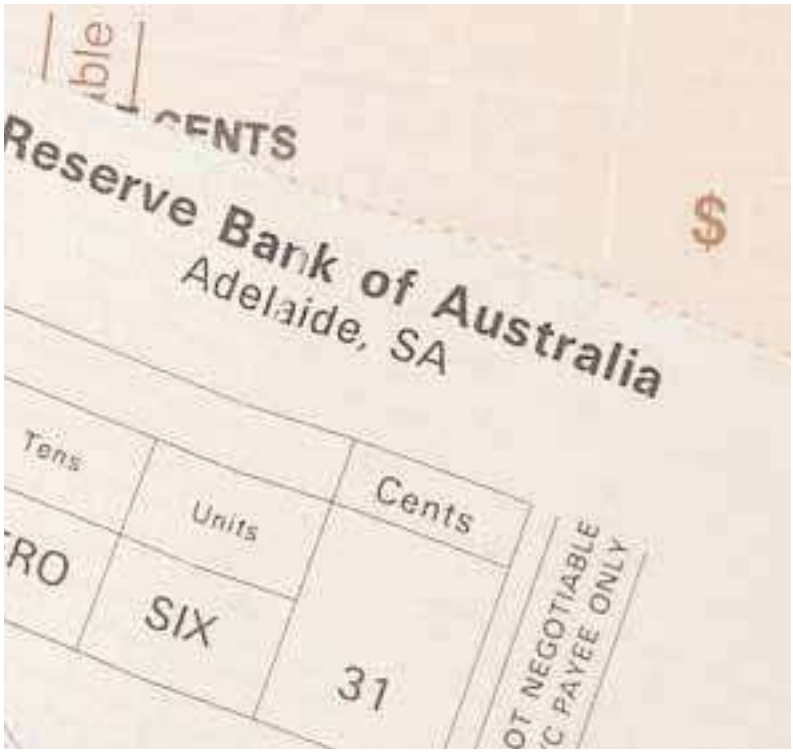
- Digital technology and image storage, transmission and evidence;
- DNA and particularly miniaturisation and the use of DNA in the field. Including DNA imbedding;
- Enhanced fingerprint detection on polymer banknotes;
- Biometric recognition; and
- Microdot technology; to name a few of the key areas.

Legislation

There are four areas of recent legislative change that will have an impact on economic crime investigations, some particularly here in NSW.

1. *Criminal Procedure Amendment (Pre-Trial Disclosure) Act 2001 (NSW)*

Soon to commence operation in NSW, the *Criminal Procedure Amendment (Pre-Trial Disclosure) Act 2001* will, for the first time, impose statutory disclosure obligations on the prosecution in complex criminal trials, with a concomitant disclosure duty placed on investigational authorities. One major practical impact will be the need to adopt far more sophisticated practices for the management of material generated and gathered in the course of an investigation. The impending obligations place a significant burden on fraud investigators in particular, given the increasing complexity and voluminous quantity of material involved in the majority of fraud briefs of evidence.



The AFP's Fraud Control Policy and Guidelines of the Commonwealth, now in final draft, places a significant emphasis on intelligence and has shifted the responsibility for the management of internal fraud to respective CEOs of Commonwealth agencies.

2. *Criminal Code (Commonwealth)*

The creation of the Criminal Code is the result of legislative reform to unify Commonwealth offences and the applicable common law principles of criminal responsibility. While the *Criminal Code Act 1995* received Royal Assent on March 15, 1995, it was not until May 24 of this year that the Code's theft, fraud and corruption offences came into effect, replacing what was recognised as the outdated and complex offences under our Crimes Act.

An enhancement of the investigative powers of search, seizure and the copying of electronically stored data will also be welcomed by investigators often hindered by the sometimes uncertain application of powers more readily applied to traditional evidence gathering processes.

Longstanding offences such as 'defraud', 'imposition' and 'false pretences' have been replaced by the simplified Code offences including 'obtaining a financial advantage by deception', 'obtaining property by deception' and 'general dishonesty'.

The principles of criminal responsibility are also codified under the legislation, which has rendered the relevant law more accessible and certain. The Code provides, for example, principles in relation to elements of an offence, the relevant defences, attempt and conspiracy, burdens of proof and the creation of corporate criminal responsibility. While the principles already apply to the theft, fraud and corruption Code offences, all Commonwealth offences will be affected from 15 December of this year.

3. *Measures to Combat Serious and Organised Crimes Amendment Act 2001 (Cth)*

In October of this year, two new important tools for Commonwealth law enforcement took effect under the *Measures to Combat Serious and Organised Crimes Act 2001*.

The first is the expansion, under strict oversight and scrutiny, of the controlled operations provisions pursuant to amendments to our Crimes Act. Previously limited to narcotics investigations, controlled operations may now be employed to investigate a wide range of Commonwealth offences including people smuggling, child pornography, money laundering and serious fraud. It is foreseen that identify fraud in particular will lend itself to the use of controlled operations.

The legislative amendments recognise that criminal activity may sometimes require law enforcement officers to carry out their duties without their true identities being known. The new provisions allow for the formalisation of assumed identities, allowing for a greater capacity to utilise undercover operatives, particularly targeting organised criminal entities.

4. *Cybercrime Bill 2001 (Cth)*

Our industry is all too familiar with the considerable difficulties that arise in the fight against cybercrime. *The Cybercrime Bill 2001* seeks to remedy identified deficiencies in the legislation relied upon to pursue computer related crime. The Bill proposes to replace the Commonwealth Crimes Act computer offences with offences under the Criminal Code and seeks to apply the Code's extended jurisdiction provisions to the new computer offences, given the borderless reality of the cyber world.

An enhancement of the investigative powers of search, seizure and the copying of electronically stored data will also be welcomed by investigators often hindered by the sometimes uncertain application of powers more readily applied to traditional evidence gathering processes.

The legislative changes outlined above are an indication that the Commonwealth and the State government continue to place criminal law reform, including fraud related crime, high on the parliamentary agenda. They reflect a general recognition that our legislative measures must undergo consistent scrutiny to ensure that investigators like ourselves are assisted in our fight to detect, investigate and prosecute those involved in the perpetration of crime to protect both our customers and the Australian public at large.