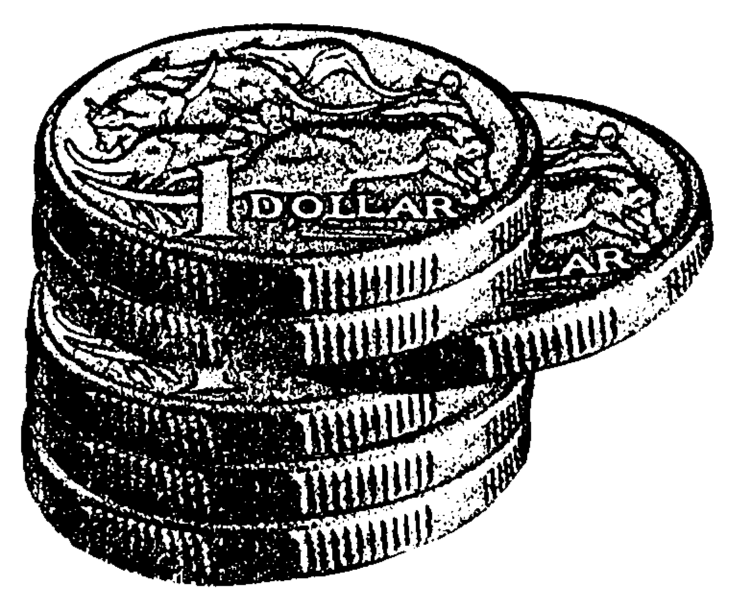
Canberra Bulletin of
Public Administration

Australian
Institute of
Criminology

FRAUD
IN THE
PUBLIC SECTOR

Editors

J R NETHERCOTE • D CHALLINGER
H F McKENNA



No 56
September 1988
ISSN 0811-6318

Australia Post Publication No NBG 1426

RRP $24.95

AIC Seminar
Proceedings No 24
ISSN 0813-7005

"No nation was ruined by trade."

Benjamin Franklin (1706-1790).
American Statesman and Inventor
American Ambassador to France and signatory of Declaration of Independence

That advice is as true for Australia today as it was for a young United States of America.

Which is why Westpac – Australia's world bank – is committed to deliver Australian business effective and competitive international trade finance.

Westpac gives you the best of both worlds.

As Australia's most experienced national bank, it understands your business. As Australia's most experienced international bank, it understands the rest of the world.

This know-how translates into innovative financing alternatives and techniques that can work for you wherever you want to do business.

With a growing global network of offices, Westpac is a significant international force in the expanding trade arenas of the Western Pacific and USA, as well as the traditional markets of the UK and Europe.

Westpac delivers what it promises – the world.

Westpac
Australia's world bank.

Westpac Banking Corporation

C0006/HI2

FRAUD

in the

PUBLIC SECTOR

Papers from the

1988 AUTUMN SEMINAR

Ethics, Fraud & Public Administration

University House, The Australian National University
2 May 1988

and

AUSTRALIAN INSTITUTE OF CRIMINOLOGY SEMINAR

Fraud on Government

Surfers Paradise, Queensland, 18-20 July 1988

The resources to advise Australia

Our skills can help you achieve results.

Peat Marwick Hungerfords is now able to provide even greater resources to assist public sector managers. Our management consulting practice puts over 150 skilled and experienced consultants at your service. In addition we have constant access to the world-wide resources of KPMG.

We are able to provide consultants to assist you on a wide variety of tasks. Our consultants have particular expertise in working with senior managers in Commonwealth, State and local governments.

Corporate and Program Management

Peat Marwick Hungerfords' consultants have assisted many government agencies in the areas of corporate and strategic planning, development of program structures and performance indicators, program evaluation and management reviews.

Organisation Design

We offer particular experience in assisting public sector managers to design outcome and results oriented organisation structures.

Information Systems

Our large information systems consulting group can assist you in most areas, including: information technology strategic planning, risk analysis and contingency planning, systems analysis, design and implementation, ADP audit, equipment and system selection, and corporate communications strategies.

Economics

Our skilled economics consultants specialise in the areas of health and community services, industry and marketing, and regional development economics and strategies.

Financial Management

Our specialist skills are available to advise you on: design and implementation of accounting systems, financial analysis, fee and rate setting studies, cost analysis and cost reduction studies, and internal audit services.

For further information about our services, please call Bill Roberts in our Canberra office on (062) 48 8777.

Management Consultants

Peat Marwick House, 64 Northbourne Avenue
Canberra, ACT 2601

Contents

	Introduction	**9**

SETTING THE SCENE

Michael Tate	Defining Fraud and Examining it as an Issue Which Governments Need to Address	**11**
	From the Newspapers	**16**
Dennis Challinger	Fraud on Government A Criminological Overview	**18**
Alan Rose	The Commonwealth Government's Fraud Control Committee Its Brief and Purpose	**25**

ETHICAL DIMENSIONS

John Enfield	Ethics, Fraud and the Public Service	**34**
Ray Whitrod	Some Problems of Police Ethics	**38**

MANAGEMENT RESPONSIBILITIES

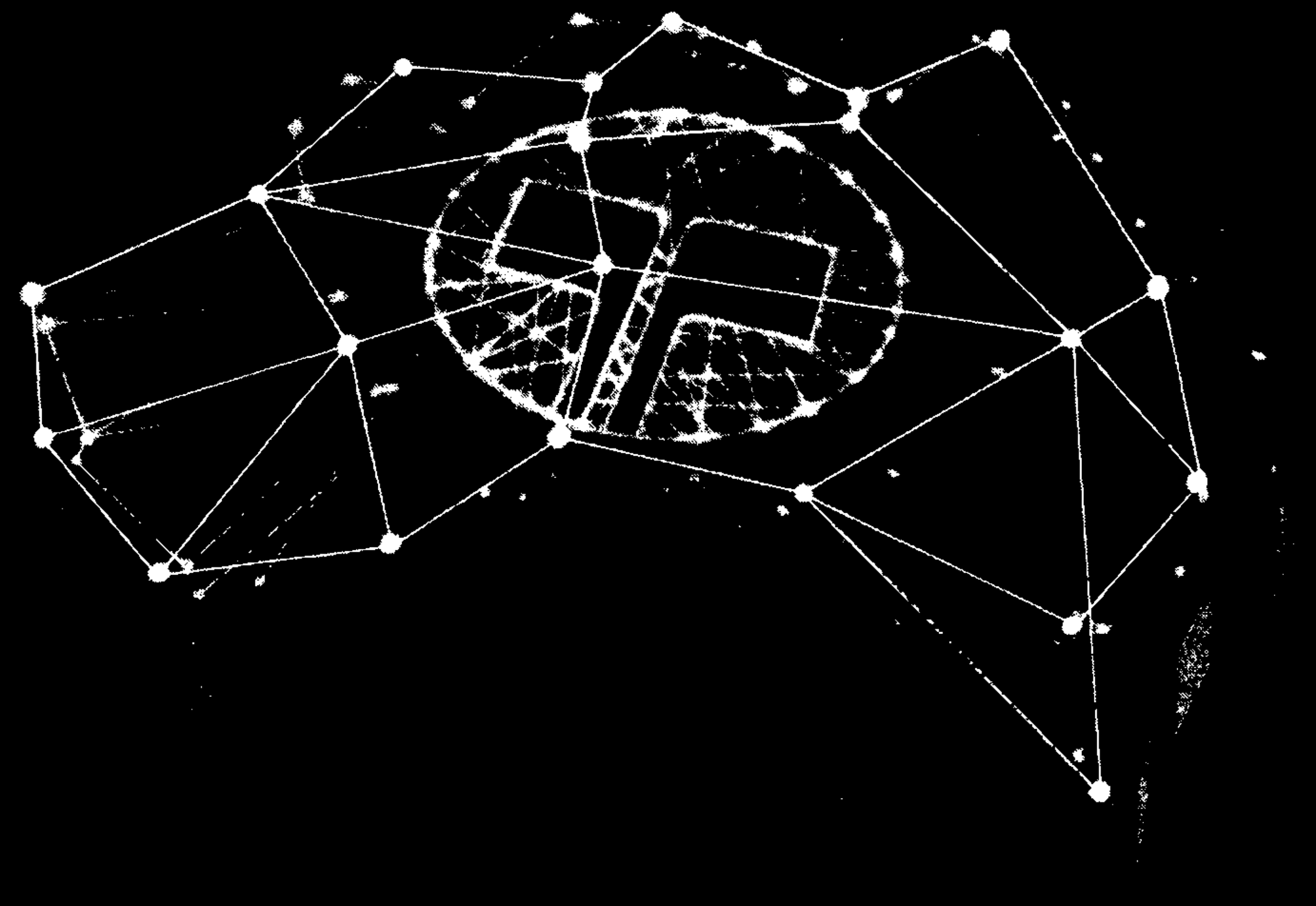
Barry S Leithhead	The Importance of Risk Analysis and Management	**42**
*** Derek Volker**	Ethics and Control of Social Security Payments	**47**
Dick Wright	Investigating Motor Accident Fraud A Case Study	**53**
Richard Daniell	Publicity and Its Impact Upon Fraud	**59**
Warren Simmons	Key Elements in Investigating Fraud	**62**

AUDIT VIEWS

R G Humphry	Risk Management and the Role of the Auditor in Preventing Fraud	**66**
V C Doyle	Fraud on Government The Role of the Auditor-General in Investigating Fraud	**72**

* Mr T C Murphy, Assistant Secretary, Benefits Control Branch, Department of Social Security, presented a paper to the AIC Seminar at Surfers Paradise. It was entitled "The Best Solution: Voluntary Compliance and How to Achieve It". It was very similar to the paper presented by Derek Volker to the RAIPA Seminar and has not therefore been published in this collection. Anyone with particular interest in the matters addressed in Mr Murphy's paper should consult Mr Volker's article.

How well are you utilizing your business' greatest asset?



The Telecom network.
An asset every Australian business can utilize.

An asset that is growing and changing to meet the needs of all businesses.

Today, the network allows you to communicate in voice, data, text, images.

Across town or across the country.

You can sell or service through telemarketing, add to your business' efficiency, build new markets, build new profits.

To make the most of your business' greatest asset, talk to Telecom by phoning **008 011 310** (Tasmania 008 006 140).

Telecom Australia

TAT 3407

INVESTIGATION AND PROSECUTION

Ian Temby	Impediments to Tackling Fraud	**77**
Kevin Zervos	Prosecution of Fraud on Government	**81**
Terry Griffin and Brian Rowe	Drawn Out and Complicated Problems with Fraud Trials	**89**
John Buxton	The National Crime Authority Its Role in Investigating Fraud	**98**
Chris Eaton	The Police Practitioner's Perspective	**101**

PREVENTION AND REMEDY

Garry D Dinnie	Minimising Fraud Through Preventive Systems	**104**
Rick Sarre	Alternative Remedies for Fraud Rule of Law Versus Administrative Remedies	**110**
John McMillan	Blowing the Whistle on Fraud in Government	**118**
P N Grabosky	Citizen Co-Production in Fraud Control	**124**

The *Canberra Bulletin of Public Administration* is published by the Royal Australian Institute of Public Administration (ACT Division). The views expressed in CBPA are those of individual authors and do not necessarily reflect those of the RAIPA.

CBPA is typeset by BELCONNEN TYPESETTING, 4 Saw Place, Macgregor, ACT (telephone 547390) and printed by KOOMARRI PRINTERS, cnr Lathlain and Wales Streets, Belconnen, ACT (telephone 513033).

CBPA is published four times a year. Annual subscription: $A40 (Australia only). Overseas rates on application. Cheques, etc, payable to RAIPA (ACT Division).

All correspondence including subscriptions and editorial matter to The Secretary, RAIPA (ACT Division), PO Box 329, Belconnen, ACT 2616, Australia.

The Expense Management System. Use it.

In any organisation large or small, managing travel and entertainment expenses can be an expensive nightmare. But it doesn't have to be.

The American Express® Corporate Card System is an unbeatable System devised to give you more effective control over travel and entertainment expenses, reduce paper work and cut administrative costs.

TIGHTER CONTROL.

Just imagine receiving a monthly statement for your organisation, which itemises who spent what, where and when.

Well, depending on how many American Express Corporate Cards your organisation will require, you can receive one of several reports that are individually designed to suit your organisation's specific requirements... you'll be better informed and you'll have more effective control over the organisation's spending.

But that's not all. The System can help you in a variety of other useful ways.

MORE THAN AN EXECUTIVE PRIVILEGE.

Many organisations who view the Corporate Card merely as a way of rewarding their senior executives are really not taking full advantage of the System.

The benefits of the Corporate Card System are even greater when it is issued to all staff incurring business expenses. It makes their travel and expense processing a lot easier... makes them even better managers in fact.

They can use the Corporate Card for hotels, petrol and car maintenance, car hire, cabs and air tickets, around the world and in Australia where it is accepted by over 68,000 establishments.

SIMPLIFIED TAX RETURNS.

The System allows you to separate business from personal expenses and provides you with all the necessary documentation.

And only American Express automatically provides you with two receipts, one when you make your charge, the other with your regular statement.

Over 500,000 organisations, large and small, have joined the System around the world and are finding it now saves them time, money and unnecessary headaches.

For more information on how to join the System please phone Narelle Fitzpatrick on (062) 57 1055.

The Corporate Card. Good for business.

Ogilvy MTM 0028

Introduction

FIGHTING FRAUD ON GOVERNMENT

Public services in the Westminster/Whitehall mould have long been held to have markedly high standards of probity. Probity has equally been seen to mark the relations of governments with beneficiaries of welfare programs and also contractors and suppliers. Examples to the contrary which emerged during the early 1980s were seen to be exceptions to a record which was otherwise scarcely blemished. The 1980s nevertheless witnessed a major change in the public confidence in which Australia's public services were held. A succession of inquiries revealed failings, to use a polite term, in particular fields. McCabe-Lafranchi, Costigan and Woodward are names which are now well-known for progressive revelations about a side of public administration whose existence had previously been seriously underestimated.

Meanwhile government agencies, notably the Taxation Office and the Department of Social Security at Commonwealth level, and, among others, insurance bodies at State level, took positive steps to assess and to address the problem of fraud. The Australian Federal Police itself took an active role in seeking to have fraud issues confronted. Eventually the Government acknowledged the importance of the issue and policies have slowly developed. Even so, fraud remains a problem whose nature and dimensions are still unknown and whose investigation and remedy continues to trouble ministers, administrators, investigators and prosecutors.

This special number of the *Canberra Bulletin of Public Administration* is intended to meet the needs of public sector executives who wish to acquaint themselves with the fraud issue. It is based on two seminars, one sponsored by the Royal Australian Institute of Public Administration (ACT Division) in Canberra in May 1988, the second sponsored by the Australian Institute of Criminology in Surfers Paradise in July. By combining papers from the two seminars, through agreement between the two Institutes involved, it has been possible to produce a single publication which will serve to inform public sector executives and the interested public of issues, policies and problems pertinent to the fight against fraud. For the time being it constitutes the most authoritative, comprehensive and timely coverage presently available. Yet it does little more than suggest the full extent of the problems involved and the hesitant, remedial steps in train.

SETTING THE SCENE The scene is set by Minister for Justice Michael Tate and Dennis Challinger, Assistant Director, Australian Institute of Criminology. Alan Rose, Associate Secretary, Attorney-General's Department provides an account of the work of the Commonwealth Fraud Control Committee.

ETHICAL DIMENSIONS Public Service Commissioner John Enfield and distinguished ex-police commissioner Ray Whitrod then address aspects of the ethical framework and environment relevant to the handling of fraud in the public sector.

LINE MANAGEMENT HAS PRIMARY RESPONSIBILITY It is generally agreed that line management has primary responsibility for identifying fraud risks and instituting remedial measures. Consultant Barry Leithhead's paper outlines this view. The following papers by Derek Volker, Secretary, Department of Social Security; Dick Wright from Victoria's Transport Accident Commission; Richard Daniell of the South Australian State Government Insurance Commission; and Westpac's Warren Simmons give the line manager's perspective based on direct experience.

AUDIT VIEWS These papers are followed by two from State government auditors-general, R G Humphry (then of Victoria and now head of the New South Wales Premier's Department) and V C Doyle from Queensland.

INVESTIGATION AND PROSECUTION The articles by Ian Temby, Director of Public Prosecutions, Kevin Zervos from the Melbourne Office of the DPP, consultants Terry Griffin and Brian Rowe, John Buxton of the National Crime Authority and Chris Eaton, National Secretary of the Australian Federal Police Association examine fraud issues on the basis of extensive participation in investigation and prosecution of fraud cases.

PREVENTION AND REMEDY Although there have been successes in the investigation and prosecution of fraud the price has often been high, the time involved considerable, and the impact on the totality of the problem probably modest. Garry Dinnie of Arthur Young & Co and Rick Sarre of the South Australian Institute of Technology in their papers consider some implications and alternatives.

Yet detection of fraud need not necessarily be left entirely to managers, auditors, the police and other investigators. Individuals, too, have a role in the fight against fraud, mismanagement and waste. But it is rarely a happy or an easy role. It is the subject of papers by John McMillan of the ANU Faculty of Law and Peter Grabosky from the Australian Institute of Criminology.

This collection of articles is, by any standards, a first effort, though a necessary step in a country still unwilling to see fraud on government as anything other than a temporary aberration from otherwise exemplary standards of conduct. The collection shows that some progress has been made, fraud is no longer quite the mystery it used to be, and some people in government are committed to vigorous detection, containment, prosecution and prevention of fraud. But there is precious little evidence that the fight against fraud is being pursued at the highest levels of government with the conviction and commitment which the situation requires. Indeed, in terms of broad strategy, there appears to be not much more than a mildly-directed form of laissez-faire leadership which, within Commonwealth administration, is a typical modus operandi these days.

There must be a question as to how adequate this approach is until the full dimensions and nature of fraud problems are known and while the fight against fraud remains in a fairly early state of development throughout government. More constructive leadership would seem to be called for and would not be out of place if the evidence contained in these articles is at all accurate.

JRN

- NATIONAL SALES NETWORK
- SOFTWARE LEADERSHIP
- SUPERIOR CUSTOMER SERVICE

Digital has built its business world-wide around a commitment to excellence.

As a result, we are the world's leading manufacturer of networked computer systems and associated peripherals.

NATIONAL SALES NETWORK.

Digital has a complete range of systems for every business in Australia and the South Pacific region.

Selecting the right system for you starts with our Sales Account Managers, and continues with our technical support capability including local manufacture and engineering.

SOFTWARE LEADERSHIP.

For large or small computer users, Digital offers a fully supported range of integrated application software.

Plus the capability for large software development projects and specialist areas, including, office automation, networking and manufacturing.

SUPERIOR CUSTOMER SERVICE.

Our education and training is second to none, and our superior field service includes automated telephone diagnosis for hardware and software.

Mobile service units complete the most responsive and effective customer service available.

DIGITAL EQUIPMENT CORPORATION
(AUSTRALIA) PTY. LIMITED 1987.
Incorporated in New South Wales
Digital logo, DEC, VAX/VMS, VAXcluster, PDP are trademarks of Digital Equipment Corporation.

DIGL0173/J&N

digital COMPUTERS

Defining Fraud and Examining it as an Issue Which Governments Need to Address

Michael Tate*

The present Government has been addressing this problem for some time now and has recently established a new mechanism for dealing with fraud on the Commonwealth which I will touch on in a moment.

DEFINING FRAUD

First, however, let me talk to you for a moment about defining fraud. This is not a simple task and frequently hinges on the particular circumstances at hand. What can be said is that fraud is conduct involving an element of deceit, including deliberate non-disclosure of information which results in misrepresentation or a misunderstanding of the truth. The common motivating feature is an intent on the part of the perpetrator to gain an advantage for him or herself or another.

In the Commonwealth legal arena, however, until the enactment by this Government (in 1984) of section 29D of the *Crimes Act* 1914, there was no substantive statutory offence of "defrauding" the Commonwealth. Neither section 29D nor the conspiracy section define "defraud". Courts also have been reluctant to define fraud comprehensively.

The term is not a tool designed for a single use or purpose, and its meaning varies according to the function it is intended to serve. Clearly, however, it includes both the deliberate evasion of a liability and obtaining a benefit by dishonest means. If we are to look at the issue broadly it may be relevant to identify fraud by asking "did the author of the deceit derive any advantage which he/she would not have derived if the truth had been known?"

In the initial investigations undertaken by the present Government in reviewing the systems for dealing with fraud on the Commonwealth the definition of fraud used was as follows:

> Inducing a course of action by deceit, involving acts or omissions or the making of false statements, orally or in writing, with the object of obtaining money or other benefit from, or of evading a liability to, the Commonwealth.

This definition is not confined to monetary gain and includes any benefit that could be gained from the government, including intangibles, such as "rights" of entry to the country, documentation conferring identity, information etc. One of the mistakes made in the past has been to assume that fraud only involves monetary or material benefits, whereas, on only limited reflection, it becomes obvious that some of the major benefits to be gained from the government are not necessarily in those forms.

One of the problems faced in the public sector is that the concept of fraud on government revenue is blurred because various instances of behaviour which you or I might generally regard as "fraud" are variously described, for example, as "overpayment" or "mispayment" or "over-servicing". This practice has, in the past, contributed to the public perception that defrauding the government is relatively innocuous behaviour.

To many in the community the government is "fair game" and citizens who would be appalled at any suggestion that they would behave dishonestly in relation to others regard misrepresenting their taxation liability not as dishonest but rather as something that everybody probably does. However, since the "bottom-of-the-harbour" taxation frauds (and the vast resources poured into their investigation and prosecution) became the major focus of media attention, the community is now beginning to recognise that any fraud on the Commonwealth involves a cost to the community as a whole.

COMMUNITY ATTITUDES

A major problem governments face in dealing with fraud on their own programs is this community attitude to defrauding the government. To many in the community the government is "fair game" and citizens who would be appalled at any suggestion that they would behave dishonestly in relation to others regard misrepresenting their taxation liability not as dishonest but rather as something that everybody probably does. However, since the "bottom-of-the-harbour" taxation frauds (and the vast resources poured into their investigation and prosecution) became the major focus of media attention, the community is now beginning to recognise that any fraud on the Commonwealth involves a cost to the community as a whole. Nevertheless, there is still ambivalence and the Government still has a major task

* Senator the Honourable Michael Tate is Minister for Justice. Text of keynote address to 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, Canberra, 2 May 1988.

CB PA *No 56, September 1988, 11-15.*

ahead of it in completely eradicating the "fair game" concept so that fraud on the Commonwealth is seen as the anti-social conduct it undoubtedly is – a task of considerable importance during a period of economic stringency and difficulty of maintaining the living standards of the average Australian. In my view, terms such as "white collar" crime do not assist as they tend to convey that certain crime has an unwarranted gentility about it. Fraud is criminal, regardless of by whom perpetrated.

PROOF OF INTENT

Another difficulty facing a government agency in dealing with an instance of suspected fraud is proof of criminal intent on the part of the suspected offender. One response to this is to use a "strict liability" approach as is used in taxation legislation, where tax assessed is due and payable unless the taxpayer can show cause, acceptable to the Commissioner for Taxation, for changing the assessment. In taxation cases where deliberate misrepresentation has occurred the Taxation Office has the power to impose a financial penalty without recourse to the courts.

Strict liability formulations derive from the late nineteenth century recognition that it was impractical to deal with certain types of offences using the full panoply of the criminal law. In the case of the Taxation Office, such formulations permit it to deal with tax evasion without the need to demonstrate to a court the fraudulent intent which is undoubtedly present in a substantial number of cases – though difficult and resource-intensive to prove.

Similarly, criminal intent in "overservicing" by medical practitioners or "mistakes" in filling out a benefit form by a social welfare recipient may be very much a matter of judgment or opinion. Proof of criminal intent in such circumstances often borders on the impossible. Frequently the intent cannot be "proved" in the strict sense but must be inferred from the entire course of conduct. In cases of this kind the use of criminal sanctions has frequently been judged to be inappropriate, and often pointless, and administrative remedies are used as a more appropriate course of action.

This approach, however, has had its disadvantages. It has recently become evident that in cases of major tax evasion or evasion of customs duty a purely monetary penalty is not a sufficient deterrent. Consequently, recourse is beginning to be made to the criminal law process in serious cases of this kind.

GOVERNMENT INVOLVEMENT IN FRAUD CONTROL

Turning now to the Government's specific initiatives in adding to the armoury of weapons to control fraud. You will all be aware that late in 1986 a review team was set up to examine systems for dealing with fraud on the Commonwealth. That review resulted from a number of internal papers and reports within the portfolio of the then Special Minister of State dealing with the need for increased Australian Federal Police resources, particularly for the purpose of investigating the increasing number of fraud cases being referred from departments and agencies of the Commonwealth.

That review was conducted by a task force headed by a representative of the then Department of the Special Minister of State under the oversight of a steering committee comprised of the Chairman of the then Public Service Board, the secretaries to the departments of Finance, Social Security, and Health, the Commissioner of Taxation, the Comptroller-General of Customs, the Director of Public Prosecutions, and the Health Insurance Commission.

Initially, its major aim was to explore alternative approaches to reduce the workload on the "downstream" agencies (AFP, DPP and AGS [Australian Government Solicitor]) which were heavily burdened with the increasing number of fraud cases.

The review found that a fundamental change of approach was needed to ensure that all agencies focussed on the need to build fraud prevention mechanisms into their programs and that a greater spirit of co-operation and information exchange for the purposes of identifying and combatting fraud was necessary if the Government's prime objectives were to be met effectively.

The Government has now adopted the majority of the recommendations of the review. The two recommendations not adopted (Nos 25 and 26) related to the need to amend the secrecy provisions in various Commonwealth acts to allow access to information by law enforcement agencies for the purposes of investigating fraud and other indictable offences. In the light of public concern regarding the privacy of information supplied to government, these two recommendations are being further reviewed by the Attorney-General's Department and the Attorney-General will report back to Cabinet on this issue later in the year.

Although the Government is still concerned with improving the effectiveness of "downstream" agencies and with limiting, where possible, the need for additional resources, the broader aim – of minimising the opportunities for fraud and ensuring that "fraud consciousness" becomes an integral part of good management practice within the Commonwealth – has now become the major thrust of the Government's efforts in the fraud area. Later, I will briefly touch on the other measures the Government has introduced to improve the effectiveness of "downstream" agencies.

ESTABLISHMENT OF FRAUD CONTROL COMMITTEE

In September 1987 the Government established a Fraud Control Committee, consisting of the Associate Secretary, Attorney-General's Department, the Secretary, Department of Finance and the Secretary, Department of Social Security (or their delegates). The Committee's major functions are:

- to monitor the implementation of the recommendations of the review;
- to evaluate risk assessments and fraud control plans drawn up by departments and agencies; and

- to facilitate information exchange and co-operation between agencies.

Cabinet has exempted the Australian Taxation Office from scrutiny by this Committee since it was already in the process of reviewing its procedures and setting up improved systems for dealing with fraudulent practices.

It is important to recognise, however, that, in line with the findings of the review, the prime responsibility for the prevention, detection and investigation of fraud remains with individual ministers and the chief officers of individual agencies. Departments and agencies are now required to undertake risk assessments on all their programs and develop fraud control plans to deal with risks identified in those assessments.

The Fraud Control Committee has not been established to take over the task of fraud control – it will not be telling agencies what to do or how to do it – but it can offer basic guidance and has already commenced to do so with the circulation of a set of guidelines outlining major factors that should be taken into account in drawing up a fraud control plan. It has also conducted a series of workshops designed to assist agencies in preparing risk assessments and fraud control plans and provide basic guidance on downstream agencies' requirements for the referral of matters for further action. Following an assessment of the outcomes of these workshops it will be providing further guidance to agencies.

Fraud has never been addressed in government as specifically as this before. The new mechanisms go well beyond previous audit requirements. Fraud prevention is now required to be an integral part of the line management of all government programs. The Government is determined to ensure that its primary objectives in the delivery of programs are not thwarted by negligence or by a blinkered approach to the real responsibilities of program managers. A lot of work is involved in ensuring that government systems are "fraud-proofed" to the maximum extent possible.

The Government's emphasis in the new arrangements is on improvement of the systems designed to prevent and detect fraud. It is important, therefore, for agencies to understand the kinds of things that can go wrong in delivering programs. A large amount of fraud against government programs is perpetrated by members of the community. It is also the case, unfortunately, that some government employees are involved in fraudulent behaviour. Few agencies in the past have had any real appreciation of how attractive they (their funding, systems, official position) are, not only to their legitimate clients but also to those whose sole or dominant purpose is unlawful profit. This lack of appreciation has unfortunately contributed to considerable vulnerabilities to fraudulent activities.

Some opportunities for fraud are obvious, such as absence of requirements for proof of eligibility or lack of checking of documentation presented. You have all also heard of companies who bill large organisations for fictitious directories or for goods or services never ordered or delivered, relying on lack of checking of initial authorisations.

The Government is giving high priority to this initiative and agencies are being asked to ensure continued high level supervision of fraud control. There is much consciousness-raising and re-education necessary within the public sector. Many agencies have expressed concerns that the new measures will require resources that they cannot spare if they are to continue to be effective in fulfilling their primary objectives. The Government is convinced, on the basis of actual recoveries so far across a number of payment and revenue collecting agencies, that over the short, and in the longer term, the savings to be achieved by these measures will be enormous. If agencies conduct a proper risk assessment of their activities they should be in a position to identify loopholes and the likely effect of remedial action so that the Department of Finance will be able to assess the cost-effectiveness of the provision of any necessary resources.

It is important, therefore, for agencies to understand the kinds of things that can go wrong in delivering programs. A large amount of fraud against government programs is perpetrated by members of the community. It is also the case, unfortunately, that some government employees are involved in fraudulent behaviour. Few agencies in the past have had any real appreciation of how attractive they (their funding, systems, official position) are, not only to their legitimate clients but also to those whose sole or dominant purpose is unlawful profit.

"IN-HOUSE" INVESTIGATION TEAMS

The Government has now endorsed the further development in appropriate cases of in-house investigation teams for handling minor fraud matters. The major and complex cases will still be dealt with by the Australian Federal Police. This does not mean, however, that minor cases will not receive proper attention. Agencies are being urged to obtain expert advice and to consult with the AFP and the DPP to ensure that their staff receive proper training in investigative techniques and brief preparation. For those agencies experiencing major fraud activity on a regular basis the AFP and the DPP have, and are looking to developing further with agencies, clear working guidelines for the proper co-ordinating of agency/AFP/DPP investigations and prosecution brief preparation.

FRAUD CONTROL GUIDELINES

As mentioned earlier the Fraud Control Committee has engaged a firm of consultants who have assisted in the preparation of guidelines to assist in the development of fraud control plans. These guidelines cover the key elements for agencies to bear in mind when developing their plans. In particular, the guidelines point out that it is important to address both external and internal fraud. The Government

is not saying that there is a high level of corruption among public servants, but recent examples here and overseas and in private enterprise suggest that internal complicity should not be ignored as a factor in major fraud. Systems must be designed, therefore, with this in mind.

Another area which is of particular concern is the protection of computer stored information. It is essential to realise that information of itself is valuable. The computer area is surrounded by mystique and managers tend to ignore it, possibly because they are not confident they understand it. It is absolutely essential that managers do understand what their computer systems can do and take steps to prevent unauthorised access, as they sensibly do in accordance with approved instructions and guidelines for the proper security of official "hard copy" information.

Governments are responsible for delivering programs to the community in accordance with their promises. They are also responsible for the use of taxpayers' money and to ensure that this is well-spent and not wasted or misappropriated. There is no question but that this Government considers fraud to be a major problem which we will pursue with vigour until such time as we can be satisfied that the public purse is safe from those who would misuse it.

"BLOCK" SCRUTINY

The report prepared for the Government recently by David Block has recommended a number of approaches to the processing of claims which some are claiming to be in conflict with the Government's new approach to fraud. The Government sees no conflict in the two sets of recommendations it has endorsed. While Mr Block recommended that agencies make a cost-benefit assessment of certain types of processing and abandon those that prove too costly, this should not be taken to mean that no accountability processes should be followed. Rather systems should be designed so that any anomalies will become evident with minimal checking processes. The whole point of fraud risk analysis is to determine where the greatest risks of fraud are and to prepare plans to counteract those risks. This is entirely consistent with the sort of efficient management proposed by Mr Block which, if followed methodically, will target accountability systems and processes where they should properly be, on areas of greatest vulnerability.

REACTION TO GOVERNMENT INITIATIVE

Many agencies are still confused about their new responsibilities and are having difficulty meeting the Government's deadlines. Others, however, have embraced the new approach wholeheartedly and are progressing with the development of their fraud control plans. The Government expected that some agencies would have difficulty meeting the deadlines set and is sympathetic to the problems a number of agencies will have in undertaking this preparatory work and overcoming, for some, a history of giving fraud control a lower priority than now is required by clear Government decision. But the Government is unsympathetic to agencies that have made little or no attempt to fulfil their obligations. The senior management of these agencies will be being contacted by the Chairman of the Fraud Control Committee. Failure to make a serious attempt to address this problem will be a matter then for ministerial consideration. The Government has indicated that it will, in cases of clear neglect, be prepared to apply the full range of appropriate management sanctions.

A lot of groundwork needs to be done, but by the end of two years the Government expects to be in a position to have had established with reasonable accuracy:

- where the most serious vulnerabilities to fraudulent practice, across the whole of the Commonwealth area of responsibility, lie; and
- what further action is necessary to minimise the risk.

The Government also expects to be able to point to the major areas of government activity that have already been fraud-proofed.

It is not expected that the problems will be resolved overnight but the Government does believe that eventually Commonwealth agencies' thinking and attitudes will move to a position where fraud-consciousness becomes second nature and an integral part of the consideration of how to deliver government programs in the most effective manner. Attitudes within the system must change to a certain extent and so must attitudes in the community. The community must be made aware that cheating on taxes and ripping off the social security system are not acceptable in a fair society. Society's attitudes can be turned around, as has been seen with the community approach to drunken driving and to smoking in public places. Development of this ethos will need to become a major focus of the agencies involved in delivering programs to the public in their particular areas. For those who target the Commonwealth as the potential source of unlawful, deceitful gain they must perceive that the community is no longer willing to see its public agencies being treated as "mugs".

INVOLVEMENT OF ORGANISED CRIME

In addition, I would like to point out that the Government is also well aware of the likelihood of the involvement of organised crime in fraud against the Commonwealth. Indeed, the Fruad Control Secretariat is located in the Criminal Law and Law Enforcement Division of the Attorney-General's Department, closely associated with the area dealing primarily with measures to combat organised crime.

Instances of the involvement of organised crime in fraud against government have been documented in Australia and overseas. Some of the more dramatic Australian cases in

recent times still involve outstanding legal action and I cannot therefore detail them. An example, however, from the Final Report of the Costigan Royal Commission, illustrates the scope of fraudulent activity which can occur when management responsibilities are not taken seriously and the high level of organisation that can be involved in government-targetted fraud.

At the Williamstown Naval Dockyard Costigan found evidence disclosing extensive frauds practised by members of the Ship Painters and Dockers Union in a highly organised fashion. The frauds included lying to gain employment and receive a higher wage, fraudulent time-keeping practices, the fraudulent practice of ghosting (that is, working under more than one name and receiving more than one pay packet from an employer at the same time), the fraudulent taking of leave, fraudulent workers' compensation claims, and theft.

This situation was able to flourish because of the procedures in place for employing painters and dockers at the Dockyard. They were employed in the first place as casuals. Recruitment was always done through the union office. Wherever a vacancy was to be filled the employment officer at the Dockyard would telephone the union office and inform it of the vacancy. The choice of the person to fill the vacancy was entirely the union's.

The candidate was expected to bring a letter from the union certifying that he was a fully paid-up member of the union. This was often not done. He was interviewed by the employment officer and the security officer. He was photographed and provided with a security card. The negative of the photograph was destroyed. The man was expected to return his card if he later left his employment. This very often did not happen. No serious attempt was made by the dockyard to recover such cards. There must still be a very large number of security cards in Melbourne which have not been returned. No attempt was made to ensure that these cards were not misused. Nor was any attempt made to ensure that the cards (with photographs) were used, for example, on collection of pay, as a means of identification.

In an example from another royal commission, the Stewart Royal Commission into the "Mr Asia" Syndicate, a low level clerk in the then Department of Immigration & Ethnic Affairs was used by the syndicate to provide false identification and passports to a number of members of the syndicate. He also removed all the files from the system after the action had been initiated so that there was no way to trace what had actually happened after the documents had been issued. This case has now been finalised and the person involved is serving a term in gaol.

In conclusion, let me make it clear: the Government means business in its attack on organised crime and in its determination to ensure that fraud on the Commonwealth is eliminated as far as is possible. Governments are responsible for delivering programs to the community in accordance with their promises. They are also responsible for the use of taxpayers' money and to ensure that this is well-spent and not wasted or misappropriated. There is no question but that this Government considers fraud to be a major problem which we will pursue with vigour until such time as we can be satisfied that the public purse is safe from those who would misuse it.

From Colony to Coloniser

John Eddy and J.R. Nethercote, editors

In its short history Australia has moved from being an infant colony whose fortunes were originally settled in Westminster and Whitehall to a nation with its own colonial responsibilities in Papua New Guinea.

The intervening period has witnessed many events whose administrative aspects shed a valuable light on how Australia has been governed in the course of its progress from colony to nationhood.

This book brings together a diverse collection of essays which examine some of these events, ranging from decision-making about the colony in Britain, law and order in New South Wales, social and educational policy in Victoria and South Australia to administrative reform in the early twentieth century, rationing during the Second World War, adult education in New England and administration in Papua New Guinea.

New from Hale & Iremonger

$19.95 pb

From the Newspapers

EX-PS MAN FACING CORRUPTION COUNT

A former officer of the Department of Primary Industry's fishery division appeared in the ACT Magistrates Court yesterday on charges of corruption, unlawful disclosure of Commonwealth information and stealing Commonwealth property.

The prosecutor, Mr Michael Lawler, said it was alleged that while working for the department, Mr Andrew Lawrence James McDermott, now resident in Tasmania, had been corrupted by a professional fisherman, Mr Tim Roberts. Mr Roberts had persuaded Mr McDermott to transfer fishing entitlements, called "boat units", worth about $500,000, to Mr Roberts from Rigil Kent Pty Ltd, a company of which Mr Roberts was once a director.

Rigil Kent is one of the largest trawl-fishing companies in south-east Australia.

– **Rob McKay**, *Canberra Times*, **21 July 1988.**

FORMER PUBLIC SERVANT SENT TO JAIL ON BRIBERY CHARGES

MELBOURNE: A former Commonwealth public servant who admitted taking bribes from a United States company after a deal struck at a funeral was jailed yesterday for 15 months by a Melbourne County Court judge.

Justice Kimm said Mr Leonard Calder Freeman took bribes of unknown value while working as a purchasing officer at the Government Aircraft Factory in West Melbourne.

Mr Freeman, 60, unemployed, of Raleigh Street, in the northern Melbourne suburb of Thornbury, pleaded guilty yesterday to seven counts of taking bribes between 1983 and 1986.

The former general manager of California-based Citicorp Aviation Industry Resources Incorporated, Mr Werner Gunther Becker, pleaded guilty to seven counts of paying the bribes.

Mr Becker, 30, a sales consultant of Stockfeld Street, Sunbury, was jailed by Justice Kimm for 12 months.

The judge said Mr Freeman had been paid 5 percent of the value of orders for aircraft parts placed with the US firm.

Judge Kimm told Mr Freeman, "You were in a position of trust and responsibility . . . and you grossly failed in that trust and responsibility.

"You admitted in a police interview that you knew what you were doing was against the law, but nevertheless you continued."

– *Canberra Times*, **2 July 1988.**

THREE FINED OVER INTERNATIONAL PHONE CALL FRAUD

Three Telecom employees, charged in connection with the fraudulent use of Telecom equipment, were convicted and fined in the Adelaide Magistrates Court yesterday.

Carl Desmond Austin, 54, operator, Janice Lorraine Clark, 38, operator, and Raymond Dennis Crunkhorn, supervisor, had all pleaded guilty to a total of 28 counts of fraudulently using Telecom equipment between July and September last year.

A fourth person, Margaret Ethel Hall, is yet to plead to a similar charge.

The addresses of the four Telecom workers were not listed on charge sheets and lawyers involved in the case would not release them.

Mrs J E Sanders, SM, recorded a conviction against the three who pleaded guilty.

She imposed a fine of $100 against Clark and $300 against Crunkhorn and Austin.

Last month, when prosecution of the three began, the court was told by Mr P Duncan, representing the director of Public Prosecutions, that Clark, Crunkhorn and Austin had been charged after a nationwide investigation, Operation Ramrod.

This operation had been established to investigate fraudulent calls made against the Overseas Telecommunications Commission which were "possibly worth millions of dollars".

He said Operation Ramrod had uncovered several Telecom employees throughout Australia who had been defrauding Telecom, including operators in NSW who had allegedly been paid thousands of dollars for their actions. It was alleged that one NSW operator had received up to $100,000 in payments.

– *The Advertiser*, **13 July 1988.**

TWO ACCUSED OF HUGE FRAUD

Federal Police had uncovered a Brisbane cottage industry of forged documents used for a massive and systematic welfare fraud, a court was told yesterday.

Commonwealth prosecutor Clive Porritt said the sophisticated fraud involved forged doctors' certificates being used to obtain sickness benefits.

Kenneth John Butcher, a 40-year-old clerk from Ashgrove, appeared on four counts of defrauding the Commonwealth.

Gary Desmond Ponsford, 30, a Gold Coast cabinet maker, appeared on four charges of aiding and abetting Butcher.

Brisbane Magistrates Court heard that the offences allegedly occurred in September and October last year and May and June this year.

– *Sunday Sun*, **31 July 1988.**

DOLE FRAUD JAIL TERM UPHELD

A mother of three sentenced to one month's jail for social security fraud had her severity appeal dismissed in Wollongong District Court yesterday.

The court was told June Margaret Cook, 57, housewife, of Berkeley, received $7935.80 in Supporting Parents Benefit from December 1983 to March 1985.

During that time Cook was living with Robert George Wales in a de facto husband and wife basis.

When interviewed by a Social Security Department officer on August 19, 1985, Cook admitted knowing she had no entitlement to the benefit.

In handing down his decision, Judge Jeremy Badgery-Parker QC said sentences for social security fraud must have some deterrent value.

– *Illawarra Mercury*, **3 June 1988.**

DOLE RIP-OFF MAN JAILED FOR 3½ YEARS

A man who used 20 fake identities to collect $23,335 in unemployment benefits was jailed yesterday for 3½ years.

Judge Duggan in the County Court in Melbourne said Thomas William Toomey was part of a carefully-planned scheme involving 11 people.

Crown prosecutor Geoffrey Horgan earlier told Judge Duggan the total fraud had probably cost the Commonwealth $500,000.

Toomey, 33, of the Melbourne suburb of Deer Park pleaded guilty to 80 counts of forging and 19 counts of uttering between July 1982 and September 1984.

Mr Horgan said people in the scheme used fake marriage certificates to create a total of 50 false identities.

He said the cheques were sent to premises rented by those involved in the racket and to false addresses.

Judge Duggan said unemployment benefits are used to support the needy. "But it is a matter of notoriety that the scheme is under severe threat," he said.

"This is not because the community does not recognise the need but because some people are abusing the system and therefore less money is available to those in need and the community is less prepared to fund the scheme.

"The scheme depends on the integrity of people making claims."

Judge Duggan said Toomey had been forced to give up a successful job as a carpet-layer about nine years ago because of arthritis in his knees.

Toomey had been unemployed since and drank and gambled heavily.

"I accept this lifestyle made the commission of these offences more likely," Judge Duggan said.

– Daily Telegraph, **20 July 1988.**

INSURANCE FRAUD MAY BE FORCING THIRD-PARTY RISE

The State Government suspects fraudulent injury claims may be forcing up the cost of third-party motor vehicle insurance.

Yesterday, it asked insurance companies to provide details of any cases where they believed injuries were "manufactured".

This followed claims at a Gold Coast criminology convention that up to 30 percent of Queensland's payout might go to bogus "victims".

Insurance companies, suspicious that some claims for hard-to-disprove injuries like whiplash may be false, have ordered closer scrutiny in processing sections.

The companies believe that in recent years the cheats have added more than $100 million to the premium bills of motorists who must carry the insurance.

Concern about the practice is growing because southern States' experience suggests corrupt doctors and lawyers are involved and plan to descend on Queensland.

Some schemes are so elaborate that driverless cars are crashed and then occupied by "motorists" who claim for non-demonstrable, soft-tissue injuries.

The Australian Institute of Criminology believes that 20 percent to 30 percent of the claims made on the two Queensland third-party insurers – Suncorp and FAI – could be fraudulent.

This estimate prompted the Finance Minister, Mr Austin, to write yesterday to the companies and the Insurance Commissioner and State Actuary, Dr A L Truslove, asking them for any details of suspected frauds.

Mr Austin said he wanted information by the middle of August when he would make a special report to Cabinet.

"If people are ripping off the system they are making third-party insurance more expensive for motorists generally," he said.

– Peter Morley, *Courier-Mail*,
23 July 1988.

CREDIT CARD FRAUD

In a few months, a former Westpac bank manager will face a judge and jury over charges that he improperly authorised the issue of half a dozen MasterCards. If convicted, he faces up to 10 years in prison. Even if well-behaved, he could still be separated from his family and the rest of the world for six years.

A harsh sentence? Not in the eyes of his banking masters, and the police. He is allegedly part of a new growth industry – credit card fraud.

Australians love plastic cards. Bankcard has never looked back from the initial mass mailing in 1974, and virtually every major international card circulates widely here. Our lives truly have come to depend on them.

Through the cards, Australians owe their banks about $220 each: when multiplied out across the nation the total is $3.5 billion. It is an impressive figure, but not enough to make us stop spending. Our banks are grateful, and so too are our criminals, for our bad habits.

The bank manager's accomplice, for example, allegedly used another 53 stolen credit cards. Over three months last year he is alleged to have defrauded various Sydney businesses of around $60,000 on those cards, and a further $20,000 on the dud MasterCards. If convicted, he will be looking at prison walls for perhaps five years and more likely three.

– Tim Blue, *Australian Business*,
17 Feburary 1988.

BANKS TAKE A LASHING OVER CREDIT CARD FRAUD

The security practices of Australian banks came under fire yesterday after the release of statistics which showed the incidence of credit card fraud had almost doubled in the past year.

Major retailers, building societies, credit unions and other issuers of credit cards were also attacked for their often-lax guidelines in providing lines of credit to individuals without taking proper precautions.

The release of figures from the Australian Institute of Criminology in Canberra highlighted a 91 percent jump in the amount of credit card frauds reported in Victoria during the year to June 30 from 22,534 to almost 43,767 cases.

While the figures related solely to Victoria, industry authorities were quick to point out that equivalent rises had occurred in other States and that the situation was now reaching crisis point.

It is understood that the total of credit card frauds in Australia over the past year involved around 150,000 cases, compared with less than 80,000 cases 12 months ago.

In spite of these facts, the major banks were yesterday eager to shrug off suggestions that they were responsible for the rise in credit card fraud, and said part of the reason was customer negligence.

The banks said customers who lost wallets containing cards often left their personal identification numbers for use of automatic teller machines in the wallet.

The general manager of Bankcard, Mr Kel Quill, said he believed the latest statistics were misleading in that they represented the number of fraudulent transactions used on credit cards and not the number of cards stolen.

He also said the difference in figures over the previous year reflected processing delays encountered by Bankcard early last year which meant some frauds were incorporated in the last financial year.

However, the Victorian Minister for Police, Mr Crabb, said the soaring rate of credit card fraud was "outrageous", and proposed seeking urgent talks with the major banks to curb the growth of financial fraud.

"If it was not for credit card fraud, police would be on the verge of reducing the number of major crimes," Mr Crabb said.

– Tony Kaye, ***AFR*****, 13 July 1988.**

CRAA, INSURERS JOIN FORCES ON FRAUD

General insurance underwriters and the Credit Reference Association of Australia (CRAA) have joined forces to beat policy-holder fraud – estimated at up to $700 million a year in personal lines insurance in NSW, and rising rapidly.

The drive to cut the fraudulent claims comes in the wake of the sharemarket crash, where the boom had generated most of general insurers' profits. Now pressure is growing for risk underwriting to produce a profit, and that means keeping a close eye on payouts.

The $700 million estimate from the Government Insurance Office of NSW includes fraudulent claims for domestic fire and theft and motor vehicle damage. From an analysis of their own claims, insurers believe that 5 to 10 percent of all claims in these areas carry an element of fraud – be it a deliberate act of setting a car alight, a false burglary claim, or merely an inflated claim – while about 2 percent of policyholders have a fraudulent intent when entering into an insurance contract.

If these figures are correct, the remaining 90-95 percent of policyholders are honest and paying for the fraud with higher premiums.

The $700 million excludes fraudulent casualty and sickness claims, which insurance companies submit are as high again, but for which they have no accurate figures. The CRAA system is now gearing up to build up its data base on these types of insurances.

The CRAA's insurance claims service was set up in 1983 and initially limited its data base to recording fire, theft and burglary claims made by individuals. It now has been expanded to include personal travel and accident insurance, plus a growing range of commercial insurance claims.

– Anne Lampe, ***SMH*****, 1 July 1988.**

Fraud on Government
A CRIMINOLOGICAL OVERVIEW

Dennis Challinger*

THE EXTENT OF FRAUD

As with many other crimes, the true level of fraud – in both the government and private sectors – is simply not known. Indeed, it could be said that the most successful frauds are never detected which may well explain why, when announcing the inquiry into fraud on government in June 1986, the Special Minister of State Mick Young said:

> Figures ranging from $5 billion to as high as $30 billion have been cited. These figures could be exaggerated. The simple fact is we don't know. (*Sydney Morning Herald*, 10 October 1987)

Unfortunately, that inquiry (*Review*, 1987) did not address this shortcoming so that we in Australia still cannot confidently state the cost of fraud against government. This is true even in quite specific areas like that of compulsory third party motor car insurance, which is predominantly carried by government insurance agencies. In Queensland, it is suggested that 20 to 30 percent of all third party claims are fraudulent, that is, false or exaggerated (Brisbane *Sunday Mail*, 5 June 1988). In South Australia, it is "generally accepted that between 5 and 10 percent" can be so described (Adelaide *Advertiser*, 12 March 1988). As shortfalls between third party claims and premiums are suggested to be $2,000-$3,000 million in each of Victoria and New South Wales, an Australian estimate of $10,000 million would not seem exaggerated. But this is still an estimate – the "real" figure is not known.

All this, however, does not make Australia exceptional. As far back as 1983, an American National Institute of Justice publication outlining ways to reduce fraud on government included the following statement:

> Fraud in government benefit programs is now widely viewed to be a serious national problem. Estimates by the General Accounting Office suggest the problem may cost the public anywhere from $2.5 billion to $25 billion per year. (Gardiner et al, 1982, V)

There is no doubt that such frauds continue to cause great concern in the United States. The growth of the non-profit organisation, the United Council on Welfare Fraud, is evidence of this. Welfare, or social security, fraud is also a problem in Australia, but it is only one element of fraud on government.

DEFINING FRAUD

The term "fraud" encompasses a great variety of offences. The following offence description is used for the compilation of Australia-wide crime statistics by the Police Commissioners' Australian Crime Statistics Sub-Committee:

> **Fraudulent Offences** are those involving deceit, misrepresentation or false promise with the intention of obtaining property, gaining an advantage, or depriving another person of his property, rights or privileges; or the misapplication of another person's propery entrusted to one's care, custody or control. [They include] impersonation with intent to defraud, valueless cheques, obtaining credit by fraud, fraud involving Medibank, Social Security and other Government agencies, fraud involving taxation returns, driver's licences, and businesses (for example, falsifying accounts, concealing bankruptcy), forging, destroying or altering signatures, wills, official seals, banknotes, records, foreign currency, trade marks etc, wilful false promises, untrue statements, retaining property in order to receive a reward, destroying valuable securities, misappropriation or embezzlement by a trustee, bailee, employee, agent, partner, clerk, or servant and fraudulent conversion or appropriation.

Such a definition obviously covers a vast spectrum of behaviour, including what is known as "workplace crime" or "workplace deviance". Those terms refer to activities that cause a loss to employers either directly (say, through theft) or indirectly (say, through inflating business expenses or conducting private business at work). The extent of such practices is considerable.

Overseas studies (for example, Hollinger and Clark 1983, Mars 1982) have indicated the commonness of workplace crime, and indicated the extent to which "fiddles" or "perks" have become institutionalised in some work environments. Such studies provide plentiful examples of workplace deviance amongst hotel staff, factory workers, taxi drivers, garbage workers, bread carters, waterside workers, hospital employees, retail employees and waiters. By way of illustration Mars (1982) quotes the following comments from a small businessman:

> Our main fiddle, in fact our only fiddle, is fiddling the government – they're the only ones we fiddle. We fiddle part of our workers' wages. All the very small businesses that I know have to be in on this kind of fiddle. If you employ someone and he earns below the amount that allows him to get the maximum family supplement as a low-wage earner – then you make sure he gets the supplement. You pay him just enough to qualify for the maximum and you make the rest of his wages up in cash. This is possible because we've a lot coming through the till.

---

* Dennis Challinger is Assistant Director, Information and Training, Australian Institute of Criminology. Text of Introductory Address to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CB PA *No 56, September 1988, 18-24.*

> This way he gets the maximum supplement, which is nine pounds plus all the other allowances that go with it . . . (which) comes to an extra three pounds a week. And then I give him ten pounds out of the till. And every week he goes round to the garage where I have my petrol account and he gets two pounds-worth of free petrol. I pay his stamp as well. If I paid him the thirty-two pounds a week he gets from me as a legitimate wage, he'd be taxed on it and he wouldn't get the supplement and I'd have to pay stamps at a higher rate because it's linked to level of wages. (Mars, 1982, 40)

"Fiddles" are virtually built into some jobs and are seen as supplementing award wages. An English journalist stated:

> The fiddles, of course, are very basic. You'll always claim first-class travel and go second class, and when you have a meal out you put it in for false entertaining. And then, of course, there's all the entertaining that you don't get vouchers for, particularly beers in hotels and taxis. The most usual fiddle is a conglomerate. For instance, it's not uncommon for you to decide you're dashing up to, say, Bletchley or somewhere after a story. You look up fares plus a few beers for fictitious informants and a taxi or two and bang it in for expenses. (Mars, 1982, 47)

Another illustration of workplace fiddling is provided by the office equipment salesman. Mars (1982) quotes one selling photocopiers as follows:

> To make a sale you might also give away paper: "I can let you have twenty pounds-worth of free paper with this" – this sort of thing. You can get out of the office with all the free paper you need. You're not supposed to do this but the manager turns a blind eye. You can also have a fiddle on paper: some people sell it. (Mars, 1982, 109)

It is not therefore surprising that some such practices occur within government agencies. Indeed, flexitime fraud, where employees dishonestly inflate their working hours, was suggested over a year ago to be costing the Queensland Public Service an annual $89 million (*Courier-Mail*, 17 December 1986). Mars (1982) makes reference to "a junior civil servant colleague of mine . . . abusing flexi-time to take a three hours a day part-time job pulling pints in his lunch 'hour'." (p 15)

The recent Telecom investigation into telephone operators making free overseas phone calls perhaps provides a case in point. Four Telecom employees who appeared in an Adelaide court last month were said by the prosecutor to have been charged after an investigation involving fraudulent calls which were "possibly worth millions of dollars". They pleaded guilty to making fraudulent overseas phone calls to the value of $23.10, $235.80 and $394.80. In their defence, counsel told the court that his clients were "not involved in any organised racket or fraud but they had taken a perk to which they were not entitled" (Adelaide *Advertiser*, 14 June 1988).

That comment suggests a view that some workplace perks are allowable, but that raises the fundamental question of where the line is drawn for behaviour that is an allowable perk rather than a fraud or theft. Plainly, it would be impossible to act against all workplace deviance and in fact some academics argue that allowing some is good for staff morale. It is therefore "real" deviance and "real" fraud that are the subjects of most investigation and prosecution.

The Australian Federal Police provide detailed information in their Annual Reports about frauds against the Commonwealth Government which have been brought to their attention. The 1986-87 Report provides 29 examples of such frauds of which the following illustrate the three modes of government activity in which most fraud occurs.

Frauds in the area of governmental *revenue raising* included:

- a $1 million sales tax fraud that was committed by purchasing blank video tapes from registered companies, quoting sales tax exemption certificates held by defunct companies;
- four "bottom of the harbour" tax evasion inquiries which were completed and briefs of evidence submitted to the DPP (Director of Public Prosecutions). The total tax liability involved was $117 million.

Frauds in the area of governmental *benefit giving* included:

- four people who were charged with fraud offences involving $200,000 gained from multiple claims for unemployment benefits and fraudulent First Home Owners Scheme claims;
- a doctor who was arrested and charged with 111 counts of making false statements regarding claims for benefits for professional services which were not provided. Those claims totalled more than $600,000;
- a $400,000 fraud which was committed against the Department of Social Security by the use of 17 false names to obtain benefits.

Frauds in the area of governmental *contracting of goods and services* included:

- an employee of the Aviation Department who submitted 687 receipts over a period of 20 months amounting to over $10,000. The receipts were obtained by the offender from various department stores, after having been discarded by store customers;
- inquiries were made into alleged secret commissions of $28,000 received by an employee of the Government Aircraft Factory for purchases from a private organisation.

POLICE DATA

The cases of fraud that are actually dealt with or detected by the police constitute no more than an indicator of the size of the problem. The number of frauds actually committed in both the public and private sectors cannot even be estimated. In the private sector, a detected fraud may even not be brought to the attention of police. A company might see it as sufficient for an employee to be dismissed, demoted, or merely cautioned (with or without

repaying any monies misappropriated). Such cases would not therefore be recorded in official police statistics.

Notwithstanding that, frauds reported to police in Australia have increased substantially over the last few years. In 1973-74, some 31,790 frauds were reported to Australian police forces. That figure had risen to 68,024 in 1984-85 (Mukherjee et al, 1987, 19). Using the same data collection methods, the figure has subsequently increased to 80,878 (in 1985-86) and to 92,526 (in 1986-87). This indicates a rise of 291 per cent over a twelve year period.

Police statistics also provide data about the people formally dealt with for the offence. In general terms, frauds have a good clear-up or solution rate – somewhere around 60 percent Australia-wide, compared with around 30 percent for armed robbery or 15 percent for burglary.

Around 30 per cent of these detected fraud offenders are female. This contrasts markedly with other criminal offences where the vast majority of detected offenders are male. For instance, only 10 per cent of those proceeded against for armed robbery are female as are only 8 per cent of burglars.

Some of the explanation for the high clear-up rate could be because many fraud offences are reported to the police precisely because offenders have been detected. Around 30 percent of these detected fraud offenders are female. This contrasts markedly with other criminal offences where the vast majority of detected offenders are male. For instance, only 10 percent of those proceeded against for armed robbery are female as are only 8 percent of burglars (Mukherjee et al, 1987).

These statistics relate to total fraud offences and thus involve for instance, fraudulent conversion, forging and uttering and credit card offences. This last category is one which has shown a remarkable increase in recent years and much of the increase in the total fraud figures may be due to it. Victoria's 1987-88 Crime Statistics, released last week, show an extraordinary increase in credit card offences to 43,767 from 22,534 twelve months previously. Nevertheless, if one assumes that frauds on government have always comprised a sizable percentage of total frauds as recorded by the police, then they have also undoubtedly increased in number over the last few years.

In fact, there are some statistics that throw a little more light on frauds on government. The Australian Federal Police indicate in their recent Annual Reports fraudulent offences that were reported or had become "known to the AFP Regional offices in Australia".

These plainly comprise frauds proscribed in Commonwealth legislation and detected around the country. It appears that some State police forces may count these in their statistics, but others do not (so they may or may not be included in the above figures).

Over the last five years, these offences have numbered:

1982-83	19,343
1983-84	7,520
1984-85	18,419
1985-86	15,869
1986-87	43,662

The reason for this last significant increase in reported fraud is difficult to suggest. As the Police Commissioner himself notes in his 1986/87 Annual Report "It is not clear whether there is an increase in frauds committed against the Commonwealth or whether there is a greater identification of frauds by the various departments involved" (p 16). Somewhat paradoxically, however, he later comments that the Department of Social Security's new system of paying benefits directly to beneficiaries' bank acounts has resulted in a significant downturn in some offences.

And therein lies the problem with crime statistics as a measure of crime. The reporting rate can vary, and administrative action itself can cause substantial change in the official statistics. Nevertheless, the statistics collected by the police certainly reveal a considerable level of offending.

PUBLIC AWARENESS

Generally, the public becomes aware of frauds on government mainly as it becomes aware of any offences, through the media. That means the public receives selective information which tends to cover either very dramatic fraudulent enterprises or fairly minor individual frauds.

The first category of frauds were probably introduced to the public by the 1982 McCabe-Lafranchi report which provided the first estimate of the cost of tax fraud, putting it (then) at hundreds of millions of dollars each year. Subsequent to that, much media coverage was given to "bottom of the harbour" tax frauds which included coverage of the notable case of Brian Maher who, while imprisoned for five years, is reported as having managed to keep $100 million he had generated through his fraudulent tax schemes (*West Australian*, 17 December 1987).

There have been other recent publicised tax fraud cases such as that of the two prominent businessmen in Perth sentenced this year to 18 months prison for conspiring to defraud the Commonwealth of $4.2 million in tax. But these sorts of offences are really very much removed from the lives of everyday Australians.

They may be more concerned by the Tax Office's recent investigation of hotels and clubs in Sydney which found 80 people working part-time jobs under false names and not paying tax. Those persons could have to pay "up to $1 million in unpaid tax and penalties", non-lodgers of taxation returns around Australia could owe as much as "$400 million a year" and pursuing them could net $3,000 million during the next 5 years according to a Tax Office spokesman (Sydney *Sun Herald*, 3 July 1988).

A further "fraud spectacular" which many Australians will remember is the debacle of the Greek conspiracy case in 1978 when 186 Greek-Australians, including 4 doctors and

a clinical psychologist, were accused of conspiring to defraud the Department of Social Security.

The majority of the court proceedings against these people concluded by June 1982 with the Commonwealth electing to proceed no further, although proceedings continued until early 1986 for the five professionals after which all charges were withdrawn.

Justice Roma Mitchell's *Royal Commission of Inquiry into Compensation Arising From Social Security Conspiracy Prosecutions* led to compensation to $1.8 million to the five professionals, and $6.17 million to the others, plus some compensation to 300 others whose pensions were affected.

The public are also well aware of "medifraud", although it is difficult to say what ordinary Australians make of allegations by the association "Private Doctors of Australia", that employees of the Health Insurance Commission were engaged in a $5 billion fraud (Perth *Daily News*, 19 April 1988). A more specific allegation of $200 million allotted through printing bogus cheques for non-existent services seems less outlandish.

The counter-claim is that unscrupulous doctors are defrauding Medicare of an estimated $300 million each year (*Weekend Australian*, 26-27 March 1988). Or is it $160 million – a figure from the Commonwealth Government's National Prices Network? (Sydney *Daily Telegraph*, 20 February 1988). Doctors seriously question these estimates and the public remain bemused but no doubt concerned about frauds involving so much money.

The second category of frauds publicised in the media – the lesser offences – are typified by the case of a 38 year old mother of four with an "unsatisfactory and unhappy" background who had fraudulently received $12,561.60 in social security benefits over a two year period. The magistrate hearing her case remarked that such cases – where women who had previously led blameless lives had resorted to fraud because of economic hardship – posed a "terrible problem for the courts when it came to sentencing".

Typified by family break-up, no financial support from fathers, and no ability to repay, it was "inevitable" said the magistrate that such women will resort to fraudulent claims. The magistrate acknowledged that the deterrent aspect was important with such a prevalent offence, but said that it was not appropriate to send individuals "who cry out for leniency from these courts" to prison. He sentenced the woman to six months imprisonment suspended on her entering into a five year good behaviour bond (*Canberra Times*, 30 June 1988).

In fact, reports of court proceedings relating to frauds on government provide further information for the public by way of judicial commentary when sentencing. One recent case involved what a New South Wales magistrate described as "a massive social security fraud" amounting to $22,846. The offences occurred between 1982 and 1985 and were heard in 1988. Before sentencing the offender to (the maximum) 12 months imprisonment, the magistrate said:

> Over a long period of time, you effectively stole from the taxpayer (sic) and others who rely on social security payments. The money should have gone to people who really needed it. (*Illawarra Mercury*, 7 May 1988)

A similar sort of statement was made by a judge who sentenced a medical doctor to three and a half years imprisonment for a "long term" systematic fraud against Commonwealth and State agencies amounting to over $300,000. According to the judge, the real victims of the offences were not those agencies, but

> the poor and the powerless whose social needs are undermined by the betrayal of systems put in place by Parliament and the destruction of confidence in those systems. (*West Australian*, 30 April 1988)

Whether these judicial statements reflect or create community rejection of frauds on government is unclear, but certainly all such comments that appear in the media do of course shape public opinion to some extent.

PUBLIC OPINION

In 1986, the Australian Institute of Criminology conducted a survey of the attitudes of over 2,000 Australian adults towards certain offences (Wilson et al, 1986). Respondents were asked to assess how much more serious than stealing a bicycle they saw 13 different events describing offences. Three of them, reproduced in Table 1, related to frauds on government. The respondents ranked social security fraud as the most serious of the three (seven times as serious as bicycle theft), with income tax fraud and Medicare fraud seen as equally serious (five times). Table 1 indicates the fraud offences were seen as less serious than armed robbery but more serious than burglary.

TABLE 1

SERIOUSNESS OF OFFENCES AS JUDGED BY AUSTRALIAN ADULTS

(N=2551)

Event	Number of times more serious than bicycle theft
A person armed with a gun robs a bank of $5000 during business hours. No one is physically hurt.	14
A person illegally received social security cheques worth $1000.	7
A person cheats on their Commonwealth income tax return and avoids paying $5000 in taxes.	5
A doctor cheats on claims he makes to a Commonwealth health insurance plan for patient services for an amount of $5000.	5
A person breaks into a home and steals $1000 worth of household goods.	3

The ranking of the fraud offences in Table 1 is roughly in accord with the situation in England where it has been stated:

> both public and political attitudes are much harsher to overpayment of benefits than to underpayment of taxes and ... prosecutions for benefit offences outnumber (tax) prosecutions by 30 or 40 to one. (Lynes, 1988, 73)

That ratio seems more pronounced than here in Australia where the Fraud Review shows that the Department of Social Security achieved 2126 successful criminal prosecutions in 1985/86 (p 126), compared with 119 fraud cases successfully prosecuted in the same year by the Australian Tax Office and leading to a pecuniary penalty (p 124). While these two categories are not absolutely comparable, they do suggest that around 20 social security cases are dealt with in court for every tax fraud case that is prosecuted there. (It should be noted that these figures relate to court prosecutions only – administrative procedures were used by the Taxation Office in 275,475 cases and by Social Security in 126,123 cases.)

But this does *not* mean that there are 20 times as many social security frauds as tax frauds. It says more about the priority of policy makers or about the ease of investigating particular sorts of offences. As the tax frauds referred to above resulted in an average "pecuniary penalty" of around $1,400,000, while the average amount ordered by the court to be paid for a Social Security fraud was only $706, it might be suggested that the tax area is a more fruitful (economical) avenue for further resources.

The relative standing of social security fraud and tax fraud is further supported by the penalties suggested as appropriate by respondents in the Australian survey if imposition of a prison sentence is considered. Prison was the favoured sentence for social security fraud by 17 percent of respondents compared with only 13 percent in the case of tax fraud (see Table 2).

However, consideration of the amounts of fines suggested by respondents can be seen as introducing a slightly contradictory finding. The most frequently suggested fine for a social security fraud was in the $1,000-$2,000 range, compared with a $5,000-$10,000 range for tax fraud and a $5,000-$50,000 range for the Medicare fraud (Walker et al, 1987).

TABLE 2

AUSTRALIANS' MOST COMMONLY SELECTED SENTENCE OPTIONS

(N=2551)

Offence	Percentage Preferring: Warning or No Penalty	Fine	Community-based order	Prison
Social Security Fraud	7	41	34	17
Income Tax Evasion	12	61	15	13
Medicare Fraud	3	60	12	24

Those features aside, the most important feature of Table 2 is that there is overwhelming support for some sanction to be imposed for fraud offenders. For the offence of stealing from a shop, 54 percent of respondents suggested no penalty or a warning would be sufficient, for "wife bashing" it was 13 percent, for "child bashing" 9 percent. The comparable figures for frauds were tax 12 percent, social security 7 percent and Medicare 3 percent.

LOOKING FORWARD

The possible ways in which frauds on government might be tackled will be discussed in other articles and the ways in which some government agencies have previously done so have been analysed by Grabosky and Braithwaite (1986). However, it is most important that analysis of fraud against the government should not be confined to text book examples of deliberate false pretence. To be sure, it is these for which the criminal sanction is reserved. But it is perhaps more constructive (certainly for the public administrator if not for the police or prosecutor) to focus on a wider constellation of phenomena which includes waste, abuse and fraud in government programs.

There is one fundamental justification for this broader perspective. Fraud against the government is much more easily accomplished in an environment of administrative laxity. Indeed, a significant proportion of revenue loss attributed to fraud flows less from deceit than from careless or inefficient management of public monies.

Given that, one might question the recent response to fraudulent activity that followed a report by consultants Price Waterhouse into the Student Allowance Scheme (*Financial Review*, 14 January 1988), namely that the maximum fine for fraudulent Austudy claims was increased from $100 to $2,000 (with the possibility of imprisonment). A spokesman for the minister indicated that the penalty changes "were designed to act as a greater deterrent", adding that the currently owed overpayments (sic) amounted to about $12 million (Adelaide *Advertiser*, 16 June 1988).

The belief that increased penalties alone are the answer to any crime is one which has been shown to be wrong. If offenders believe they have no chance of being detected then the possible penalty is irrelevant to their behaviour. A more likely approach to preventing further offending is to concentrate on reducing opportunity.

However, it seems that in some areas the opportunities for fraud are actually increasing. For instance, the *Defence Report 1986-87* (at page 43) reveals that 3,038 contracts valued at $4,326 million were let that year (three times the value of those in the previous year). And "for the first nine months of 1987-88 Commonwealth Departments increased their use of consultancy services during the year by an amazing 362 percent over the previous year" ... spending $358.8 million (*Canberra Times*, 2 July 1988).

These huge amounts of money provide additional opportunities for fraudulent activity by either those supplying goods or services under contracts, or those contracting them. There are those providers of goods and services who charge for goods not delivered or for services not rendered, or who knowingly provide defective or

substandard products. As such contracts grow in number, so too do the chances of fraud occurring. Some consultancies contracted by government are more risky than others:

> Management consultants in particular benefit from ambiguity over time that derives from constructed ambiguity over status. Since training on the job is the norm, a good job done by a trainee can therefore be charged for at the same rate as that of a fully qualified professional. It is among management consultants, too, though to a degree in all consultant jobs, where the rate is charged by daily time, that we find the well-established institution of "invisible days". If a job takes five days but the customer appears well satisfied, an extra "invisible day" (or days) can be charged under such heads as "consulting with colleagues", for "explorations", for "liaison", for "research", or "report-writing" – all of which are less visible than days spent on a site. In this kind of practice the consultant is then available to sell the same time to more than one client (Mars, 1982, 51).

Fraud against the government is, of course, by no means the exclusive province of unscrupulous citizens. Frauds can be perpetrated by individuals and by companies as taxpayers, contractors, or as beneficiaries of public payments. But government employees themselves can be offenders. And certain types of fraud require the collaboration of public servants and citizen offenders.

Such collaboration occurred in the meat substitution racket in 1981. The Royal Commissioner investigating that found widespread cheating and "bribery and corruption by a number of departmental meat inspectors, veterinary officers and police officers". Yet he went on to report that:

> the people concerned were not evil – many of them would have been regarded as reliable and effective officers. They were ordinary Australians, in positions of some responsibility, who were either demanding, or at least accepting, clearly improper payments which could only have the effect of compromising them in the performance of their duties. (Royal Commission, 1982, 12)

Perhaps times are changing, but in a recent case in Melbourne the judge was not so kindly. The case involved a former Commonwealth Government purchasing officer in aviation equipment who pleaded guilty to seven counts of corruptly receiving bribes (of unknown amounts). He was sentenced to 15 months imprisonment, with the judge commenting that the convicted man had "grossly failed" in his position of "trust and responsibility" (Melbourne *Sun*, 2 July 1988).

Reducing opportunities for ordinary Australians, whether employed by Government or not, to engage in fraudulent activities is obviously sensible. A recent English study provides two examples of the prevention of fraud through administrative change alone (Smith and Burrows, 1986).

In one case, internal fraud by hospital employees was not known to management until police received an anonymous tip off, although obvious signs of previous financial difficulties had been previously investigated. Unfortunately, that internal investigation was undertaken by precisely those staff who were involved in the "large-scale and long-standing fraud" relating to hospital supplies. According to the researchers:

> The root of this fraud, as with so many workplace crimes, lay in the abuse of responsibility by key personnel and the omission of other staff to check supplies. (Smith and Burrows, 1986, 18)

Fraud against the government is much more easily accomplished in an environment of administrative laxity. Indeed, a significant proportion of revenue loss attributed to fraud flows less from deceit than from careless or inefficient management of public monies.

In the event, "inexpensive revision of administrative procedures" led to annual savings of around $100 000, and further measures to aid prevention are being explored by hospital management. The researchers observe that while the remedies effected

> may with hindsight seem simple and obvious, it is the obvious which is so often overlooked. Systems sometimes appear to take on sacrosanct qualities in the minds of those operating them and administrative procedures are often taken for granted and their efficiency only rarely questioned. Thus in this case study it took the discovery of a major series of abuses to effect a radical overhaul of existing practices. (Smith and Burrows, 1986, 19)

This was no less true with the second case which involved underpayment of customs duty on cars imported into England from the Continent. Once again, police provided the impetus for administrative changes which made it much more difficult for importers (whether car thieves or entrepreneurs who understated the value of cars) to avoid paying legitimate government charges. Those changes involved the simple redesign of the appropriate forms which were then pre-numbered and security printed on watermarked sensitised paper, kept under lock and key and required cars' chassis numbers to be noted on them.

However, if opportunities for fraud are closed off (one way or the other), there is then the chance of what, in criminology, is called displacement, where those still minded to make money illegally find alternative ways to do that.

As it is, there are offenders who are known to engage in fraud against a variety of different government agencies. For instance:

> one man who has claimed on [third party insurance for] 55 car smashes since 1974 was sentenced to six months jail and ordered to repay $22,000 for 54 offences against the Department of Social Security. (Sydney *Sun*, 15 December 1987)

There is also a possibility that if fraud against government becomes harder, offenders might move into the private sector. There are already instances of existing overlap in this regard. As an example, two sisters jailed recently (for eighteen months and three months respectively) for a major credit card racket, admitted falsely claiming more than $74,000 in supporting parents' benefits. The District Court judge indicated that there was no alternative to imprisonment for frauds of this type and passed additional sentences of nine months and five months on the two. The judge further said that:

> social security fraud had to be punished because it caused lack of confidence in the system and affected those who really were entitled to the payments. (*West Australian*, 2 December 1987)

The concern that honest Australians are caused to suffer as a result of the fraudulent activities of some of their fellows is precisely why continued action against fraud on government is most necessary. That action should, however, start from within the government agencies that may fall subject to fraud. As criminologist Clinard (1983) has pointed out, managers create a moral climate which influences the values and behaviour of those who work for them. The public service manager with a half-hearted commitment to fraud control is unlikely to inspire a different attitude within his or her department.

REFERENCES

Clinard, M, 1983, *Corporate Ethics And Crime*, Sage Publications, Beverley Hills.

Gardiner, J A, Hentzell, S W and Lyman, T R, 1982, *Fraud on Government Benefit Programs*, National Institute of Justice, Washington.

Grabosky, P and Braithwaite, J, 1986, *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*, Oxford University Press, Melbourne.

Hollinger, R C and Clark, J P, 1983, *Theft By Employees*, Lexington Books, Lexington.

Lynes, T, 1988, Book Review of Enforcement of the Law Relating to Social Security, *The Howard Journal, 27*, 73-4.

Mars, G, 1982, *Cheats At Work: An Anthropology of Workplace Crime*, George Allen & Unwin, London.

Mukherjee, S, Walker, J, Psaila, T, Scandia, A and Dagger, D, 1987, *The Size of the Crime Problem in Australia*, Australian Institute of Criminology, Canberra.

Report of the Royal Commission Into Australian Meat Industry, 1982, AGPS, Canberra.

Review of Systems for Dealing With Fraud on the Commonwealth, 1987, AGPS, Canberra.

Smith, L J F and Burrows, J, 1986, "Nobbling the Fraudsters: Crime Prevention Through Administrative Change", *The Howard Journal, 25*, 13-24.

Walker, J, Collins, M and Wilson, P, 1987, How The Public Sees Sentencing: An Australian Survey, *Trends and Issues No 4*, Australian Institute of Criminology, Canberra.

Wilson, P, Walker, J and Mukherjee, S, 1986, How The Public Sees Crime: An Australian Survey, *Trends and Issues No 2*, Australian Institute of Criminology, Canberra.

Broker's Employee Charged for Deception

An employee of stockbroker, Bridges Son & Shepherd Ltd, has been charged with obtaining benefit by deception over allegations that he traded shares on the Australian Stock Exchange on behalf of fictitious clients.

The identity of the 24-year-old client adviser has not been revealed, but a spokesman for the NSW Fraud Squad said that the man had been granted bail and was due to appear in Sydney's Castlereagh Street Court on March 9.

The Fraud Squad alleges that during April 1987, the client adviser opened two share trading accounts with Bridges in the names of Mr Tony Moore and Mrs Julie Moore.

The spokesman said that between April and August, transactions to the value of $125,000 were traded through these two accounts. All the shares bought and sold were traded by way of credit.

— Janet Saunders, *AFR*, **19 February 1988.**

The Commonwealth Government's Fraud Control Committee
ITS BRIEF AND PURPOSE

Alan Rose*

Attention to the prevention, detection, investigation and prosecution of fraud on the Commonwealth is not new. But there have been considerable changes in the environment, both with respect to the nature of fraud practised on the Commonwealth and the Government's approach particularly to the organisation of its administration and personnel and financial management processes over the last 10 to 15 years, and most recently in July 1987 following the return of the Hawke Government to office.

It is instructive to note that it was not until Section 29D was added to the Crimes Act 1914 in 1984 that there was a statutory offence of "defrauding" the Commonwealth although there had been an offence of conspiring to defraud the Commonwealth.

Investigations made by, and the reports of, a series of royal commissions and inquiries, especially the McCabe-La Franchi Report and the Costigan Commission, and concentration by the media on the community's concern about fraud practised, for example, on health, social security and the taxation administrations, have raised the political profile of law enforcement.

Strong legislative and administrative action has been taken since Costigan in the taxation, social security, health and government solicitor areas as well as through general law enforcement initiatives. Since 1982:

- Special Prosecutors Gyles and Redlich have completed their work on "bottom of the harbour" and other prosecutions;
- the Charter of the AFP has been recast to place larger scale fraud against the Commonwealth high on the list of priorities;
- the Office of the Director of Public Prosecutions has been established;
- the National Crime Authority has been set up with, among other things, fraud and tax evasion being included as "relevant offences" and therefore subject to the NCA's special powers;
- in June 1985 a Private Trustee Task Force was established to conduct investigations with a view to detecting fraud or other criminal activity by registered trustees involved in administering estates under the Bankruptcy Act 1966; follow-up action continues to be taken following successful investigations by the Task Force;
- the Proceeds of Crime Act 1987 and the Cash Transactions Reports Act 1988 have been commenced and the CTR Agency is about to be established; and
- the Government intends to put to the Parliament in the Budget sittings proposals for an enhanced Tax File Number System.

Concern by governments to be seen to be doing something effective to deal with fraud has coincided with the economic necessity for far greater restraint in the growth of public sector expenditure and something approaching a "revolt" especially by PAYE taxpayers.

One need common to dealing with fraud and economic restraint is improved management performance in public enterprise. The concentration now is on the measurement of performance – of outcomes including increased productivity and sensitivity to client and community demands and expectations.

In the twelve month period before the 1987 double dissolution election the Government, among other things, established the Block Scrutiny Process and the Review of Systems for Dealing with Fraud on the Commonwealth. The first has produced a number of reports for the better targeting of departmental administrative resources, particularly from a risk management perspective. The second, through a series of recommendations, sought to establish in the minds of departmental and agency managements a clearer understanding of their responsibilities for specifically dealing with the real risks of internal and external fraud being practised on their programs.

Some commentators have seen the Block approach, for example, the removal of detailed checking during the processing of accounts, as being in some way in conflict with the Review's emphasis on the need for enhanced prevention and detection of fraud. As the Minister for Justice, Senator Michael Tate, said in his keynote address to a Royal Australian Institute of Public Administration Seminar on "Ethics, Fraud and Public Administration":

> The Government sees no conflict in the two sets of recommendations it has endorsed. While Mr Block recommended that agencies make a cost-benefit assessment of certain types of processing and abandon those that prove too costly, this should not be taken to mean that no accountability processes should be followed. Rather systems should be designed so that any anomalies will become evident with minimal checking processes. The whole point of fraud risk analysis is to determine where the greatest risks of fraud are and to prepare plans to counteract those risks. This is entirely consistent with

---

* Alan Rose is Associate Secretary, Attorney-General's Department. He was Secretary, Department of Community Services, 1986-7. Text of an address to Australian Institute of Criminology Seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CB PA *No 56, September 1988, 25-32.*

the sort of efficient management proposed by Mr Block which if followed methodically, will target accountability systems and processes where they should properly be, on areas of greatest vulnerability.**

The Government has, therefore, consistently in the financial reforms it has made, stressed that it no longer believes that managements can acquit their responsibilities for guarding against fraud merely by going through the motions of maintaining systems in accordance with central co-ordinating authority prescriptions such as those laid down in the past by the Treasury, the Department of Finance and the Public Service Board, and followed through in compliance audits by the Auditors-General. Procedures are still important but are not a substitute for actual, measurable performance by well trained staff.

Ignoring criminals who target, for example, large expenditure programs because their activity is not revealed by standard and traditional clerical checks is no longer, if it ever was, acceptable bureaucratic performance. While ensuring legitimate clients receive benefits and services might be the primary corporate objective, preventing the criminal wasps from raiding the honey pot is now of equal importance.

In future, Commonwealth ministers, departments and agencies are required to make broadly based appreciations of the management tasks which face their administrations including their vulnerability to fraud and to so manage those responsibilities that positive public interest outcomes in line with government policy and legitimate community expectations are maximised and negative outcomes, particularly those resulting from fraud, are reduced to the absolute minimum. Ignoring criminals who target, for example, large expenditure programs because their activity is not revealed by standard and traditional clerical checks is no longer, if it ever was, acceptable bureaucratic performance. While ensuring legitimate clients receive benefits and services might be the primary corporate objective, preventing the criminal wasps from raiding the honey pot is now of equal importance.

It was against the background of progressive management reform in the Commonwealth public sector, and a period of concentrated attention on the difficulties facing Commonwealth law enforcement agencies in mustering resources to deal with fraud, that the Government, just after its return in 1987, considered the recommendations in the Report of the Review of Systems for Dealing with Fraud on the Commonwealth. The Government's response to the Report was announced by the Attorney-General in a news release of 29 September 1987. The Review had been established on 2 June 1986 by the Government because it recognised that significant areas of fraud were dealt with by arrangements spanning several portfolios and that therefore the formation of policy required a study of similar breadth. The Review was not asked to determine the scale of fraud, nor to inquire into the detail of measures for preventing or detecting fraud, nor to examine loss by the Commonwealth other than financial loss.

The Government, in response to the Review's recommendations, agreed to the establishment of the Fraud Control Committee (FCC). The FCC comprises, in addition to myself, the Secretary to the Department of Finance and the Secretary to the Department of Social Security, or their nominees from time to time. The terms of reference of the Review and its outcomes as accepted by the Government are at Appendix I. The Attorney-General's news release announcing the Government's decisions is at Appendix II. In brief, the Government has asked the FCC to:

- evaluate risk assessments and fraud control plans;
- co-ordinate and monitor the implementation of the recommendations of the Fraud Review;
- facilitate the sharing of skills and knowledge between agencies for preventing, detecting and dealing with fraud;
- identify areas in which priority should be given to new arrangements for dealing with fraud; and
- monitor the use of resources required for dealing with fraud.

The Government, in taking its decision, included within the ambit of the FCC's responsibilities the administration of all departments and agencies, except for the Australian Taxation Office which was already well down the track in the process of reviewing its procedures and in setting up improved audit systems for dealing with fraudulent practices.

The Attorney-General, in making his announcement, stressed that the prime responsibility for the development of strategies and systems to prevent, detect and in appropriate cases investigate fraud lay with individual agencies. The Government had open to it the alternative of appointing either an existing "downstream" agency or a new body as an "overlord" which would have assumed primary responsibility for fraud control. To have adopted this alternative would have gone against all the other devolutionary decisions taken by the Government in recent months which have stressed the primacy of individual ministers, departments and agencies for management outcomes. A more centralised solution appears to have been adopted by the establishment in the United Kingdom of a Serious Fraud Office to be staffed by 80-100 accountants, lawyers, police and administrative personnel.

The FCC has been very conscious of the individual responsibility of Commonwealth ministers, and that it was not established to take over the task of fraud control. It is not in the business of telling agencies what to do or how to do it but it is prepared to offer basic guidance and to bring agencies with skills into contact with others which may be approaching the fraud control issue for the first time.

** See pp 11-15 for the text of the Minister's address to the RAIPA seminar.

The FCC quite consciously did not establish a large secretariat. Initially it depended on only part-time assistance and limited support from consultants. Now that workloads are increasing with the receipt of risk assessments from departments and agencies, its Fraud Policy Unit has four officers.

The FCC and its Policy Unit operate primarily through contact/liaison officers in departments and agencies. The potential is for some 250 agencies to have working relationships with the Committee. At present some 20 agencies have submitted risk assessments which, under the recommendations accepted by the Government, were to be the first major step in the identification of vulnerabilities to which fraud control plans would then be directed.

To assist departments and agencies in the preparation of risk assessments and plans, the FCC engaged consultants Griffin and Rowe to prepare a set of guidelines which have been circulated to all agencies. The circulation of guidelines was followed by the conducting of workshops in March and April in Canberra, Brisbane, Sydney and Melbourne. At those workshops, sessions were conducted by members of the FCC, the consultants Griffin and Rowe, officers from a number of departments and agencies with a variety of functional responsibilities, for example, major income maintenance, revenue collection and purchasing and from the principal, "downstream" agencies, the Australian Federal Police, the Director of Public Prosecutions and the Australian Government Solicitor. These workshops provided departments and agencies with an opportunity to clarify processes for undertaking risk assessments and to meet with officers of the Fraud Policy Unit and "downstream" agencies who could assist with particular analytical approaches training and other contacts who could be of assistance in developing assessments and plans.

It is the hope of the FCC that it will be able to advise the Government that it should be wound up at least by the end of the Government's current term of office.

What will be the basis of the FCC's providing that advice – not that there is no longer any threat of fraud on the Commonwealth – but that ministers individually are satisfied that departments and agencies for which they have responsibility have adequate fraud control plans, that there are workable guidelines between agencies with major investigation and prosecution loads and the AFP and the DPP respectively, and the other recommendations of the Review have been or are well on the way to implementation.

So far I have been talking about the broad responsibilities of the FCC which we have been keen to view as an adjunct to the primary responsibilities borne by ministers. The FCC has sought to follow a course of action which makes it clear that it is in no way a substitute for, nor is it looking to absorb the proper management responsibilities of ministers, departments and agencies.

I might now make some references to a number of specific recommendations of the Review accepted by the Government. You will see from the material attached to this paper that apart from confirmation of the AFP's role in investigating major fraud, individual agencies have been asked by the Government to build into their ongoing corporate responsibilities the responsibility for investigating routine instances of fraud against them whether those investigations are likely to be followed by the application of administrative remedies or by reference of the matter to the Director of Public Prosecutions for consideration of whether or not criminal law charges should be laid. The alternative of continually expanding the resources of the AFP to investigate minor matters was not accepted by the Government on the basis that this was an inappropriate use of highly skilled resources and could not be seen as cost beneficial.

The routine, vague and repetitive minor occurrences of fraud should and must be controllable by normal vigilant management action. The principal law enforcement agencies, while needing intelligence links with a number of program management agencies, should be able to concentrate on organised and sophisticated fraud which, as we have seen in the recent past, has the potential to disrupt if not to threaten the fabric of the Australian democracy.

The Government has further exhorted departments and agencies in taking decisions which have implications for "downstream" agencies to estimate clearly the likely impact on those "downstream" agencies through early consultation and allow for, among other things, appropriate resources including any specialised or additional personnel to be taken on.

The FCC is satisfied that there has been in the last twelve months or so considerable improvement in consultation arrangements between major departmental users of the services of the AFP and the DPP and that practical working guidelines have been established between all "downstream" agencies and their major clients. Adherence to these guidelines is likely to go a long way to ensuring that many of the resource difficulties experienced in recent years by, for example, the AFP will not be met again in the future.

The FCC was also pleased to record progress that has been made following correspondence and discussion between the Attorney-General and his State and Territory counterparts on completion of the computerisation of corporate affairs and real property titles records which will facilitate more effective access, for example, by the AFP, the DPP, the AGS, the Taxation Office, the Customs Service and the Official Trustee in Bankruptcy, to those records. Arrangements have also been settled between the Comptroller-General of Customs and the DPP for consideration in appropriate cases involving fraud of the use of criminal prosecutions rather than relying totally on administrative penalties.

The FCC, in furthering its responsibilities to facilitate the sharing of skills and knowledge between agencies, will be on a regular basis looking to convene discussions between

"upstream" and "downstream" agencies to ensure that intelligence and perceptions of the criminal environment are shared and arrangements are in place to:

- minimise unproductive investigations;
- implement cheaper administrative remedies where possible; and
- assist the training of in-house resources to meet the investigative needs of agencies and relieve pressure on bodies such as the AFP.

The Government's clear aim in adopting the approach to fraud on the Commonwealth that it has is that fraud control must be included as an integral part of each department's and agency's corporate planning arrangements. Part of what the FCC will need to be in a position to say to the Government at the end of its current term of office is that fraud control plans have been adequately integrated into agency management plans and that in future there will be no need to repeat what has been done on this occasion as a one-off and extraordinary exercise. In future the periodic reviews required of corporate plans under the normal governmental arrangements will include a review of the appropriateness of the particular agency's strategies for dealing with its vulnerability to fraud. If those strategies are being effectively implemented each department and agency will be making a major contribution at the source to deterring and controlling fraud. If the opportunity for fraud is markedly reduced, the aim of the Government of striking a blow at major organised criminal elements through recent legislative action such as the Proceeds of Crime Act 1987 and the Cash Transaction Reports Act 1988 which followed earlier action taken to establish the Australian Federal Police, the National Crime Authority and the Director of Public Prosecutions will be given a better chance of success. The routine, vague and repetitive minor occurrences of fraud should and must be controllable by normal vigilant management action. The principal law enforcement agencies, while needing intelligence links with a number of program management agencies, should be able to concentrate on organised and sophisticated fraud which, as we have seen in the recent past, has the potential to disrupt if not to threaten the fabric of the Australian democracy.

For those in the community with dishonest intentions and for those who can but need to be kept honest, the Government's fraud control initiatives are intended to signal that the Commonwealth public purse is no longer a soft touch. For this to be the reality the FCC has been asked to assure ministers that failure to comply with reasonable standards of honest dealing will be met routinely by all departments and agencies by effective "front doors" and adequate investigation and detection methods leading where appropriate to prosecutions, the imposition of pecuniary penalties and/or imprisonment with the confiscation of property if this is justified. And that this anti-fraud system has been achieved at the best value for money.

APPENDIX I

REVIEW OF SYSTEMS FOR DEALING WITH FRAUD ON THE COMMONWEALTH

Terms of Reference

"The purpose of the review is to describe existing methodologies and systems by which Commonwealth agencies interrelate in dealing with fraud on revenue and expenditure programs and to make any recommendations that may be necessary for improving the efficiency of present arrangements.

In particular, the review is to:

- examine the effects that enforcement action by one agency has on others, including cost consequences;
- examine means for achieving equilibrium in the demand for and supply of services to deal with fraud;
- consider whether any improvements may be made in existing arrangements for consultation between agencies; and
- examine means of improving information sharing between agencies in relation to fraudulent activity.

In conducting the review, due regard is to be paid to:

- existing and proposed measures to deal with fraud; and
- the differing requirements of agencies as a consequence of the size and nature of the programs which they administer.

For these purposes, and accepting that the roles of some agencies require that they apply more limited definitions, the term 'fraud' is taken to mean inducing a course of action by deceit involving acts or omissions or the making of false statements orally or in writing with the object of obtaining money or other benefit from or of evading a liability to the Commonwealth."

APPENDIX II

FRAUD REVIEW AND FRAUD CONTROL COMMITTEE

NEWS RELEASE BY LIONEL BOWEN
Deputy Prime Minister and Attorney-General

The Attorney-General, Mr Bowen, announced today the release of the Report of the Review of Systems for Dealing with Fraud on the Commonwealth and the establishment of a Fraud Control Committee to monitor the development and implementation of fraud control mechanisms within Government agencies. A copy of the terms of reference of the Fraud Control Committee is attached.

In announcing the release, Mr Bowen said the Government had either accepted or extended all of the Review's

recommendations except two, and would proceed immediately with their implementation. The exceptions involved changes to existing secrecy provisions in legislation. These will be further reviewed by the Government giving full consideration to civil liberties and privacy implications.

Mr Bowen said the Fraud Review recognised it was preferable that fraud be prevented in the first place. The main thrust of the Review's findings, therefore, was that agencies affected by fraud should have the principal responsibility for its prevention, detection and (in appropriate cases) its investigation, should properly assess the effectiveness of their revenue and expenditure programs, and should monitor the means and resources by which those programs are protected.

Consistent with these arrangements, only the larger and more complex cases would usually be referred to the Australian Federal Police for investigation. Mr Bowen said that all agencies which do not already have them would now be required to adopt explicit plans and arrangements for fraud control, to be developed on the basis of risk assessments. Such arrangements are intended to ensure that the most efficient and effective use is made of the trained resources available.

The review also recommended improved arrangements for consultation and information exchanges between agencies, and methods of improving the quality of the information available in relation to fraud through the use, for example, of sample surveys, compliance audits and alternative means of measuring performance in order to assess the effectiveness of systems, resource allocations and present approaches to dealing with fraud.

Mr Bowen said that the Fraud Control Committee would monitor the implementation of the Fraud Review's recommendations and other Government decisions in relation to fraud. The Committee is to comprise Mr Alan Rose, Associate Secretary, Attorney-General's Department, Dr Michael Keating, Secretary, Department of Finance and Mr Derek Volker, Secretary, Department of Social Security. The heads of other agencies would be involved in the Committee's work as appropriate.

Mr Bowen emphasised that the Committee was not a further review.

He said that in addition to monitoring and co-ordinating the Fraud Review's recommendations, the Committee will identify areas in which priority should be given to improved arrangements for dealing with fraud, and will assess the effectiveness of existing and proposed arrangements for fraud control. The Committee's terms of reference do not extend to the operations of the Australian Taxation Office which has independently established a comprehensive audit program to deal with tax fraud. This program is subject to external evaluation by the Australian Audit Office. It has already demonstrated considerable success, as demonstrated by the 1986-87 revenue outcome.

The Committee's terms of reference will require it to provide the Government with a continuing assessment of the effectiveness of resource use in dealing with fraud. A principal role will be facilitation of the sharing of skills and knowledge between, on the one hand, agencies with highly developed means of preventing and detecting fraud and, on the other, agencies whose equivalent systems are less well developed.

"Implementation of the Review's recommendations and the establishment of the Fraud Control Committee will improve the Government's capacity to reduce the present abuse of revenue and expenditure programs and to deliver its benefit programs as intended, to those most in need," Mr Bowen said.

Mr Bowen said that the decisions taken today are a further step in the Government's commitment to the development of an effective law enforcement strategy.

"The Government is approaching the problem vigorously, using detailed analysis and taking constructive action, to ensure that systems for preventing, detecting and investigating fraud are as co-ordinated, efficient and effective as possible. It is the first time any Australian government has done so".

ATTACHMENT

FRAUD CONTROL COMMITTEE TERMS OF REFERENCE

The role of the Fraud Control Committee is to evaluate the continuing effectiveness of systems for dealing with fraud in those agencies which have such systems and to co-ordinate the development of effective plans and arrangements for fraud control and monitor their implementation in those agencies which do not. Emphasis will be placed on liaison between agencies (both upstream and downstream).

Primary responsibility for the development of strategies and systems to prevent, detect and (in appropriate cases) to investigate fraud lies with individual agencies, which should adopt a positive and preventive approach to areas with potential for fraud rather than accepting a reactive role to its occurrence. In order to assist agencies in meeting this responsibility, the Committee will:

- co-ordinate and monitor the implementation of the recommendations of the Fraud Review endorsed by Cabinet;
- facilitate the sharing of skills and knowledge between agencies as to means of preventing, detecting and dealing with fraud;
- identify areas in which priority should be given to new or improved arrangements for dealing with fraud;
- monitor the use of resources required to deal with fraud, and in particular:
  - assess agencies' existing and proposed plans and arrangements for fraud control, information recording systems and methods of training to ensure the effectiveness of the Government's strategy against fraud;

- assist in the provision to agencies of expert advice in relation to the development of fraud control strategies and systems;
- recommend guidelines to agencies, individually or generally, as to desirable means of preventing, detecting or otherwise dealing with fraud;
- monitor co-ordination arrangements between agencies in dealing with fraud.

The Committee will report to the Attorney-General on progress at regular intervals.

REPORT OF THE REVIEW OF SYSTEMS FOR DEALING WITH FRAUD ON THE COMMONWEALTH

RECOMMENDATIONS

1. That the principal responsibility for the prevention and detection of fraud rest with the agencies against whose programs fraud is attempted. (para 3.2.12)

2. That all agencies accept the responsibility of investigating routine instances of fraud against them, whether the investigation is likely to be followed by the application of an administrative remedy or by reference of the matter for prosecution, and that instances of fraud referred to the AFP for investigation should generally be those which are more complex or larger in scale than the most routine cases. (para 3.2.12)

3. That all agencies be required to pursue a systematic and explicit approach to the control of fraud and, to this end, that:

   - those which have not already done so assess the risk of fraud against their programs and report to their respective ministers within six months of the date of acceptance of this recommendation;
   - agencies whose programs are subject to a significant risk of fraud, and which have not already done so, develop detailed plans for fraud control (however described);
   - other agencies with programs subject to a less significant risk of fraud, and which have not already done so, develop arrangements for fraud control for inclusion in corporate plans, internal audit plans and/or other internal management plans as appropriate; and
   - assessments of the risk of fraud and arrangements for fraud control be reviewed at intervals of no more than two years. (Such reviews could be included as part of each agency's management improvement plan as appropriate). (para 3.3.4)

4. That, where new or altered arrangements for fraud control have implications for downstream agencies, the minister responsible for the relevant upstream agency be required to advise the minister responsible for the downstream agency of the anticipated impact of those arrangements on the latter agency. (para 3.3.4)

5. That, unless they have already done so, within six months of acceptance of this recommendation, all agencies which within the preceding three years have referred a total of more than 20 matters involving fraud (excluding cheque frauds) to the AFP or the DPP, in consultation with the AFP or the DPP, develop and implement criteria and guidelines on the basis of which future references are to be made. (para 3.4.3)

6. That the Attorney-General's Department convene regular meetings at State and national levels involving the AFP, the AGS and other agencies affected by or involved in dealing with fraud, as appropriate, the principal purpose of which would be to:

   - provide the DPP with information as to trends in handling common form cases (dealt with in aggregate) and affording early warning of forthcoming workload; and
   - provide all participants with an opportunity to assess capacity to deal with fraud against demand for relevant services, to discuss priorities, information flows and alternative means of dealing with fraud. (para 3.4.4)

7. That, in developing plans and arrangements for fraud control referred to in recommendation 3, agencies which do not already do so consider the use of administrative remedies as a means of dealing with minor instances of fraud and, where necessary, bring forward proposals for appropriate legislation. (para 3.5.7)

8. That, in order to assist evaluation of the efficiency of resource usage flowing from decisions to adopt administrative remedies in cases involving fraud, appropriate records be maintained of the application and use of such remedies, details of the type and extent of records to be considered as part of the negotiation between agencies referred to in recommendation 9. (para 3.5.7)

9. That all agencies maintain appropriate records of activities and resource allocations in relation to fraud sufficient to show the nature and outcome of activities to prevent and detect fraud, the allocation of resources to deal with fraud and the extent of reliance on services provided by other agencies in dealing with fraud; and that details of the type and extent of such records be determined in negotiation between agencies and the Attorney-General's Department within six months of the date of acceptance of this recommendation. (para 3.6.7)

10. That the results of the first year's records collected in accordance with recommendation 9 be provided to the Attorney-General's Department within three months of the end of the financial year 1987/88 and that, in consultation with relevant ministers, he determine whether, as a result of an analysis of the records, further consideration by Cabinet is required. (para 3.6.7)

11. That agencies provide appropriate training to staff in the prevention, identification and detection of fraud and, where appropriate, liaise with the AFP about training in investigative skills and techniques and with the DPP or, as appropriate, the AGS about training in the preparation of briefs of evidence. (para 3.7.4)

12. That, where it is appropriate to do so, agencies publicise in general terms the fact that information is matched between them and that this and other techniques are used to detect fraud. (para 3.8.3)

13. That the Comptroller-General of Customs and the DPP consider the use of criminal sanctions in appropriate cases involving fraud on customs programs and prepare a joint report on the matter to the Attorney-General and the Minister for Industry, Technology and Commerce. (para 4.4.3)

14. That the Attorney-General at the next meeting of the Ministerial Council for Companies and Securities:

    - urge all States and the Northern Territory to expedite current programs to computerise corporate affairs records and develop an analytical capacity to facilitate data gathering for the purpose of investigations and legal proceedings;

    - seek agreement that such records and analytical capacity be made available online to the AFP, the DPP, the AGS, the ATO, the ACS, the Official Trustee in Bankruptcy, and to other agencies as appropriate;

    and bring forward proposals for any consequential amendments to legislation as soon as possible. (para 4.5.4)

15. That the Attorney-General, at the next meeting of the Standing Committee of Attorneys-General:

    - urge all States and the Northern Territory to introduce or to expedite programs to computerise land titles records and to develop an analytical capacity to facilitate data gathering for the purpose of investigations and legal proceedings; and

    - seek agreement that such records and analytical capacity be made available online to the AFP, the DPP, the AGS, the ATO, the ACS, the Official Trustee in Bankruptcy, and to other agencies as appropriate. (para 4.5.5)

16. That, where budget bids involve significant changes in activities concerned with controlling fraud, relevant upstream agencies be required to consult with, and seek advice from, downstream agencies as to likely resource consequences for the latter, and that any advice given be included as part of the upstream agencies' budget estimates explanations to the Department of Finance. (para 5.1.5)

17. That costs accruing to the AFP in retaining specialist services agreed by the agency concerned to be necessary for the conduct of a particular investigation be reimbursed to the AFP by the agency under whose program the matter investigated arose. (para 5.1.13)

18. That, within six months of acceptance of this recommendation, and in consultation with the AFP, the DPP and the AGS, agencies determine their requirements for training in investigative skills and techniques and in the preparation of briefs of evidence; and that consideration of resource requirements of upstream agencies as a consequence of training needs should follow adoption by those agencies of plans or arrangements for fraud control as contemplated in recommendation 3. (para 5.3.2)

19. That, where appropriate and cost effective, agencies which now make payments by cheque develop a timetable for moving to direct crediting, and that it be incorporated into plans or arrangements for fraud control. (para 5.6.1)

20. That Finance Direction 10/28 be withdrawn and replaced by guidelines developed by the Department of Finance in consultation with the AFP and the DPP on the basis of which agencies may exercise some discretion as to cheque cases referred to the AFP. (para 5.7.1)

21. That, within six months of the date of acceptance of this recommendation, the Attorney-General report to Cabinet as to whether and the most appropriate means by which a charge might be attached to the real property of persons who owe a debt or are liable to refund money to the Commonwealth, identifying any necessary legislation. (para 5.8.5)

22. That, within six months of acceptance of this recommendation, the Attorney-General and the Minister for Finance report to Cabinet as to whether debts owed by a client to one agency or under one program might be set-off against moneys to be paid by or under another, the means by which this might be done, and the circumstances in which it is appropriate, identifying any necessary changes to present arrangements and legislation. (para 5.9.4)

23. That, for a trial period of one year, agencies which believe their efforts to recover moneys owed to the Commonwealth are hampered by lack of access to locator information possessed by other agencies record relevant details and provide them to the Attorney-General's Department for an assessment as to what action may be required including, if necessary, the need for a submission to Cabinet by the end of the financial year 1987/88. (para 6.3.17)

24. That, in order to reduce the incidence and maximise the detection of financial loss, and where it is consistent with the terms of present legislation, agencies adopt cooperative policies in providing information to other agencies and, in particular, where it is cost-effective, consider matching of information relevant to identifying instances of fraud. (para 6.4.23)

25.* *That, to meet the immediate needs of the AFP, the DPP and the NCA for adequate access to information from the ATO, the HIC, the DSS, and the ACS (the disclosing agencies) for law enforcement, prosecution or civil remedy purposes, the Attorney-General bring*

forward as soon as possible a proposal for legislation which would override secrecy provisions otherwise applicable, to enable the AFP, the DPP and the NCA to obtain adequate access to and use of information held by the disclosing agencies where that information is relevant to the alleged or possible commission of an indictable offence or to a related civil remedy, subject to the following:

- *information to be provided at the discretion of the disclosing agency, which may disclose it at the request of the AFP, the DPP or the NCA, or of its own initiative. The exercise of this discretion should be exempt from review under the Administrative Decisions (Judicial Review) Act 1977;*
- *constraints (now provided in draft form) on access to information relevant to defence, national security, telephone interception or the opening of mail;*
- *other specified constraints essential for the protection of information the disclosure of which would be unreasonable having regard to the proper administration of justice;*
- *information provided by a disclosing agency to the AFP, the DPP or the NCA should be available only for use for or in relation to a law enforcement, prosecution or civil remedy purpose within the scope of the functions of the AFP, the DPP or the NCA respectively in connection with an alleged or possible indictable offence;*
- *the recommendation does not apply to self-incriminating information supplied under compulsion in accordance with any statute which expressly states that the information cannot be used in prosecution proceedings against the person who has given it;*
- *the Commissioner of Police, the Director of Public Prosecutions and the Chairman of the NCA should be entitled to delegate to officers holding specified positions the ability to seek information;*
- *the public should be informed as appropriate that information provided to the specified agencies may be made available to the AFP, the DPP and the NCA for law enforcement, prosecution and civil remedy purposes.*

For the purposes of this recommendation, "indictable offence" means an offence against a law of the Commonwealth or law of a Territory, that may be dealt with as an indictable offence (even if the offence may, in some circumstances, be dealt with as a summary offence).

It is noted that further restrictions on information in the possession of the ATO may be necessary in the light of Cabinet's consideration of the matter in the context of the initiatives against organised crime. (para 6.5.18)

26.* *That the present review of secrecy provisions by the Attorney-General's Department be completed within twelve months of the date of acceptance of this recommendation, that it place particular emphasis on the removal of unnecessary constraints upon the flow of information between agencies in relation to fraud, and that upon conclusion of the review the Attorney-General report to Cabinet recommending any desirable changes to legislation.* (para 6.6.3)

27. That, except in relation to recommendation 25:
    - the term 'agencies' used in the above recommendations means all Commonwealth Government departments, the Australian Customs Service and the Health Insurance Commission, and such other Commonwealth statutory authorities and other bodies as relevant ministers may determine;
    - ministers are to advise the Attorney-General within six months of the date of acceptance of this recommendation of the reasons for which it is considered any statutory authority or other body should not be so defined; and
    - when the context requires, the term 'fraud' includes 'possible or suspected fraud'.

28. Agency plans or arrangements for fraud control should include either the conduct of sample surveys, compliance audits or appropriate alternative assessments as means of measuring the effectiveness of systems, resource allocations and present arrangements for preventing and detecting fraud.

* the Government has requested further advice on this matter.

AUSTRALIAN SOCIETY

KATE AHEARNE, *Allan Ashbolt,* Wendy Bacon, **DAVID BOWMAN** , *Veronica* *Brady,* Judith Brett, **DAVID BURCHELL,** Paul Chadwick , MANNING CLARK, *Gay* *Davidson,* Sol Encel, **HUW EVANS,** *Adam Farrar,* Liz Fell, **JANE FREEBURY,** Peter Hanks, ADELE HORIN, *Amirah Inglis,* Ken Inglis, **STEPHEN KNIGHT,** *Terry Lane,* Sylvia Lawson, **ROSALEEN** **LOVE,** Ian Lowe, *Stuart* *Macintyre,* CHRIS McCONVILLE, Humphrey McQueen, **DAVID MARTIN,** *Brian Matthews,* Jan Mayman, **JOHN O'HARA,** Robin Osborne, MARIAN SAWER, *Jocelynne* *Scutt,* Bernard Smith, **DAVID** **SOLOMON,** *Hugh Stretton* , Paul Wilson, **KEITH** **WINDSCHUTTLE,**

...Just a few of the writers featured in AUSTRALIAN SOCIETY over the past twelve months.

Each month AUSTRALIAN SOCIETY*'s contributors look at the issues that really matter — economic policy, the media, health policy, the future of Australia's cities, arts and culture, federal politics . . .*

Monthly at your newsagency, or on subscription from PO Box 274, Fitzroy 3065.

Ethics, Fraud and the Public Service

*John Enfield**

The Australian public service has been subject to a series of major reviews and reforms in recent years aimed at improving its efficiency. At the same time, new technology has had an impact on most areas of the public service, and there have been major changes in the management of financial and other resources.

As a means of achieving a more efficient, streamlined administration, departments and agencies have been encouraged to decentralise and devolve decision-making and to reduce the number of management layers. The public service has been urged increasingly to adopt private sector management styles, including risk management. The aim is now value for the dollar, not, as in the past, accounting for the last cent. In this, Australia is moving along the same path as the public services of many other countries.

As a result of these developments, many of the traditional institutional "checks and balances" against fraud and other criminal or unethical behaviour have been removed. If administrative power is the source of the ethical issue, then the processes of devolution and decentralisation have the potential to increase significantly the numbers of public servants who may be confronted with ethical dilemmas.

Furthermore, the emphasis on private sector business practices and value for the dollar are leading to a major shift in the values which form the bases for ethical conduct in the public service. Indeed, it would seem that now, more than ever before, public servants are faced with a multitude of competing values. Other factors affecting public service ethics are the community's perception of the service and the personal commitment of individuals in the service to their career and to serving the public faithfully and well.

I believe that RAIPA's selection of the theme "Ethics, Fraud and Public Administration" for its 1988 Autumn Seminar is timely, and I welcome the opportunity to contribute to it.

I should like to speak briefly about:

- the Public Service Commission and its role in promoting ethics; and
- the broad checks and balances which are designed to promote ethical behaviour and deter fraud in the APS.

I shall not attempt to deal with fraud of public monies by those outside the public service; nor do I propose to speak about internal audit and the role of auditors.

---

* John Enfield is Public Service Commissioner. Text of an address to 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, Canberra, 2 May 1988.

CBPA No 56, September 1988, 34-37.

I shall then proceed to outline the ways that the Public Service Commission sees that it can fulfil its responsibilities for promoting ethical conduct in the currently changing public service environment.

THE PUBLIC SERVICE COMMISSION AND ITS ROLE IN RELATION TO PUBLIC SERVICE ETHICS

The Government's objectives in considering successor arrangements to the Public Service Board included the following:

(a) to maintain the independence of the essential personnel functions of recruitment, promotion, discipline and retirement from political involvement; [and]

(b) to ensure that the public service reform initiatives and other essential functions of the Board are maintained at least at the same standard.

David Block's Efficiency Scrutiny Unit's Report of July 1987 noted, in respect of the former Board, that it "has been an important force in the development of a professional, efficient, merit-based, non-partisan public service. The Board has been the guardian of a system which avoided both patronage and victimisation and which maintained high levels of integrity and honesty".

In making recommendations about the allocation of functions to the Public Service Commission and to other departments, the Efficiency Scrutiny Unit did not make any specific reference to policy responsibility for public service ethics. However, the Report recommended – and the Government agreed – that the Commission be responsible for (amongst other matters) "the policy aspects of recruitment, promotion, dismissal, mobility and retirement". With the background of the Government's objectives, we have taken this firmly to include the ethical aspects of public service employment.

In so far as the Commission was given specific responsibility for the APS discipline code, I would not see it as appropriate to limit our role to setting down what public servants should not do, and administering sanctions where breaches occur. Rather, we see a need to provide a broad framework which includes positive guidance on standards of conduct and performance and mechanisms for helping to resolve ethical dilemmas.

In addition to promoting ethical conduct amongst public servants, the Commission considers that it also has an important role to play in helping to maintain public confidence in the integrity of the Service.

CHECKS AND BALANCES

I shall now turn to the broad "checks and balances" that we have in the Australian public service for promoting ethical behaviour and deterring fraud and other criminal or unethical conduct.

A system based on merit

The Australian public service is derived from the Westminster system, involving the notion of a neutral career public service, appointed on the basis of merit. It is worthwhile reminding ourselves of the background of corruption and patronage which preceded the establishment of the Westminster system. One could argue, indeed, that the merit-based system is our most important threshold check against corruption, fraud and unethical behaviour in the public service.

EXPECTED STANDARDS OF PERFORMANCE AND CONDUCT

There is a substantial body of law in the *Public Service Act* and *Regulations* and in other legislation which relates to the duties and obligations of staff. In addition, public servants as employees have various common law duties, and there is a special body of law relating to Crown Service. The main duties of staff are set out in Public Service Regulations 8A and 8B. I believe Regulation 8A is worth quoting in detail. It says:

An officer shall –

(a) perform with skill, care, diligence and impartiality the duties of his or her office, or any other office, whose duties he or she is directed to perform to the best of his or her ability;

(b) comply with any enactments, regulations, determinations, awards or departmental instructions applicable to the performance of his or her duties;

(c) comply with any lawful and reasonable direction given by a person having authority to give the direction;

(d) have regard to any official guidelines or recommendations applicable to the performance of his or her duties;

(e) in the course of his or her duties, treat members of the public, and other officers, with courtesy and sensitivity to their rights, duties and aspirations;

(f) provide reasonable assistance to members of the public in their dealings with the Service and help them understand any requirements with which they are obliged to comply;

(g) avoid waste, or extravagance in the use of public resources;

(h) not take, or seek to take improper advantage, in the interests, pecuniary or otherwise, of the officer, any other person or any group, of any official information acquired, or any document to which he or she has access as a consequence of his or her employment;

(i) at all times behave in a manner that maintains or enhances the reputation of the Service.

I shall now turn to what public servants are expected not to do. This area is also the subject of extensive and specific legislation, for instance:

- the *Crimes Act*
- the *Audit Act*
- the *Secret Commissions Act*
- the *Public Service Act* and *Regulations*
- other specific Commonwealth laws, and
- the Common Law

To quote some of these provisions: The *Crimes Act* sets out a range of offences and penalties, for example:

- Section 70: unauthorised disclosure of information, which carries a penalty of imprisonment for 2 years.
- Section 71: stealing or fraudulently misappropriating property belonging to the Commonwealth, which carries a penalty of imprisonment for 7 years.
- Section 72: falsifying books or records, which carries a penalty of imprisonment for 7 years.
- Section 73: corruption and bribery of Commonwealth officers, which carries a penalty: imprisonment for 2 years.

The *Public Service Act* sets out the grounds for disciplinary action of officers. Discipline may range from counselling, through to a fine, or demotion, through to dismissal. In brief the grounds are:

- misconduct, and
- the commission of a criminal offence relevant to the officer's employment situation.

The Australian public service has an extensive and detailed discipline code which was developed through the Joint Council process. The processes and sanctions are set out in detail in the *APS Discipline Handbook*.

As far as criminal behaviour, including fraud, is concerned, the law is quite specific and clearcut, and no-one can be in any doubt about the unlawfulness of their actions, and the penalties, if they proceed down that path.

The most common response to cases of fraud in the APS is in fact dismissal. In the last three years there have been fourteen dismissals for a range of serious offences, including fraud. It is likely that at least twice this number have resigned as a result of facing disciplinary action expected to lead to dismissal.

This does lead one to ask whether prosecution would be an appropriate course because resignation may carry a substantial penalty in terms of salary and pension foregone.

Overall, I think it would be true to say that, in relation to the size of the public service, serious offences are still relatively rare. Where breaches are detected, they tend to be highly publicised.

I shall take the opportunity to mention one problem that we are faced with in administering the discipline code. Where officers are charged with criminal offences, it is usual to defer action under the APS discipline provisions pending the outcome of the court case. This is because the APS discipline process is considered to be a civil matter. It is not uncommon for lengthy delays to occur in the court system before the case is heard and this presents serious difficulties for employing departments.

The most common response to cases of fraud in the APS is in fact dismissal. In the last three years there have been fourteen dismissals for a range of serious offences, including fraud. It is likely that at least twice this number have resigned as a result of facing disciplinary action expected to lead to dismissal.

There are many situations that public servants are faced with which are not addressed in the legislation. This is the "grey", difficult area of ethics. The former Public Service Board attempted to provide guidance on a range of such issues in its *Guidelines on Official Conduct of Commonwealth Public Servants*. This document was first issued in 1979, around the time of the Bowen Inquiry into Public Duty and Private Interest. Prior to the Board's demise, it was revised substantially following a review by a Joint Council sub-committee and changes flowing from the public service streamlining legislation. Accordingly, the *Guidelines* can be taken to represent the standards of management and staff in the public service.

The *Guidelines* are based on three main principles, namely that:

- public servants should perform their duties with professionalism and integrity and efficiently serve the Government of the day;
- fairness and equity are to be observed by public servants in official dealings with the public and other public servants; and
- real or apparent conflicts of interest are to be avoided.

The *Guidelines* cover a wide range of issues, for instance:

- Relationships between politicians and public servants. Because this is topical, I should like to take the opportunity to refer to the guidelines concerning requests by ministers for material or facilities believed to be for party or political use. These say: "Public servants are asked to provide a wide range of materials including information and advice and facilities to Ministers, and these requests reflect the various roles of Ministers. On many occasions the services provided by public servants might be relevant to a Minister's role as a member of a political party, and will not relate solely to that Minister's portfolio responsibilities within the Government. This is inevitable and completely acceptable under the conventions relating to the role of public servants";
- Public Comment and Use of Official Information;
- Participation in Public Interest Groups, including political parties and unions;
- Financial and other Private Interests, including registration of interests by senior public servants, and acceptance of business appointments on retirement or resignation, outside employment, acceptance of gifts and other benefits, undue influence through financial arrangements; and
- Personal behaviour, including fairness and equity.

I believe that the *Guidelines* provide an invaluable source of information and guidance for officers. However, given the major changes that are taking place in the public service – and the shift in values towards private sector practices, getting more for the dollar and so on – perhaps we need to look at whether the principles on which the *Guidelines* were based are still valid and whether we need also to take into account other wider principles. What in fact should be the guiding principles for public servants today? How can officers reconcile, for instance, the need for fairness and equity (which often cannot be measured in dollar terms) with the pressure to be more "business-like" and obtain greater value for the dollar? These are some of the issues which I believe will need to be addressed.

INVESTIGATION AGENCIES

I shall mention the role of internal and external investigation agencies in detecting fraud.

Many departments which have major revenue collecting roles or substantial benefit programs, or where clients may be prepared to pay bribes for favourable treatment – and therefore major potential for employee fraud – have established internal investigation units for fraud detection. Because they are part of the department, internal investigators have expert knowledge and understanding of what are invariably complex departmental procedures, legislation, organisational arrangements and the like. In the initial stages, at least, of fraud prevention and detection, internal agencies are particularly well-placed for recognising areas of potential fraud and warning signs. Indeed, the very existence of such units may serve as a disincentive to staff to become involved in fraud.

An external investigation agency such as the Australian Federal Police, on the other hand, has wider knowledge across the system and is better placed to recognise and investigate fraud spanning a number of agencies. An external agency is also in a position to form an overview of the

extent of fraud and to identify any emerging trends or new techniques – particularly if organised crime is involved.

Clearly both internal and external agencies have an important role to play in fraud detection and investigation in the Service. It is essential that there be continuing and efficient liaison amongst such agencies, so that sophisticated fraud cutting across departmental barriers does not go undetected and so that wider trends can be detected.

MANAGEMENT/SUPERVISION

A discussion about checks and balances would not be complete without some reference to the role of managers and supervisors. It is the responsibility of managers and supervisors to make sure that staff are aware of and familiar with relevant legislation, required standards, departmental procedures and instructions. They are responsible for monitoring the work of their units and checking, or instituting procedures for checking that work is carried out and standards are maintained. They also have primary responsibility for counselling where staff fall short of required standards.

In view of their close day to day contact with their staff, supervisors are in a position to influence and shape the attitudes of staff. They can play a positive role by firmly instilling in their staff the notion that fraud is not something that they should tolerate or ignore amongst their co-workers. Staff becoming aware of fraud have an individual responsibility to speak out and notify their supervisors. Supervisors in turn have a duty to take corrective action, including reporting to appropriate authorities.

THE COMMISSION'S APPROACH

Finally, I shall outline briefly the ways in which the Commission sees that it can fulfil its role in furthering awareness of ethical issues and promoting ethical conduct in the public service.

Promoting Ethical Conduct

Promoting ethical conduct can be viewed as two stages:

(1) getting staff to *comply* with a code: telling them what they are required to do or are forbidden to do and hoping that respect for the law will lead them to comply; and

(2) *influencing values:* so that staff share a set of values or norms about how it is proper to conduct oneself at work, having regard to duties to the Commonwealth as employer, to clients and to other staff.

The first stage can be addressed fairly readily by means of training and familiarisation of staff with relevant legislation, instructions and the like.

The second stage, however, is more difficult. Traditional modes of training are not sufficient to change ethical attitudes. Staff involvement in organisational values and culture is, however, likely to be more effective. There may be value in organising seminars or workshops to raise awareness of and to discuss ethical issues in the organisational context. I am aware that at least one department (Community Services & Health) has recently run a two-day workshop on ethics for its staff, which was apparently very well received.

The Commission could for instance organise workshops for Senior Executive staff and encourage departments to co-operate in running workshops/seminars for non-SES staff.

CODE OF ETHICS/GUIDELINES

We believe that there is continued value in having a set of guidelines or code of ethics:

- to provide a frame of reference for behaviour by individual public servants;
- to give a clear indication of commitment by the Commission, as the independent personnel agency for the APS, to uphold a professional ethical posture; and
- to assure the public of the integrity and probity of the public service.

Codes of conduct alone cannot achieve ethical behaviour. Particularly in the present time, however, because of the strains caused by ever-increasing demands and competing values, staff need to be informed as far as possible of what is acceptable and what is not. As individual perceptions and judgments may vary widely, this should not be left to chance.

Codes of conduct alone cannot achieve ethical behaviour. Particularly in the present time, however, because of the strains caused by ever-increasing demands and competing values, staff need to be informed as far as possible of what is acceptable and what is not. As individual perceptions and judgments may vary widely, this should not be left to chance.

CONCLUSION

I have outlined some of the existing checks and balances (other than audit) within the APS which are designed to encourage ethical behaviour and deter fraud, and the approaches the Public Service Commission is considering in this field. I see this forum as providing an excellent opportunity to explore and identify emerging issues in public service ethics. I would welcome any comments or discussion about the issues I have raised.

Some Problems of Police Ethics

Ray Whitrod*

In the 1974 Sir Robert Garran Memorial Oration the then Governor-General, Sir John Kerr, said:

> I believe that there should nowadays be a continuing public debate about ethical questions in relation to public office because such a debate must inevitably bring to the surface precise questions about departures from, or variations in, traditional standards.

The Royal Australian Institute of Public Administration is again offering in Canberra an opportunity for a public discussion about ethics, fraud, and the public service. I am grateful for an opportunity to participate, and hope you will excuse me for concentrating on that aspect I know best – the problems of police ethics.

I realise this is a choice open to most Australians for we all seem to know more about misconduct by the police than by members of other government agencies. This may only mean that corruption elsewhere is better protected from exposure. A recognised authority on police, Lawrence Sherman, says that when police forces are pervasively corrupt, and I suspect we have a couple in that class in this country, such corruption will extend beyond the police to include courts and politicians. The outcome of Queensland's Fitzgerald Inquiry is awaited with interest by many, and with anxiety by an unknown number.

Sir John Kerr's belief that continuing public debate would inevitably bring to the surface precise questions about deviant conduct by government officials has proved to be an over-optimistic one. It is true, however, that some of the fraud, some of the corruption, and some of the unethical conduct by people on the public's payroll, has surfaced and become known to the community.

This knowledge has emerged, not as the direct outcome of any intellectual discussion, but rather as one of the end results of a long and courageous campaign by a few investigative journalists. Among them is Mr Phil Dickey, of the Brisbane *Courier-Mail*, to whom the creation of the Fitzgerald Inquiry owes much.

Mr Dickey is currently in receipt of eight writs for damages, and Mr Andrew Olle of the ABC, has been a similar target for process servers for the same reason. In these circumstances it takes individuals of some courage, even when backed by their employing organisation, to make any sort of public denunciation. In other states, Mr Bob Bottom, of *The Age* tapes fame, has received the same treatment.

* Ray Whitrod has been Commissioner for the Commonwealth Police, the TPNG Police and the Queensland Police Force. Text of an address to the RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, Canberra, 2 May 1988.

No 56, September 1988, 38-41.

A former ALP Federal Minister, Mr Clyde Cameron, is concerned at the smothering effect of our present laws of defamation. A few weeks ago he had this to say:

> It is unfortunate for believers in decency that our defamation laws prevent the safe exposure of corruption in Australia. Under the laws of Britain and the US truth is a complete defence against an action for defamation, but not under Australian laws.
>
> Even so, there have been occasions when a few brave souls have taken the risk of exposing the behaviour of corrupt politicians on both sides. The public is entitled to hear the truth about bribery and corruption.
>
> The Fitzgerald Inquiry proves Australia urgently needs tougher new laws against a person offering or receiving a bribe. We need a law that will give immunity to the first party who exposes the other party to a crime.

And he went on to declare:

> Unless those who are honest rise up and strike down those who are venal, our country will soon match the Philippines and countries like the Philippines, to become the political cesspool of the South Pacific. (*The Advertiser*, 14 March 1988)

There are other obstacles to the public exposure of deviant conduct. Writing in *The Age*, Mr Ian Davis commented that it was a great pity that the public service and the government had combined to restrict the scope of the *Freedom of Information Act* and to abolish the House of Representatives Estimates Committtes (*The Age*, 22 August 1982).

Much of the new information now forthcoming is presumably because of Mr Fitzgerald's ability to give immunity to his witnesses. There are difficulties in obtaining evidence in crimes of prostitution, illegal gaming, drug abuse, and their associated bribery. Both parties to the transaction are beneficiaries, and only the community is a loser. In the case of bribery, both the corruptee and the corrupted have strong motives to keep the transaction secret.

Because of this secrecy a valid estimate of the extent of official wrong-doing is hard to come by. Only now are police anti-corruption units starting to identify the available indicators and to record their trends.

In any case, corruption, and especially police corruption, is a term used to describe a wide range of unlawful or unethical behaviour. It can range from the almost innocent acceptance of a cup of coffee to complicity in the worst crimes. Perhaps the most useful definition of police corruption is "an act involving the misuse of authority by a police officer in a manner designed to produce personal gain for himself or for others". Obviously not all unlawful activity by a police officer is covered by this definition. A

police officer may murder his spouse, may shoplift, may do a number of illegal acts, but they do not come within the definition.

As students of public administration well know, all bureaucracies have their advantages and their defects. Police forces are a class of bureaucratic organisation, designed on a semi-military model, to prevent crime and to maintain order. I mention the organisational aspect early because some observers claim it is the unique form of police organisation that makes its officers so vulnerable to corruption. These observers believe it is because a police force is composed of ordinary people encountering extraordinary temptations under conditions of remote supervision. I suppose the recent capture of heroin worth $80M illustrates the extraordinary temptation aspect.

Sociologists, psychologists, and management experts all offer differing explanations: unsuitable recruits, faulty training, low pay and status, personality defects, political interference, weak leadership, lack of professional standards, the community's demand for illegal services, and the pressure of police peer groups.

James Q Wilson's approach is helpful. He divides police forces into three categories of administrative philosophy – legalistic, service, or watchman style. This last category describes those forces with low entrance qualifications, minimum training at the recruit level, and little in-service follow-up. Learning therefore is by apprenticeship on the job. Officers are not encouraged to seek higher education. Promotion is by seniority.

Under the watchman style police officers emphasise order maintenance over law enforcement, and the seriousness of breaches is gauged less by what the law says about them than by their immediate and personal consequences. The Queensland Police Force fitted this category more closely than the other two, that is, the legalistic or service styles.

Wilson goes on to explain that there is a corresponding political ethos adopted by some governments which attaches a relatively high value to favours, personal loyalty and private gain, and a relatively low value to impersonal efficiency and probity.

A senior public servant told me, shortly after my arrival in Brisbane, that the overriding ethic in government was "loyalty". When I asked him what that meant in practice, he said "the Minister always gets what he wants".

This is a dictum that may well be most appropriate for public service departments generally, but for police commissioners it presents problems. Loyalty is an ethic that can determine decisions at the administrative level on many occasions without any suggestion of improper practice, but in law-enforcement activities the requirement for probity cancels out any claims for favours, personal gain, or personal preferences.

Luckily I had the friendship and support of my Minister, Mr Max Hodges, for most of my term in office. He shared my understanding of what were correct responses, and until he was moved from that position for defending my actions, provided me with protection.

However, members of the Queensland Police Force could not fail to see that the sun shone more kindly on all "loyal" folk, while "disloyal" persons kept receiving set-backs of one sort or another. They would also have noted that the practice of this principle failed to incite much criticism from the community. Whether this silence was due to acquiescence, timidity, or apathy, I do not know.

It was under these conditions that I began to implement reforms which had been recommended by Brigadier McKenna and accepted by the Government. I was aware there had been some corruption uncovered earlier, but I was never given any account of the massive network of SP bookmakers who paid an annual fee to the former commissioner of around $2M (in 1967 values).

The large proportion of officers in the middle ranges do not perceive themselves dishonest or otherwise corrupt, and, speaking generally, any unethical activities they participate in can easily be classed as trivial. It is thought that many will not proceed further. On the other hand, there is a school of thought which suggests that the first free cup of coffee or schooner of beer is the first step down a steep decline.

In 1969 there was no manual of operations available to new police chiefs imported to clean up a scandal. Most police chiefs still regarded cases of police corruption as merely the actions of a few individual "bad apples" in a barrel of good ones. Their remedial action was usually confined to questioning the named suspects, perhaps charging them in those rare cases where the evidence was forthcoming, or more likely, just putting the squeeze on them to leave the Force by voluntary resignation.

About this time there were a number of police departments coming under new chiefs because of public scandals. Among these were the Chicago Force which was being sanitised by Orlando Wilson, a highly qualified and experienced administrator; the Kansas City Police Department was in the hands of Clarence Kelley, who later became a much-respected head of the FBI; and, in England, another outsider, Robert Mark, was trying to overcome corruption at New Scotland Yard.

The four of us, independently, developed similar campaigns: purge the detective branch, especially the vice and related squads for they were major sources of corruption, insist on rotation of duties, implement promotion by merit, introduce an effective examination scheme, raise the general educational standards, minimise any political influence on internal administration and day to day operations, improve the quality of recruits, encourage a force *esprit de corps*, transfer the incompetent, and get rid of corrupted officers.

The outcome varied from force to force. There were failures in London, Chicago and Queensland, and success in

Kansas City. The crucial factors appear to be the degree of support received from the political apparatus, the community's level of tolerance or corrupt activities, the length of tenure of the new chief, the intensity and perseverance of police union opposition, and the development of pride in the force and personal integrity.

The average American reform police chief seems to last about two years before the former corrupt network secures his removal and achieves his replacement by their nominee. Orlando Wilson, as I have noted, an exceptional man, lasted seven years, Mark, five years, and I retired after seven years. After twelve years in Kansas City Chief Kelley reported his force was clean. Kansas City Police Department is a small urban force of 1500, highly concentrated. Queensland has a much larger force spread over an area, 1000 miles by 1000 miles, and personal contact was much more difficult.

The five crucial factors just mentioned can be influenced by the police commissioner in varying degrees. Probably he can affect the community's level of tolerance of corruption least of all. On the other hand it is possible for him to be able to achieve much progress in developing a source of pride in membership of the force, and increasing personal integrity.

Mark's Internal Investigations Unit at the Metropolitan Police produced great results, and was a device which was later followed by Australian commissioners. I chose to install a Crime Intelligence Unit, the first of its kind, because I think a pro-active approach is needed. The internal investigation units, together with the police complaints tribunal, tend to await complaints. In more recent times there have been government-appointed inquiries and national crime investigations to help uncover corruption.

Police administrators well know the effect on their force's morale when there is a public exposé of graft or bribery or any one of the other forms of corruption. From media accounts it often seems that most of the force are corrupt officers, but a more considered assessment usually reveals the number involved to be quite small. One American assessor making an educated guess considered that in some forces regarded as being among the worst, there would be only 15 percent corrupt, 15 percent completely honest, and the main bulk stretched from mainly honest to sometime corrupt.

I can offer only a similar guess, but my figures would be much lower. Possibly up to 1 percent who, from time to time, engage in serious crime, and another 9 percent who benefit regularly from other unlawful activities in lesser or larger amounts. At the other end of the scale I would think 5 percent would cover those who are absolutely honest – that is, by my rather puritanical standards which prohibit, for example, the free use of the office phone or the photocopier, for personal reasons.

The large proportion of officers in the middle ranges do not perceive themselves dishonest or otherwise corrupt, and, speaking generally, any unethical activities they participate in can easily be classed as trivial. It is thought that many will not proceed further. On the other hand, there is a school of thought which suggests that the first free cup of coffee or schooner of beer is the first step down a steep decline.

As far as I know there has been very little research carried out on the moral career of a police officer. All that there is, is some anecdotal material and some guessing. Many departments now produce a career plan, at least for those with potential for supervisory rank, but this concentrates on the officer's professional skills and experiences.

Police recruits are required to adapt to a new code of ethics when they enter the police culture. Indeed they quickly find that there are in fact two such codes, the official and the unofficial. Where the two are in conflict it is usually resolved in favour of the latter. The long hours spent in the company of a more experienced officer encourage the acceptance of the traditional values as opposed to those taught at the police school.

Police operate in a world of opportunity, good and bad, secrecy, and isolation shared only with their peers. Supervision is necessarily sporadic, and so the police officer is a difficult person to control. Powerful pressures drive the police together. They share the risks and the dangers, the frustrations and the small triumphs. They quickly learn to depend upon each other. These all create strong peer group influences and loyalty to each other. It becomes exceedingly difficult to persuade one officer to testify against another. Astute police union executives exploit this situation in their opposition to reforms.

But the recruitment of more intelligent, better educated men and women into our forces, and improved training techniques and objectives, is producing a corps of younger officers with the capacity to question and reappraise the long accepted group values. To that extent the peer group pressure is reduced. But it takes time. In Queensland, by 1976, we had reached a female component of 10 percent . . . the highest in the western world. Yet the old guard set of values remained largely unchallenged except for a few exceptional women officers who were prepared to buck the system. It may have been my fault in that I did not have enough time to give to their personal development, and they had no role model to follow.

It is only within the last two decades that police chiefs have begun to accept that it is just as important to catch the police officer who is protecting the drugpusher, as it is to catch the pusher. Some of us would argue that it is more important. Some administrators even consider that corruption in the criminal justice system is capable of inflicting more damage to the social system and our quality of living than drug abuse.

Two strategies are being followed by some forces. The first is to identify and penalise those officers who are corrupt, with a flow-on benefit of deterring others from participating in similar practices. The second is to try to reinforce each officer's resistance to temptation by strengthening their moral code of behaviour.

Most Australian forces, if not all, now have internal investigation units whose responsibilities seem largely to be reactive in response to complaints. In Victoria, where there are over 40 officers attached to Internal Affairs, there is a smaller section contained within it whose duties are titled "security". This appears to have some anti-corruption duties.

In South Australia Commissioner Hunt has established a unit with the title "the policy audit" whose objective is understood to be to prevent corruption and improper practices. Among its tasks is to identify potential corruptive influences in the community and recommend to the commissioner ways of combatting them.

In New South Wales Commissioner Avery has placed greater accountability on each of his commanders to suppress corruption. And, in addition, the new government has decided to set up a replica of the highly successful Hong Kong anti-corruption unit. In Hong Kong the local police union was sufficiently powerful to insist that the new unit should not have any authority to pursue its enquiries retrospectively.

The wealth of information about corruption by both officers and community members which has been produced in recent times by various royal commissions and other enquiries has been a demonstration of what is available if the investigative strategies are widened. I suspect that internal investigation units are careful to adopt programs which would be largely acceptable to their critics. But if police corruption is a serious crime, then surely all lawful methods normally used in serious crime investigations should apply. Dishonest officers have been caught and "turned around" so that they provide evidence against the network; paid citizen informants deserve consideration; police recruits who volunteer to report on any corrupt practices when they are posted to units "at risk" have worked successfully in New York; and the possibility of telephone interception and bank account surveillance could be utilised in special cases. As far as I know, there has been no evaluation of these units, at least, made public.

The other approach is to strengthen the internal resolve of each officer not to become corrupt. Again, as far as I know, there has been no systematic plan introduced in any Australian force, and there does not seem to be the resources available to do it. Departmental psychologists and chaplains to whom I have spoken are unaware of the possibility; some were uncertain as to whether the responsibility came within their jurisdiction.

Reiss has pointed out that there are ample opportunities for corruption by all officers. They are, to a large extent, exempt from law enforcement. This fact, combined with the pressures on an officer to deviate in many situations, make each crime opportunity for him a more likely criminal event. Reiss goes on to say: "The question is not what makes officers violate the law but what protects officers from deviating more often than we have observed?"

Perhaps Sergeant Durk has part of the answer. Durk worked with Serpico to expose the large scale corruption in the New York Police Department. It took the pair five years of bitterness and courage. When asked why, Durk said, "for me, being a cop means believing in the rule of law. It means believing in a system of government that makes fair and just rules and then enforces them."

My closing comment is . . . what is police corruption? It is the sacrifice of the public good for the sake of private gain. A cynical journalist publicly described my aim of reforming the Queensland force as naive because selfishness would always triumph over altruism. I happen to accept that we are born with a selfish trait, but that we can learn to give others equal consideration. It is possible to change.

My closing comment is . . . what is police corruption? It is the sacrifice of the public good for the sake of private gain.

Police codes of ethics can help in this regard, but we need to give them more than just intellectual assent. They require of us a deep and continuing commitment to their values if they are going to affect our daily behaviour. Police forces have not realised their responsibility to provide the stimulus and the resources to maintain this commitment. Perhaps it is because some of us administrators do not understand that the change may need to start with us.

It seems some of us have not realised that probity in the public service is not a matter of personal choice, but a national necessity. To help bring this about we need to campaign for two things: an even more open press, and for this our defamation laws need reform. Second, the National Crime Authority must have the facilities originally sought, and its crippling shackles removed. I join with Athol Moffitt, the first royal commissioner to investigate organised crime in this country. The time is truly a quarter to midnight.

REFERENCES

Gardiner, John A & David J Olson, *Theft of the City*, Indiana UP, London, 1974.
Goldstein, Herman, *Police Corruption*, Police Foundation, Washington, 1975.
Sherman, Lawrence W, *Police Corruption*, Anchor, New York, 1974.
Wilson, James Q, *Varieties of Police Behaviour*, Harvard, 1968, 1978.

The Importance of Risk Analysis and Management

Barry S Leithhead*

The subject of "Fraud on Government" can be approached from many angles. The orientation of this presentation is:

- The accountability of management to set and achieve specific objectives, with limited resources.
- The need to manage risks, recognising the capability of the organisation to afford some level of retained risks.
- Fraud as a significant risk, a mixture of high and low probabilities, cost impacts and embarassment factors.

Fraud control is regarded as problem *for* management and *of* management (that is, *for* management's attention and action and *of* management techniques and attitudes).

Risk analysis has a broad application across the full range of management's responsibilities. Risk analysis also has a specific application to fraud control.

While the theme of this seminar is "Fraud on *Government*", the application of managing for results, risk analysis and fraud control has equal application to the private sector. Indeed, practical examples can be drawn from the private sector to shorten the learning curve of the public sector.

Organisation life is a kaleidoscope of interactions and interfaces. There are very few simple cause and effect relationships. In a sense it is fortunate that efforts to create a better "control environment" will impact not only on fraud risks but on aspects of economical operations and efficient resource utilisation. My observation is that elements of success (and failure) are related in a complex that is not always recognised or understood.

THE ACCOUNTABILITY OF MANAGEMENT

Managers are responsible for the effective, efficient and economical use of resources in order to accomplish objectives and goals. To do this, public sector managers, at both organisational and functional/program levels, must:

- adopt a sense and practice of "corporacy" that establishes total mission and purpose, creates an identity to which staff can respond positively;
- structure the organisations' mission and purpose into recognisable and achievable "programs", so that group and team energies are directed towards desirable outcomes;
- design the organisation's human and information resources to support and enhance the achievement of objectives;
- evaluate performance so that the prime responsibilities of management for the effective application of resources are achieved.

In this process, managers have the opportunity to create the "control environment" which can actively and almost silently assist the organisation's processes. Three elements are involved:

- *Management attitude* to control, expressed through interest, involvement, policies and procedures.
- *Quality people*, the most valuable and often scarcest of resources. "Quality" of course has both inherent and developed levels of expression. The appropriate application of leadership and training will enhance the quality of performance and control.
- *Monitoring systems*, whether of informal information gathering, active supervision, information systems or an independent performance evaluation function, such as internal audit.

This combination of management attitude, quality people and monitoring systems is vital to control effectiveness, including when applied to fraud exposures.

The control dimension of managing has undergone change in recent years. "Control" is now different, more difficult and generally less in quantity, than previously. To some degree, however, the need for control effectiveness remains unchanged. For example:

(a) The tradition in public sector management has been to centralise authority and decision-making. This relied on a hierarchy of approval with limited release of authority. The current move to devolution places authority and responsibility closer together at the action level. To a degree, devolution improves informed decision-making and makes for more interesting work. But "control deteriorates with distance" and distributed authority occasionally dissipates control.

(b) Layers of clerical work have been removed, for a variety of reasons. The work was an uneconomical use of resources (cost-*in*effective control) and staff limitations removed the available people.

(c) Internal Auditing has changed away from concern with checking compliance with procedures to matters of efficiency and effectiveness of operations.

(d) The demands on managers have multiplied. Often, staff and the community at large do not have the

---

* Barry Leithhead is a consultant in risk analysis and internal auditing, based in Sydney. Text of a paper presented to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

No 56, September 1988, 42-46.

acceptance or tolerance or priorities, *the ethics*, expected in prior years.

These changes to the control framework make the achievement of objectives difficult. Additionally, changes to control influence the incidence of fraud and the ability of organisations to prevent or detect it.

Fraud control is a management responsibility, because *control* is management's responsibility.

In establishing and maintaining an effective, objectives-oriented organisation, management puts in place a system of control to assist the achievement of objectives. The control system which assists the effective, efficient and economic use of resources also prevents those resources from fraudulent use or diversion.

RISK MANAGEMENT

The term "risk management" is traditionally related to insurance.

Many organisations (and individuals) have been happy to pay insurance premiums, provided their claims equalled or exceeded the premium. It was a "honey pot" approach. But this was not in the insurance companies' interest or those insured who did not claim. The outcome was for premiums to rise eventually, often selectively, against those with high claims, until "dollar-swapping" was seen as a pointless exercise.

Sensible managers (and insurers) have recognised that the key to property conservation is to minimise losses through investing the protection. Risk management was the resulting process, which:

- Identified exposures, those conditions which may produce loss.
- Evaluated risk, both for the probability and cost dimensions.
- Established controls, to prevent or minimise the probability of occurrence and the cost effect of a loss.
- Appraised the financial effect of potential risks and the cost of controls, deciding on the levels of investment in control and affordability of retained risk.

Risk management has an application to the whole of management, not just to property conservation or those risks normally regarded as insurable.

When applied in a "management by results" environment, risk management helps to ensure that "the right things happen and the wrong things don't happen", that successes are achieved and failures are avoided. In a football sense, that attack is rewarded and defence prevents the opposition from being rewarded.

Consider a private sector organisation which wants to develop a new product or service. There will be consideration of:

- The market: needs, attitudes, acceptance, pricing.
- Competition: existing strengths, developments, responses.
- Development: design, testing, time, cost.
- Manufacture: facilities, quality, cost, delivery.
- Promotion: direction, effect, pay-off.

A public sector organisation faces most of these challenges in providing new services to their clients, often with less resources available for development, promotion and delivery.

When applied in a "management by results" environment, risk management helps to ensure that "the right things happen and the wrong things don't happen", that successes are achieved and failures are avoided. In a football sense, that attack is rewarded and defence prevents the opposition from being rewarded.

At each stage there are risks to be managed, to help ensure that "the right things happen and the wrong things don't happen".

The traditional, insurance-related risk management approach concerned the protection of assets, to recover from the financial effects of a loss of assets.

The management of business risks, in the product development example above, is principally concerned with protecting the objectives of the organisation from the variety of exposures which may apply. That is, the objective to establish or maintain a particular market position or reputation, to achieve a particular level of sales volume, profit or return on investment.

Business risk management is as easily applied to the aspects of efficiency and economy, as it is to the effectiveness of achieving organisation objectives.

Consider the private sector organisation, developing a new product, requiring to purchase a significant item of material or a service from another organisation. This material (or service) is *vital* to the product, in terms of quality, service life, performance, even the eventual selling price. This sourcing concentration creates an almost dependent relationship, which must be managed carefully to ensure that quality, reliability, cost and supply continuity are satisfactory to the product development and manufacturing processes. These business risks must be managed.

Consider the public sector organisation establishing a new benefit program. Decisions need to be taken on the human resources to be allocated; the number, grades, skills, structure, training etc. Similar decisions need to be taken on information systems, performance measurement, systems

design, data collection, computing resources – mainframe or PC.

Each of these decisions need to be considered from the risk management aspect, to help ensure the appropriate level of efficiency and economy of the program operations.

FRAUD CONTROL

The management of business risks includes managing the fraud risk. It is necessary to:

- *Identify the exposures* which may result in fraud occurring.
- *Evaluate the risks*, both probability and cost, to dimension the problem (and the solution).
- *Establish and evaluate controls* to prevent or minimise the probability of fraud occurring and the cost of the loss.
- *Appraise the costs* of risks and control and decide on the levels of affordability.

Consider the previous examples a little further. With the concentration of the supply source, the competitive pressure on the cost of the material (or service) is diminished. The supplier may fraudulently seek price increases, abetted by a complicit purchasing officer. It may be that a technical specification is biased in favour of the supplier, with encouraged complicity from the client's engineering representative.

With the government benefit program, the quality of staff will influence the effectiveness of determining entitlement for benefits. Sufficient evidence being supplied and the appropriate level of supervisory review will contribute to controlling the risk of fraudulently established entitlements.

The integrity and security of information systems is vital to help ensure the control of the program. Data must be complete, accurate and authorised. Systems must be protected from unauthorised access and amendment.

To some degree, the risk management questions which related to the efficiency and economy of the program staff and information services also apply to fraud control. An apparent saving of resources to improve efficiency/economy may be more than offset by failing to prevent significant fraud. This is the challenge that managers face.

FRAUD RISK ANALYSIS

Risk analysis requires the identification of exposures and the evaluation of risks. In developing a fraud control plan, many departments are regarding risk analysis as the first stage of the total process. Later stages relate to control evaluation and improvement, with consideration for the cost effectiveness of control and the affordability levels of retained risks.

The initial fraud risk analysis allows the subject to be opened up and considered, for awareness to be developed and ideas generated. Information can be collected, shared and compared with an enhanced level of understanding. Some priorities can be established, major items brought forward, minor items deferred.

The starting point for the analysis is exposure identification.

What is exposed?

- *Program objective*. Fraud may threaten the basic purpose of a program. The consequences are severe.
- *Financial transactions*, both inflow and outflow.
- *Assets* of all kinds Money in trust accounts, furniture, equipment, personal computers, information (particularly if confidential).
- *Information System integrity*, particularly where this is the basis of benefits, entitlement or status of some future value.
- *Staff ethics*, particularly in advisory, decision-making and authorising positions.

Where do exposures come from?

- *Internal*, from staff who alone or in collusion, are intent on advancing their personal interests fraudulently.
- *External*, from clients, suppliers or other constituents, who are intent on advancing or protecting their self interests fraudulently, usually by misstating or omitting to state their true position.
- *External/internal*, from clients, suppliers or other constituents, who in collusion with staff, advance or protect self interest fraudulently.

The meat substitution fraud of some years ago illustrates some of the exposures:

- The then Department of Primary Industry had an objective to develop the export orientation of Australia's meat industry. International agreements were negotiated.
- The meat substitution fraud severely damaged Australia's reputation as a reliable supplier of quality meat products.
- Meat exporters who substituted non-beef as beef made (short-term) financial gains.
- Meat inspectors neglected their responsibilities in favour of secret commissions.
- The levy income of the Department was (most likely) *not* understated.

The principal issues from the Department's viewpoint were the impact on an important policy objective and the ethical position concerning staff.

There may be a tendency to concentrate on financial fraud exposures, whether generated from external or internal

sources. This case illustrates the importance of the non-financial fraud, one with limited impact on inflows or outflows, but with a substantial effect on the achievement of objectives. Although such frauds are fortunately rare, the incidence is offset by the overall financial effects on the market.

FRAUD RISK ANALYSIS METHODOLOGY

In my recent consultancy for the Department of Primary Industries & Energy, it was necessary to define relevant terms and adopt a simple but appropriate methodology (see appendix). More importantly, the orientation for the fraud risk analysis was provided by recognising that:

- Fraud control was an additional dimension of program management.
- The risk management approach not only provided a useful, simple methodology but indicated a priority for management attention and cut-off point for management concern. The "indication" is not capable of precise measurement.
- Fraud control was generally not a front line topic of interest or attention, but raising awareness was an important part of the analysis.

An initial classification was made of *inherent* fraud exposures, without regard to the presence or effectiveness of control processes. High fraud risk was indicated by:

- Known fraud incidents against the Department.
- The combination of incentive, opportunity and concealment of fraudulent activity.
- The difficulties in verifying or validating misstated information or otherwise detecting fraudulent activity.
- Diminished standards of ethical behaviour.

Because of the wide and varied range of the Department's activities, there appeared to be a number of different inherent fraud exposures. The fraud risk analysis did not review the effort or effectiveness of the Department's control systems. It was evident, nevertheless, that appropriate management action had been taken on all known or suspected exposures, viz.

- Revenue understatement
- Benefit payment overstatement
- Licencing and registration of premises
- Payments to the States/Northern Territory
- Research grants
- Information confidentiality and integrity

INTERNAL AUDIT AND FRAUD CONTROL

Internal Audit is an independent appraisal function established within an organisation to examine and evaluate its activities as a service to the organisation. The objective of internal auditing is to assist members of the organisation in the effective discharge of their responsibilities.

As part of the organisation's control system, internal auditing can assist management to prevent and detect fraud. While managers must supervise effectively to ensure the quality of work performed under their responsibility, internal auditing is able to monitor and test that delegated authorities are exercised within the limits of management's intention.

No control system gives absolute protection against fraudulent activity. In particular, the actual detection of fraudulent activities is often occasional and fortuitous and not the direct result of supervision or auditing.

No control system gives absolute protection against fraudulent activity. In particular, the actual detection of fraudulent activities is often occasional, and fortuitous and not the direct result of supervision or auditing. However, the exercise of due professional care by internal auditors requires them to be alert to those conditions and activities where irregularities are most likely to occur.

It is important for management to utilise effectively internal auditing, giving proper priority to the allocation of this resource, including to fraud control.

SUMMARY

The Australian Government is giving attention to fraud control to ensure that scarce resources are being properly and equitably applied.

A significant supplementary benefit from fraud control is that the control of other management responsibilities, viz, the effective, efficient and economical use of resources, will also be enhanced.

A simple result from establishing fraud control plans, with high level encouragement and support, is that management attitudes are focussed on control and awareness of fraud exposures is generated. These almost cost-free results have widespread impacts on improving an organisation's control environment.

Risk management is a natural partner of "results management", providing a simple cause-effect analysis, prioritising issues for management attention, on an affordability scale.

Fraud control is an important if unintended element of the Australian Government's Financial Management Improvement Program.

APPENDIX

Definitions

Fraud

A broad description has been adopted to include actions involving deceit which cause:

- any actual or possible financial loss to the Commonwealth, of either inflows or goods or services received for outflows
- undue gain either financial or non-financial by a third party whether directly from Commonwealth resources or otherwise
- loss or unauthorised access to or use of DPIE information
- frustration to the achievement of DPIE objectives.

Fraud Risk

In adopting a broad description and recognising a wide application, the following matrix is a relevant illustration.

	Financial	Non-Financial
Internal		
External		

Fraudulent Actions

- Internal/Financial: Overtime and travel cost overclaiming; converting inflows or outflows for own gain.
- Internal/Non-Financial: Kickbacks, bribes, sale of information, giving advantage to a client or suppliers.
- External/Financial: Levy and subsidy cheating.
- External/Non-Financial: Third party competitive advantage, external frustration to achieving DPIE objectives, fraudulent registration or licensing.
- *Fraud Risk Analysis:* The process by which:
  - fraud exposures are identified. An exposure is a set of hazardous circumstances which may result in a loss due to fraud
  - fraud risks are evaluated. Risk is loss with probability (% chance of occurrence) and financial dimensions.

Fraud Control

Actions taken to reduce or eliminate the probability of occurrence and/or the financial impact of fraud risk.

Often the control processes introduced to contain fraud to acceptable levels also have an effect on waste, efficiency, economy and security.

Fraud Control Plan

The deliberate combination of Fraud Risk Analysis and fraud control together with specific implementation of improved controls and follow-up to ensure effectiveness.

High Fraud Risk, is indicated by:

- known incidents of fraud against DPIE
- the combination of incentive, opportunity and concealment of fraudulent activity
- difficulty to verify or validate misstated information or otherwise detect the incidence of fraudulent activity
- diminished standards of ethical behaviour.

Inherent Fraud Exposure (or Risk)

The underlying condition which is identified without considering the type or effectiveness of control necessary to manage the related risk.

Ethics and the Control of Social Security Payments

Derek Volker*

In talking to social security organisations in other countries, it is striking how similar many of the issues are in the policy and administrative areas. What may be seen as a particularly Australian phenomenon of welfare fraud and welfare cheating or whatever term is used is, in fact, present on at least the same scale in other countries.

There has not been much effort put into analysing why increasing numbers of overpayments arise in social security systems and as to why there seem to be variations in attitudes towards compliance with legislation and procedures. The reaction usually is to adopt a pejorative approach, talking about "welfare fraud", "welfare cheats" and "dole bludgers" as if there are some deficiencies in the national character or at least in the characters of many citizens which explain why there are blow-outs in the numbers of social security overpayments.

Research is being done by the OECD in this area but it seems opportune for work to be done of a comparative kind about experience in comparable social security systems as well as in Australia. In the Department of Social Security we shall be seeking to find suitable research avenues for studies of this kind covering both behavioural and administrative aspects.

In the longer run, if we can find ways of avoiding patterns of noncompliance with legislation and procedures and administrative mechanisms to encourage compliance from the beginning of sharp changes in economic circumstances, many of the problems which have been seen to arise in terms of social security overpayments may be avoided or at least minimised.

We make a mistake if we believe that social security legislation and policy are always clear and precise. There are some extremely difficult and complicated areas of decision making in the social security area where judgments and discretion are necessary. Examples are in applying the work test for the Unemployment Benefit and even more so in the area of personal relationships associated with the Supporting Parent Benefit. What are sometimes listed statistically under the general heading of overpayments and may be seen or referred to as "welfare cheating" or even "welfare fraud" turn out, on closer examination, to be concerned with matters of judgment about relationships.

In some instances, the same set of circumstances could well be interpreted differently by different delegates. This should sound a warning in interpreting statistics about overpayments, particularly where sweeping comments are made about the extent of welfare fraud based simply on the level of overpayments detected. The real position with welfare fraud is more difficult to determine. It is enough at this stage to say that welfare fraud comprises only a very small proportion of the number of incorrect payments made. Moreover, the amount of overpayments represents only a very small proportion of total expenditure in the portfolio.

It is enough at this stage to say that welfare fraud comprises only a very small proportion of the number of incorrect payments made. Moreover, the amount of overpayments represents only a very small proportion of total expenditure in the portfolio.

THE SCALE OF DSS OPERATIONS

By any Australian standards DSS is a large and complex operation providing services and payments which affect the lives of a large number of Australians.

The Department administers 13 different forms of payment under the Social Security Act with a total program expenditure of $17.0 billion. It makes 15 different forms of payment on behalf of other agencies and other countries with total expenditure of $1.2 billion.

There are 2 million people receiving pension payments of one form or another, about 600,000 people receiving unemployment, sickness or special benefit payments, and just under 2 million families receiving family allowance payments. We are also paying family allowance supplement for about 400,000 children of working families.

SOCIAL SECURITY ADMINISTRATION

The main elements of the Department's administrative structure are:

- A Central Office in Canberra responsible for direction, policy, systems and procedural developments and management.
- State administrations in the seven State/territorial capital cities responsible for operational direction and management of service delivery.
- A new group of 20 area offices reporting to State offices, and supporting/supervising regional offices.

* Derek Volker is Secretary, Department of Social Security. Paper read to the 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, 2 May 1988.

CB PA *No 56, September 1988, 47-52.*

- 220 regional offices providing service delivery facilities and undertaking the bulk of clerical processing tasks. The average staffing level of a regional office is 60 to 70 people, with variation depending on local workloads.

We are currently in the middle of a comprehensive review of that structure, the main objective being a devolution of responsibilities from the Central and State administrations to area and regional offices. This will emphasise our aim to keep responsibility and accountability closely joined rather than separated as can happen in large organisations.

The Department's claims processing system is a blend of traditional document processing and storage and the use of ADP technology. Payment is claimed by completing a standard form and providing specified documents which provide basic substantiation of eligibility. These are stored on one or more personal paper files for each client, together with records of decisions made, results of reviews of those decisions, enquiries and other administrative actions. Some information from the documents is also stored in the Department's ADP system.

Decisions on program payments are made under delegations by the Secretary authorising staff to exercise secretary powers under the Social Security Act. Most decisions to grant or refuse a pension, benefit or allowance and to raise an overpayment are made in regional offices. Reviews of decisions are made in regions and by more senior staff in area and State offices and in Canberra. Delegations to waive or write off recovery of an overpayment of pension, benefit or allowance are available at the regional, State and central office levels. Most such decisions are made in regional offices.

Decisions are implemented by data entry of an ADP transaction which authorises payment by direct credit to a financial institution or, in a very few cases (about 5 percent), of a cheque. A number of staff are required to be involved in claims processing from receipt of an application through to payment. This provides a form of safeguard against fraud.

Delegations and procedures applying to administrative expenditure (for example, salaries, travel, purchasing) broadly parallel those for program expenditure, subject to the public service-wide requirements set out in the Audit Act and the Finance Regulations. The direction of change in the Department and in the public service generally is towards devolution of decision making to areas and regions and towards more extensive use of ADP technology in information storage, decision making, accountability and management information.

The Department relies heavily on computer technology. It operates an ADP system in which 8 large mainframe computers, housed in computer centres in Canberra and State capitals, control a distributed ADP network consisting of some 250 mini-computers linked to about 8500 terminals located in regional offices and in all other major locations. The ADP system stores client and payment information for most programs, calculates the amount to be paid for some and is used to control payment, in most cases by direct credit.

The relative importance of paper documentation in the Department will decrease with the introduction, over the next two years, of a system of "on-line benefits processing". Under this system, clients will still have to complete application forms and provide supporting documentation, but staff making decisions will work with information stored in the ADP system rather than on a paper file. Decisions will be made at an ADP terminal and recorded directly into the system at that time.

REVIEW AND CONTROL

The DSS charter is –

> To deliver social security with fairness, courtesy and efficiency.

There are strong social justice implications in those words; implications which require us to recognise the Australian tradition of helping those in need and to do it in such a way as to uphold the dignity of people and recognise that the vast majority of clients are honest.

That does not mean that we should remain oblivious to the reality that some people will seek payments (or larger payments) to which they are not entitled. To ignore that would be to abrogate the duty which is imposed on the public service by the community. It expects the public service to administer the laws of the Parliament in a balanced way, meeting the objectives of the particular program but also protecting the interests of the population at large, particularly as far as accountability for expenditure is concerned.

There is a recognisable public interest in adopting mechanisms which ensure that government payments and services go only to those entitled to receive them. That indeed can be seen as one of the elements in social justice.

The task is to make sure always that the systems and procedures we use are the most accessible and effective available, given the environment and pressures which may exist, and that they are supported as such by the community and its representatives.

Large administrative systems take a long time to change and that is a feature which applies as much to private enterprise as it does to the public sector. While the need for change may be recognised, agreements on the substance of the change and on the implementation of new strategies may not be forthcoming so quickly, particularly if the environment keeps changing.

An example can be drawn from the history of the Department of Social Security. It faced a substantial increase in the number of people receiving Unemployment Benefit in Australia between the years 1974 and 1979. There was nearly a ten fold increase. There were 32,000 people being paid Unemployment Benefit in June 1974 and 312,000 in June 1979.

The increase occurred because of the deterioration of the labour market. The effect on the Department was dramatic. In recognition of the need to check the correctness of payments periodically, the Department regularly used to review the circumstances of every one of its unemployment benefit clients. It was what we would now call a saturation review process.

Such reviews became less practicable, and then impracticable, as numbers rose and economic circumstances made checking eligibility, including work testing, a more demanding task.

With the benefit of hindsight, people could say that it was unwise to continue with that approach. But, while there were numerous predictions about the likely peak of unemployment in Australia, there was no certainty that numbers would continue to rise. In this environment, it was not clear which procedure would be the most effective. So the review arrangements in use at the time were retained and it was not until the late 1970s that intolerable pressures on resources made it obvious that a much more cost-effective approach had to be found.

A similar situation occurred in relation to Supporting Parent Benefit clients with the number of persons receiving that payment also rising.

The search for a better way of handling reviews of client eligibility and entitlement led to the development of a risk-based methodology. Reviews are now directed towards groups of clients where there is believed to be a higher than average risk of incorrect payment. It is a very successful way of using resources because it keeps unproductive work to a minimum. It also allows the great majority of the Department's clients, who are honest, to go about their daily business without being interrupted on the off-chance that their payments may be incorrect. But I am jumping ahead of the story.

As the risk-based methodology was tested in the early 1980s, it became obvious that the continuing increase in the number of people claiming Unemployment Benefit included some who, at one point or another, were being incorrectly paid because they did not advise the Department of changes in their circumstances. It was a relatively small group but it had the potential to increase if something was not done. Included in that group was a smaller number whose activities involved fraud.

This situation had arisen because of the continuing pressures on the administrative arrangements of the time. For example, the annual number of new claims for Unemployment Benefit rose from 229,000 in 1973/74 to 810,000 by 1978/79 – nearly a four-fold increase. The constant review activity which might have identified changes in circumstances had been scaled down because most staff were working on processing claims and there was no other review system to replace them. It is a sort of natural law of resource availability that in times of economic stringency staff restrictions have the greatest effect on those areas where blowouts in expenditure are most likely.

Some people used the opportunity presented by these pressures to present false documents to the Department, hoping they would pass unnoticed. Some were detected but others were not.

What had become obvious was that if there are pressures on administrative systems which lead to a reduction in emphasis on accountability aspects, in favour of allowing available resources to concentrate on the main objective of the agency – paying pensions and benefits – there will be incorrect payments in those systems. Part of that incorrectness will be the result of fraud, whether perpetrated by external or internal sources. In such circumstances, the word soon gets around that there are gaps in the administrative system and the problem of incorrect payments is compounded.

Many of you will now be thinking that the solution is to provide more resources. I do not believe that is the nub of the solution. If those in DSS had gone to the Government with pleas for resources to handle the potential incorrect payment problem, it would have been an invitation for severe criticism about failure to accept accountability for what now amounts to over one-fifth of Commonwealth outlays.

We have sought staff for specific initiatives or projects from time to time. But we have also done a great deal of work on our own, refining the administrative processes. Our approach has been two-fold – to look at the whole administrative process – program admission requirements, administration of claims while they are in payment, and client reviews and, second, to have it understood that solutions lie in the acceptance of responsibility by everyone associated with the delivery of client services in all elements of the department.

It is a sort of natural law of resource availability that in times of economic stringency staff restrictions have the greatest effect on those areas where blowouts in expenditure are most likely.

The process starts at the point of lodging a claim for a benefit or pension. Re-designed claim forms have improved the quality of documentation completed by claimants. The new forms allow "streaming" of clients into those who require a comprehensive interview because of the nature of their claim and those who require a less detailed interview because the Department already knows their circumstances. A new information package designed to give clients more information about the payment process is part of the new procedures. The package includes general information about payments, preparing for an interview, and client rights and obligations.

Admission arrangements direct a good deal of attention to proof of identity. The procedures require clients to produce three documents from a list of those acceptable. The procedure is flexible enough to help people who have genuine problems in establishing their identity while deterring or detecting those who might otherwise be tempted to make false claims. Where staff in regional offices believe that the identity documentation might not be legitimate, the case is referred to the benefits control area. Because of their skills and abilities in computer analysis the staff in benefits control can examine the material to check whether the particular claimant is being paid in another place under another name.

The admission procedures also include a requirement for claimants to provide evidence of eligibility for the particular type of payment being sought. In the case of

unemployment benefit, for example, the department now requires presentation of an Employment Separation Certificate. Those documents are supplied to employers in bulk, in conjunction with group certificates, the intention being that employers will see the filling in of both items as part of the employee separation process. It also allows them to share in the community responsibility to prevent incorrect social security payments.

For employees, the certificate is the evidence they need to prove eligibility for payment of unemployment benefit, that is, that their employment has been ended for reasons outside their control. Voluntary termination of employment incurs a postponement of payment of Unemployment Benefit.

For the Department of Social Security, the employment separation certificate is a key document in considering the legitimacy of the claim and the details are recorded on computers. Given that the certificates are supplied independently to employers, in conjunction with the Australian Taxation Office issue of group certificates, and given that the issue details are recorded, the authenticity of any individual certificate can be checked when suspicions are aroused about a particular claim.

I want to emphasise that we do not rely just on suspicions being aroused. We are also able to compare periodically the details of all the certificates presented by claimants to ensure that we detect cases of abuse which might not have been obvious at the time an individual claim was accepted at one of the Department's regional office counters.

The second point of emphasis in the arrangements for dealing with possible fraudulent behaviour is the processing of the claim over the period payments are made. Again the Unemployment Benefit program is a useful example.

There is now a requirement in the Social Security Act that, to be eligible for payment of Unemployment Benefit, a person must be continuously registered for work with the Commonwealth Employment Service. That status is checked regularly by DSS and close liaison between both agencies ensures that the CES records and ours stay "in kilter" as much as possible. It has to be recognised, however, that differences will creep in from time to time. To make sure they do not permanently negate the effectiveness of the liaison, we match the records of both agencies when we think it is necessary.

As long as an Unemployment Benefit recipient continues to receive payment he/she is also required to lodge what we call continuing income statements at a DSS office personally each fortnight. The statements are required to indicate whether there has been any change in the person's income or other circumstances during the preceding two weeks.

The Department needs to know these things because they can affect the amount the person will be paid in the following fortnight. Lodgement in person is required. To do otherwise would provide opportunities for clients to work (even full-time) while on benefit payments, or to adopt false identities in the knowledge that they would not be found out because the person was not required to go anywhere near an office other than at the time of making the claim. Our regional offices can conduct signature checks when those continuing income statements are being lodged to ensure that the people presenting them are in fact who they claim to be.

The measures I have outlined are just a few of the steps which have been taken to close off the opportunities for incorrect payments and fraudulent behaviour. In adopting them the Government has made a clear statement that it will not tolerate abuse of welfare programs.

Perhaps the most complex work we have done in this area is the development of a risk-based methodology for reviews of client eligibility and entitlement.

We try to have clients tell us about changes in circumstances as they occur. This ensures that continuing payments are correct. This objective is often difficult to achieve because clients do not always meet their responsibilities, either unwittingly or deliberately. So we set out to develop an approach to the review of individual client entitlement to help staff to know where to look for incorrect payments. Without this approach, there would have to be many more staff checking cases on the off-chance that payments might be wrong.

The basis of our checking work is the characteristics of groups of clients who have a higher than average risk of incorrect payment. We work out what those characteristics are by doing statistically accurate surveys of the particular benefit or pension population. These involve detailed interviews with the clients selected for the survey to establish that the payments they are receiving are correct, given their current circumstances.

All the answers given during the survey are validated and at the end of the project we know the characteristics of the clients in the survey group who are being paid incorrectly. Our statisticians convert those characteristics to a formula – we call it an algorithm. That algorithm is applied, on a weekly basis, to the recorded circumstances of all clients receiving that type of benefit or pension payment.

The recipients whose circumstances meet the algorithm test are selected for a review of their payments. Reviews are done by letter or personal interview.

We also randomly select cases for review. This means that no one can deliberately arrange an incorrect payment in the knowledge that they can avoid the case being checked.

Because the Department uses risk analysis to select clients for review of their circumstances, resources are not wasted on unproductive checking work. Consequently, we achieve the best possible distribution of staff across all the things for which the Department is responsible.

The arrangements I have just outlined deal effectively with the client reviews of eligibility and entitlement. They are a successful method for handling the responsibility which the Department has to demonstrate accountability for the funds under its control.

We do some other things. Among our clients are some people who have constructed fraudulent schemes which incorporate a variety of lies to make it appear that the claimants are eligible for payment. The computer analysis

expertise which has been developed in the Department is able to detect such schemes, some of them having successfully avoided earlier efforts to find them. Continuous high speed computer matching facilities enable analysts to turn DSS computer files in on each other to find the records which are part of a scheme to defraud the Commonwealth.

For obvious reasons, these cases are handed over to the police for investigation. You will have noticed media reports as arrests were made and court hearings commenced. The Department receives excellent co-operation from the police as it does from the Office of the Director of Public Prosecutions. Our relationship with both those agencies is an excellent example of effective liaison on law enforcement matters.

THE RESULTS

The effectiveness of the Department's detection facilities can be judged from prosecution results. As at June 1987 prosecutions under the Crimes Act for social security offences had increased by 76 percent over a two year period. There was a 160 per cent increase over the same period in cases prosecuted where the overpayment amount exceeded $30,000.

Prosecutions for individual people who commit offences against the Social Security Act are continuing at approximately the same level as last year, but there has been an increase in the number of sentences involving gaol terms either to be served or suspended.

Lest it be thought that highly selective reviews of eligibility have merely led to our identifying a great deal of debt which we have no hope of recovering, it is worth mentioning that, because of steps we have taken to recover overpayments, the collections this year show an increase of $12 million over the figure at the same time last year.

Risk analysis has helped the Department to direct the government's accountability measures in the Social Security portfolio to those types of cases where they have the most effect. As well as the direct effects, that is, detecting incorrect payments, there is an indirect deterrent effect. The overall result has been a rise in the extent of voluntary compliance. I shall return to that.

The task has not been an easy one and it will continue to receive constant attention. Many of you will already be aware that there are going to be reductions in resource numbers in Social Security over the next four years but our staff are aware that the success of our efforts on accountability matters will not be allowed to dissipate through reduced attention to correctness.

If that sounds like self-congratulation it is because I believe the Department of Social Security has achieved a great deal. The risk-based methodology is being applied to admission procedures as well as to client reviews and has been refined to the point where those who cheat with social security payments have a much greater chance of being caught than ever before.

Every aspect of the review process has been given attention even to the point of re-designing the forms our field officers use when they are interviewing clients in their homes. Staff training has been a very important element.

It has been an evolutionary process, designed to raise the level of voluntary compliance among social security clients. There are two reasons for wanting to do this. First, encouraging people to "jump the wall" into employment provides economic benefit to the people themselves and to the country as a whole through the best possible take-up rate of available jobs. Second, through proper administration of income support programs and accurate identification of people being paid incorrectly, the Department can maintain a proper allocation of resources to checking work. There is a responsibility to provide sufficient opportunities for people to advise changes of circumstances so that the effectiveness of the risk-based approach as a stimulus to voluntary compliance is not nullified.

There is some fraud on DSS programs. Most of the incorrect payments encountered by the Department of Social Security are not fraud but, for those which are, DSS has developed and refined methodologies to deal with them. There are no special secrets about how to tackle the problem, just plain hard work, some common sense, some committed people with the right expertise and ADP systems and, above all, committed staff at all levels.

Perhaps the best measure of success for these efforts has been the outcome of the measures adopted in the 1986 and 1987 budgets and the 1987 May Economic Statement. You will recall that there were many items in those packages which related to social security administration. In March 1988 there were approximately 100,000 fewer people receiving unemployment benefit than at the same time last year and, for obvious reasons, we have monitored the reduction so we know which steps were effective. We know that most of them were successful but there are no individual figures available because they do not lend themselves easily to measurement. There are some for which we do have such results. In the Unemployment Benefit program, they include initiatives directly concerned with reviews of client eligibility and entitlement such as the introduction of mobile review teams. Where suitable, these processes were introduced using the risk-based methodology referred to earlier.

We also have data on the labour market and on participation rates. That information tells us that there have been improvements in the labour market. When we take into account all the data we have on the effects of the measures and labour market changes, we are left with a significant proportion of the drop in numbers which cannot be explained thereby. It seems reasonable to attribute this gap to a rise in the level of voluntary compliance on the part of

unemployment benefit clients generally, that is, both old and new.

The success of applying specially selected measures, including the risk-based methodology, and a proper balance of resources to the problem of incorrect payment is shown by the reduction of 100,000 in the number of persons receiving unemployment benefit. A crucial point is that the evidence available suggests that overwhelmingly those going off unemployment benefit have gone into employment. This applies also to school leavers on the new job search allowance (JSA). The only logical explanation for the reduction in the number on JSA in recent weeks is that the young people concerned are obtaining jobs.

FINAL COMMENTS

There is some fraud on DSS programs. Most of the incorrect payments encountered by the Department of Social Security are not fraud but, for those which are, DSS has developed and refined methodologies to deal with them. There are no special secrets about how to tackle the problem, just plain hard work, some common sense, some committed people with the right expertise and ADP systems and, above all, committed staff at all levels.

I believe that our overall result is good. The process of obtaining social security payments is still reasonably straightforward, prompt and uncomplicated. There is inconvenience, particularly for beneficiaries, in having to lodge continuation forms personally every fortnight and in having to attend interviews at set periods in DSS offices. There can be inconvenience for some people in having review teams interview them at home. Employers have some additional work to do too.

At the same time the chances of getting away with abuse of the social security system are very small and reducing virtually by the month as we improve our risk analysis and matching skills. Indeed, any people thinking about abusing the system should heed the warning that they will almost certainly be caught and face substantial penalties.

I hope that we can find ways of fostering even more voluntary compliance with the law. At the same time we shall pursue our review and matching strategies.

The savings being achieved are contributing to the strengthening of the economy and giving more scope for improvements in benefits and pensions for those who are genuinely in need.

The Changing Shape of Government
in the Asia-Pacific region

John W Langford and K Lorne Brownsey (editors)

Australia • Bangladesh • Canada • Hong Kong • Korea

Malaysia • Singapore • Thailand • United States

Available from RAIPA (ACT Division) — $A34.95 (paper)

Investigating Motor Accident Fraud
A CASE STUDY

Dick Wright*

All organisations involved in the payment or collection of monies will be subject to fraud. History has proven there is a criminal element within society which will systematically develop methods to defraud corporations and governments. No organisation can say it is "fraud proof" and it would be foolish to say so. However, an organisation can significantly reduce the risk of fraud by developing an effective anti-fraud strategy which is relevant to its organisation. Fraud can never be eliminated, but it can be kept under control. In this session, I will talk about the development of such an anti-fraud strategy.

I would like to share some of my experiences in establishing and implementing the Anti-Fraud Strategy for the Transport Accident Commission. What I have to say is relevant to all organisations, both corporate and government, who have as a role the payment or collection of monies.

ENVIRONMENT

It is important to understand the background environment at the time against which the Anti-Fraud Strategy was to be developed. At the time, the Third Party System in Victoria was "haemorrhaging" badly with fraud being estimated as high as 30 percent or in excess of $100 million annually. In the first ten annual reports of the Motor Accidents Board, no mention was made of fraud – this covers from 1974, the year of commencement of the Motor Accidents Board, to 1984. Few claims were being denied and those that were denied, were usually successful on appeal to the Administrative Appeals Tribunal. In one year alone, the incidence of whiplash rose 30 percent. Many staff within the organisation felt frustrated as there appeared little they could do whilst others accepted the process.

Anyone you met in the community usually knew of someone who was taking the third party system for a "ride". The legal community was comfortable with the process, particularly in the processing of common law claims, as huge incomes were to be "made". Legal firms had become specialists in the area. It had the atmosphere of a club. The medical profession was also profiting handsomely and many doctors within the profession had taken an amoral stance. Para-medical services had sprung up rapidly and in one year alone, para-medical payments increased by 100 percent. Payments, when broken up by injury type, showed that demonstrable injuries such as fractures etc accounted for 40 percent of all payments, whilst non-demonstrable injuries such as whiplash etc, the basis of most fraudulent claims, accounted for 60 percent of all payments.

Contrasting strongly with all of this was the fact that registrations of motor vehicles rose consistently on average only 4 percent each year. Such was the environment at the time. Considerable success has been achieved in reversing the process mainly due to three things – strong mangement commitment to solve the problem, combined with an effective Anti-Fraud Strategy, backed up by an effective investigational team.

POLICY PARAMETERS

In approaching the problem, four policy issues were decided:

> Firstly, fraud would be defined as "any claim which was not bona fide", thus payments were to be made only in respect of "bona fide" claims.
>
> Second, the organisation was in no position to pursue past cases of fraud; that is, there is no point in crying over "spilt milk".
>
> Third, the present system was "haemorrhaging" badly and the objective of the exercise was not to adopt a "bandaid" solution but a "permanent healing"; hence it was decided to adopt a pro-active or preventative approach; and
>
> Fourth, the strategy, when put into effect, must not reduce speedy and effective service to bona fide claimants.

The theme of the Anti-Fraud Strategy was to be:

PREVENTION IS BETTER THAN RECOVERY

and its objective was

TO IDENTIFY FRAUDULENT CLAIMS IN THE INITIAL STAGES OF PROCESSING, THUS PREVENTING POTENTIAL FRAUDULENT PAYMENTS.

Such were the broad policy parameters of the strategy. I should point out here that each organisation must develop its own strategy rather than "borrow one".

ANTI-FRAUD STRATEGY

In developing an Anti-Fraud Strategy, five tasks are essential.

Risk analysis/trend analysis

Firstly, an "analysis of risk areas" needs to be carried out. Questions such as:

* Dick Wright is Assistant General Manager, Claims Division (Systems), Transport Accident Commission, Victoria. Text of an address to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CBPA *No 56, September 1988, 53-58.*

- In what areas is the organisation most vulnerable? – that is, high risk areas.
- In what areas is the organisation least vulnerable? – that is, low risk areas.

Policies supported by effective administrative/processing procedures should be developed for each of these areas once identified.

For example, why have the same initial processing procedure for a mild whiplash case as opposed to a case involving a major fracture. A high risk area for the Transport Accident Commission is "whiplash" whilst major fractures are considered to be in the low risk category. Coupled with the analysis of risk areas, a continuing system of trend analysis should be set up for the organisation. The risk analysis is only valid for a period of time and as the environment changes, trends will need to be monitored and, where necessary, appropriate changes made to policy and procedures. For example, "whiplash" has been the phenomenon of the 1980s but, as we move into the 1990s, I fear that "psychiatric problems" will replace "whiplash". A trend analysis would provide an injury profile so that any significant changes within the profile, for example, psychiatric problems would be monitored. This provides the organisation with an opportunity to control the problem before it achieves major proportions.

Global data architecture

Second, a global view (data architecture) of an organisation's information needs to be established. What do I mean? Management of information is a much used term these days. In many large organisations, each area develops its own strategy for managing information and, in most cases, manages it efficiently. However, each area is only one piece in the jigsaw of information. A global view of an organisation's information is one which successfully interconnects all the jigsaw pieces of information from each of the areas to produce a corporate image of the information. This is a major role for the computer to assemble the image. The first requirement in the process is to stand back and identify the jigsaw pieces. Having done that, logically set about interconnecting the jigsaw pieces of information.

Processing review

Third, a review of the administrative processing environment needs to be conducted with the objective being to identify the basic policies to be applied in processing, coupled with any additional processes required as a result of the risk analysis undertaken and the establishment of the corporate global view. The review should result in a discriminatory approach to processing taking place.

Consider this process as it has been applied to the Transport Accident Commission's initial acceptance of a claim. The policy of the Commission requires the following "proofs" to be established before a claim is accepted:

Proof that the accident occurred;

Proof that the applicant was involved;

Proof that the applicant was injured;

Proof of causal link between injury and accident; and

Proof of identity.

This is the policy but the processes required to establish the "proofs" vary as a result of the risk analysis conducted. The risk analysis established high and low risk categories. In all cases of non-demonstrable injury, coupled with minimal damage to the vehicle, the applicant will be contacted and a range of issues discussed. In cases of major injury, this is not necessary.

Policy forum

Fourth, a high level forum for policy-making needs to be established. It should not be left to individuals within the processing environment to make policy decisions "on the fly". This will lead to inconsistency in approach and in time a lack of sense of direction and purpose. A climate perfect for the processing of the fraudulent claim.

Systems audit

Fifth, a complete systems audit needs to be done on the processing environment of the organisation. The audit team, whilst operating independently of the investigations team, should liaise with the investigations team about processes with weaknesses or those which have broken down leading to potential abuse and fraud.

ORGANISING INFORMATION ON THE CORPORATE DATABASE

When organising the Corporate database, that is, the database which will house all the pieces of the jigsaw, consideration should be given to the following questions:

On what basis should the information be organised?

For example, should it reflect a person-based system, a claims-based system etc.

What data should be captured?

For example, do we capture enough information simply to process claims or should we capture additional data which will assist the detection of fraud. Comprehensive data capture is an investment in fraud prevention. Data capture costs are usually high and trade-offs are often made by organisations in this area. Examination of the trade-offs should occur to ensure all essential fraud prevention information is retained. Contrast the Transport Accident Commission's database against the Motor Accidents Board's database. The Motor Accident Board simply recorded enough information to pay claims. Therefore witnesses, passengers were not recorded. In addition, it was claims-based, that is, if a person had five claims, that person would have five person records. Very confusing. The Transport Accident Commission has a person-based system, that is, one person can have five claims etc, but in addition, records all persons involved in an accident, not simply the claimant. The recent example shown on *60 Minutes* is an

illustration of how the payoff in recording additional data might occur.

INVESTIGATIONS

So far I have spoken about the way in which the Commission tightened the administrative processes of the organisation, an essential component in any anti-fraud strategy. No organisation will have a successful anti-fraud strategy without a highly professional and skilled investigations team. The processing environment in most organisations is concerned with number crunching and is not in a position to devote sufficient time to investigate fraud matters. Nor does it have the necessary skills to do so. Prevention and detection of fraud is the role of the investigations team.

Prevention

Any investigational arm of an organisation should concern itself with preventing abuses. It is far better to prevent fraudulent payments from being made than to obtain convictions for past fraud cases where the offender has expended the gains. There is little chance of recovery in these cases. It is my view that an organisation should forget about the "spilt milk" and set about the task of prevention.

Reporting structure

The investigations team must be independent of the processing environment of the organisation and preferably should report directly to the chief executive office of the organisation. This reporting structure allows for control of internal fraud at senior levels.

Pro-active vs reactive within investigations

A pro-active approach allows the Commission to identify the operations of targeted groups and individual persons before such persons can perpetrate the planned fraud against the Commission. This in turn helps the Investigations Branch to organise its resources in a way which will maximise the impact of its *strategic* investigations.

The Commission does not wait until an offence is committed or a fraudulent claim is settled. It is a combination of *pro-active* and *reactive* approaches which have been successful in targeted areas.

INVESTIGATION TECHNIQUE

The organised group

Consider organised groups. Once a claim is received, it is checked to see if it may be connected in any way to an organised fraud pattern or group. It is checked against current identified groups, and to see if it is related to another as yet unidentified group. The claimant is checked, the vehicle, addresses, telephone numbers, virtually all details are relevant at this time, as a link to an organised group, be it a small family grouping or a large social or other grouping may be identified. All factors including medical and legal practitioners, time of accident, location of accident, accident circumstances, persons involved are taken into account.

Once a group has been identified, information is obtained through various sources to provide a background as to the structure and operation of the group. Its leadership, be it a family head, or criminal organisation is identified, and the main principals are immediately targeted. Benefits claims which are identified are denied, that is, payments of benefits are stopped, and common law files are investigated in order to defend such claims in the courts adequately. It has been found that once principals are investigated and their claims defeated at common law, which is the area where they stand to gain the most, their associates also tend to withdraw from their actions.

At this time the actions of associated legal practitioners and medical service providers is also monitored to ascertain if these persons are acting in conjunction with identified targets, or if such persons are committing offences against the Commission in their own right. It also allows for knowledge to be gained as to the operation of the group. During this process an analysis is conducted to establish the group's interrelationship, its membership, and, where possible, the aims and objectives of the group.

Investigations of this type are *strategic* and by nature *pro-active.*

Various tools are used to provide the investigator or solicitor with a clear picture of the group, the target individual, the accident and other information, and the use of a computer flow charting program enables visual presentations to be constructed in a relatively short time.

Group identification

Before an effective investigation into an organised group can be initiated, the group and its structure must be first identified.

The identification of a group can commence from some of the more common areas, but there are many points from which to approach. For example, a common law claim is received containing surveillance reports, various medical reports, interviews with defendants and witnesses. This information is analysed to reveal discrepancies and patterns of behaviour which illustrate fraudulent activity. All persons appearing in this file are checked for related claims, or any involvement in previous or pending claims, as it has been found that at times, the defendant in one matter, is the plaintiff in a seemingly unrelated accident, or indeed the witness. At this time additional claims are identified, and all items of information are collated to reveal any pattern in group activity or structure. Identified groups can vary greatly, from relatively small family groups, to large groups based on proper organisational lines including several hundred members.

It should be noted that whilst we are mainly concerned with claims against the Commission, similar trends or "organised fraud" have been identified involving other welfare agencies. This can include the provision of finance

for the purchase of homes, as well as persons engaging in fraud against the various welfare systems, and fraudulent acts against insurance companies, that is, auto theft, burglaries involving theft of jewellery or similar items, arson of various types.

Why not prosecute the offenders you may say? Where an organisation can prosecute, it should prosecute. However, in the criminal courts, the case must be "proved beyond reasonable doubt" and in many cases it is difficult to obtain the necessary evidence to establish the elements of proof. In the civil courts the case is determined on "the balance of probabilities".

Civil courts

The Transport Accident Commission is taking the fight against "fraud" into the civil courts. Why not prosecute the offenders you may say? Where an organisation can prosecute, it should prosecute. However, in the criminal courts, the case must be "proved beyond reasonable doubt" and in many cases, it is difficult to obtain the necessary evidence to establish the elements of proof. In the civil courts the case is determined on "the balance of probabilities". There is a lower level of proof required in the civil courts. Success in the civil courts has the major added advantage of "preventing or reducing the level of payment" and can indirectly impose a heavy fine on the civil litigant who loses. It also begins to lower "market expectation" within the legal fraternity and the courts provide an excellent forum for media coverage.

INVESTIGATING TEAM

Analysts

The role of the analyst is worthy of discussion. Analysts within the Investigations Branch of the Commission primarily deal with organised fraudulent activity, as seen in group investigations, and as such they identify groups engaged in organised fraud. Information pertaining to offences, activities or plans of persons engaged in fraudulent activities is assessed by the analyst.

The function of the analyst is basically one of crime intelligence.

Consideration should be given to matters of strategic and tactical intelligence.

Strategic intelligence

Strategic intelligence is vitally important and "Within the Investigations Branch, STRATEGIC INTELLIGENCE, allows for an overview of a targeted area. It enables management to allocate resources to combat fraud/prevent fraud, at a higher level . . . it is a PRO-ACTIVE APPROACH, allows for adequate planning and the Commission to combat the criminal/fraudulent activity before it occurs and also assists in the defence of Common Law cases. Requires extensive knowledge of specific criminal areas of activity. Allows for recommendations and changes to be made in other areas, i e Payment Procedures; Medical Treatment; Assessment of Claims".

Tactical intelligence

"Having identified the "ORGANISED GROUP", the Commission now commences to neutralise the specific CRIMINAL activity and the OFFENDERS, i e the Commission now specifically gathers TACTICAL INTELLIGENCE to achieve some of the following aims:

Obtain sufficient information/intelligence to enable the INVESTIGATING TEAM to:

a) Adequately prepare for the defence of an identified Common Law Claim (i e a Common Law Claim which will have a strategic effect);

b) Fully investigate a Fraudulent Claim, i e, a claim where it was the intention of the claimant to obtain (i) a financial advantage; (ii) property (money) by deception; or the claimant has in fact been successful in his fraudulent activity.

c) Adequately prepare for the defence of an identified Commission claim before the Administrative Appeals Tribunal, such claim having been (i) identified and payments denied before any payments were made; (ii) identified and payment then stopped.

At this stage the Commission is more concerned with obtaining INTELLIGENCE to deal with the INDIVIDUAL or SPECIFIC ACTIVITY OF A GROUP, however, INTELLIGENCE obtained at this level will modify the processes at the STRATEGIC and OPERATIONAL level and vice versa."

Investigators

Investigators will generally deal with two types of claim investigation, that is, the one-off matter, or the strategic investigation.

When engaged in a strategic investigation the senior investigator will work in close liaison with the analyst to obtain (i) information for the analysis section; (ii) evidence for the brief. Strategic investigations are co-ordinated with the analyst's role being to advise the investigators on areas of further enquiry, tactical target selection and tactics to achieve the maximum effect against an organised group. A close team approach is used at this level of investigation, which has similarities to a task force approach.

Investigators work in teams under the direction of a Senior Investigator who is responsible to the division's Chief Investigator.

LAWYERS

Lawyers are primarily concerned with two areas within this division:

(i) Prosecution Branch which undertakes the prosecution of persons charged with criminal offences, and which also makes recommendations with a view to changes to legislation.

(ii) Defendant Panel Solicitors who act for the Transport Accident Commission in the defence of claims before the County or Supreme Court, or the Administrative Appeals Tribunal.

INVESTIGATIVE COMPUTER SYSTEMS

Most investigation areas I have visited usually have many four drawer filing cabinets to house the information they have acquired over the years. Whilst this information remains in the four drawer filing cabinets, it is of little preventative value, when in reality it has a major role to play in the prevention of fraud. Those filing cabinets contain the total known history of fraud cases experienced by the organisation. It is my experience that fraud offenders are not easily deterred and will continue to offend. Therefore, the fraud history in the filing cabinets is material through which all new claims should be filtered. In cases where matches occur, the cases should be automatically referred to the Investigations team. This cannot be achieved whilst the information remains in the four drawer filing cabinets. It is common for the processing environment to be on computer and the investigations environment not to be. This is a conceptually poor approach to prevention. The information in the cabinets is simply gathering dust. The function of the investigative database is to provide a depositary to house all the information contained in the four drawer filing cabinets.

Information requirements of investigations

When conducting an investigation, an investigator obtains information from a variety of sources and it is not possible during the course of an investigation to predict what information is to be recorded in the computer. Consider the following sources of information:

- Births, Deaths and Marriages records
- Corporate Affairs records
- Electoral Roll
- Municipal records
- Newspapers/Media
- Telephone Directory
- Titles Office
- Motor Vehicle Registration records
- Licence records
- Electricity/gas records
- Estate agents records
- Bank records
- Claim files, etc
- Documents for other insurance companies
- Employer's documents
- Doctors' and Hospitals' records
- Credit Reference Association records
- Insurance Council of Australia and other similar agencies records etc.

This is not an exhaustive list by any means.

Therefore, any computer system developed to support the investigations team must be flexible and cater for the unknown.

Data within the investigative database should be organised on a person basis, that is, all information about a particular person should be assembled in the one place in chronological order. All information within the investigative database should be event dated, thus allowing for the development of automatic chronologies. All material recorded in the investigative database should be tagged with the case it belongs to and have a reference back to the hard copy document the information was obtained from. It is pointless to record information on the computer and not be able to trace that information back to an original document. The purpose of the investigative database is to follow the paper trail. Fraud offenders leave a record on paper throughout the community. It is the fraud investigators' role to follow this paper trail and it is the function of the investigative database to provide a depositary for the information gleaned from the paper trail.

Information likely to be recorded in the investigative database consists of names, personal data, vehicles, licences, addresses, aliases, etc all fully cross-referenced.

The investigative database should be capable of producing chronologies of cases or individuals etc as well as displaying networks of offenders for the analyst to work on. It should have built into the system a complete case management system and where possible, routine and repetitive tasks of the investigator should be automated. For example, the task of assembling a Brief of Evidence takes some four to five hours to collate. With the appropriate input from the investigator, the computer should be able to assemble the Brief of Evidence automatically.

Fraud profiles

A *fraud profile* is a method of detecting a potential fraudulent new claim as it is received. It is a process whereby the information contained in the application form is "scanned" against a set profile, to ascertain any matches to set criteria which have been predetermined.

Data used to construct a Fraud Profile may be obtained by the use of (i) Information held by the Analysis Section; (ii) Statistical Information; (iii) Information on current trends and patterns; (iv) the analysis of previously scanned files to recognise developing patterns and trends.

The aim of the *fraud profile* is to detect a potential fraudulent claim before any payments are made.

"Profiles refers to FRAUD INDICATORS that consist of NAME, OWNER (of profile), FACTORS (Fraud Indicators), PROFILE MAXIMUM (score) and THRESHOLD (score)."

The following is a sample of the selection criteria which apply:

(a) Admission of Fault;
(b) Employer;
(c) Job type;
(d) Job hours;
(e) Offer of Employment;
(f) Tax/Profit – Loss Docs;
(g) Sick/Invalid Pension;
(h) Claimant's home post code;
(i) Non-Demonstrable injury;
(j) Ongoing incapacity;
(k) Dr in same suburb;
(l) Claimant represented;
(m) MAB/SIO/IND (Claim);
(n) Pre-existing injury;
(o) No Vehicles;
(p) Driveway Accident;
(q) Unknown Vehicle;
(r) Struck rear;
(s) Sudden braking;
(t) Day of week;
(u) Hour of day;
(v) Locality;
(x) Independent Witness;
(y) Police attendance;
(z) Late/No Police report;
(aa) Ambulance called; etc.

GATEKEEPER APPROACH

The Transport Accident Commission has developed a systematic preventative strategy known as the Gatekeeper Approach.

It is the objective of a Gatekeeper Approach to identify suspected fraudulent claims in the early stages of processing. It relies on the investigative database interacting with the corporate processing database so as to screen all incoming claims against all the data held on past known fraudulent cases and against the fraud profiles held in the investigative database.

It is not possible in this short paper to discuss all the features of an investigative database but it suffices to say that all organisations should develop such a database to house all their investigatory information.

CONCLUSION

In conclusion, I would like to say the task appears daunting at times, but it is a rich, exciting and rewarding road to follow.

Insurance companies in Queensland are out to trap insurance cheats in an effort to stem rapidly increasing multi-million dollar personal insurance fraud.

The rip-offs have become so hot in recent years that insurance companies claim it has cost motorists more than $100 million in increased third party insurance premiums.

The money involved is big. There is evidence in southern states of involvement of corrupt interpreters, doctors and lawyers.

There is also evidence that new tactics by insurance companies in New South Wales, Victoria, South Australia and Australian Capital Territory, have driven some organised insurance fraud groups into Queensland.

One ethnic group, complete with an interpreter well-schooled in describing symptoms of non-demonstrable, hard to disprove, soft tissue injuries, like whiplash, has set up shop in Brisbane.

Queensland insurance companies plan to counter this by actively seeking to charge cheats with serious offences such as perjury, as a deterrent.

They have acknowledged that their previous "soft" approach to attempted fraud has contributed to the massive problem.

In the past, small claims — those under $10,000 — were inclined to be passed, even when suspect, because they were too expensive to fight in court.

Also, when a "try-on" became unstuck, the insurance company often allowed a fraudulent claimant to withdraw.

— **Peter Hansen,** ***Sunday Mail,*** **5 June 1988.**

Publicity and Its Impact Upon Fraud

Richard Daniell*

THE PROBLEM

The extent of exaggerated and outright fraudulent claims, whether on the social security or the insurance systems, is difficult – indeed nigh impossible – to establish. Figures as high as $1 billion a year have been freely touted. The Chief Executive of the NRMA, George James, calling upon the NSW Government to take a tougher stand against alleged victims of motor vehicle accidents suggested this figure as far back as January 1987.

Even amongst our own ranks, that is, the so-called insurance group, the extent of exaggerated-cum-fraudulent claims varies between 5 percent and 20 percent. My own organisation believes it to be between 5 percent and 10 percent.

In a recent article appearing in Adelaide's evening paper, *The News*, the Commissioner for Employees' Compensation, Dennis Corrigan, is reported as saying that "a blitz on workers compensation last financial year saved the government almost $35M." A survey of 7,900 retirees found that 144 were better off by more than $100 a week. A further 2,067 got more by staying off work than by working.

GEOGRAPHICAL SIGNIFICANCE

Fraud is universal. The UK Insurance Ombudsman, James Haswell, in his annual report for 1987, warned policyholders that making invalid or exaggerated claims "could be pushing their luck and their undoing".

In British Columbia, Canada, "a province-wide attack against insurance fraud – launched by the provincial police and special investigators of the Insurance Corporation of British Columbia – is meeting with success" was how efforts there were reported recently. The report stated that fraudulent Hit-and-Run motor vehicles alone were costing $5M each year.

THE JUDICIAL VIEW

There are clear indications of courts now expressing their concern about fraudulent and/or attempted fraudulent matters far more frequently than before. This is not to suggest that the administration of justice has changed.

In the matter of *R v Guiseppe Antonio Traino* (February Sessions No 37/1987) Mr Justice Grubb, the presiding Judge in the criminal charges proceedings said this in his judgment:

> In my experience the prosecutions for perjury are not frequent. However, after some experience of some 23 years as a judicial officer in the courts I am equally satisfied that the crime of perjury is as flourishing today as it was 23 years ago. And, in particular, it is flourishing in the kind of claims for damages brought before the courts by people like yourself who see an opportunity of obtaining money by deception, and by falsely swearing.

The case went to appeal. The Chief Justice, Mr Justice King, in his judgment said:

> Perjury is a serious and all too prevalent crime. Few judges who try personal injury claims can doubt that there are occasions, not infrequent, on which plaintiffs give false evidence for the purpose of inflating claims for damages. The effect on the community which contributes to the satisfaction of such claims by means of insurance premiums, is considerable. The burden of such premiums leads to measures to limit the damages necessary to compensate fairly the genuine claimants. Justice suffers when witnesses tell lies with impunity. It is therefore important to the administration of justice that perjury be followed by prosecution and conviction. (Action No: CCA No 27 of 1987)

The Chief Justice of South Australia, the Honourable Justice L J King, in an address titled "The Challenge for the Judicial System" presented at the Criminal Justice Conference held recently in Adelaide, had this to say:

> The prevalence of crime tends to affect a community's attitude towards and respect for the law. Tax evasion, fraudulent commercial practices, shoplifting and other common and often undetected crimes gradually become the behavioural norm of the community. When others are escaping their fair share of tax by fraudulent practices, even the honest citizen is tempted to emulate those practices. When shoplifting is carried out with impunity, other people, particularly young people, are tempted. With the diminution of respect for law, the community becomes less safe, less secure and less happy. Crime should be understood and tackled as a major social evil which erodes the foundations of a good life for the citizens of any community.
>
> I see no prospect of the diminution of the influence of any of these factors, with the possible exception of the age composition of the population, during the next quarter of a century. I approach the subject therefore in the belief that the rate of crime will not diminish and may well increase during the period under consideration. This consideration serves to emphasise the need for energetic measures to endeavour to bring under control

---

* Richard Daniell, ACII, AAII, JP, is General Manager, Compulsory Third Party and Agencies, State Government Insurance Commission, Adelaide. Text of an address to Australian Institute of Criminology Seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

the escalation of the crime rate and to reverse the trend if possible.

The Chief Justice and the thirteen other Supreme Court judges were interviewed for the purpose of an article that appeared in the *Sunday Mail*, an Adelaide newspaper, on 3 July 1988. The Chief Justice is reported to have said that "the biggest problem facing society is a deterioration of moral standards".

"Moral", it is useful to remind ourselves, is defined as "the standard of conduct respected by good men independently of positive law and religion".

ATTITUDES

As a general proposition it can be stated that the vast majority of consumers would take the view that if they can get away with making an exaggerated or fraudulent claim then it is all right – after all, it was only the Insurer or the Welfare System that was being ripped off!

Research done in the United Kingdom and here, in this regard, is indeed illuminating.

Overall, "dobbing in a fraud" was unacceptable but if it involved a crime of violence or drugs then this was seen in a different light than "ripping off" the social security system. Insurance companies and the welfare system were seen as fair game.

The UK study, undertaken by a Dr Roger Litton and reported in the *Post Magazine* issue of 18 February 1988, used questionnaires, with domestic burglary being the basis of questioning. Sixty nine subjects participated and they fell into five groups as follows:

A. Mainly retired middle class people.

B. Mainly middle-class mature students enrolled on a residential weekend course.

C. Nine police officers (three inspectors, one sergeant, five constables) and two prison officers.

D Twelve senior insurance officials (eight insurers and four brokers) based throughout the country.

E. University students and their parents (the questionnaire being completed by whoever was the householder).

Whilst there were a number of questions, the two which specifically related to exaggeration/invention were:

(i) "People have been said to invent losses (for example, burglaries, fires, breakages, car thefts etc) so as to improve their home (or finances) at the expense of insurance companies. Has anyone you know done this, to your knowledge? If you would care to do so, please amplify".

(ii) "People have been said to exaggerate losses they suffer in genuine misfortune so as to recover from insurance companies more than they are entitled to. Do you know of any cases of this? If you would care to do so, please amplify".

The responses are summarised as follows:

KNOWLEDGE OF FRAUD

Group	Losses Invented				Losses Exaggerated			
	Yes	(%)	No	Total	Yes	(%)	No	Total
A	1	6%	16	17	4	24%	13	17
B	4	29%	10	14	5	36%	9	14
C	10	91%	1	11	10	91%	1	11
D	5	25%	7	12	9	63%	3	12
E	4	44%	5	9	6	67%	3	9
	24		39	63	34		29	63
Percentage	38%		62%	100%	54%		46%	100%

Research of a like kind was commissioned by us in May 1988. It related to Compulsory Third Party Insurance, that is, Bodily Injury type of insurance that is generally arranged on an automatic basis when car registrations are being taken out or renewed. Those interviewed fell into two groups:

Group 1 – comprising car owners with Comprehensive Insurance.
Group 2 – without

Because of the quantitative and diagnostic nature of the research, numbers did not play a significant role, the Groups' attitude to fraud being tested by non-directive interview techniques. Under this method the researcher remains passive unless a particular point needs probing.

Five questions were put to the Groups as follows:

1. Was it legitimate sometimes to "rip-off" an institution such as an Insurer?
2. Would apprehending "Frauds" reduce overall costs?
3. Would participants be prepared to "dob in a fraud"?
4. Should one institution (only) do something about publicising/taking action against such people, or should it be done collectively?
5. If one institution should initiate action should this be initiated through media advertising, public relations or letters with registration renewals?

The responses were many and varied:

Initially the attitude of the Groups towards contacting the appropriate authority with relevant information, was negative. Some of the responses were:

"I'm not going to dob anyone in – even if it costs me money".

"There's a big difference between a little old lady being mugged and the Government being 'ripped off' ".

"We can't become a nation of dobbers".

"I wouldn't do it. I wish someone else would do it".

"It'd be very petty. They wouldn't really be getting any of the big people. They (major swindlers) cover themselves too well".

Overall, "dobbing in a fraud" was unacceptable but if it involved a crime of violence or drugs then this was seen in a different light than "ripping off" the social security system. Insurance companies and the welfare system were seen as fair game.

If there was a need for fraud investigation (and participants agreed that *regular* fraudulent claimants and business manipulators should be stopped), this should be promoted on an industry basis not by one organisation.

When it was pointed out by the researchers that it was not the Government or insurance company who were losing, but the consumers themselves, a perceptible change was apparent. The groups now felt that:

"If there was a campaign to dob in frauds, I'd dob them in".

"I'd dob my neighbour in for claiming that jewellery had been stolen if it hadn't been".

"They could have a thing like Operation Noah" [Operation NOAH was a campaign conducted in South Australia by the Police Department to encourage people to report drug offenders.]

THE MEDIA

Use of the media, whether electronic or print, is an excellent way of capitalising on successes against fraudulent claimants and in deterring would-be claimants.

Indeed, it is advertising at no cost to the institution, and, depending on the medium used – and such things as the program/articles, audience/reader mix – is a swift way of conveying a message to specific target groups.

Some appreciation of the extent of the penetration of the subject matter can be gauged from the survey results published recently:

TELEVISION RATINGS (HOMES)

Percentage of homes watching

Program	Channel	Adelaide	Sydney	Melbourne	Brisbane	Perth
Hinch	(7)	19	17	19	–	–
Carroll at 7	(7)	–	–	–	16	–
State Affair	(7)	–	–	–	–	24
60 Minutes	(9)	22	25	27	27	25
Current Affair	(9)	24	25	30	30	25
Sunday	(9)	4	8	6	4	5
Page 1	(10)	10	10	11	7	6
7.30 Report	(2)	13	13	13	17	14
Four Corners	(2)	12	12	12	9	12

Source: McNair Anderson 4/88

RADIO (CURRENT AFFAIRS/TALKBACK)

Percentage of available audience

			Station Shares
5AA	Bob Francis	9am – 12 midday	2.4
5DN	*Leigh Hatcher	5.30am – 9am	15.8
	*Vincent Smith	9am – 12 midday	14.0
5AN	AM	8am – 8.30am	8.8
(ABC)	Keith Conlon	8.30am – 11am	6.0
	Philip Satchell	3pm – 6pm	7.0

* recently resigned.
Now replaced by Bob Byrne (breakfast), Jeremy Cordeaux (morning).

Source: McNair Anderson 2/88.

NEWSPAPERS' CIRCULATIONS (at 31/3/88)

The Advertiser	214,550
The News	143,418
Sunday Mail	236,335

Opportunities for some free publicity can be created by means of press releases, tip-offs to press personnel, and by being involved in talk-back shows etc.

The subject that triggers off favourable publicity does not have to be a successful conviction. Appointment of more investigators, enhancement of a computer system, reduction in claims costs and a host of other similar subjects could well be the basis of media support.

PUBLICITY AND ITS IMPACT ON FRAUD

It is difficult to give precise figures as to what deterrent effect this has on the community, but it can be said that whenever favourable publicity is received, it results in telephone calls and letters from members of the public. The response depends somewhat on the source of the public's information.

It is interesting to note that the majority of callers refer to fraudulent claimants costing *them* money.

Since adoption of a higher external profile through the press, a clearly measurable decline in the number of "whiplash" claims have been noted.

Even when cases involving issues in other States are reported interstate, as occurred recently on national television programs, people contact the Commission with information.

One of the difficulties, however, is being able to maintain continuous media coverage of fraudulent claims cases. As is well known, the time from when a matter first appears in court to when a sentence is delivered can be considerable.

Both Victoria and the ACT embarked on vigorous campaigns to stamp out fraudulent claims in their third party systems and received extensive coverage in the media of their activities. This has resulted in premiums being reduced.

Although it will never be possible to eradicate the problem completely, there is no doubt that continuous publicity on an Australia-wide basis can have the desired effect of reducing fraudulent claims to an acceptable level of control. Whether that saving is 5 percent or 20 percent is difficult to quantify. It is a fact that publicity of any kind is beneficial.

It is also a fact that by reason of the publicity given to such matters, much more discussion takes place, particularly when there is a realisation by individuals that they are the ones funding the system.

The groundswell that is building up against persons attempting to exploit the system is encouraging and augurs well for the future.

To succeed even further, the pressure must be relentlessly maintained.

Key Elements in Investigating Fraud

Warren Simmons*

On the 22 June 1988, Mr Justice Stewart, the Chairman of the National Crime Authority, at a public sitting in Sydney, appealed for help from the public for information that would assist in investigations into a wide range of law-breaking businesses including heroin-running, extortion, fraud and money-laundering.

Suspicion was attached to secret Chinese criminal societies based on Hong Kong's infamous Triad gangs and gangs of Italian criminals drawn particularly from the Calabrian community known as the Honored Society and also allegedly busy in similar rackets.

Organised crime, fraud and corruption are well entrenched in Australia. The recent busting of a huge heroin distribution operation and the seizure by Customs of the largest shipment of cannabis ever, on boats off Pittwater in New South Wales, really demonstrates the size of the profits to be made and the laundering of money.

It will be a very long fight before we see a reduction in organised crime.

Fraud is the gaining of some advantage by unfair means. It is really a false representation of a fact knowingly, or made without belief in its truth, or made recklessly not caring whether it is true or false. A charge of fraud cannot be maintained unless it is shown that the accused had a wicked mind. An intent to defraud or an intent to deceive must be proved.

The crime of forgery is the counterfeiting in any particular by whatever means effected with intent to defraud. The title of forgery covers many documents and instruments. It is not restricted to the forging or copying or tracing of a person's signature but may be attributed to the altering of a date, an amount in figures or letters or in the manufacturing of money. In all instances there must be an intent to defraud.

The crime of uttering goes hand in hand with forgery and again the intent to defraud knowing the document to be forged is the essential proof for conviction. Uttering is the mere passing off or disposing of a forged document or instrument.

There is a saying in banks that "Strangers are not always crooks but crooks are always strangers".

How would you respond to an urgent fac's message from an overseas bank to the effect:

> Your $A100 Travellers Cheques have been counterfeited. Over the holiday weekend 100's were cashed in six countries in Europe.

This is only make-believe this time. Do not kid yourself that if you are a financial institution it will not happen to you.

Have you ever stopped to think just what effect a counterfeiting attack could have on your business?

Better still, have you ever thought about what action you might take?

- Are you going to suspend the sale of your travellers cheques?
- Are you going to reimburse the banks that cashed the forged travellers cheques?
- Are you going to warn all banks and financial institutions of the counterfeit attack on your paper?
- What steps are you going to take to alert money changers, hotels, airports, shopkeepers etc?

* Warren Simmons is Chief Investigation Manager, Westpac Banking Corporation. Text of an address to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

No 56, September 1988, 62-66.

- Are you going to advise the police? Just how are you going to inform the police in the countries of Europe?

- How about the adverse publicity?

- Just how are you going to answer the counterfeit travellers cheques? Are you going to endorse them "Refer to Drawer" or "Payment Stopped counterfeit"?

- How are you going to investigate a fraud of this magnitude several thousand kilometres away?

- What data base design and operational experience do you have to co-ordinate the investigation?

These are just a few of the important issues that require immediate attention when you are confronted with a major fraud attack. Just how well are you prepared? How would you handle an extortion threat to contaminate your products? How do you investigate demands of money with menaces?

To answer the questions I am posing to you, let us first recognise the form of threat that may be used against business.

Fraud is one of the oldest forms of crime and its practice in all likelihood will be pursued to the end of man. There is always someone out there who is prepared to take risks for money.

Let me assure you that no matter what your product, there is a way of defrauding you – all that is required is a criminal mind bent on threatening your business.

All businesses fear the possible damage to their corporate image and the damage to public confidence in their corporation. We fear imitative attacks from other fraud offenders, and so the corporation and individuals within the corporation do not disclose fraud – not even to the police. I wonder how many corporations have not disclosed counterfeit attacks to the police and other government authorities?

Apart from the moral and legal issues involved, a corporation, by concealing the fraud from the authorities, presents itself as a very nice soft attractive target for counterfeiters to use repeatedly. It is like paying secret commissions. The way you start will be the way you finish unless that matter is reported to the appropriate law enforcement agency.

Major fraud such as counterfeiting travellers cheques and other valuable securities is the result of careful planning. It is not undertaken as a spur of the moment decision. Consider the skill associated with the paper used, the printing and art work design as well as the warehousing distribution and sales of counterfeit travellers cheques. It leads you to the conclusion that there is a professionalism among certain major fraud offenders that compares with strategic group planning.

Put yourself in the place of the counterfeitor: how would you go about it? Well, you would more than likely:

- Firstly, select a series of financial institutions.

- Second, investigate each institution.

- Third, identify the way each institution will react.

- Last, pick the softest institution, the institution which is least prepared for attack and least likely to report the attack.

Following deregulation and increased financial market competition as well as financial institutions displaying an increasingly high profile in the international scene, it must be anticipated that Australian enterprises will face fraud threats. A financial institution or major business without an effective program or contingency plan to investigate and combat fraud is a much more attractive target. It is a soft target.

Let me assure you that no matter what your product, there is a way of defrauding you — all that is required is a criminal mind bent on threatening your business.

Just what are the correct responses?

Should employees be told of a counterfeit attack?

How do you protect your business?

How do you protect your customers? Are they going to be subjected to delays and interrogation?

How do you avoid publicity and possible litigation arising from the situation?

A well-tried and tested method for preparing for and investigating major fraud and handling of critical situations is management planning that has goals:

- to protect the Corporation;

- to provide efficient and stabilised management;

- to determine and implement a co-ordinated response to the problem.

Every major enterprise in Australia should have a contingency plan based on these goals in place now.

A top team of head office executives accountable for finance, marketing, public relations, legal and security/investigation should be formed to deal with the situations.

The top team should meet at intervals and review policy. It will convene immediately in the event of calamity.

The top team should leave to its investigation manager and support staff the operational strategy associated with the detection and prosecution of the offenders, thus restricting disruption to normal corporate business.

It is paramount that specialist officers of the police force be involved at operational level as soon as an attack or attempts have been made. Information and complaints of this kind must be carefully and discreetly guarded.

Communications with police need to be clearly identified and linked with the corporation's management plan.

It is vital to establish a data base with restricted access and password control to record the multifarious vouchers and documents generated by the fraud attack. Programs can be refined and extended to encompass a broad application with security provisions.

The most adequate precaution is a fully alerted, well-trained staff, who not only display initiative but clearly understand the reason why the corporation's rules and procedures need to be so closely observed. Thus when dishonesty occurs something must be done to minimise the effect. Firstly by prevention, second by deterrent, and third by reducing the aftermath.

The investigation manager is really the manager of the entire operation and should report to the top team for policy decisions. The top team should review objectively the performance of the operation.

It is essential that the corporation ensures that the investigation manager or security consultant has the qualifications and skill to provide guidance to the top team in developing the management's policies as well as investigate and manage the fraud operation.

The investigation manager requires a sound knowledge of the criminal proofs necessary to establish fraud charges, to be able to think clearly, have empathy with people and negotiating skills.

Banks with multi-state and overseas points of representation find themselves involved with numerous police forces because the fraud attack overlaps State boundaries and countries. Many of the police forces have varying policies and it is important that the investigation manager establishes and maintains a sound relationship.

The investigation manager should have at his or her fingertips the confidential information as to the make up of the corporation's genuine valuable securities, such information should include:

- The composition texture and thickness of the paper used.
- Whether the paper is sensitised (that is, impregnated with a chemical which reacts to bleaches etc).
- Ingredients of the ink used in the (background body) of the valuable security.
- Whether the encoding is printed with magnetic ink.
- Shades of colour etc.

At regular intervals the investigation manager should inspect and verify that the security printers are producing the valuable securities in the identical form as to the sample comparison advice brochure distributed to the corporation's agents. Any departure should be immediately corrected.

At intervals, major corporations should arrange for a security audit to determine its vulnerability to major fraud and verify that the management plan procedures are being observed. This assurance will inspire confidence that the top team can deal with major fraud or other criminal attacks.

In the course of employment it is not uncommon to be confronted with the problem, when funds have been unlawfully obtained as a result of a fraud, with a proposition by the offender to return the money if no prosecution is launched. Perhaps the first thought is to recoup the funds. In all cases where a felony or serious offence has been committed it is your absolute duty and the only safe course of conduct of the person aware of the circumstances to reveal it as soon as possible to some person in authority. You should not convert a crime into a source of profit or benefit.

Investigators who seek and cultivate informants should be mindful of the danger of associating with this type of individual as many are of the criminal class.

The investigators should take steps to protect themselves from any backlash and I would commend the establishment of a register maintained by a responsible appointed officer in the corporation.

This appointed officer should record in code details of the informant and the investigator utilising the informant. A register of this nature may assist the investigator in the event of allegations of impropriety being made.

STAFF FRAUD

Westpac Banking Corporation employs some 31,157 salaried and services staff in Australia and operate from a range of specialised points of service delivery.

1412 local banking centres, branches and agencies

113 district commercial banking centres

32 international business centres

57 personal investment centres

13 district commercial agribusiness officers

675 automatic teller machines (Handybanks)

1500 EFTPOS Terminals (Handyway)

The traditional functions of banks are the safeguarding of deposits entrusted to them and the making of loans to customers.

In carrying out the business of a large banking institution there is a great amount of organisational and administrative work which is common to any large business.

To be a custodian of other people's money means that the bank must not only be trustworthy in every sense of the word but it must appear to be so. In perhaps no other type of business is the quality of personal integrity so important as in the business of banking.

Whilst banks enjoy public confidence they are vulnerable to any decline. The responsibility for protecting the corporation's assets rests with our staff and we must take every sensible precaution to preserve our assets as well as discourage and detect all attempts to defeat this aim.

The most adequate precaution is a fully alerted, well-trained staff, who not only display initiative but clearly understand the reason why the corporation's rules and procedures need to be so closely observed. Thus when dishonesty occurs something must be done to minimise the effect. Firstly by prevention, second by deterrent, and third by reducing the aftermath.

No internal control can by itself guarantee protection against dishonesty. The two things that will do most to reduce the incidence of theft are.

1. A determined attitude of branch executive towards security and the observance of the corporation's standing instructions.
2. A positive and unstinted audit.

Fear of consequence is a powerful deterrent to the penetration of dishonesty and it follows that when the consequence is only mild, the force of the deterrent diminishes.

I believe that honesty is related to opportunity and temptation.

The corporation has a legal and moral obligation to its proprietors and the community and indeed it has a duty to all staff, to support and confirm their honesty by taking strict action against the offending employee. To do otherwise is to condone dishonesty and thereby reduce morale among staff.

It is our responsibility to ensure that young staff, in particular, are not corrupted by observing colleagues taking advantage of reduced or weakened controls.

An atmosphere of disapproval must be encouraged so that fraud resorted to by staff will be contained and readily brought to notice. There is no longer room for leniency in staff fraud.

As an investigator you should not measure loss of time and the trouble in detecting and investigating staff fraud as this must be accepted if the incidence is to be reduced.

If we have alert managers that display initiative then the risk of detection is increased, or at any rate more time for and care in negotiating the obstacles is required. This is an important deterrent. The best that can be done is make the task as difficult and detection as risky as possible.

It must be remembered that the fraud offender has the overwhelming advantage of the initiative, for it is he or she who chooses the time, place and strike. On the other hand the employees have to perform the daily task of protecting and watching the Bank's property all the time and can easily become a victim of carelessness and a feeling of "it can't happen to me".

Security against fraud can be positively and successfully applied. It depends for its success on a continuing awareness of the need for it, constant review of the measures in the light of changing conditions and technological advance.

The community recognises that a thief is a thief whether he be a bank manager, company director or school dropout and when they violate standards of conduct they reveal the same basic greed as the common car thief or housebreaker.

During the Costigan Royal Commission, Mr Douglas Meagher, QC, who was assisting Mr Costigan, said:

> Thus if a Manager holds a senior position in a Bank, demands for favours are made upon him. Those demands may be merely the operation of Bank Accounts on behalf of the organisation under a variety of names. One example before the Costigan Commission was of a Bank Manager who had half a dozen accounts at the Bank in his own name, with his own home address recorded as the address of the account. He operated the account on behalf of the criminal, moving monies in and out as requested and thus concealing from law enforcement agencies and the Taxation Office the ownership of that account by the criminal. In another case the Bank officer held a position relating to the international movement of money. In his case he was asked, and he agreed, to arrange for the movement of monies out of Australia without the necessity of Reserve Bank approval and in such a way that it would be concealed from the enquiries of law enforcement agencies. In yet another case, the Manager of a Branch of a Bank was persuaded to open 4 or 5 false names, extending overdraft facilities to the limit of his authority in respect of each account. The limit that he could allow was $10,000, and so the criminal gained access to $50,000 of Bank's money. In that particular case, that together with other schemes supported by the same Manager, cost the Bank something in the order of $450,000.

It is not just bank managers who can have such demands made upon them. There are others in the community who hold jobs that would allow much use to be made of them by organised crime. It might be a position of a financier, such as credit manager or credit officer where credit is allowed to a variety of people under false names without appropriate checks being made. Such a case was found in Victoria. Members of law enforcement agencies and government taxation and regulatory agencies are obvious marks. There is considerable evidence that the corruption

of these people arises, in the majority of cases, from the extension of credit at the gaming table.

The community recognises that a thief is a thief whether he be a bank manager, company director or school dropout and when they violate standards of conduct they reveal the same basic greed as the common car thief or housebreaker.

When we terminate the employment of staff for serious and wilful misconduct we do not take this action because the corporation wants to punish the employee even though it may seem that way, but rather that the corporation has decided that employee cannot or will not meet the corporation's standard of integrity.

Many people in our community believe that crimes, such as major frauds, are the responsibility of law enforcement agencies and the government.

In my view if we, as individuals and corporations, neglect this responsibility, then serious crime will continue to flourish.

Lack of preparedness and the failure to take reasonable precautions against crime imposes a serious burden on the community and government. A clear duty falls upon all to prevent and discourage crime.

Risk Management and the Role of the Auditor in Preventing Fraud

R G Humphry*

Recent developments in public sector administration have emphasised management initiative and flexibility, to let the managers manage. These developments have placed a particular focus on the management of risk and the consequential need to have in place an effective risk management strategy. In this paper I will examine the options for managing risk, with particular emphasis upon the roles played by both public sector managers and auditors.

To set the context for this presentation it will be useful to provide some details on the recent changes in public sector administration and to analyse the concepts of risk management and fraud.

THE CHANGING ENVIRONMENT

What are the emerging issues in public sector administration?

There has been a major political and community realisation in recent years that government is by far the biggest spender in the economy (comprising in 1986-87 some 43 percent of Australia's gross domestic product). As a result, relatively small efficiency gains in public sector administration can provide comparatively large monetary savings in government outlays.

Public sector administration has also been characterised by greater commercialisation of activities and the use of organisational units additional to the traditional department/ statutory authority classification. These trends have been greatly influenced by the deregulated financial environment that has emerged in recent years.

For example there has been the:

- establishment of a multitude of non-statutory boards;
- payment of grants and subsidies to a greater number of recipient organisations;
- trend towards increased use of public sector equity participation in companies, joint ventures and trusts, often in partnership with the private sector;
- expanded investment powers and the use of innovative financing and debt management techniques such as debt defeasance, leveraged leasing, currency swaps and futures trading.

What major changes in public sector administration have taken place in recent years?

The major focus of change has been devoted to improving the efficiency of program administration through the devolution of authority to managers with responsibility for delivery of programs.

Major initiatives have included the introduction of:

- financial management improvement programs, incorporating program budgeting;
- greater flexibility to management in decision making, for example, in terms of managing resources within a

---

* R G Humphry was Auditor-General of Victoria when he delivered this address, developed with the assistance of the Research and Development Section, Victorian Auditor-General's Office, to the 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", in Canberra on 2 May 1988. He has recently been appointed to head the Premier's Department in New South Wales.

No 56, September 1988, 66-72.

"block" appropriation. Associated with this have been enhanced accountability requirements which enable management performance to be monitored and assessed at the individual agency, central agency and parliamentary level;

- recognition of quality of performance, for example, provision for limited carry-over of unspent appropriations to succeeding years and, for certain States, Senior Executive Service performance assessments;

- greater decentralisation of administration and program delivery as evidenced in the increased delegation of management functions consequent upon the abolition of public service boards in the Commonwealth and a number of States;

- revised management information systems and processes, including increased computerisation of major data sources; and

- broad scope auditing comprising efficiency reviews in addition to traditional compliance and attest audit functions.

What has been the impact of the changes and reforms on public sector risk management?

Recent changes and reforms place greater emphasis on management initiative and flexibility. In providing greater flexibility for management initiative there can be the perception that there is an increased risk to government and organisations of waste, mismanagement, and fraud.

It is important to recognise that opportunities for fraud have always existed and what is at issue is not whether a changing environment is introducing the risk of fraud but rather the need to develop an appropriate strategy to the management of risk. It is therefore my view that the more relevant issue is the need for a modern approach to achieving accountability through an appropriate risk management strategy. In this context, I emphasise that the concept of accountability should not be viewed as being limited to traditional checks and balances.

For the effective implementation and control of more streamlined, decentralised and cost effective systems and processes it is important that appropriate risk management strategies be developed.

APPROACHES TO RISK MANAGEMENT

What is meant by "risk management"?

A technical description of risk management is as follows:

> The process, activity or study of reducing the risk of loss to a firm, particularly loss caused by accidents. Risks, once they have been identified may be reduced by:
>
> (i) taking preventative action;
>
> (ii) setting aside a fund to pay for losses; or
>
> (iii) transferring the risk to someone else.

A recent writer has provided a more practical description:

> A grand description for the age old concept of making sure you do not lose any more than necessary. Good risk managers cut down the odds of losing but should be able to spot a worthwhile opportunity.

Is there a relationship between materiality and risk?

Preventative measures for the reduction of risk should be related to the materiality of the risk an organisation seeks to manage. The cost of safeguarding certain funds or property should not be greater than the risk of potential loss emanating from possible fraud or error in systems. In this respect it is often the case that 80 percent of total expenditure is confined to only 20 percent of transactions.

However, materiality should not be evaluated only in the context of dollar values as transactions may also have other sensitivities.

It is important to recognise that opportunities for fraud have always existed and what is at issue is not whether a changing environment is introducing the risk of fraud but rather the need to develop an appropriate strategy to the management of risk. It is therefore my view that the more relevant issue is the need for a modern approach to achieving accountability through an appropriate risk management strategy.

What has been the traditional approach to risk management in respect of an organisation's finance functions?

Traditional approaches to the evaluation of systems and the risks of their being susceptible to fraud and error and resultant financial management in organisations (encompassing investment, collections, payments, annual reporting etc) have entailed generally the comparison of existing practice to those desirable internal controls contained in check lists of some "model" system, for example, as to division of duties, level of supervision, authorisation process etc. This has certainly been the case in respect of the auditor's evaluation of risk in the initial assessment of the adequacy and reliability of systems and the extent of detailed testing necessary to determine the validity of transactions processed through them.

In the public sector there has been a particular emphasis on the establishment of, and strict compliance with, such controls. These controls have often been incorporated into legislative, regulatory or other requirements. A by-product of this environment has been limited scope for management flexibility and initiative in developing more efficient and effective systems that reflect changing circumstances and technologies, for example, procedures for the payment of accounts.

In my view these approaches have concentrated heavily on ensuring controls are in place to minimise all known risks of fraud and error often without continuing consideration of the cost effectiveness of the preventative controls established.

RISK OF FRAUD, WASTE AND MISMANAGEMENT

What is the meaning of fraud in its general community usage?

The community perception of fraud is generally that of the improper use of funds or other property resulting from the abuse of positions of trust and/or responsibility in an organisation. It also can be seen to include kickbacks, secret commissions and use of privileged information for financial advantage, for example, stock market manipulation.

Statement of Audit Practice, "Fraud and Error", defines fraud as follows:

> The term "fraud" refers to misappropriation of assets or intentional misrepresentations of financial information by one or more individuals among management, employees, or third parties. Fraud may involve:
>
> (i) manipulation, falsification or alteration of records or documents;
>
> (ii) suppression or omission of the effects of transactions from records or documents;
>
> (iii) recording of transactions without substance; or
>
> (iv) misapplication of accounting policies.

Should fraud be viewed in a wider context within the public sector to also embrace waste and mismanagement?

In the public sector it is my view that the potential for fraud, waste and mismanagement should be given the same importance when undertaking risk evaluation of systems. These shortcomings in management control processes all involve a misuse of taxpayers' funds with the only difference being related to intent to misuse those funds. In terms of financial significance waste and mismanagement would be expected, on most assessments, to far exceed losses from fraud.

What are the causes of fraud, waste and mismanagement?

To put in place effective measures to reduce the risk of fraud, waste and mismanagement it is necessary to appreciate its underlying causes.

Studies have shown that there are three variables or forces which taken independently or in interaction may indicate potential for fraud. These are:

Personal Pressures	– financial difficulties – excessive personal needs – situational stress
Opportunity	– weak controls – structure and relationships – accounting record and staff inadequacies
Attitude or Integrity	– personal and psychological characteristics – background – treatment by superior/employee

There are a number of indicators of potential fraud including:

- *situational pressures*, life style such as gambling, drugs and sex;
- *opportunities to commit fraud*, such as related party transactions, high level of computerisation, turnover of key staff, bad accounting practices; and
- *personal integrity issues*, such as association with suppliers, low moral character and code of ethics, and career stagnation.

What has been the incidence of public sector fraud, waste and mismanagement?

There have been no authoritative surveys of the incidence of public sector fraud, waste and mismanagement although mention of certain fraudulent activities has been highlighted in reports of Auditors-General both in Australia and overseas. There has been an interesting survey conducted on a United States General Accounting Office fraud hotline which indicated that over the five years of operation 53,000 calls were received of which 1,100 cases were substantiated with millions of dollars of misspent federal funds being identified.

I think it is fair to say that there is significant fraud that goes undetected. Often this is despite the extensive controls established in systems designed to prevent such fraud (such as those referred to above). Adding support for this contention is the Victorian experience of identified frauds in the public sector having been detected not only through structured audit programs and management control systems but often by "tip offs" and by a combination of chance circumstances resulting in subsequent detection. It is perhaps not surprising, having regard to the causes of fraud, that traditional audit testing and management controls have not been fully successful in the prevention and detection of fraud.

CONTROLLING THE RISKS OF FRAUD, WASTE AND MISMANAGEMENT

What action should be taken by management to minimise the risks of fraud, waste and mismanagement?

The provision of greater authority, flexibility and responsibility to management highlights the need for an appropriate and modern interpretation of public accountability to accommodate the changing environment. I consider it is important to ensure that such an interpretation enhances management's capacity to analyse risk potential and to determine the nature and level of

control mechanisms required. In pursuing this line, the emphasis should not be on whether there is increased scope for fraud, waste or mismanagement (opportunities for such actions have always existed) but rather on management's authority and responsibility to implement risk control strategies derived from its own assessment of the organisational climate.

Central agencies can play an important role in the above process particularly in terms of defining a framework for risk management within agencies. This task could be achieved through the issue of guidelines or principles on risk management aimed at enhancing the perception of risk factors in agencies and assisting management to implement risk management procedures. Such an approach would be far more preferable than imposition on agencies from central sources of detailed control requirements which may be quite out of step with individual organisational needs and have the potential over time to impede organisational efficiency.

In my view, an important contributor to the development of effective risk strategies within agencies is use by management of realistic assessments of risk and materiality factors. There is a clear relationship between risk and materiality which suggests that preventative control measures should be systematically determined according to management's perception of the materiality or signficance of particular systems or functions. In reaching these decisions, management needs to take into account factors relevant to the organisational setting, for example, political sensitivity and impact on program or service delivery as well as magnitude of financial resources involved.

The implementation of an effective system of internal control is the primary means for management to control its risks. The statement of auditing practice, "Study and Evaluation of the Accounting Systems and Related Internal Controls in Connection with an Audit", defines an internal control system as:

> . . . the plan of organisation and all the methods and procedures adopted by the management of an entity to assist in achieving management's objective of ensuring as far as practicable, the orderly and efficient conduct of its business, including the adherence to management policies, the safeguarding of assets, the prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information.

The key controls which should be developed in an effective internal control system include:

Organisation controls

Enterprises should have a plan of their organisation, defining and allocating responsibilities and identifying lines of reporting for all aspects of the enterprise's operations, including the controls. The delegation of authority should be clearly specified and the responsibilities of officers fully understood.

Segregation of duties

One of the prime means of control is the separation of those responsibilities or duties which would, if combined, enable one individual to record and process a complete activity. Segregation reduces the risk of intentional manipulation and error. In particular the functions of authorisation, execution, custody and recording should be separated.

Physical controls

These are concerned mainly with the custody of assets and involve procedures and security measures designed to ensure that access to assets is limited to authorised personnel. This includes both direct access and indirect access via documentation. These controls assume importance in the case of valuable, portable, exchangeable or desirable assets.

Authorisation and approval

In principle all transactions should require authorisation or approval by an appropriate responsible person. In this context, materiality is an important factor and different strategies would need to be adopted for material as against immaterial transactions. The limits for these authorisations should be understood by those exercising the approval procedures.

Arithmetical and accounting controls

These are the controls within the recording function which check that the transactions to be recorded and processed have been authorised, that they are all included and that they are correctly recorded and accurately processed. Such controls include checking the arithmetical accuracy of the records, the maintenance and checking of reconciliations, control accounts and trial balances, and accounting for documents.

Personnel

Personnel should have the capabilities commensurate with their responsibilities. Inevitably, the proper functioning of any system depends on the competence and integrity of those operating it. The qualifications, selection and training as well as the innate personal characteristics of the personnel involved are important features to be considered in setting up, monitoring or modifying any control system.

Supervision

Supervision and review are important considerations but the extent of the application needs to be evaluated in the context of the operating environment.

Management controls

These are the controls exercised by management outside the day-to-day routine of the system. They include the overall supervisory controls exercised by management, the review of management accounts and comparison thereof with budgets, the internal audit function and any other special review procedures.

In the context of the changing environment it is important that management systematically evaluates the effectiveness of controls. The controls in a system should be analysed with the objective of improving their effectiveness. In this context a practical approach to the review and evaluation of internal controls would emphasise:

- concentration on the types of transactions and the related controls that materially affect the operations of the agency;
- segregation of the agency and its component operations, and the related systems, into interrelated cycles of activity;
- identification of weak or missing controls and resultant risks created; and
- identification of unnecessary controls.

The recent reforms in public sector administration are essentially aimed at sharpening management's perception of policy issues and equipping management with the necessary tools and flexibility to achieve policy objectives. There is a need for this emerging environment to be accompanied by appropriate risk control measures which are management devised and driven, and which are given high priority among organisational strategies and procedures.

THE ROLE OF THE AUDITOR

What is the auditor's responsibility for the detection of fraud, waste and mismanagement?

In Australia, the statement of auditing practice on "Fraud and Error" is the key professional guidance for the determination of the responsibility of auditors. This statement specifies that the responsibility for the prevention and detection of fraud rests with management through the implementation and continued operation of an adequate system of internal control. In this context an audit should be planned so that there is a reasonable expectation of detecting material misstatements in the financial information resulting from fraud or error. But the statement also specifies that "*due to the inherent limitations of an audit there is a possibility that material misstatements of the financial information resulting from fraud and, to a lesser extent, error may not be detected.*"

Recent developments have, however, questioned the continued acceptability of this interpretation of the responsibilities of auditors. The increasing incidence of fraud has resulted in the courts, the financial press, regulatory agencies and the general public, particularly concerned investors, all pushing for auditors to be more effective in the detection of fraud.

The following recent developments have direct implications for the issue of the auditor's responsibility for the detection of fraud:

- In the United States the National Commission on Fraudulent Financial Reporting (Treadway Commission) issued its final report in June 1987 which recommended:
  - generally accepted auditing statements should be changed to recognise the auditor's responsibility for detecting fraudulent financial reporting;
  - the auditor should take affirmative steps to assess the potential for fraudulent financial reporting and design tests to provide reasonable assurance of detection;
  - audit guidance should be improved in the area of identifying risks; and
  - the auditor should be required to make greater use of analytical review procedures to identify areas with a high risk of fraudulent financial reporting.
- The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) issued in February 1987 a series of exposure drafts that propose improved standards for audit performance and auditor communications.

  The major intention of the statements is to reduce the difference between what the public believes is an auditor's responsibility for the detection of fraud and what the auditor believes it to be. To do this the proposed standards express positively the duties and responsibilities of auditors.

  The proposed standards would require auditors, among other things, to:
  - design their audits to detect material errors and irregularities;
  - make a preliminary assessment of the risk of material irregularities and of the likelihood of management misrepresentation;
  - ensure that the audit committee, or its equivalent, is adequately informed about any reportable conditions, irregularities or illegal acts;
  - consider continued existence in all audits and to modify the audit report when there is substantial doubt about the entity's ability to continue; and
  - apply analytical procedures in the planning and final review stages of an audit.
- The Stewart Royal Commission into the collapse of the Nugan Hand Bank made a number of recommendations, which, if adopted, could have a significant impact on the accounting profession. These recommendations included:
  - the requirement to codify in the Companies Code the scope of an auditor's duty to detect fraud;
  - making it a criminal offence for an auditor to certify company accounts which he knows to contain false statements; and
  - separating the roles of the accountant and the auditor in respect of a public company and prohibiting the company's auditor from also carrying out the duties ordinarily performed by an accountant.

What implications do these developments have for public sector auditors?

These developments have direct and significant implications for auditors in both the public and the private sectors.

Modern audit techniques involve auditors in conducting examinations of systems of internal control which

management has in place. Based on these examinations the auditor establishes the amount of reliance that can be placed on the system for determining the nature, timing and extent of these audit testing procedures. These techniques do not involve 100 percent checks of all auditable areas but involve placing audit emphasis upon the points in the processing of transactions and handling of assets where errors or fraud may occur. This audit methodology is referred to as systems based auditing.

The public sector auditor not only applies systems based auditing but also adopts a comprehensive audit approach. This audit approach involves not only the audit of financial statements and the extent of compliance by agencies with legislation and government directives, but also the review of resource management efficiencies. In conducting comprehensive audits an assessment is made of how efficiently and effectively public funds are being utilised on programs, and includes suggestions for improvements to existing management practices.

In this context the role of the public sector auditor is not only directed towards the provision of advice to the Parliament on the efficiency and management effectiveness of administration but also towards assisting the Executive Government and its management through complementing risk management practices in place in government agencies. The recent trend towards efficiency auditing is an effective way of enhancing the detection and prevention of fraud, waste and mismanagement.

These developments in audit approach are consistent with the objective of improving the efficiency of the public sector and complement the changing public sector environment. But the key issue is whether or not the comprehensive audit approach gives the necessary attention to the issues of fraud, waste and mismanagement – especially in the context of the risk management environment. Unfortunately, I feel that it does not, as is evidenced by the experience to date that identified frauds in the public sector have not been fully detected by structured audit programs and management control systems but often by "tip-offs" and chance circumstances.

What alternative audit procedures should be implemented to address the risks of fraud, waste and mismanagement?

To address the "fraud gap" which exists the options are to either revise the existing audit procedures or to supplement those procedures. In terms of revising procedures the option is to return to the traditional audit approach, where 100 percent checks are conducted. I certainly do not favour this option as it would not be cost effective and would be unlikely to result in a signficantly higher level of fraud detection.

Auditors need to investigate and develop supplementary procedures aimed at detecting fraud, waste and mismanagement. In this regard consideration should be given to:

- developing auditors' awareness of the causes of fraud and training auditors in techniques for fraud detection, that is:
  - know the exposures;
  - know the symptoms;
  - understand and be alert for symptoms;
  - build audit programs to look for symptoms; and
  - follow through on all symptoms observed.
- specialist training of officers for specific "fraud squads"; and
- increased penalities for fraud.

the key issue is whether or not the comprehensive audit approach gives the necessary attention to the issues of fraud, waste and mismanagement — especially in the context of the risk management environment. Unfortunately, I feel that it does not, as is evidenced by the experience to date that identified frauds in the public sector have not been fully detected by structured audit programs and management control systems but often by "tip-offs" and chance circumstances.

A further supplementary audit technique which could be considered is the establishment of a "Fraud Hotline". The General Accounting Office in the United States established such a hotline in January 1979 and in the first 5 years of its operation the hotline received over 53,000 calls. Over 10,600 of the allegations were referred for investigation with 1,100 cases being substantiated. The hotline has identified millions of dollars in misspent federal funds.

The awareness that these supplementary procedures are being conducted is as important, if not more important, for minimising the potential for fraud, waste and mismangement. The knowledge that these procedures are to be conducted or that a hotline is to be established should create the necessary perceptions which would act to reduce the incidence of fraud, waste and mismanagement.

CONCLUSION

The developments in public sector administration which are placing greater emphasis upon risk management should be encouraged as they provide potential for significant benefits to be obtained through the efficient operation of the public sector. But, in conjunction with these developments, it is vitally important that management has in place an effective risk management strategy.

The public sector auditor has a key role to play in the context of this risk management environment. The ability to adapt to a changing environment is reflected by the adoption of the comprehensive audit approach. I am confident, therefore, that auditors will be able to meet the demands of an environment which is placing greater emphasis on risk management and to also support the

government's initiatives and reforms, which are aimed at providing for the more efficient use of public sector resources.

REFERENCES

AICPA Auditing Standards Board, "Illegal Acts by Clients", Exposure Draft – Proposed Statement on Auditing Standards, New York, February 1987.

AICPA Auditing Standards Board, "The Auditor's Responsibility for Assessing Control Risk", Exposure Draft – Proposed Statement on Auditing Standards, New York, February 1987.

AICPA Auditing Standards Board, "The Auditor's Responsibility to Detect and Report Errors and Irregularities", Exposure Draft – Proposed Statement on Auditing Standards, New York, February 1987.

Albrecht, W S, Howe, K R and Romney, M B, *Deterring Fraud: The Internal Auditor's Perspective*, The Institute of Internal Auditors Research Foundation, August 1984.

Arthur Andersen & Co, *Guide for Studying and Evaluating Internal Controls in the Federal Government*, Revised August 1986.

Australian Society of Accountants, "Statement of Auditing Practice Fraud and Error – AUP16", Members Handbook.

Bologna, J, *The Fine Art of Fraud Auditing*, Computer Systems, Inc Michigan, 1985.

Comptroller-General of the United States, *5 Year Summary of Results of GAO Fraud Hotline – United States*, General Accounting Office, September 1984.

Comptroller-General of the United States, *7 Year GAO Fraud Hotline Summary*, General Accounting Office, February 1986.

Comptroller-General of the United States, *Standards for Audit of Government Organisations Programs, Activities and Functions*. General Accounting Office, United States, 1981 Revision.

Cormier, P, *Responsibilities for Fraud Detection and Investigation*, Canadian Conference of Legislative Auditors, Quebec City, July 1987.

Gwilliam, D, "Be alert to the Possibility of Management Fraud", *Accountancy*, February 1986, pp 104-105.

Legislative Commission on Economy and Efficiency in Government, "Preventing Fraud, Waste, Abuse and Error: Internal Control Reform in New York State Government", New York State, Second Edition, November 1983.

National Commission on Fraudulent Financial Reporting, "Fraud Commission Issues Final Report", *Journal of Accountancy*. November 1987, pp 39-48. Reprinted with permission from the "Report of the National Commission on Fraudulent Financial Reporting", 1987.

Romney, M B, Albrecht, W S, and Cherrington, J, "Auditors and the Detection of Fraud", *The Journal of Accountancy*, May 1980, pp 63-69.

Stewart Royal Commission into the Collapse of the Nugan Hand Bank.

Fraud on Government

THE ROLE OF THE AUDITOR-GENERAL IN INVESTIGATING FRAUD

V C Doyle*

I am indebted to one of the more cynical of my senior officers for the following description of an Auditor-General, the authorship of which, as could be expected, he attributes to some source now lost in the history of my Department:

> The typical Auditor-General is a man well past middle age, wrinkled, intelligent, passive, non-committal, polite in contact but at the same time unresponsive, calculating, cold, calm, as damnably composed as a concrete post and completely devoid of emotion or a sense of humour.
>
> Happily they rarely have an opportunity to reproduce and all of them inevitably finish up in hell.

I must say that the portraits of some of my predecessors of 100 years or so in the past which hang in the halls of my Department's premises lend some credence to this description.

And so I stand before you with this image to live up to, or perhaps live down, and, it seems, doomed to a future of celibacy culminating in eternal damnation.

While we are contemplating definitions I offer you another – that of "fraud" as documented by the *Oxford English Dictionary* which, in essence, describes it as

> *Criminal deception;*
> - *use of false representations to gain unjust advantage;*
> - *dishonest artifice or trick;*
> - *person or thing not fulfilling expectations or description.*

Applying that last interpretation to my colleague's perception of an Auditor-General I might hope that I could be seen as a fraud.

Be that as it may, there is a point I wish to make which has as its focus the reality of what the Auditor-General is *vis a vis* what many, or most, people think he is or expect him to be, particularly in the area of fraud prevention, detection and investigation. The role and function of the Auditor-General is somewhat at odds with the popular perception of his position and responsibilities.

Many people are aghast, wring their hands in despair and cry "heresy!" when they are told –

- that Auditors-General, or auditors generally, are not the impregnable bastion which protects our governmental and other structures from the forces of evil and corruption that might emerge within them;

* V C Doyle, AAUQ, FASA, is Auditor-General of Queensland. Text of a paper presented to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CBPA No 56, September 1988, 72-77.

- that modern audit methodologies offer no absolute or reliable assurances that fraud, in any form, will be prevented or detected;
- that the prime responsibility for prevention and detection of fraud does not reside with the auditor; and
- that most fraud discoveries are not a direct result of audit.

These are, however, facts of life and to understand why it is so it is necessary to understand a little of the evolutionary processes that have changed the nature and objectives of audit over the years and the reasons for them.

I will be covering these briefly in the course of this paper, touching on the philosophies, principles and objectives on which modern audit is based and explaining the place of fraud surveillance in our processes. Most importantly, I will be emphasising the responsibility of the managements of organisations to establish their own mechanisms for protection against fraud.

Many of my comments and observations will reflect developments and approaches as they have occurred, or apply, in the context of the Queensland public sector and my own Department. They might not be always completely relevant to circumstances in other public sector areas or the private sector.

THE AUDIT FUNCTION – THEN AND NOW

The position of Auditor-General in Queensland goes back to October 1860 when Mr H Buckley assumed office following appointment by the Governor in Council. The Constitution Act of 1867 referred to the need for audit.

The rules under which the Auditor-General functions and the objectives of the position are prescribed in later laws enacted by the Queensland Parliament. The first of these was the Audit Act of 1874. This was by no means a definitive statute insofar as the charter of the Auditor-General was concerned and consequently this charter and the manner in which it was fulfilled were dictated mainly by the historic conventions and traditions of the Westminster system under which Auditors-General had or could assume powers and authorities which, by present day standards, can only be described as awesome.

Modern day law governing public financial administration and audit is much more definitive and prescriptive. It clearly circumscribes the role of the Auditor-General, establishes his relationship with the legislature, the executive government and the administration and, at least here in Queensland, effectively identifies his charter by specifying the matters on which he must issue certificates and the procedures to be adopted for his reporting function. The only real areas of flexibility and discretion left with the Auditor-General are determination of the manner in which audits are conducted and decisions as to whether matters are of sufficient significance to be reported to the parliament or elsewhere.

The former of these is quite critical because it allows the Auditor-General to vary the methodologies, depth, scope and emphasis of his Department's activities to accommodate changes in circumstances and need and to take advantage of new techniques and technologies that are emerging within the profession at a rate which is, and has been for the last decade or so, almost alarming.

I have already mentioned the difference between the general community expectations of audit and the realities as they exist in practice. In my view this gap has arisen because a great number of people still see the auditor as an individual in the mould of the person portrayed in that rather lurid definition I quoted earlier, poring over books and documents, up-ticking or down-ticking every figure and book entry to establish beyond doubt that every one is correct – that there have been no errors and, of course, no fraud or any evidence at all of "sticky fingers".

This was audit one hundred years ago – even 30 years ago – a 100 percent verification of the probity and regularity of all recorded transactions leading to a form of certification which was absolute in nature. It was extremely resource-intensive and thus very costly. Further, to many people it was intolerably tedious and, in many respects, not especially professionally challenging or satisfying.

Most importantly, I will be emphasising the responsibility of the managements of organisations to establish their own mechanisms for protection against fraud.

It did offer, however, a quite high level of protection against fraud, the prevention and detection of which was one of its principal, if not the prime, objective.

The late 1960s saw the dawning of what, for auditors, was to become an era of new challenge and enlightenment in their profession. Cost considerations forced the time honoured 100 percent check process to be put under scrutiny by auditors and clients alike and it was progressively replaced by a process of random checking, and then selective testing, by which the auditor formed a conclusion as to the regularity and probity of the overall affairs of the organisation on the basis of experience with those financial activities which had been fully scrutinised.

This change reduced the cost and the tedium of audit and it brought with it the need for a much higher degree of professional judgment on the part of the auditor – judgments as to what type of transactions to check, what proportion of transactions would be a fair indicator and, having completed the self allotted program, the formation of a conclusion as to whether these efforts and the results of them supported the issue of a clean audit report.

It also brought risks, the principal one being that fraud or error could have been perpetrated within unchecked transactions and remained undetected – and the risk that the auditor would be seen to have failed in the basic responsibility and be held professionally and financially responsible for it.

This situation evidenced the need for a much more sophisticated and scientific approach to the audit task. The whole thrust of audit changed as did the skills necessary to carry out an effective audit. Auditors began to focus on financial systems of organisations, the methods by which transactions were initiated, processed, documented and recorded in the accounting records and, by an evaluation of these, identify areas of potential risk to which audit emphasis should be directed.

They began to direct the attention of management to the protective and economic value of instituting systems and procedures which contained inbuilt checks, balances and control mechanisms, to provide automatic safeguards against impropriety and human error.

They decided that audit resources were too scarce and costly to be devoted to the scrutiny of transactions of relatively insignificant value; it was not sensible to spend thousands of dollars if only hundreds were at risk — the concept of audit materiality was born.

They decided that audit resources were too scarce and costly to be devoted to the scrutiny of transactions of relatively insignificant value; it was not sensible to spend thousands of dollars if only hundreds were at risk – the concept of audit materiality was born.

The methodology became known as systems based audit. The distinguishing and, to some extent, worrying feature of it was that because of its highly judgmental nature and despite the degree of professional knowledge and skill behind the judgments, it was no longer possible for auditors to provide certificates implying unequivocal guarantees as to the probity of an organisation's activities or the complete accuracy of its records and accounts.

The objective of audit became the formation of professional opinions on the matters addressed and the certificates and reports of audit became expressions of those opinions

RESPONSIBILITY FOR FRAUD PREVENTION

Where, then, does responsibility for fraud prevention and detection lie in this scheme of things?

The auditing profession says it rests fairly and squarely with management. The auditor's position in the matter is "all care taken but no responsibility accepted". The validity of this approach to fraud is authenticated by all professional postulates and standards in Australia and internationally.

INTOSAI, the International Organisation of Supreme Audit Institutions – the rather grandiose title of an august body comprising Auditors-General (or equivalent) at national level of some 90 countries throughout the world, states in support of one of its auditing postulates:

> It is the responsibility of the audited entity to develop adequate internal control systems to protect its resources. It is not the auditor's responsibility. It is also the obligation of the audited entity to ensure that controls are in place and functioning to help ensure that applicable statutes and regulations are complied with, and that probity and propriety are observed in decision making. However, this does not relieve the auditor from submitting proposals and recommendations to the audited entity where controls are found to be inadequate or missing.

INTOSAI also says:

> Auditors need to be alert for situations, control weaknesses, inadequacies in record-keeping, errors and unusual transactions or results which, if significant, could be indicative of fraud, improper or unlawful expenditure, unauthorised operations, waste, inefficiency or lack of probity.

Auditing standards issued by the Auditing Standards Board of the Australian Accounting Research Foundation contain statements of a similar nature alluding to the respective responsibilities of management and audit, and audit's obligation to exercise due care and attention without any inference of ultimate audit responsibility for fraud detection, viz –

- The responsibility for the prevention and detection of fraud and error rests with management through the implementation and continued operation of an adequate system of internal control.
- In forming an opinion, the auditor carries out procedures designed to obtain evidence that will provide reasonable assurance that the financial information is properly stated in all material respects. Consequently, the auditor seeks reasonable assurance that fraud or error which may be material to the financial information has not occurred.

The *Financial Administration and Audit Act*, the very modern Queensland public sector law which, in 1978, supplanted the old 1874 *Audit Act* and has been revised and updated in a number of respects since then, imposes a responsibility on the administration to implement systems and procedures designed to prevent fraud and error and requires the Auditor-General to review these and report any instances where this duty has not been complied with.

Despite all these authoritative and statutory edicts, the fact remains, however, that a thorough or even casual study of accounting journals today will show that the auditor's role in the detection and prevention of fraud is receiving quite a deal of attention worldwide. The push generally is for audit not to be able to skate out from beneath saying "it's management's responsibility". However, it *is* management's responsibility to prevent and detect fraud through the systems it puts in place and, clearly, no one can realistically argue that audit can contribute to the prevention of fraud except, perhaps, by its constant presence and through the auditee's awareness that an audit will be performed at some time or other. The psychological factor is a great deterrent. As to detection, that is where the real dilemma lies.

Some very enlightening statistics appeared in an overseas journal on this question of who believes who is responsible for the prevention and detection of fraud. The survey showed that 60 percent of management were of the opinion that detection and prevention did form part of an auditor's role while only 10 percent of auditors believed they had some responsibility. The same survey showed in a sample selection of fraud cases that 51 percent came to light by sheer accident. Internal control mechanisms were responsible for unearthing 10 percent, a very disturbing feature which reflected poorly on the management control systems.

While this is a reflection of overseas experience, the figures are interesting and are worthy of contemplation. By far the principal factors contributing to the occasion of the frauds in the Queensland public sector have been either the absence of worthwile controls or a failure of management to ensure that those controls which were believed to be in existence were operating in the manner intended. There is no better deterrent to fraud than effective and functioning internal controls. To decide a control's true level of assurance is crucial to the worth of any audit and the auditor's evaluations and advices in this respect are the prime contribution to the prevention of fraud.

Although the systems-based audit methodology and the consequential devolution to management of increased responsibility for fraud protection are comparatively modern developments, the profession quite often tends to seek some comfort in the Kingston Cotton Mill case of 1896 where the judge declared an auditor is not bound to be a detective. He is a watchdog but not a bloodhound. I would suggest that a lot of water has flowed under the bridge since then. The trend in the courts in modern times has been to place more rather than less emphasis on audit responsibility for the detection of fraud.

While I feel it is true to say that auditors are more watchdogs than bloodhounds, they must be very alert watchdogs and forthrightly bring to notice those areas where control mechanisms are weak or non-existent and situations where management's attitude has been reduced to one of complacency. For the profession to cling to some attractive case judgment of the past is foolish. The law is not made by the repetition of past situations. Professional pronouncements and standards are a useful guide but they, too, cannot become absolute refuge nor do they make the law.

FRAUD SURVEILLANCE IN THE QUEENSLAND PUBLIC SECTOR

Speaking at least for public sector audit in Queensland, fraud surveillance constitutes a very important aspect of audit activity. Lest someone should read some sinister connotations into this statement I hasten to explain the reasons somewhat more attention is given to this aspect of audit than modern edicts would seem to necessitate.

The principal reason lies in recognition of the social and political sensitivity of fraud in the public sector. Understandably, I suppose, the public at large, stimulated by the media, attain great heights of indignation about someone with their fingers in the public till whereas the same sort of thing in a company rarely attracts more than passing interest. Quite justifiably the taxpayers expect their elected representatives and others who are entrusted with the management of their affairs and their property to be beyond reproach. Importantly from an audit viewpoint, for the reasons I mentioned earlier, it seems they also have expectations of the auditor that are not altogether in keeping with the modern definition of the role or indicated by professional pronouncements. I believe these expectations, be they justifiable or not, must be given some degree of acknowledgement and this is taken to account in the audit methodologies of my Department.

By far the principal factors contributing to the occasion of the frauds in the Queensland public sector have been either the absence of worthwhile controls or a failure of management to ensure that those controls which were believed to be in existence were operating in the manner intended. There is no better deterrent to fraud than effective and functioning internal controls. To decide a control's true level of assurance is crucial to the worth of any audit and the auditor's evaluations and advices in this respect are the prime contribution to the prevention of fraud.

Auditors are advised that whilst they must not become obsessed with fraud, they must be constantly vigilant and adopt a lower level of tolerance in their materiality assessments where fraud risks are evident. They are told to be on the alert for such things as –

- High rate of employee turnover (particularly in accounts branch) which might suggest that top management in that area does not want any one employee to learn the ropes too well.
- Excessive and unjustified cash transactions.
- Failure to reconcile bank accounts.
- Excessive number of bank accounts which do not appear to have a true business purpose.
- Business dealings with no apparent economic purpose.
- Questionable leave practices; such as the failure of an employee to take leave. Many schemes of fraud in all of its manifestations (including computer-assisted fraud) require careful monitoring by a perpetrator.
- Reticence, sensitivity, defensiveness, diversionary tactics, etc when explanations are sought.

In effect, fraud surveillance is, within reasonable bounds, an audit function in its own right and not simply an automatic

spin-off from the systems based audit approach to the attest/regularity/compliance/value for money audit.

No discussion on fraud these days would be complete without some reference to computer fraud which can present particular and unique difficulties in terms of both prevention and detection. Basically the approach to prevention is no different from that for any other fraud – the inclusion in computer systems of inbuilt checks, controls and balances.

This is facilitated in the Queensland Government area by a standing requirement that my Department be consulted in the course of development of all projects involving the computerisation of financial administration systems. Thus my officers are in at the ground floor, as it were, and in a position to contribute substantially to the inclusion of security controls.

There has been no incidence of significant computer fraud in the Queensland Government.

Auditors are not intended to be, do not pretend to be and, in fact, are not an impregnable barrier between the integrity of the government's operations and the temptations of the devil. Management must build the fences to protect the system from the inequities within and without.

ONCE FRAUD IS DETECTED – WHAT THEN?

The Auditor's (or the Auditor-General's) capacity to pursue fraudulent activities through to their ultimate conclusion, the prosecution of the culprit, is quite limited and in reality other people are far better qualified and professionally equipped to carry the action beyond a certain stage of the processes. Essentially the auditor's job is done once he or she has fully explored all avenues from which evidence is available within the structure being audited, and has documented and reported all findings which constitute evidence of fraud. From there on the issue has to be taken up by police investigators who have access, which audit does not have, to sources external to the auditee body through which audit suspicions can be confirmed and/or further evidence can be obtained.

It is true that the Queensland law empowers the Auditor-General to examine anyone under oath in the course of investigations and this might mean that people other than officials of the auditee body can be questioned. This has not been tested to my knowledge. In any event, I take the view that as police officers are expertly trained and skilled in this function and they have the responsibility of gathering and collating the evidentiary material on which charges are to be based, it is far better if I and my officers confine our activities within our traditional function and area of expertise.

Of course, every possible assistance is given to the police investigators and my officers give evidence as witnesses when required in consequential legal proceedings.

I was interested to read very recently some advices given to auditors in 1959 by the then chief crown prosecutor of Queensland, Mr R F Carter (later Judge Carter). Amongst other things he said –

> Be very careful in questioning the suspect. Remember, you are carrying out your investigation as an auditor, not as a detective. Much harm can be done to the police investigation when the auditor tries to usurp the role of the police officer and seeks to get a confession. This is one of the pitfalls against which . . . I would warn you.

CHALLENGES FOR THE FUTURE

I will conclude with a brief comment on developments which have potential for increasing the scope for and thus the incidence of fraud in government. I have in mind the growing movement towards autonomy of decision making, reduction in prescriptiveness in regard to financial procedures and other changes all designed to provide flexibility to organisations – in effect, to "let the managers manage".

I must preface my comments by saying that I support the concept wholeheartedly subject to the proviso that this devolution of responsibility and authority is accompanied by the third essential element – effective accountability.

From an audit viewpoint, however, it presents the prospect of a further philosophical and attitudinal adjustment. The compliance aspect of audit will take on a different dimension in that instead of the fairly straightforward black and white decision as to whether an organisation has conformed with a quite definitive requirement, the auditors will find themselves in the grey judgmental areas of decision as to the adequacy of management's attainment of the objectives of comparatively broad principles.

I do not see this as a significant problem for public sector auditors. It simply brings a further judgmental dimension into the audit function.

The problems will arise if management makes a decision on economic grounds that results in loss of internal controls and securities to an extent seen by auditors as creating an unacceptable risk of fraud, error or misapplication of resources. In such circumstances, where management is prepared to accept the consequentially increased risks despite audit objections, audit will have to recognise management's rights.

Auditors must, however, also protect their own flanks through clear documentation of their viewpoints, the reasons for them and management's attitude to them, and, if appropriate, report through the proper channels.

CONCLUSION

Auditors are not intended to be, do not pretend to be and, in fact, are not an impregnable barrier between the integrity of the government's operations and the temptations of the

devil. Management must build the fences to protect the system from the inequities within and without.

Audit will review these systems, counsel and advise and in so doing make a very significant contribution to the integrity of the functions of government and its instrumentalities. It cannot assume, however, the prime responsibilities and must report any serious failures of management.

Finally, despite professional and even legislative decrees defining the obligations of management and audit respectively, the reality is that public expectations have an important influence on the emphasis given to fraud surveillance in the public sector.

Impediments to Tackling Fraud

Ian Temby*

The sad truth is that crime against the Government often does pay.
– Comptroller-General, US General Accounting Office, Report to Congress, 7 May 1981.

We are gathered here to discuss a timely and important general topic, namely fraud within and upon the public service and its programs. The particular question which I will address is this: what are the principal impediments to tackling such fraud?

Those impediments fall into two areas. One is detection which necessarily precedes investigation and prosecution. It is a matter of extraordinary difficulty to find out that there is a fraud problem within an agency or one of its programs, and that difficulty is exacerbated by a natural organisational desire not to know. Secondly, if and when that problem has been overcome and a case of serious fraud is detected, there are grave difficulties in investigation and prosecution. They arise from the undoubted fact that these cases are generally of great complexity and the legal system within which those responsible for tackling fraud must work is both antiquated and inefficient.

It is proposed to expand upon these propositions and in so doing make some reference to the Review of Systems for Dealing with Fraud on the Commonwealth (the Fraud Review). Because despondency is negative in effect I will point to the various ways in which improvements have become manifest. Finally it will be suggested that policy officers and prosecutors can only do so much, and it is in the best interests of those who run public sector programs, as well as being in the national interest, for them to heighten their awareness of the fraud problem and tackle it with vigour rather than wishing the problem away. Principal responsibility must reside with those at senior level who run programs.

As to detection, let me state my position plainly. Whenever large sums of money flow to or from government there will be fraud. To the extent that individuals are telling lies to reduce taxes or increase transfer payments, and the amounts involved are modest the problem is of no staggering significance. All that is necessary is to have those people looked out for and dealt with as appropriate. But if the pot of gold is large enough some will cream off big sums of money. Those cases must be watched for and a strong, positive approach is necessary. Often large financial benefits will be derived by organised groups. The problem is then so much the worse because those in a criminal conspiracy which reap big rewards almost invariably move on to other areas. It is essential if the integrity of programs is to be maintained that those responsible start with the assumption that large payments to or from government invariably attract fraudsters. To say that no fraud problems have come to light is a pitifully inadequate answer. Such problems must be looked out for. Great ingenuity is called for, because there will be great ingenuity on the other side.

Areas of large government expenditure where few if any incidences of fraud have been brought to the attention of my office for prosecution include defence procurements, agricultural subsidies and overseas aid. In the United States of America, where fraud in defence procurement is known to be a serious problem, the Department of Defense Office of Inspector General published a booklet titled *Indicators of Fraud in Department of Defense Procurement.* It identified matters such as bid rigging, offering of bribes or gratuities, mischarging costs to the government under cost reimbursement contracts, knowingly submitting defective cost or pricing data, and product substitution. I am not to be taken as suggesting that the same situation exists in this country: safeguards may be perfectly adequate, and the contracting conditions might be quite different. I am suggesting that there is need for vigilance. Nor would I advocate what may be seen as a peculiarly American response to fraud in government contracting. It involves the resurrection of an obscure law passed during Abraham

* Ian Temby, QC, is Director of Public Prosecutions. Text of an address to the 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, Canberra, 2 May 1988.

CBPA No 56, September 1988, 77-80.

Lincoln's administration, after the public expressed outrage about Civil War contractors who mixed sawdust with gun powder or sold the Government the same horse twice. The Lincoln Law,[1] as it came to be known, provided a percentage of the recovery to the person who exposed the fraud. It fell into disuse after a series of restrictive court decisions. Under the False Claims Amendments[2] introduced in 1986 anyone who knows of fraud by a government contractor is empowered to take that contractor into a Federal Court filing suit for triple damages on behalf of the United States Treasury. The law includes a powerful incentive for potential whistle blowers. They get a minimum of 15 percent of any recovery.[3]*

Whenever large sums of money flow to or from government there will be fraud. To the extent that individuals are telling lies to reduce taxes or increase transfer payments, and the amounts involved are modest, the problem is of no staggering significance. All that is necessary is to have those people looked out for and dealt with as appropriate. But if the pot of gold is large enough some will cream off big sums of money. Those cases must be watched for and a strong, positive approach is necessary.

Significant action has been taken to improve dealing with known areas of fraud. An example is a change in procedure by the Department of Social Security, which now transmits most of its benefits by bank transfer rather than by cheque. This greatly reduced the opportunity for both the theft and the forging and uttering of these cheques. Whilst not major crime, these had been a major problem because of the prevelence of the offences. The Australian Federal Police had a mouldering pile of cases that they could never investigate. This problem has been largely overcome by this quite simple administrative procedure.

There have been significant improvements in dealing with taxation fraud. Prosecution of large scale income tax fraud known as "bottom of the harbour" cases is as large and difficult as Australia has seen. Each typically involves several hundred stripped companies. To prosecute it is usually necessary to select a representative sample of stripped companies, but even then the evidence may involve tens of thousands of documents. The conduct of these cases highlighted the difficulties that the traditional legal system has in coping with fraud cases of this size and complexity. Nevertheless successes have been achieved and, in combination with legislative changes, the schemes eliminated.

This experience increased awareness of the need to be alert for large scale abuses in any area and the desirability of taking decisive action quickly. A more recent area of increased fraudulent activity is sales tax. Sales tax schemes divide into two main categories. Both are being dealt with. One category involves schemes which are highly artificial and arguably illusory aimed at drastically reducing the sale price upon which tax is paid. The other has to do with more flagrant and crude methods of evading sales tax. These include quoting false or stolen sales tax exemption numbers to purchase goods tax free, preparing fraudulent invoices and submitting false returns. In this second category, loosely termed cash economy schemes, the goods are usually sold in the markets and other places where sales are difficult to trace. A somewhat surprising and disturbing feature of the cash economy schemes has been the involvement of major criminal figures in two of the largest matters — a murder today, a drug importation tomorrow, and next week collecting payments that should have gone to the government as sales tax.

The Australian Taxation Office has established intelligence units to detect tax avoidance schemes as they emerge. In more recent times particular attention is being paid to arrangements involving international transactions.

Taxation offences have been consolidated under the *Taxation Administration Act* 1953, penalites have been increased and there has been increased use of the prosecution process with subsequent deterrent effect. The offences involved are matters such as failure to lodge returns, failure to keep records, and failure to provide information. While not direct fraud in themselves they can be symptomatic of the type of behaviour that is used to disguise fraudulent practices.

There have been a number of significant advancements which directly touch on my office. In the Director of Public Prosecutions Annual Report for 1984-85 I raised the difficulties caused by the lack of Commonwealth provisions allowing the obtaining of evidence overseas in criminal matters. One prosecution had to be abandoned because evidence obtained overseas could not be made admissable in Australian courts. Operators in the area of revenue and other fraud frequently resort to tax havens and the like. It has been observed on a number of occasions that sometimes what is essentially a domestic fraudulent enterprise will have an overseas loop built in so as to frustrate investigation. It was a notorious fact that investigators and prosecutors had great difficulty in pursuing paper and money trails overseas. Since then there have been amendments[4] to the *Commonwealth Evidence Act* 1905 to overcome these problems. While the procedures are involved and there have been some teething difficulties there are a number of important fraud prosecutions currently proceeding which would not be viable without the assistance of this legislation.

The Government conferred wider civil remedies functions on the Director of Public Prosecutions with effect from 1 July 1985.[5] The Office of the Director of Public Prosecutions had been given a civil remedies function, initially on a limited basis, since it was established on 5 March 1984. The function does not involve additional powers of recovery or confiscation of money or assets. It empowers the DPP to become involved in civil recovery actions by or on behalf of government agencies as against actual or suspected criminals who might owe them money.

* On this matter see also Peter Grabosky's paper below.

It allows a co-ordinated approach of criminal prosecution and civil recovery against persons who engage in criminal activity to defraud the Commonwealth. The 1985 amendments enable the Director to exercise this civil remedies function in matters connected with or arising out of actual or proposed prosecutions or a matter connected with a course of activity which is being considered for the purpose of deciding whether to institute a prosecution. The ability to exercise civil remedies prior to the commencement of the prosecution is important. It allows the securing of assets before they can be dissipated.

Acknowledging that the extended civil remedy function was a novel one the legislation also required that I report to Parliament at the completion of two years of operation. In the two year period to 30 June 1987 the amount recovered pursuant to this function was over $37.5 million. The direct cost was $5.8 million. The main agencies concerned were the Australian Government Solicitor, the Australian Taxation Office and the DPP. It is an example of what can be achieved through a co-ordinated and co-operative approach. The main area of recovery was taxation; there were also recoveries in the Social Security and Medifraud areas.

A major government initiative has been the *Proceeds of Crime Act* 1987. This Act enables the recovery of the proceeds of indictable offences following conviction. Property used in or in connection with the offence or property derived or realised directly or indirectly from the proceeds of the offence can be forfeited to the Commonwealth. Also a pecuniary penalty equivalent to the value of the benefit derived by a person from the commission of the offence can be ordered. This can then be enforced as a civil judgment against the property of the defendant which cannot be connected to the offence. The Act also provides for restraining orders to be obtained over property at any time up to 48 hours prior to charging. This preserves the property until a final determination of the forfeiture or pecuniary penalty application. It is early days in the application of the legislation but indications to date are promising. Substantial assets have been restrained in respect of offences in areas including Social Security fraud, Medifraud and Customs duty fraud.

The Fraud Review also concentrated on areas of known fraud. It looked at relationships between agencies involved in dealing with fraud on the Commonwealth. It concentrated on arrangements for dealing with detected financial fraud. Its terms of reference were somewhat limited in that it did not consider the extent or scale of fraud, areas of undetected fraud or examine in detail measures in place to prevent or detect fraud or any lack thereof.

There have been a number of positive effects resulting from the Review's recommendations. The thrust of the recommendations is that agencies are to be responsible for the prevention, detection and investigation of fraud against their own programs. All agencies are required to assess and report on the risk of fraud against their programs. Agencies are then required to develop arrangements for fraud control for inclusion in corporate plans or where necessary develop detailed plans for fraud control. A fraud control committee has been established to monitor the implementation of the Fraud Review's recommendations as well as other government initiatives in relation to fraud.

One result of these requirements seems to be a change in organisational attitude in some agencies which previously assumed that they had no fraud and had few if any systems or resources in place to detect and deal with fraud. A number of agencies which have had little if any previous contact are now starting to liaise with the DPP concerning the possibility of prosecuting persons for defrauding their programs.

Some of these agencies are aware of an extent of overpayments in connection with their pograms and have used traditional steps for recovery with varying success. They find the possibility of taking prosecution action with its deterrent effect and co-ordinated recovery options not unattractive. One of the difficulties they face is lack of investigative experience sufficient to enable a prosecution to be mounted. They can be assisted in this area. It will take time but it is expected that extra fraud prosecutions will be the eventual result.

Accepting that there is a need to safeguard the handling of information which may be private, confidential and sensitive nevertheless it becomes an absurdity when fraud on the Commonwealth is facilitated by the enforced lack of communication between agencies. Appropriate amendments are not difficult. Reform in this area has been mooted for some time. Unfortunately nothing has occurred to date.

The Fraud Review also recommended that the Comptroller-General of Customs and the DPP consider the use of criminal sanctions in appropriate Customs fraud cases. On-going liaison has commenced and criminal action has been taken in a number of Customs matters and more are under consideration.

A constant impediment to dealing with fraud on the Commonwealth is posed by secrecy provisions in Commonwealth legislation. In carrying out its various functions the Commonwealth Government gathers and retains a considerable quantity and variety of information concerning the affairs of its citizens. That information is collected by the various agencies responsible for programs and held in separate repositories. The information is needed, among other things, to determine entitlement to benefits and liability to contribute to revenue.

Secrecy provisions generally restrict the sharing of this information between Commonwealth agencies. Such sharing of information would greatly assist the detection of fraud. For example, a common method of defrauding the Department of Social Security is for employed people to claim unemployment benefits. Because they are employed they are required to file tax returns. A comparison of information would reveal welfare cheats as well as possible non-disclosure of income for revenue purposes.

An exchange of this type of information between agencies would clearly be a straightforward and effective method of detecting and deterring fraud. The vagaries of criteria for release of information can also lead to anomalies. During the investigation of a doctor alleged to have defrauded the Health Insurance Commission it became apparent that the amount received from the Health Insurance Commission was likely to be at variance from the amount declared to the Australian Taxation Office. Each agency was prevented by secrecy provisions from disclosing information to the other: each could disclose the information to the DPP but on condition that the DPP did not reveal it to the other.

Secrecy provisions and their effects were considered in some depth by the Fraud Review. It was of the view that "if it ever was possible to deal adequately with fraud without access to relevant information, that time is past". It recommended that agencies co-operate in providing information to each other and that where it was cost effective they consider matching of information relevant to identifying instances of fraud. Importantly it also recommended that the DPP, the Australian Federal Police and the National Crime Authority have adequate access to information from the Australian Taxation Office, the Health Insurance Commission, the Department of Social Security and the Australian Customs Service. The information had to be for or in relation to law enforcement, prosecution or civil remedy purposes within the scope of the functions of the receiving agencies, and be in connection with an alleged or possible indictable offence.

Whilst recognising that there are always privacy considerations involved in allowing the release of any information, it is difficult to see any justification for not allowing access along the lines of this recommendation. There are more than 17,000 thousand taxation officers with potential access to tax information. Disclosure to law enforcement agencies would involve a relatively small increase in the numbers with potential access. The released information could only be used within the functions of the receiving agency. The subject of the information must be suspected of having committed an indictable offence against the Commonwealth, that is to say, a distinctly serious offence. It is my view that officers in the agency receiving the information ought to be placed under the same individual confidentiality constraints as apply to officers in the agency where the information is held. Given the great benefits that would flow, it is hard to understand why this suggestion has not been adopted. What can be wrong with it?

Accepting that there is a need to safeguard the handling of information which may be private, confidential and sensitive, nevertheless it becomes an absurdity when fraud on the Commonwealth is facilitated by the enforced lack of communication between agencies. Appropriate amendments are not difficult. Reform in this area has been mooted for some time. Unfortunately nothing has occurred to date.

In concluding I should say that I am generally optimistic about the current ability to deal with detected areas of fraud on the Commonwealth. The Australian public and institutions received quite a jolt from the magnitude of large scale income tax evasion in the 1970s and the apparent inability of institutions as they were then organised to deal with it. The implications if fraud of that size continued undeterred are quite staggering. There has since been a recognition of the resources and the will necessary to tackle such difficult cases and quite important successes have been achieved both in recovering the funds and in prosecuting the offenders. The length and complexity of these cases has been exacerbated by the traditional legal framework within which they have been conducted. Given the ingenuity of the human mind and greed of human nature large scale assaults on the public purse will continue from time to time. The area of operation will vary depending on perceived weaknesses in the system. There is a demonstrated ability to deal with such assaults when they are discovered. The level of expertise in doing so has increased significantly. It is important that there are systems in place to enable their discovery at an early stage before large scale harm is caused.

ENDNOTES

1. *False Claims Act* of March 2, 1863, Ch 67, 12 stat 696.
2. *False Claims Amendments Act* 1986, Pub L No 99-562, 100 stat 3153.
3. Ibid, section 3.
4. *Evidence Amendments Act* 1985.
5. *Director of Public Prosecutions Amendment Act* 1985.

Prosecution of Fraud on Government

Kevin Zervos*

The prosecution of fraud on government is as difficult and daunting a task as is its detection. Fraud by its nature lacks fixed characteristics; it is a broad concept and varies in type, size and complexity. Whether the fraud is within or upon government it will generally occur in the areas of benefit giving, revenue raising and contracting of services. While much attention has been focused on the general problem of fraud on government an aspect that still remains neglected is large complex commercial fraud. It is this type of fraud that I wish to examine.

Large complex commercial fraud occurring on government today is a relatively new phenomenon which cannot be restrained simply by using traditional methods. Consequently, new methods and techniques need to be employed to investigate and prosecute large complex commercial fraud.

It is only recently that law enforcement agencies and governments have come to realise the enormity of the problem of fraud on government.[1] This problem has been further exacerbated by a criminal justice system that is mainly geared towards dealing with offenders of the more traditional crimes of violence and property. It is, therefore, not surprising to find that the criminal law, rules of evidence, judges, lawyers, law enforcement officers, and courts do not adequately deal with large complex commercial fraud.[2] The recent "bottom of the harbour" frauds exposed the difficulty the legal system had in handling such matters. At the time the "bottom of the harbour" frauds occurred "defrauding the Commonwealth" by way of a conspiracy was the only available offence and there was no offence for someone acting alone in "defrauding the Commonwealth". When the offenders were brought to justice it was generally acknowledged that the maximum sentence for conspiracy to defraud the Commonwealth was signficantly inadequate.[3] Clearly, the legal system had not envisaged the scale and type of fraud and was therefore unable to appropriately respond. The matter was summed up by Carter J in *Queen v Maher and Donnelly*:

> In respect to the first matter, that is the conviction for conspiring to defraud the Commonwealth, it is obvious from the comprehensive material placed before the jury that the Commonwealth was the victim of a massive fraud. In saying that, it necessarily follows that the real and ultimate victims were the many millions of honest citizens in this country who, as a result of this fraud, have had to bear the burden of the revenue lost through the implementation of this fraudulent scheme.
>
> The maximum penalty of three years imprisonment for conspiring to defraud the Commonwealth was fixed decades ago. The framers of the legislation could never have foreseen the formation and implementation of a conspiracy to defraud which would deny to the public revenue, millions and millions of dollars of revenue and which have such far reaching consequences for the citizens of the Commonwealth. Had they done so, one could readily have conceived the fixing of a more substantial maximum penalty.[4]

Large complex commercial fraud occurring on government today is a relatively new phenomenon which cannot be restrained simply by using traditional methods.

WHAT IS FRAUD?

Crimes committed within or upon government will generally be covert and often detected well after the event. The Roskill Report[5] observed that for fraud to succeed it must be concealed from its victim and even when detected the offender would take steps to conceal the way in which the fraud was perpetrated. This made the process of investigation and prosecution more difficult. It was also noted that in serious cases "documents may be falsified or destroyed and arrangements may be made for some transactions to take place in other jurisidictions, and for the proceeds of the offence to be removed there later perhaps to be followed by the fraudsters themselves."[6]

A recent example of this type of fraud in Australia was seen in *R v Rosenthal and Ors.*[7] This was an appeal on sentence and the Court of Criminal Appeal had this to say about the fraudulent conduct:

> We are satisfied the proper characterization of this scheme is that it was a sophisticated and large scale conspiracy designed to defraud the Commonwealth. It was sophisticated, insofar as its creation, manipulation and operation required devious intellects to devise, professional and technical skills to manage, application and tenacity to operate. The scheme, in its pristine condition, was intricate and deliberately embellished with legitimate aspects in order to make it appear attractive. The manoeuvring of the taxpayers' money into and out of superannuation funds in Liechtenstein and Swiss banks gave the scheme, to the uninitiated, a superficial reality. It was deliberately designed to beguile. The very heart of the scheme was to make it complicated, and thus less easily detectable. The scheme had inbuilt "audit breakers" which were devices for making it impossible for an auditor or the Commissioner to follow

* Kevin Zervos is Senior Assistant Director, Office of Commonwealth Director of Public Prosecutions, Melbourne. Text of an address to Australian Institute of Criminology Seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

the flow of funds. This was a deliberate ingredient of the scheme, designed not to obscure its workings, but to go further and make the various fraudulent transactions undetectable. It is probably this reason which inhibited the Commonwealth authorities from speedily untangling the scheme.[8]

Admittedly, considerable inroad has been made in combating fraud on government but we have only seen the tip of the iceberg. The emphasis in Australia has been on prevention of fraud with little attention being given to the problems of investigation and prosecution. It has been inappropriately left for the legal system to sort those problems out.

The Review of Systems of Dealing with Fraud on the Commonwealth[9] provides the following useful analysis of fraud:

> What is contemplated under the heading "fraud" is a variety of offences which may be defined in part by use of such words as "fraud", "defraud", "fraudulent", or "fraudulently", which usually require deceit, an intention to deceive or deliberate non-disclosure, and some actual or possible injury or loss to the victim of the offence. Until the enactment of Section 29D of the Crimes Act 1914 in 1984, there had been no offence of "defrauding" the Commonwealth (as distinct from "conspiracy to defraud").
>
> Section 29D does not define "defraud", and courts have not limited themselves by putting forward a comprehensive definition of "fraud". The term is not a tool designed for a single use or purpose, and its meaning varies according to the function it is intended to serve. Clearly however, it contemplates both the deliberate evasion of a liability and obtaining a benefit by dishonesty. In lay terms it may be relevant to identify fraud by asking "did the author of the deceit derive any advantage which he could not have had if the truth had been known?"

WHY TACKLE FRAUD WITH CRIMINAL SANCTIONS?

In the United Kingdom the Roskill Committee[10] was established due to public concern at the effectiveness of the methods of combating serious commercial fraud. The Roskill Report made this telling observation:

> The public no longer believes that the legal system in England and Wales is capable of bringing the perpetrators of serious fraud expeditiously and effectively to book. The overwhelming weight of the evidence laid before us suggests that the public is right. In relation to such crimes, and to the skilfull and determinable criminals who commit them, the present legal system is archaic, cumbersome and unreliable. At every stage, during investigation, preparation, committal, pre-trial review and trial, the present arrangements offer an open invitation to blatant delay and abuse. While petty frauds, clumsily committed, are likely to be detected and punished, it is all too likely that the largest and most cleverly executed crimes have escaped unpunished.[11]

While the picture may not be as bleak in Australia, it is true to say that most of problems identified by the Roskill Report exist in Australia today. Admittedly, considerable inroad has been made in combating fraud on government but we have only scraped the surface. The emphasis in Australia has been on prevention of fraud with little attention being given to the problems of investigation and prosecution. It has been inappropriately left for the legal system to sort those problems out.

Mr Ian Temby, QC, the Commonwealth Director of Public Prosecutions provides three main reasons why it is important and worthwhile to tackle revenue and corporate crime:

> The first main reason why it is necessary to pursue transgressions of the type under consideration is that satisfactory law enforcement is possible only given public support and that support is at risk of being forfeited if there are certain areas which remain out of reach. It cannot be good enough to justify any prevailing lack of activity by saying that investigations and prosecutions in the problem area are difficult, require the dedication of substantial resources, are therefore expensive, and tend to become protracted. As long as there is room for the perception that law enforcement is ineffective in relation to certain types of misconduct, then the consequences will be an upsurge of dishonesty in that area, and a severe diminution of public confidence. That was the main lesson taught by the taxation conspiracies which flourished unabated for many years.
>
> The second reason is that effective law enforcement against commercial criminals tends to have salutory discouraging effect. Much serious crime is committed in the heat of the moment while passions are aroused, or the motivation is need rather than greed. Such crimes will always be with us. But those who commit crimes in or about the world of commerce have generally indulged in much prior planning, and they are ostensibly respectable citizens living in comfortable circumstances. For people such as this the prospect of imprisonment has a special dread. Even an occasional successful prosecution will send out messages which are very powerful. It is particularly satisfying for prosecutors to do work which is likely to provide a general deterrence, actually rather than theoretically.
>
> The third reason, already adverted to, is that if commercial crime is widespread then the impact upon the average citizen is very great. Just as the activities of those who steal from shops increase the cost of goods to honest shoppers so it is in relation to revenue and corporate frauds.[12]

It has been realised for some time now that there are more serious instances of fraudulent activity (causing or calculated to cause loss to the Commonwealth) requiring the utilisation

of full criminal sanctions, with imprisonment as a likely final outcome. The advantage of following this course is that it will serve to remind and warn major fraudsters, and those inclined to behave in that manner, that the direct consequence of their criminality can be the loss of their liberty.[13]

In *R v Rumpf,*[14] McGarvie J (with whom the other members of the court agreed) identified three significant effects as a result of the perpetration of serious revenue fraud:

> The offences to which the respondent pleaded guilty are serious offences. They involve preying upon the public to satisfy his greed for large amounts of money. I agree with Mr Uren's submission that crimes such as these have three significant effects. They lessen the ability of the Government to provide for the community out of taxation funds; they impose unfair burdens on honest citizens who pay their taxes; and citizens who see people prosper on the proceeds of crimes are tempted to follow their corrupt example.[15]

THE PROBLEMS THAT ARISE IN PROSECUTING FRAUD

Until recently, there has been only limited consideration as to whether the ingenuity of the tax avoidance industry has trespassed into the area of fraud. Apart from the rather crude tax frauds involving the transfer to straw directors, who cannot be traced, of companies that had been stripped of their current year profits and rendered incapable of meeting their tax liability, there are schemes which include the purported treatment of current year profits. Then there are schemes where the fraud may be said to lie in the manner of their implementation rather than their conception. The difficulty facing prosecutors is that schemes which are apparently fraudulent are often put forward as lawful and this blurring between avoidance and evasion makes detection all the more difficult, especially when the criminal activity becomes more sophisticated. Further, the diverse nature of revenue frauds, and the fact that they vary in form and degree, also creates problems. Nevertheless, the issue is not one of commercial validity but of criminal liability and the prosecution must therefore prove dishonesty. On this question Carter J in *R v Maher and Donnelly*[16] noted:

> The essence of this scheme was dishonesty. Behind the so called facade of respectability there was a well designed process which involved the receipt by you of huge sums of money, and one in which advantage was taken of persons who were, for the most part, commercially ignorant and who for a pittance, relatively speaking, were induced to sign documents and cheques so as to present a false picture. The misuse of these so called "commercial illiterates" was at the heart of this dishonest and fraudulent process.[17]

The greatest difficulty in the prosecution of fraud arises well before that process commences. The mounting of a successful prosecution for fraud will always be dependant on those responsible for the investigation identifying at an early stage the matters most likely to reveal the commission of criminal offences and what those criminal offences might be. Their efforts need to be concentrated on building up a case founded on admissible evidence and focusing on the main participants.[18] To do otherwise could result in an enormous waste of time and effort.

Furthermore, it is difficult for a police force to generate within its own organisation the wide range of skills and experience necessary for the investigation of complex commercial fraud. Consequently, there is a need for a collective effort, bringing together the relevant skills and experience. Basically, such skills include accounting expertise, with particular reference to any specialist background relevant to the investigation, and legal expertise in respect to the fraudulent conduct, criminal practice and procedure and the complex rules of evidence.[19] Fundamental to a successful prosecution is the early involvement of lawyers, ensuring that the investigation and evidence gathering are proceeding on the right track.

The early detection and investigation of fraud is crucial to the chances of successful prosecution. Adequate systems of discovering fraud also act as a deterrent and help prevent fraud occurring in the first place.[20]

Law enforcement responsibilities within government agencies are either inadequately defined or non existent, this problem is further compounded by a fragmented approach to enforcement. The Roskill Report concluded that the principal weakness in the process of investigation and prosecution of fraud was the fragmentation of law enforcement organisations and the diverse nature of their responsibilities.[21]

Special Prosecutor Robert Redlich observed that "poor administration, structure, training and resources"[22] allowed organised crime the opportunity to flourish. In addition, he noted that extensive criminal activity was successful because it traversed the areas of responsibility of a number of government departments which failed to co-operate with each other.

The Review Report found that in most government agencies there was little or no training of agency staff in the prevention, detection or investigation of fraud.[23] It also found that the secrecy provisions in Commonwealth legislation can act as an impediment to the exchange between agencies of information which could facilitate investigation, prosecutions, the pursuit of civil remedies and debt collection. The report also noted that the matching of data is an effective means of preventing and detecting fraud and that its wider use should be considered and publicised.[24]

Arie Freiberg in an article entitled *Enforcement Discretion and Taxation Offences* examined the commitment of regulatory agencies to law enforcement and formed the view that:

> If the primary agency responsible for law enforcement is the police force it is more likely that criminal prosecutions will follow than if a regulatory agency is involved. The major difference between the police force and regulatory agencies is that the latter do not see their task as catching "criminals" but as containing deviants. They do not seek to prosecute and stigmatise their subjects but rather to obtain compliance through negotiation. Most crucially,

for non police bodies, the criminal law is regarded as a last resort.[25]

Regulatory agencies tend to see their primary task not as the investigation of crime, but the administration of their Acts. Unfortunately, there appears to be a disincentive for regulatory agencies to seek out and deal with fraud due to a variety of reasons including, the embarrassment of the fraud and the deficiencies in the agency it would reveal, the disruption it would cause the agency, and the revelation of the fraud may encourage others to do likewise.

It has been my observation that the Australian Federal Police (AFP) lack the appropriate mechanisms and resources to investigate effectively large complex commercial fraud. My experiences with the AFP indicate that while senior officers are skilled and dedicated, they sometimes have to rely on inexperienced and untrained officers to do the tasks of many.

The reluctance of regulatory agencies to seek the involvement of police has been the subject of concern and this was acknowledged in the Review Report. The major thrust of the Review Report is that the responsibility and accountability for preventing, detecting and handling fraud should be more clearly directed to the agencies whose systems are the subject of the fraud and that, generally speaking, the Australian Federal Police, the Director of Public Prosecutions and the Australian Government Solicitor should be required to deal only with the more significant cases.[26] The Review Report sets out a number of recommendations that deal comprehensively with the issue of fraud on the Commonwealth. The following specific recommendations identify the need for regulatory agencies to investigate and prosecute fraud on the Commonwealth, and to train staff to meet that end.

RECOMMENDATION 1:

That the principal responsibility for the prevention and detection of fraud rests with the agencies against whose program fraud is attempted.[27]

RECOMMENDATION 2:

That all agencies accept the responsibilities of investigating routine instances of fraud against them, whether the investigation is likely to be followed by the application of an administrative remedy or by reference of the matter for prosecution, and that instances of fraud referred to the AFP for investigation should generally be those which are more complex or larger in scale than the most routine cases.[28]

RECOMMENDATION 5:

That, unless they have already done so, within 6 months of acceptance of this recommendation all agencies which in the proceeding 3 years have referred a total of more than 20 matters involving fraud (excluding cheque frauds) to the AFP or the DPP, in consultation with the AFP and the DPP, develop and implement criteria and guidelines on the basis of which future references are to be made.[29]

RECOMMENDATION 11:

That agencies provide appropriate training to staff in the prevention, identification of detection of fraud, and where appropriate liaise with the AFP about training in investigative skills and techniques and with the DPP or, as appropriate the AGS about training in the preparation of briefs of evidence.[30]

It has been my observation that the Australian Federal Police (AFP) lack the appropriate mechanisms and resources to investigate effectively large complex commercial fraud. My experiences with the AFP indicate that while senior officers are skilled and dedicated, they sometimes have to rely on inexperienced and untrained officers to do the tasks of many. I have seen far too often the AFP unable to cope with large complex commercial fraud due to no fault of its own. The AFP is under-staffed and with insufficient resources. The officers in the fraud area need training and additional support.

To tackle fraud on government efficiently it is essential that you have a dedicated and effective police force trained and appropriately staffed to deal with such criminal conduct. Apart from dealing with the problems of detection and concealment of a crime, the investigation will generally involve an inquiry of considerable duration requiring the location and compilation of thousands of documents and the interviewing of numerous witnesses. As observed in the Roskill Report "any failure in the early stages to gather all the necessary evidence and any wrong decisions about the course of the investigation will very likely prejudice the chances of a successful prosecution."[31]

The prosecution process also has its problems. The observations of the Roskill Report concerning the need for reform in the area of the substantive criminal law and rules of evidence in relation to fraud are equally relevant to Australia. The range of offences that are available under the criminal statutes that cover the criminal conduct found in fraud are still inadequate. It was only in October 1984 that a substantive offence was created to deal with defrauding the Commonwealth. Furthermore, the substantive criminal law as it presently relates to fraud is obscure and this causes doubt as to the interpretation of the law. Moreover, there should be appropriate offences created that reflect the ambit, nature and seriousness of fraudulent conduct.

Our legal system has historically relied upon oral testimony and this is reflected in the development of the rules of evidence which "seem increasingly inappropriate and burdensome in cases of fraud and dishonesty which themselves arise from business transactions which are the subject of written records."[32] One of the most significant problems in fraud cases concerns the state of the rules of

evidence as they relate to documents. The rules of evidence as they stand today did not and do not envisage large document fraud cases, where documents may be generated by computer or facsimile machines and, in some cases, with no original document ever being created.

As observed in the Roskill Report there are instances when the rules of evidence prolong trials and confuse the jury. Some accused persons take advantage of every conceivable opportunity to play the system and this has been seen during committal proceedings where all too frequently decisions of the magistrate are the subject of review under the Administrative Decisions (Judicial Review) Act 1977 which interrupt and delay the proceedings and provide a further opportunity in another forum to take issue generally on the same matters.

In *Newby v Moodie & Director of Public Prosecutions*, the Full Court of the Federal Court in an unreported decision, 3 June 1988 said:

> Cases abound in which the Court has said that the power to make an order of review in respect of committal proceedings should be exercised only in the most exceptional cases. What was said in *Lamb v Moss* (supra, at 564) to this effect has been consistently followed in subsequent decisions of this Court. We are of the view that the same principle should be applied to applications of this sort. The High Court has recently said: "The undesirability of fragmenting the criminal processes is so powerful a consideration that it requires no elaboration from us" (*Vereker and Ors v O'Donovan*, application for special leave to appeal, 18 March 1988).
>
> Since the application in the present case was not made within a reasonable time after the decision sought to be reviewed was made, the trial judge had, at least, a discretion to refuse to entertain the application. (As we have observed above, it may be a question whether he was obliged in law not to entertain it). In our opinion the facts to which we have already referred ought to have led the trial-judge to conclude that he should not entertain the application. Several considerations lead us to this conclusion. First, the delay was very considerable. Secondly, the appellant made a considered decision to pursue in the Local Court his claim that the proceedings were an abuse of process. Thirdly, as the learned trial judge pointed out, the appellant would not have suffered any prejudice had this Court refused to entertain his application because the Local Court stood ready to hear it. Finally, the Local Court or the court in which the applicant is tried (should he be committed for trial) is so obviously the appropriate court in which the applicant should seek a stay of the prosecution that it was inappropriate that this Court's jurisdiction should be invoked.

It is my view that the right of review under the Administrative Decisions (Judicial Review) Act 1977 is an inappropriate interference in the criminal process. Inherent in the criminal process are numerous checks and balances as administered by the State courts. The recent experience of the DPP has shown that defendants involved in major revenue fraud prosecutions are inclined to make applications for review at some stage of the pre-committal or committal process.

HOW TO PROSECUTE FRAUD

The office of the Commonwealth Director of Public Prosecutions was established by the Director of Public Prosecutions Act 1983 which came into operation on 5 March 1984. The principal aims of the office of the Director of Public Prosecutions are:

- to prosecute alleged offences against the criminal law of the Commonwealth in a manner which is fair and just, but is also vigorous and skilful, with a view to appropriate punishment of those found guilty;
- to make alleged offenders disgorge profits or pay monetary penalities, or at least pay their taxes, in accordance with the law;
- to strive to render the law enforcement activities of the Commonwealth and its agencies as effective as is practicable;
- to contribute to the improvement of the Commonwealth criminal justice system by providing sound, constructive and timely advice and recommendations;
- to do all of this to the highest standards capable of achievement;

and thereby encourage compliance with the law, and discourage breaches of it.

Under Section 6(1)(fa) of the DPP Act it is the function of the Director to take, or co-ordinate, or supervise the taking of, civil remedies for the recovery of taxes, duties, charges or levies due to the Commonwealth in matters connected with an actual proposed prosecution or a matter being considered with a view to prosecution. In addition the DPP has been given significant new functions under the Proceeds of Crime Act 1987 in relation to the tracing, freezing and confiscation of the proceeds of indictable offences against the Commonwealth law.

The Major Fraud Branch of the office of the Commonwealth Director of Public Prosecutions is now handling a myriad of matters which are revenue related. These matters are extremely time consuming and resource intensive due to their size and complexity.

The investigation of major fraud will never be an easy task but the difficulties that will inevitably arise can be reduced with the involvement of the DPP in the investigation process at the earliest possible point of time. Past experience has demonstrated that early involvement will reduce the period of delay in laying charges and/or in instituting proceedings.

An essential feature in the handling of major fraud is the close working relationship between the DPP and the investigatory agencies that may be involved. The multi disciplinary approach that proved to be a most effective way of investigating "the bottom of the harbour" matters continues to be used in relation to other areas of revenue based fraud. Large scale fraud cases prosecuted by the DPP have not infrequently come to light some years after the event, and involve lengthy periods in investigation before any sensible assessment can be made as to whether there is

sufficient evidence available to justify charges being laid. There is also usually considerable preparation required thereafter to organise the evidence in a manner sufficient to present it in committal proceedings and trial.

Delay in bringing proceedings may, in all circumstances, be so oppressive to an accused as to amount to an abuse of process.[33] Consequently, one must always be aware of the need for expedition in considering the time a particular matter has been under or requires further investigation.

Apart from what might be described as the logistical problems in investigating and prosecuting fraud cases the central issue will always be whether the available evidence is sufficient to establish the guilty intent.

TACKLING FRAUD WITHIN THE EXISTING FRAMEWORK

In addition to the various provisions under specific legislation, there are provisions in the Crimes Act 1914 that apply to fraud matters. Among the more important provisions likely to cover the activity of fraud are section 5 (aiding and abetting), section 7A (inciting the commission of an offence), section 86A (conspiracy to defraud the Commonwealth), section 86(1)(conspiracy), section 29A(1) and (2) (false pretences), section 29B (imposition), and section 29D (defraud the Commonwealth).

Section 29A makes it an offence for a person, with intent to defraud by false pretence, to obtain from the Commonwealth or a Public Authority a chattel, money or valuable security or benefit. Subsection 2 deals with similar conduct where a person causes or procures money etc to be paid to another person by a false pretence. The benefit need not be in money. However, it is important to remember that the pretence must be a false statement as to an existing fact. A statement of opinion or intention will not usually form the basis of a false pretence charge.

Section 29B makes it an offence to impose or endeavour to impose upon the Commonwealth or a Public Authority by an untrue representation made in any manner whatsoever with a view to obtaining money or other benefit or advantage.

This offence is commonly used in more serious examples of Social Security offences. For example, where a person is receiving a pension in one name and applies for a pension in another name, the application usually contains a false representation as to the name of the person and the fact that the person is not in receipt of other benefits. There are specific offences under the Social Security Act but this section is used for far more serious offences.

The benefit or advantage obtained need not be money; it may, for example, be employment with the Commonwealth. It is not necessary actually to obtain the benefit; the offence is complete when the false representation is made.

In *R v Cerullo*[34] a company director had been charged with imposition arising out of untrue representations made with the view to avoiding the payment of sales tax by his company. The question arose as to whether the untrue representation must be made by the accused person with a view to obtaining a benefit for *himself*. Fullagar J, (the other members of the court concurring) stated that this interpretation was correct. However, his Honour construed the consequent saving of money by the company as an advantage to the accused, who was characterised as the company's "alter ego".[35]

The analysis of section 29B by his Honour highlights the difficulty of applying this provision to the type of fraudulent conduct found in a modern, commercial world. It was noted that the words of section 29B were originally taken from the wording of various State enactments which had in turn been earlier taken from the English Poor Law legislation of 1824 and 1834.

This case highlights the sort of problems and issues hitherto foreign to the Courts that prosecutors have to contend with when deciding the laying of appropriate offences. The use of companies is becoming a characteristic feature in the perpetration and concealment of fraud.

As previously noted the commencement date of section 29D was 25 October 1984. When this section was introduced into Parliament, it was explained that the purpose was to remedy an anomaly whereby the plural offence of "conspiracy to defraud" was provided for by section 86(1)(e) of the Crimes Act 1914, while the singular offence (in other words, committed by one person acting alone) had not been provided for. It is useful to consider the provision of section 29D in a little bit more detail even though there has been little judicial consideration. In *Parker v Churchill*[36] a case involving the non-payment of sales tax, Jackson J confirmed the definition of Hodges J in *Steven v Abrahams*[37] of an intent to defraud the revenue as an intent "to get out of the revenue something which was already in it, or to prevent something from getting into the revenue which the revenue was entitled to get."

The case of *Scott v The Metropolitan Police Commissioner*[38] was also applied and as Viscount Dilhorne, with whose reasons the other members of the House of Lords agreed, said:[39]

> To defraud ordinarily means, in my opinion, to deprive a person dishonestly of something which is his or something to which he is or would be or might be but for the perpetration of the fraud be entitled.

Accordingly, the question arises as to what is dishonesty? What may constitute dishonesty will depend on particular circumstances but nearly always deception will constitute dishonesty.[40] In *R v Ghosh*[41] Lord Lane formulated a test for dishonesty when he said:[42]

> In determining whether the prosecution has proved that the defendant was acting dishonestly, a jury must first of all decide whether according to the ordinary standards of reasonable and honest people what was done was dishonest. If it was not dishonest by those standards, that is the end of the matter and the prosecution fails.
>
> If it was dishonest by those standards, the jury must consider whether the defendant himself must have realised that what he was doing was by those standards dishonest. In most cases, where the actions are obviously dishonest by ordinary standards, there will be no doubt

about it. It will be obvious that the defendant himself knew that he was acting dishonestly.

It is dishonest for a defendant to act in a way which he knows ordinary people consider to be dishonest, even if he asserts or genuinely believes that he is morally justified in acting as he did.

In general, fraud cases are complex not only in the large number of documents but also in their facts. Therefore, prosecutors are required to take an active role in advising an investigatory agency on the investigation and evidence from an early stage. In most cases, a team approach is adopted. Each agency nominates a case officer and the DPP nominates a case lawyer and representative from the Criminal Assets Branch.

Thereafter regular meetings are held at which a program of investigatory tasks are settled, and direction and timing of the investigation is organised.

In general terms, the role of the investigatory agency is to be in charge of the investigation of the alleged criminal conduct, the investigation being specifically directed to obtaining evidence to form the basis of a decision as to the laying of charges, and for use in any subsequent court proceedings.

It is noted in the prosecution policy of the DPP that "it is the duty of the DPP solicitor to objectively assess the available evidence and make recommendations as to the laying of charges, the tests are whether the available evidence establishes a prima facie case and, secondly, whether the public interest requires a prosecution to be pursued."[43]

WHERE DO WE GO FROM HERE

Issues of reform and indeed the investigation and prosecution of fraud will require a balance to be struck between two competing, and at times, conflicting public interests, that wrongdoing should be detected and punished, and that the rights of the individual be preserved.

As recommended by the Roskill Report there is a need to reform the substantive criminal law and rules of evidence in criminal proceedings arising from fraud to ensure the "just, expeditious and economic disposal"[44] of such proceedings.

Following the Roskill Report the Criminal Justice Act 1987 was enacted in England introducing major reforms in the investigation and prosecution of fraud. For instance, the Act places evidence obtained under letters of request on a formal footing and facilitates the admission of the evidence as a result.[45] Another feature under this Act is the provision for evidence to be taken live by video linked between the court room in England and a place in the country where the witness is resident. This innovation will ensure that the party wishing to adduce the evidence does not lose the benefit of the evidence simply because of the unwillingness of the witness to travel but at the same time enable the other parties to cross examine that witness.

In accordance with the recommendations of the Roskill Report changes have been made to the rules relating to documentary evidence. The hearsay rule has been modified so that a statement made by a person in a document shall be admissable in criminal proceedings as evidence of any fact of which direct oral evidence by him would have been admissible.

Clearly, there must be reform to the criminal justice system to at least stay abreast of the ever changing world that we live in. The world around us is completely different to what it was two decades ago and the days when this country mainly conducted its commercial activity within its boundaries are well and truly gone. Markets have grown and become international in character and operate on a financial scale of immense proportions. Computers, facsimile machines and telegraph transfer of funds are but a few devices of modern technology and the commercial world. In addition, governments as well as private entities are also operating internationally and huge funds are transferred to and from government.[46]

However, as the market place becomes international in character so does fraud. Consequently, fraud is becoming increasingly international in nature. It is in this area in particular that the existing provisions for obtaining evidence overseas are cumbersome, expensive and at times impracticable.[47] The operation of these provisions will need to be closely monitored and if necessary revised, in light of the growing international nature of fraud.

The Roskill Report makes some innovative and overdue recommendations in relation to the investigation and prosection process of serious fraud and most of them should be introduced into Australia immediately.

It is interesting to note that the Criminal Justice Act 1987 also provides that the Director of the Serious Fraud Office "may carry out in conjunction with the police investigation into any suspected offence which appears to him to involve serious or complex fraud."[48]

In addition, the Director of the Serious Fraud Office may require any person whose affairs are to be investigated or any other person whom he has reason to believe has relevant information, to answer questions and to provide information on any matter relevant to the investigation.[49] The Act also pushes aside restrictions on disclosure of information by government departments that would normally be kept confidential.[50]

CONCLUSION

There is much to do. As our society becomes more complex and sophisticated, so does criminal activity. Changes are occurring at a rapid rate. It is therefore imperative that law enforcement organisations and the legal system generally make the appropriate changes to keep up with, let alone stay ahead of, new forms of criminal conduct. The international nature of fraud is where our attention should be focused immediately. If we fail to do so, we will see a repeat, but this time in even greater proportions, of the taxation conspiracies which flourished unabated for many years and we will watch hopelessly as our legal system clumsily attempts to tackle a far superior foe that has grown on our inactivity.

ENDNOTES

1. The Review of Systems for Dealing with Fraud on Government, March 1987, commissioned to review "existing methodologies and systems by which Commonwealth agencies inter-relate in dealing with fraud on revenue and expenditure programs and to make any recommendations that may be necessary for improving the efficiency of present arrangements". This was the first serious examination of fraud on government in Australia.
2. A significant number of bottom of the harbour prosecutions have yet to be completed even though they were commenced some years ago. It is not unusual to find committal proceedings running for many months and in some cases years. Most of the committal proceedings have taken over 100 hearing days, generally involving over 100 witnesses and thousands of exhibits. Most have been strenuously defended. In a bottom of the harbour trial a Court was constructed to appropriately deal with the case involving approximately 60,000 documents and evidence from over 100 witnesses. Special facilities were provided for the Court and jurors to be able to handle the vast number of exhibits.
3. When sentencing those convicted of bottom of the harbour frauds the courts have commented on the inadequacy of the maximum penalty of three years imprisonment for conspiring to defraud the Commonwealth in contravention of section 86(1)(e) of the *Crimes Act 1914*. See: *R v Opitz*, a decision of Judge Wall of the District Court of New South Wales, unreported, 29 October 1986. *R v Freedman and Young*, a decision of Judge McGuire of the District Court of Queensland, unreported, 5 December 1985. *R v Cantwell*, a decision of Brownie J, the Supreme Court of New South Wales, unreported, 5 May 1987. Fullagar J in *R v Beames*, unreported decision of the Supreme Court of Victoria, 23 September 1985 at p 88, "I think the scale was of an order undreamt of by those who seventy years ago fixed a maximum penalty in respect of the relevant section of three years imprisonment."
4. Unreported decision of the Supreme Court of Queensland, 14 October 1985 at p 456.
5. Fraud Trials Committee Report (Lord Roskill) published 1986, p 9.
6. Id, p 9.
7. *R v Rosenthal & Ors*, unreported decision of the Victorian Court of Criminal Appeal, 26 June 1987.
8. Id, pp 5 & 6.
9. Supra note 1, paragraph 2.5.
10. Supra note 5.
11. Id, p 1.
12. I D Temby QC, "The Pursuit of Insidious Crime", paper presented at the 24th Australian Legal Convention, 1987, pp 4 & 5.
13. In response to the report of the Review of Systems For Dealing With Fraud on the Commonwealth the Comptroller General of Customs and the Director of Public Prosecutions presented a joint report in 1988 concerning the investigation and prosecution of serious infractions in the customs area. Since then the Australian Customs Service and the Director of Public Prosecutions put into effect an arrangement to deal with the investigation and prosecution of serious customs frauds. A number of matters have so far been referred to the DPP resulting in charges being laid. However, until this initiative very few, if any matters had previously been referred to the DPP.

    Paragraph 1.1.2 of the Review Report acknowledges that infractions of the Customs Act have been traditionally dealt with by way of pecuniary penalty and/or forfeiture and condemnation of goods. It was noted in cases of major fraudulent activity whereby extensive financial loss to the Commonwealth was caused, imprisonment had a very different and arguably more salutory discouraging effect.
14. *R v Rumpf*, unreported decision of the Victorian Court of Criminal Appeal, 26 May 1987.
15. Id, pp 13 & 14.
16. Supra note 4.
17. Id, pp 456 & 457.
18. John Wood, Director, Serious Fraud Office, London Fraud Investigation Group, "The New System of Investigation and Prosecution of Major Fraud", paper presented at Third International Conference on Corruption, Hong Kong, November 1987, p 6.
19. Id, p 5.
20. Roskill Report supra note 3, p 11.
21. Supra note 5, p 11 & 12.
22. R F Redlich, Annual Report of the Office of the Special Prosecutor, Canberra, 1983 p 45.
23. Supra note 5, p 4.
24. Id, p 5.
25. A Freiberg, Enforcement Discretion and Taxation Offences, Australian Tax Form Vol 3, No 1, 1986, p 65.
26. Supra note 1, p 1 and 2.
27. Id, para 3.2.
28. Id, para 3.2.
29. Id, para 3.4.
30. Id, para 3.7.
31. Supra note 5, p 9.
32. Id, p 65.
33. Herron v McGregor (1986) 6 NSWLR 247.
34. Unreported decision of the Victorian Court of Criminal Appeal, 29 November 1986.
35. Id, p 2.
36. (1986) 17 ATR 442.
37. (1902) 27 VLR 753.
38. (1975) AC 819.
39. Id, p 840.
40. See *The Queen v Horsington and Bartolus* (1983) 14A Crim R 118.
41. (1982) 2 ALL ER 680.
42. Id, p 696.
43. Prosecution Policy of the Commonwealth, Guidelines for the making of decisions in the prosecution process, January 1986, para 2.10-2.18.
44. The Terms of Reference of the Roskill Committee, supra note 5.
45. Cf Sections 7T-7Z Evidence Act 1905. Examination of Witnesses Abroad.
46. Sections 7A-7S Evidence Act 1905. Admissibility of Business Records. Proclaimed in 1978.
47. Sections 7T-7Z Evidence Act 1905. Examination of Witnesses Abroad. Proclaimed in 1985.
48. Section 1 of the *Criminal Justice Act* 1987.
49. J Wood supra note 10, pp 11 & 13. The *National Crime Authority Act* 1985 provides similar powers as seen by section 25 although the Authority is not a prosecuting body like the Serious Fraud Office.
50. Id, p 13 & 14.

Drawn Out and Complicated
PROBLEMS WITH FRAUD TRIALS

Terry Griffin and Brian Rowe*

"Drawn out and complicated" is a fair description of most major fraud trials. Many people would describe them as "impossible". In this paper we explore some of the reasons why the prosecution of fraud matters is difficult. We also suggest that with planning, expertise, reasonable resources and a great deal of hard work, no matter need be "too hard".

There can be no doubt that fraud cases, particularly large ones, present a number of special problems. Usually the public becomes aware of these problems at trial stage. However, although the actual conduct of fraud trials is difficult, given proper controls, the biggest obstacles that must be confronted will be overcome long before trial. If these problems are not recognised and dealt with from the outset the cases do not reach the court process or they are modified/defeated at committal. Accordingly this paper touches on some of the problems surrounding the investigation, preparation and actual presentation of fraud matters.

The paper is mainly centred around the experience we gained when employed by the Special Prosecutor's Office and Commonwealth Director of Public Prosecutions Office. It should not be assumed that our comments are only of relevance to the Commonwealth sphere or, indeed, that they are limited to fraud and the public sector. We believe that it is beyond debate that fraud is as active, if not more so, in the private arena. Large public companies, including banks and other finance houses, insurance companies, credit card agencies and the like are extremely attractive and, according to our research, vulnerable targets. (It has been suggested in America that commercial organisations can expect losses from fraud of between two and five percent of gross turnover.)

We have also drawn on our experience in private practice and particularly that gained as consultants to various agencies and organisations in relation to the assessment of their vulnerability to fraud and the measures required to control it. This experience has confirmed our belief that the incidence of, or vulnerability to, fraud is extremely high and that, at present, there is a vast amount of unreported and even undetected fraud. The majority of our comments are directed at criminal litigation but, with few variations, they apply equally to civil litigation.

Many of the constant stream of frauds being perpetrated in our society are unexceptional, at least in the legal sense, and are adequately dealt with by the criminal justice system. Equally, there are obviously many large, complex matters that seem to be beyond the capabilities of the system. It is these larger matters with which this paper is primarily concerned.

We have seen figures that suggest that the cost of fraud in the Commonwealth sphere is somewhere between $11.00 and $87.00 per week to every taxpayer. Whatever the amount is, it is not some book entry, but the amount each taxpayer is actually out of pocket, and those figures only take into account the recognised trouble areas like Social Security, the Tax Office and Customs. The unidentified fraud in other Commonwealth departments, State Government departments, local government areas, stock exchanges and the private sector generally is probably greater and in any event must be massive.

The Commonwealth Government, in particular, has recognised the problem and instituted an innovative and much needed initiative against fraud in its programs. Full implementation of the overall plan, a complex and massive task, will take time and it is too early to judge its effectiveness. Two things are certain, however: without serious and continued commitment the initiative will fail; and, any agency that cannot or will not see and adopt the benefits of proper controls will suffer both financially and politically in the long run.

In our view there is only one long term solution to the problems created by major fraud cases but that is a lateral one and no direct concern of this paper. There are areas where legal and procedural reforms can assist. Things like full disclosure of brief, trial without committal, compulsory pre-trial conferences, trial by a judge without jury and/or with expert assistance have been mooted. It behoves us all to do what we can to that ensure useful reforms are achieved but in any given matter we have to take the law as we find it; accordingly, in the short term, we have to be most concerned with finding solutions within the present structures.

The management of really large criminal cases has always been a headache for all involved. Almost invariably these cases have been fraud-related document matters. Investigators have ranged their very limited resources against seemingly impossible tasks, prosecutors have strained to push the cases into traditional and recognisable shapes, defence lawyers have railed at the difficulties presented to them, and the courts have attempted to do the impossible and handle the cases promptly within the existing frameworks. Unfortunately some contemporary initiatives have not helped – for example, proceedings under the *Administrative Decisions (Judicial Review) Act* 1977 in Commonwealth matters are, in our opinion, frequently unnecessary, and commonly used as a delaying tactic in criminal matters.

In civil cases the problems have been similar but economic considerations take on much greater importance. Major

* Terry Griffin and Brian Rowe are partners in Griffin Rowe and Associates, Sydney. Text of an address to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CB PA *No 56, September 1988, 89-97.*

complex litigation can cost hundreds of thousands of dollars in all, or any of, investigation, preparation and presentation. We have heard of cases that have cost millions. Efficient management is crucial. Many organisations cannot afford major litigation and some are obviously not convinced of the cost effectiveness of legal action. A survey conducted in Victoria in 1986 found that two out of three companies that had experienced fraud took no legal action. It has been suggested that it is sounder commercially to pay criminals to stay away from an enterprise than it is to take security measures and use the legal system if they fail. We have some difficulty with the morality of such an approach but more importantly we do not accept that it represents good commercial sense in the present environment.

A survey conducted in Victoria in 1986 found that two out of three companies that had experienced fraud took no legal action. It has been suggested that it is sounder commercially to pay criminals to stay away from an enterprise than it is to take security measures and use the legal system if they fail. We have some difficulty with the morality of such an approach but more importantly we do not accept that it represents good commercial sense in the present environment.

Today, decisions to bury or ignore matters do not stay secret for very long. The burgeoning area of shareholder litigation, managers being sued for negligence, mismanagement etc, will also mean that such decisions may come back to haunt the decision-makers in ways not yet contemplated. We are sure that major insurance companies, like the NRMA, will tell you that every fraudulent claim paid will generate at least another five similar claims. It does not take very much imagination to build a frightening scenario.

Whilst there were only a handful of really large cases every couple of years the administration of justice did not suffer too much. No doubt individuals from all sides suffered a great deal but the system coped, even though you could be excused for wondering how many major cases were left in the too hard basket.

Times have changed, however. Society generally is becoming more sophisticated and electronics have revolutionised the handling of information. Both the quality and the quantity of information available to the public has reached staggering proportions. The technology has not been totally ignored by either law enforcement agencies or their quarry. Indeed, it is relatively common for major cases to have electronic assistance.

The end result of all this is, in our opinion, that the system is breaking down. Even where investigators, prosecutors and the courts act with all possible speed, in some cases citizens accused of offences are being asked to defend themselves years after the commission of the alleged offence/s. In a few notable cases delays of over a decade have occurred.

Clearly long delays are unfair to those accused of offences and unacceptable to those charged with the administration of justice. The courts have provided part of the solution by deciding that they will stay proceedings where there has been unjustifiable delay. Delay can constitute harsh and oppressive conduct such as to render proceedings an abuse of process. As a by-product of the courts' move to protect the basic rights of defendants they have created, perhaps inadvertantly, a situation where all agencies will have to re-evaluate their old matters; and they will have to be very carefully examined indeed. Many should never see the light of day. That is not to say that these cases should be buried away in bottom drawers. They should be closely analysed and final, public decisions taken about their fate.

The importance of several recent cases in New South Wales cannot be underestimated. We are speaking about *Gill v McGregor* and *Herron v McGregor,* which together are commonly known as the Chelmsford hospital case, and *Whitbread v Cooke* and *Purcell v Cooke* which are known as the Cambridge Credit case. The decisions in these landmark cases were handed down in the latter part of 1986 and the principles established have been applied in several notable cases since. There has been a slight tendency for the courts not to be as quick as they initially appeared to be in staying proceedings and there is some suggestion of legislation to overcome the problem (that is, from a prosecution perspective). The principles enunciated in those decisions are, nevertheless, still of relevance.

Although both matters are well known in legal circles, it will not hurt to touch on the facts and summarise the practical effect of the authorities.

In the Chelmsford Hospital case, which arose out of the much publicised deep sleep therapy, disciplinary proceedings were being undertaken by the Disciplinary Tribunal constituted under the *Medical Practitioners Act* 1938 against some of the doctors involved in the treatment.

The allegations of misconduct depended on proof of acts and omissions which allegedly occurred in the years 1973, 1976 and 1978. Complaints were laid in 1982, 1983, 1985 and 1986. The investigating committee set up under the Act found that a prima facie case had been made out on all complaints on 11 March 1986.

In reaching the conclusion that the delay had been such as to support a stay of proceedings the court found inter alia:

> Once knowledge of the facts exists, one cannot stand by and allow time to pass.
>
> The public interest requires that complaints be lodged and dealt with as expeditiously as possible.

The case also supports the view that delay is to be judged objectively, and that the total delay between discovery of the facts and final disposition is the relevant delay.

The Cambridge Credit case reinforced and extended the principles set out in the Chelmsford Hospital matter.

Briefly the facts in the matter were as follows: From 1966 to 1974 Cambridge Credit Corporation grew to a massive conglomerate with 75 subsidiary companies and a wide range of business activities across Australia. In September 1974 a Receiver was appointed and in February 1975 the Attorney-General appointed an inspector from the Corporate Affairs Commission to investigate the matter. The final report was delivered in 1980 and steps to prepare a prosecution case began. Charges were laid in 1985 and the hearing began in 1986. It should be clear that this was a big case. One CAC officer described it thus: "the collapse of Cambridge was so big an event and the elements leading to its collapse so multifarious that those involved in the conduct of the prosecution have been simply bemused by the size of the thing. My own perception of the matter, which took about four weeks to form, was that the thing was the size of an elephant and I was like a small boy wandering around it wondering where I should begin to take hold".

That is a very understandable reaction but we suggest that there are ways to avoid the problems created by such a limited perspective. At least in the first instance, all large and dangerous things are best observed from a reasonable distance, otherwise panic and thoughts of self-preservation are likely to set in.

I will mention some of the facts that emerged from the case that contributed to the delay and eventual downfall of the matter. None of these will be novel to those of you who have had the responsibility for managing large litigation:

- Investigators resigned and were not replaced for several months; they then had to familiarise themselves with the matter.
- Officers could not be assigned solely to the one case.
- Counsel changed, took silk etc, and had to be replaced.
- Counsel requested expert opinion on aspects of the matter.
- Counsel took many months to provide advice.
- Requests for additional staff were made but not met.
- Available word processing facilities were inadequate.
- Photocopying resources were likewise inadequate.
- General financial restrictions were in place.
- Clerical support was not adequate.

Unfortunately, many agencies still have to operate in such circumstances.

From the current authorities it is possible to make the following points in summary form.

- The courts have inherent power to prevent an abuse of process in both civil and criminal cases.
- The courts will investigate circumstances leading to the institution of proceedings regardless of bona fides.
- Delay in instituting or prosecuting a matter can constitute harsh and oppressive conduct and can render such proceedings an abuse of process.

In Australia at the moment long delay per se is probably not enough to bar action but it will certainly base enquiry into cause. The prosecution can attempt to justify delay but justification is not the same as explanation. The following are unlikely to be considered justifications:

- Delay caused by an overcrowded court system. This includes delays caused by lack of courts or transcript.
- Inefficiency of the prosecution team, including inefficiencies beyond the control of the person or authority ostensibly in charge of the case.
- Complexity of the inquiry and preparation of the case even where proper attention is given to the inquiry. (The proper question is unfairness to the accused.)
- Company accused involved in other proceedings.
- The court will look objectively at the facts and will not accept the prosecutor's subjective view of proper expedition in a matter.
- Even where unavoidable delay in bringing on the hearing can be foreseen, proceedings should be instituted promptly.

No society that can deal with petty offenders against its rules but cannot effectively handle major transgressors can expect to prosper. Not very long ago we heard a popular rumour to the effect that to avoid prosecution, if not detection, criminals only had to operate on a sufficiently large scale. The artificially created paper chase is a well-known device of both the criminal and the commercial world. We have to have systems that can render it ineffectual where necessary. It will not benefit any one of us in the long run if that rumour becomes fact.

Earlier we suggested that by their attitude to delay, the courts had provided part of the solution. Old and mismanaged cases will not be heard. At least as far as the citizen is concerned the courts' approach ensures some justice. But the solution creates great pressure on the law enforcement agencies. Without massive injection of resources, which seems unlikely in the short term, or a highly streamlined approach, it is possible the only way most major cases will end is with an application to stay proceedings. Some might argue that it is perfectly just and proper that some limits be put on the bringing of

proceedings and that if prosecution authorities cannot effectively self regulate themselves the courts must intervene.

We submit, however, that investigators, prosecutors and administrators require a much less dramatic solution. There is a real need for those persons who are prepared to flout the criminal law on a major scale to be brought to book. Equally there is a need for those civilly wronged to be able to obtain redress. No society that can deal with petty offenders against its rules but cannot effectively handle major transgressors can expect to prosper. Not very long ago we heard a popular rumour to the effect that to avoid prosecution, if not detection, criminals only had to operate on a sufficiently large scale. The artificially created paper chase is a well-known device of both the criminal and the commercial world. We have to have systems that can render it ineffectual where necessary. It will not benefit any one of us in the long run if that rumour becomes fact.

WHAT THEN IS TO BE DONE

We suggest that there are short term solutions – not universal solutions and not absolute solutions but methods and attitudes and applications of current technology that can overcome many of the problems.

Before advances are able to be made, many, if not all, preconceived ideas have to be forgotten. The methods we all developed over the last decade or so to deal with the harder cases have to be revised:

- First, we must look at the use of resources. Resources are difficult to obtain in most areas but they are completely wasted if they are inadequate for the task in hand. In these troubled times, half a job, threequarters of a job, or even nine tenths of a job, is not better than none.
- Second, it is important to reappraise the traditional approach taken to the gathering of evidence. It is not vital that every available piece of evidence is collected, collated and evaluated. Not every witness has to be proofed, spoken to, or even identified. Quite clearly, if that is attempted, even a merely large case will soon get out of control and, worse, become uncontrollable.
- Third, not every criminal has to be caught and charged and there is no obligation to throw the proverbial book at those who are charged. It is of little value to the community if all the players in a fraud are investigated, arrested and charged but the system is unable to handle the additional steps necessary to obtain convictions.

Our experience with major case management involving corporate crime was gained from the time we joined Roger Gyles QC in late 1982. It continued unabated until we resigned from the Office of the Director of Public Prosecutions in early 1987. We have experienced the "pre-Gyles" era, the "Gyles" era and the "post-Gyles" era.

The Office of Special Prosecutor to which Roger Gyles was appointed in September 1982 was established to investigate and prosecute those involved in the tax avoidance schemes, colloquially known as the "bottom of the harbour" schemes. After initial problems, the resources available to that office were quite remarkable, at least by comparison to those that had hitherto been available in the Commonwealth sphere and in law enforcement agencies generally. We do not believe that the reasons for this commitment are open to debate; there was strong political commitment. Many will remember the lead up to the 1983 Commonwealth election which saw Robert Hawke become Prime Minister and recall:

- the McCabe/Lafranchi report
- the black box sales tax scheme
- the allegations, by both the media and the Opposition, of government inactivity
- the Government response
- the Costigan revelations.

Political parties went out of their way to promise action and commitment and one can easily understand why they did. The bottom of the harbour schemes alone involved over 6000 companies and about $800-$900 million in fraud on the Commonwealth. From humble, tentative beginnings in the early 1970s it had become probably one of our largest growth industries by the end of the decade. The media kept tax avoidance an issue and, although not pursued as rigorously these days, the topic is still revived from time to time. It should not be forgotten that the bottom of the harbour schemes were not the only ones around at the time. It would be naive to think that, because there is no current hue and cry, organised tax avoidance/evasion has ceased or is on the decline.

The Special Prosecutor's Office provided an opportunity for those involved to investigate and prosecute massive documentary cases without the crippling effect of completely inadequate resources. Over 500 search warrants were executed and literally millions of documents were seized or otherwise obtained. The Office operated on a multi-discipline team approach, combining lawyers, police officers, taxation officers, financial investigators and clerical support staff in operational groups. A management committee comprising the Special Prosecutor, two senior lawyers, the senior police officer, the senior taxation officer, the executive officer and counsel assisting was established and met frequently. The marriage of the assorted disciplines worked quite well although it was necessary to devise procedures to assist the resolution of disputes between the teams, members of the teams, and the various disciplines.

In our experience the most difficult dilemma arises out of the need to make the right legal/management decisions. They are the key to major case management and the importance of having the best possible operators making these decisions cannot be overstated. They take experience, practice and often a lot of intestinal fortitude.

Once those management decisions have been made, and only remain to be implemented, we believe one of the most useful weapons available to attack major investigation and litigation work is the computer. Used only like a card index a computer can provide significant support; used properly it can be formidable. Even the smallest personal computers

can be useful but a moderately powerful machine with a reasonable data base and a well-structured retrieval system can save a massive amount of effort. And effort is time . . . and time is very much of the essence.

As a federal office we had free access to a very large FACOM computer located in the Attorney-General's Department in Canberra. The system that was originally installed operated on a full text retrieval system called STATUS which is very similar to the STAIRS software developed by IBM and used fairly commonly around Sydney. We set up a series of data bases designed to compartmentalise the information we had, or hoped to get. The idea was that these data bases were to be loaded on a full text basis with all the documents we obtained during the investigation. We used multiple word processing terminals to capture data, running double shifts of 25 operators in Sydney for most of the two year term, and relayed the information to the mainframe in Canberra electronically every night.

Clearly there are difficulties with using computers. Everyone is aware of the horror stories. Many have had an unwanted role in them. However, we believe the incredible technical progress and the learning process of the last few years make them mandatory equipment. When we were in the Special Prosecutor's Office we were told we had a perfect system. We believed all we had to do was enter our data, shuffle it around and then press the print button and out would come the answers to all our questions. Ignorance was bliss; it did not work. We fell into a lot of traps, some we knew about, such as the need to ensure data integrity, but did not then know what steps were necessary to achieve satisfactory accuracy. Others were less obvious but equally basic. For example, we accepted a system with full text retrieval; it was enormously powerful but we had such a mass of material that it was not possible to capture it all despite the fact we had 25 data entry operators working on shifts. One afternoon we made a decision not to attempt to put in the material seized in one police operation. We worked out that the decision saved 80 years input time. That was fairly important; the Special Prosecutor's commission was only for two years.

One of the most difficult questions facing those about to construct a data base to support major litigation is what form the retrieval system should take. In some matters you may want to be able to recover all or any of the information entered into the system in a variety of ways, some not even thought of. A full text retrieval system like STATUS, where every piece of information has its own "address" can be manipulated in almost limitless ways. The IBM STAIRS program has similar capacity. Equally you may only want a limited number of identifiable reports with nothing more than an alpha sort. In this case most of the good word processing programs would suffice. You have to consider time and resources. It is no good attempting to set up a huge unstructured data base which requires skilful searching if there is not time to get the material into the system, or, perhaps, to train staff in searching techniques.

That may sound obvious but it is difficult to obtain reliable advice about the capacity of any system. By the same token the strictly formatted approach requires much greater intellectual input at the initial data capture stage but it makes for much easier retrieval. One of the great debates in this area went on between Mr Costigan, QC, and Mr Gyles, QC, and their staff. Mr Costigan (or at least Douglas Meagher, QC), strongly advocated the use of formatted material. Although oversimplified to make the point, the approach was something like this: his officers examined documents, made judgments about the contents and, where appropriate, provided summaries for capture. Only a small proportion of the available material was held on the computer. From an investigator's point of view the primary objective to the approach was that at the early stages when the officers were looking at the documents, they did not necessarily know enough to recognise all important information and once summarised it was unlikely to see the light of day again. There were also problems guaranteeing consistency between the various officers. A major objection from the information management point of view was the restrictions on information retrieval.

One of the most useful weapons available to attack major investigation and litigation work is the computer. Used only like a card index a computer can provide significant support; used properly it can be formidable. Even the smallest personal computers can be useful but a moderately powerful machine with a reasonable data base and a well-structured retrieval system can save a massive amount of effort. And effort is time . . . and time is very much of the essence.

The approach taken by Special Prosecutor Gyles was diametrically opposite. All the information was put into a very powerful system in a raw form, the idea being that it would be available at all stages of the investigation. The intellectual input would come in towards the end of the investigation when sophisticated search techniques would be used to retrieve required information in a useful form. Whilst the approach answered the objections to the previous system, as we said earlier it was unworkable because of the volume of material on hand and unrealistic expectations about input rates.

Recent studies on full text retrieval systems have concluded that, at least when dealing with major cases, the effective retrieval rate is about 25 percent. Suffice to say that a compromise between the two provides a satisfactory starting point for most designs, but because of the importance of the question and the horrendous consequences if an inapt approach is used, the problem has to be carefully considered.

The bottom of the harbour work commenced by Roger Gyles, QC, was carried on by the newly appointed Director of Public Prosecutions Ian Temby, QC, when Gyles' term expired in 1984. The balance of our experience with computers in the public sector occurred in the Sydney Office of the Director of Public Prosecutions (DPP) where we spent most of our time post-Gyles. The DPP in Sydney, now an office of around 150 people, operated out of the

premises previously occupied by the Special Prosecutor, so the automated Litigation Support System (LSS) developed in the SPO was already in place. When the DPP assumed responsibility for the mass of prosecution work previously carried on by the Attorney-General's Department we decided to use some of our data processing capacity to handle file management. As a result of a lot of hard work by some of the staff and cautionary tales from those of us who had survived the Gyles' experiments the system now in place is an excellent advertisement for ADP systems as management tools. For completeness I should say that the DPP also uses several small structured packages to provide assistance with revenue fraud matters and in the civil remedies area.

It is our view that the introduction of automated data processing into the law generally, and LSS particularly, is inevitable. There are a plethora of reasons why this should be so. If any of you doubt it, ponder the history of the workhorse of the office, the photocopier. Today they are common place, taken for granted, yet when they were first introduced into commercial use they met with tremendous resistance – they were labelled unreliable, uneconomic, and generally untrustworthy . . . a familiar cry. The same probably applies to calculators, dictaphones, word processing machines and commander telephones.

The sheer volume of documentation in major fraud cases is such that without automated assistance these cases would be under investigation and preparation for inordinately long periods of time. Many matters would be stayed as a result of the principles enunciated in cases like Cambridge Credit. In short, without automated assistance, these matters probably cannot be dealt with in an efficient, effective and appropriate manner.

The following summary of the development of computer support systems in cases we have been involved in may be of some assistance to others faced with similar tasks in the future.

Originally we identified the tasks to be performed as:

(1) record property and identify relevant document types;

(2) analyse documents; and

(3) present a subset of the documents as a "brief" of evidence to court.

The approach initially taken to perform these tasks with necessary variations from case to case was basically as follows:

(1) document lists (prepared by word processing) were produced. These lists contained information such as the document number, type, name and some textual data. This was usually followed by

(2) Where appropriate, documents were entered in either a structured or full text form into specially designed data bases in the STATUS system. STATUS was then used for searching purposes. The following difficulties occurred:

(a) where more than one document detailing similar information had been input and misspelling of names had taken place;

(b) where, due to the inflexibility of STATUS, it became necessary to update data and generate reports;

(c) because the recall rates for large textual systems are not particularly high.

However, as we gained more experience and refined the systems the need for full text searching declined and occupied only a minor percentage of time taken on overall searching. The later cases adopted a more flexible approach and thereby avoided many of the problems previously encountered. The SPO had a powerful Wang system and catalogue and reference information about the documents were held on this system. The document content itself, however, was still kept in textual form and transferred from the Wang to STATUS for searching purposes. This approach was refined even further as time went by. The catalogue and reference information support was extended to incorporate data validation, reporting, enquiries and generation of exhibit lists. Also, the information kept on STATUS became more structured according to document type, the case and the data subject. In STATUS, each article (usually corresponding to a physical document) was consistently input into structured data bases. The use of "key" fields [which further structured the data] also made it easier for searching, sorting and generating spread sheets of selected information. This was about the stage of litigation support in 1986 and it probably represented the state of the art at that time.

Even this approach had some problems. The Wang utilities whilst better than STATUS were still very limited. It was still difficult to validate data, link data from separate files, add or delete fields and generate all the types of reports investigators, lawyers and management required. The STATUS data bases are perhaps as good as they can be. They nevertheless have limitations, the most obvious being their inability to handle structured data. For example, some documents represent information in a very formalised way, for example, Corporate Affairs Commission documents show the name, capacity and relevant dates for people involved in companies. STATUS does not take advantage of this structure and relatively, or what should be relatively, straightforward information cannot be as expeditiously retrieved as is possible. Obviously this does not unduly concern the skilled users but it does necessitate training and practice.

In summary, at the beginning, all information was stored as free text [a form of "photocopying" the documents into the computer data bases] because there was little indication, at that stage of the cases, what the documents contained or what facts would be of interest or relevance later. As the matters became more clearly defined, the data bases were structured to an increased extent to facilitate searching of relevant facts and to save on input time. It became quite apparent relatively early that many lengthy documents (for example, sale agreements) were highly repetitive and that only select data was of interest (for example, date, consideration, parties etc). However, STATUS was still being used to handle what were essentially structured data

bases. This allowed the DPP to take advantage of all the facilities that a structured data base system possesses while retaining the enormous flexibility of searching on STATUS.

When time permitted a review of the system was undertaken and new techniques applied. The need to review was made more important when the DPP became active in the area of civil remedies and consideration was being given to using the power of the machines to assist in locating, freezing and ultimately forfeiting the proceeds of crime. The techniques now involved rely more heavily on analysis of the content of each document and class of document. Information is predominantly entered in structured form rather than full text. This is possible because a lot of the work now performed by the DPP involves documents of a formalised kind (that is, they convey specific facts in a standard form – for example, bank statements, cheques, CAC documents, memoranda of transfer etc). The office also acquired a development tool called Speed 11 which improved the linking facilities and made data validation, report generation, maintenance and modification easier. This has made the search, link and relate capabilities of the LSS even more powerful particularly in analytical and investigative work. STATUS still retains a strong role because some data demands full text entry, the majority of the staff are experienced in using STATUS and competent with full text retrieval systems, and STATUS is available nationally whereas the Wangs are not yet networked. For these reasons the system is "backed up" by reproduction of all material, both structured and free text data on STATUS. Users can then search on either STATUS or through the local Wang system.

Our enquiries have not revealed a more effective system to assist prosecutors and although that covers an admittedly small field, our experience during the developmental stages should prove useful to all players in any major litigation. The power in the system is not just the function of having all the information in an easily retrievable form. It comes from the ways in which the information can be shuffled around and cross-matched.

Computers would clearly assist the investigation and prosecution of those involved in corporate crime in at least the following areas:

- Pre-court document control
- Records of exhibits/MFIs
- Witness control
- Transcript
- Case management
- Current awareness.

PRE-COURT DOCUMENT CONTROL

The foundation of any major case involving masses of paper is the control of that paper. If you do not have an effective control system you will end up in a mess. We found that there is a need to ensure as far as possible that investigation support systems are designed with litigation in mind – even aspects as basic as ensuring compatibility between systems. Until quite recently it was a fact that the three major law enforcement agencies in the Commonwealth sphere, the Australian Federal Police, the National Crime Authority and the Director of Public Prosecutions Office all used different computer support. Whilst data bases used for investigation will usually contain far more information than is required for a LSS much of the information will be common. Statements from witnesses and relevant details like addresses, availability etc, will be recorded. Documents, their contents, pedigree and source will be recorded, details of activities conducted under statutory authority (search warrants/listening device warrants etc) could be included. In short, all the briefing material will be held in a machine readable form.

If that material can be simply lifted off the investigator's computer and read by the prosecutor's litigation support system there is an enormous saving in both time and money. If a conversion program has to be written it will take around four to six weeks even if all goes well, and all rarely goes well, especially if there is a panic on.

A little less obvious is the need to capture the data in a form that will facilitate dual use. For example, the system adopted by the investigators for recording document source and continuity has to be adaptable to the later requirements of prosecutors and courts or all the information will have to be rekeyed.

It is the need to control documents during all the pre-court shuffling that makes the use of the litigation support systems important. In major document handling exercises in the DPP, where no other system is in place, each document is given a computer generated number. This number is keyed into the data base and is used to record the source and all movements of the doucment. It also forms the basis of a code within the LSS for identifying the relevance and importance of the particular document as the understanding of the case develops.

EXHIBITS/MFI's

This is an area where the infallible memory of the machine is best demonstrated and, because of the heavily structured nature of the data, problems of retrieval that are apparent in full text systems are not or should not be apparent. Even so, there are several matters that have to be addressed. The prosecution has to be prepared to provide lists to the court and the defence; the lists have to be absolutely accurate. The courts have to be flexible enough to allow for prepared exhibit lists that do not necessarily follow the course of the evidence, and will often contain multi-lettered codes for each article. These codes will often only be meaningful to investigators or prosecutors but they have no sinister or unreasonable purpose. Although irrelevant, they should be explicable, usually consisting of numbers and letters that identify, for example, source, data, data capture relevant charge, etc.

WITNESSES

Obviously if you are using a LSS all witnesses will be entered. The LSS enables the details to be resorted in various ways to assist in whatever planning is deemed necessary. It can provide check lists for subpoenae, write a diary of available dates and sort them against court days; it can sort against

charges, record effectiveness or departure from proof, list all relevant documents for a given witness, check that all expenses have been paid. In short, a properly set-up LSS can assist with all the little things that have to be done before, during and after a case and it can do it all without error or overtime.

TRANSCRIPT

There is room for considerable debate about the capture of transcript in LSS. So far the only transcript we have seen on LSS has been typed in or captured by optical scanners after the court transcript has become available in hard copy. The evidence has been taken, reduced to writing, reiterated in court – often the statements are produced, taken down either in shorthand or by typewriter, reproduced and disseminated. *Then* it is rekeyed into a LSS. There is a lot of double handling.

Personally we favour a system where the courts key directly into a system that provides the material in a common machine readable form. We saw, however, little enthusiasm for change within the courts system. We could understand such an attitude if the transcription services were effective, but there are many cases being held up for substantial periods just because transcript is not available. Recently we were told that to obtain a transcript in writing of the entry of default judgment would take twelve months.

Personally we favour a system where the courts key directly into a system that provides the material in a common machine readable form. We saw, however, little enthusiasm for change within the courts system. We could understand such an attitude if the transcription services were effective, but there are many cases being held up for substantial periods just because transcript is not available. Recently we were told that to obtain a transcript in writing of the entry of default judgment would take twelve months. We find such an obvious saving in time and materials in having the court reporter typing straight onto a word processing machine that can provide the parties with the material in electronic form almost immediately that we see little arguments of merit that can be advanced by the detractors of the idea. Such a system could be instituted without addressing the LSS question. If the transcript is to be taken in such a form that a LSS could load it directly onto a data base, some thought has to be given to the structure. For example, if the usual heading showing the parties is used on each page of the transcript it is difficult to search the data using one of those names sensibly. Likewise, it is necessary to provide key fields to allow simple searches for things like exhibits and articles marked for identification.

Proper handling of documents in court has always been a problem in large cases. In some of the "bottom of the harbour" cases we used overhead projectors and large screens to display the documents to the juries. All the relevant documents had been photocopied onto transparencies and were displayed at appropriate times during the case. There is little doubt that this sort of presentation speeds up hearings and enhances the understanding of the jury. It is, however, expensive and labour intensive. What is required is a system whereby documents held in a LSS data base can be identified and displayed by use of a terminal in court. It is now relatively easy to generate a visual image of any document held in a data base. In other words the technology is available and whereas it was extremely expensive a couple of years ago there are now small, effective and cheap units on the market. One thing we should mention is that it is possible to separate data bases within a LSS thus enabling a single system to be used for multiple purposes. In a case in Queensland, for example, where the Supreme Court proved fairly receptive to computer assistance, the Judge was provided with a terminal which had access to the SPO/DPP LSS. He had access to the transcript and to the exhibits/MFI's but all the investigative material was locked off.

CASE MATTER MANAGEMENT SYSTEMS

Basically these systems are structured data bases that can be used for daily management and control of files. Typically they can generate reports and statistics in a variety of forms. They are excellent devices for preparation of information in an arranged form. In legal administration things like parliamentry reports and comparative sentencing figures come to mind (it could easily incorporate any other statistics you may need in your particular practice – for example, verdicts, number of trials, number of fraud cases, amount of fraud, length of hearings etc). A good system acts as a file tracking device. It enables you to find out the current position of a matter. It also allows for exception reporting on any number of matters including, for example, matters that have not been actioned for a period of time, court hearings that have not been allocated or briefed and are pending etc. It is a relatively simple system to establish provided the proper staff are put on the task to ensure the fields of relevance to your particular type of work are identified and provided for. There will be differences of emphasis between your requirements and those of another office organisation, court etc. You must ensure that your fields are unambiguous and clearly understood by your input operators.

These simply structured systems can be used to assist in many areas, for example, post-court procedures and diaries. If the system has been properly structured and maintained things like returning exhibits, paying witnesses, and generating reports can all be done by the push of a button. If not done the machine can alert you. Diaries are another area. It is easily possible for a computer to organise your own or the court's diary. All dates can be accessible via terminals so parties can access the court's terminal and settle dates. The court lists can be generated and maintained very effectively by machine.

There are other areas where the power of these machines could be very useful; things like preparation of appeal books, compilation of sentencing statistics, and extraction of common material from a variety of cases come to mind.

CURRENT AWARENESS SYSTEM

By this we mean a system to cope with specialist data along the lines of CLIRS. We believe CLIRS is a valuable concept but at the moment it is going through some teething problems. It may be that these problems will not be overcome or that they will not be overcome before many users and potential users have been turned off sufficiently, never to return. One apparent problem is the effectiveness (or lack of it) of retrieval in full text systems. Another is that it may be too broad or cluttered for most users' needs. Many lawyers operate in specialist areas of practice. They do not need the enormous amount of information that is stored in CLIRS and, indeed, it is probably not efficient in either cost or time for inexperienced operators to search through mountains of material. What many of those involved in pursuing corporate crime want is a subset of information relevant to their particular specialty.

The continuing development work by those behind CLIRS into such assistance tools as IQ and RANKING of answers may assist but until the techniques are perfect and verified and the cost is more affordable (currently we believe about $20,000) you may consider the establishment of in-house data bases using experienced lawyers to select matters for input and to preside over quality control. These systems could be textual, structured or mere indexes leading to hard copies stored in another area (for example, the library). They could include such material as advices, unreported judgments, office policies/directions, precedents pleadings, material on topics that are unlikely to feature in textbooks or authorised reports but which occur in practice. It may be that some people are involved in a developing area of the law such that reports and text books may not catch up with developments for a while and the most effective way to keep abreast or ahead of the pack is to establish a specialised data base at least until matters stabilise (for example, mareva injunctions, proceeds of crime, etc).

One matter that must be addressed and constantly borne in mind is security. To date security is a major problem which has not received the consideration it deserves. This neglect has made all systems vulnerable and extremely expensive to protect to any reasonable degree. The phenomenon of hackers is only the best publicised portion of the problem. But the difficulties have been recognised within the industry and it is likely the machines will soon be able to recognise intrusions and deal with them at least to the extent that the data is protected and the attempted breach is recorded.

CONCLUSION

It should be constantly borne in mind that those on the prosecution side have a duty to investigate and prosecute as fairly and as expeditiously as possible. They must work within the existing legal framework whatever its disadvantages and imperfections and should, if they think it appropriate, strive for effective statutory reform. It is imperative that they do not seize upon the enormity of these cases to justify their abandonment or use their size to overwhelm defendants, courts and juries. There is a corresponding duty on those representing defendants. It also behoves the courts to reexamine their procedures. All parties should combine to devise strategies to overcome the current difficulties in a spirit of compromise and commitment. Preconceived ideas and entrenched positions should be put aside.

Assuming adequate evidence is available the proper management of fraud cases, and major fraud cases in particular, depends almost entirely on planning and sound management. Such management must have the ability to deal with multidisciplined teams and electronic aids. It is no longer efficient or effective for any one discipline to handle these cases in isolation.

In relation to computer support we caution against investigators and lawyers being at the leading edge. There are many dangers in being at the forefront of technology. We also believe that agencies should not attempt to develop their systems in isolation. In some respects there appears to be a competition going on. In this area, as with others covered in this paper, a united front and shared ideas are essential.

The foregoing outlines some of our experiences and approaches to the conduct of major fraud work. Hopefully it will generate discussion and provide some ideas for investigators, prosecutors, defence counsel and others involved in this area. But it is our view that it does not represent the answer to dealing with corporate crime. Individual agencies may adopt or pursue some of the ideas but acting in isolation will not overcome the problem. A united, thoughtful and committed effort is required from all participants.

The National Crime Authority
ITS ROLE IN INVESTIGATING FRAUD

John Buxton*

One of the catalysts that led to the establishment of the National Crime Authority (NCA) in 1984 was the acknowledgement that there were major and widespread taxation frauds being perpetrated on government which up until the early 1980s had gone unchecked.

You will recall that the initial National Crime Commission bill was first introduced by the then Liberal Government and actually passed through Parliament in late 1982. The bill was never promulgated. This bill was drafted following the tabling of the Fourth Interim Report of the Costigan Royal Commission which drew prominent attention to the bottom of the harbour taxation scheme. When Labor won government in 1983 it introduced its own National Crime Authority bill.

There followed considerable debate in Parliament which left no doubt that there would be a truly national body with extensive powers and jurisdiction to investigate serious crime.

Public opinion seemed to be swayed away from the concept that the Commissioner of Taxation is "fair game", towards a more equitable approach to paying tax. Tax avoiders lost the aura of respectable clever dicks and were branded as tax cheats and bludgers.

Not only did that and other royal commissioners' reports lead to the introduction of the NCA Act and the establishment of the Authority, but also led to the establishment of the Gyles and Redlich Special Prosecutors' Offices (the forerunners to the DPP) and the consequential active investigation and prosecution of the major perpetrators of the bottom of the harbour frauds.

The consequences were quite dramatic and felt across the whole community, particularly sections of the business community and the legal and accounting professions. It also had very favourable effects on the public purse. Public opinion seemed to be swayed away from the concept that the Commissioner of Taxation is "fair game", towards a more equitable approach to paying tax. Tax avoiders lost the aura of respectable clever dicks and were branded as tax cheats and bludgers.

One of the objectives of government in establishing the National Crime Authority was that it be given the resources and powers to investigate major fraud in both the Commonwealth and State jurisdictions. Parliament vested the Authority with a number of significant powers to assist in this rather formidable task – formidable because investigations of major fraud inevitably involve:

- The collection and analysis of massive amounts of paperwork;
- The dedication of a team of investigators to a case for a considerable period, sometimes measured in years;
- The purchase and programming of computers to assist investigations;
- Fighting off vigorous legal challenges brought by targets of the investigation;
- Unmeshing the often complex and varied activities of the accused and their associates and entities;
- Identifying material evidencing the alleged frauds amongst a sea of paper, and
- Undertaking a full financial analysis of the targets' business and other affairs.

When embracing the concept of the Authority, Commonwealth and State governments recognised shortcomings in our traditional policing system. It has been said often enough that police forces generally lack the resources to dedicate a large team of investigators to a single case for a significant period. They also lack the legal and accounting expertise and sophisticated computer systems which are generally required to investigate large frauds. They lack the power to require persons to answer questions under oath and produce documents under compulsion, and they lack access to taxation records.

Added to this was the problem that when fraud transcended State and national boundaries or involved a mixture of Commonwealth and State frauds, there was rarely any co-ordinated effort involving State and Federal law enforcement agencies and any comprehensive exchange of information. There have been steps taken by Federal and State police to co-ordinate investigations into serious drug related matters by establishing joint task forces but such action has not, to my knowledge, been taken to any significant extent in respect of fraud related matters. It was Parliament's intention that the Authority bridge these gaps.

In establishing the National Crime Authority, Parliament gave it a capacity to dedicate resources to particular matters

* John Buxton is Senior Legal Adviser, National Crime Authority, Melbourne. Text of an address to Australian Institute of Criminology Seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CBPA *No 56, September 1988, 98-100.*

referred to it for investigation. It also gave the Authority the power to compel the production of relevant documents and persons to give evidence. The Authority was given access to taxation records and developed a computer technology to assist its investigations in the fraud area.

The Authority structured its staff so as to ensure its investigation teams comprised a mix of lawyers, accountants, police, intelligence officers, clerks and supporting records, computer, and word processing staff. The objective was to bring together different professions, disciplines and expertise within the investigative team environment and all working towards a common objective. The Authority was also given the power to co-opt onto an investigation team, members of other agencies, thereby bringing into the Authority such persons' specialised knowledge and experience.

It is with these resources that the Authority has undertaken a number of major fraud investigations involving a variety of Federal and State alleged criminal offences. In each investigation the Authority:

- established a discrete team comprising members of the different disciplines referred to above;
- established computer systems to control the vast amount of documentation and information acquired during the course of the investigation;
- co-opted into the investigation team members of other law enforcement agencies;
- gained access to taxation records where the investigation was tax related; and
- used its coercive powers to acquire documents and examine witnesses under oath.

In addition to the above, the Authority had also used some traditional policing methods in carrying out its investigations, such as developing informants and executing search warrants.

The Authority will, hopefully in the near future when the *Telephone Interception Act* comes into operation, be assisted in serious fraud investigations by having the power to obtain warrants for the installation of listening devices.

Investigation staff in the Authority working on fraud matters find it essential to have regular contact with other agencies pursuing their own functions relating to the same target. Such agencies include the Official Receiver's Office, the Australian Taxation Office, corporate affairs commissions and police forces. The Authority favours the communication of information acquired by it in the course of its investigation to such other agencies as they require. We have found that this has a consequential effect of not only assisting agencies in their investigations or instituting civil remedies actions but brings considerable additional pressure on the targets themselves.

The investigation by the Authority of large fraud matters usually involves the following stages:

1. A preliminary investigation to determine jurisdiction of the Authority to investigate the alleged fraud and whether, in view of the interest (if any), of other agencies and the resources available to the Authority, it should be investigated by it.
2. Assuming the Authority adopts the investigation, acquisition of relevant material.
3. Assessment and analysis of information with a view to determining offences and persons responsible for offences.
4. Isolating documentary and other evidence relevant to the commission of the alleged offences and taking statements from witnesses.
5. The preparation of a brief of evidence.
6. Liaison with the DPP about the matter and possible proceeds of crime action.
7. Transmittal of the brief of evidence to the Director of Public Prosecutions for consideration as to whether, and if so, what charges should be laid against potential accused.
8. Providing continued support to the DPP during the committal and trial.
9. Preparing a report on the investigation.

The Authority's policy in the investigation of fraud matters is to involve the Director of Public Prosecutions as early as practicable in the matter. This involves the Authority advising the DPP Office, usually informally at first, that it is conducting a major fraud investigation which it anticipates will be concluded in "x" months and referred to the DPP for advice. An outline of the matter will also be given.

Later, more formal communications will take place leading to the transmission of a brief of evidence to the Director of Public Prosecutions with a request to advise whether the evidence supports the laying of charges. Usually the Authority makes a recommendation on the charges it considers appropriate and the accused who it considers should be charged.

Early communication with the DPP is considered advantageous as it assists in highlighting areas requiring further investigation before a brief is completed and ensures that the charges laid are considered appropriate by the prosecuting agency.

The National Crime Authority has co-operated closely with the Director of Public Prosecutions over such matters, and the Authority provides considerable support during the commital proceedings and trial.

MATTERS INVESTIGATED BY THE NATIONAL CRIME AUTHORITY

The Authority has been involved in investigating serious fraud since it was first established. Each fraud it investigates invariably involves breaches of various federal laws and laws of several States, such as the Commonwealth *Crimes Act*,

Taxation Administration Act, Brankruptcy Act, State *Crimes Acts*, the Companies Code and the Common Law.

The major fraud matters investigated by the Authority had, to a certain extent, been previously investigated by corporate affairs offices and/or State and Federal Police without resolution. When such agencies carried out their investigations they were usually concerned only with offences falling within the limits of their own respective jurisdictions.

The Authority's investigations encompassed, with the blessing and co-operation of such agencies, an investigation of all the major allegations. After conducting investigations and assessing and processing massive amounts of information, the most serious and best supported offences were selected and the brief building process commenced.

The investigation of one of the Authority's major fraud matters has taken three years to complete. It involved the accumulation and analysis of over one million pages of material acquired in the course of the investigation; the interviewing of many hundreds of witnesses; proving thousands of documents to be tendered as exhibits in criminal proceedings; establishing and entering data on computer systems designed to assist the investigation process, and examining numerous witnesses under oath pursuant to the coercive powers of the NCA Act.

Whilst the primary task of the Authority is to assemble briefs and refer the same to the relevant prosecution agencies, it must also consider civil remedies and proceeds of crime actions arising from its investigations. The Authority has an obligation to co-operate with government agencies over such matters which has already resulted in recovery by the Commonwealth of substantial sums.

DIFFICULTIES

Not all goes according to plan during investigations and it can fairly be said that we have gone through a learning curve in investigating such matters, particularly in the matter which took three years to complete. This was inevitable because the Authority was a new and evolving organisation investigating multi-jurisdictional fraud of the size rarely tackled in this country.

We found that our desire to investigate all the serious allegations in that matter stretched the resources of the investigation team and spread it over a far too broad front. Such a course can be counter-productive and we have learned that early action to confine the investigation to the most serious, best-evidenced and most representative of the principal allegations is the one to follow.

We also encountered difficulties in finding suitable computer programs to "handle" relevant documents from the commencement of the investigations through to the prosecution stage. We developed adequate systems ourselves and in conjunction with the Commonwealth DPP, but an investigation and litigation support system to meet all our requirements is yet to be developed – but we are working on it.

It is pleasing to see the initiative of the Government in establishing the Fraud Control Committee. It is hoped that such a body will encourage government agencies to exchange information and co-operate, not only in the area of fraud prevention and control but also in the area of detection and investigation of fraud.

One might be tempted to speculate that, unless the Costigan Royal Commission stumbled across the bottom of the harbour scheme when investigating the Ships' Painters & Dockers Union, the frauds and a number of the perpetrators may never have been stopped.

A more sophisticated approach is required to ensure that serious frauds are recognised by agencies and are appropriately drawn to the attention of relevant law enforcement agencies or the National Crime Authority. The same comments apply to organisations at risk in the private sector. The cost to the community of not doing so is too high.

The Police Practitioner's Perspective

Chris Eaton*

Police generally, and especially Australian Federal Police (AFP), are in a unique position to make detailed observations and analysis of fraud in the community.

It probably goes without saying that police see some things quite differently to the vast majority of Australians. This is a product of their environmentally-generated perspective. That does not, however, mean that there is anything wrong with the way police see things; indeed, the police environment is a very real one, not an imagined or assumed one, and therefore their perspective is often more accurate than most Australians.

Specifically, police are in a singular position to see crime and criminals in a "total picture" way, not just a highly and often microscopically studied fragment. This is particularly true of full community policing when it is performed at its best. But today with the long term operations (or investigations) conducted by the AFP, a new "total picture" view has emerged. With the sort of investigational techniques employed on these long term operations, police probably know more about the target suspect under investigation than his own family, and sometimes more than he knows about himself.

With this unique advantage, police are able to see fraud in its connected way with crime and criminals generally. Fraud is a major component of the so-called "organised crime" activities portfolio. Without wishing to sound too trite, large scale (or organised crime) is about money and power, in that order, and fraud one way or the other, is both actually and potentially, a magnificent source of money. You would make a grave mistake to categorise and consider the defrauder as a different criminal from his apparently less attractive kinsmen. The "Maigret" view of the timid silk suited clerk or the unfortunately trapped solicitor belongs in the novels they came from. The reality is decidedly different.

The reason government funds are so attractive to fraud is, I think, obvious. Governments, particularly the Commonwealth government, handle more money and transact more cash than any other institution in this country. The percentage of annual gross domestic product moving through government accounts is astounding. Its mere size (a confusion in terms!) is the attraction, both in seeking ways to evade giving it to them and ways of illegally getting it from them.

The AFP has the largest police fraud unit in Australia, and simply that is because the Australian Government has the largest fraud problem. In addition to the resources of the AFP directly sighted towards fraud, almost every Commonwealth department has a team of "investigators" (for want of a more appropriate term) tasked with fraud detection and prosecution.

The contemporary history in this country of identifying huge losses commenced with the McCabe-Lafranchi Report in 1982, which recognised the full implications of the "bottom-of-the-harbour" schemes. Following this report we saw the establishment of the Costigan Royal Commission, and later the appointment of the Special Prosecutors Redlich and Giles. The level of fraud identified was truly staggering. But equally astonishing was the admission that the Taxation Office had been told of the import of these schemes many years earlier by one of their own employees, and had miserably, culpably, failed to respond.

large scale (or organised crime) is about money and power, in that order, and fraud one way or the other, is both actually and potentially, a magnificent source of money. You would make a grave mistake to categorise and consider the defrauder as a different criminal from his apparently less attractive kinsmen. The "Maigret" view of the timid silk suited clerk or the unfortunately trapped solicitor belongs in the novels they came from. The reality is decidedly different.

One outcome of the major frauds that either reduces government income or bleeds its funds is the increased burden placed on PAYE taxpayers. The PAYE taxpayer is an easy target for income tax and indeed taxation investigation. Within history we have seen revolutions raged on taxation issues, particularly when its spread was so obviously uneven or unfair. As a postulation then, vigilance against government fraud has a vital role to play in the stability of the political system.

This brings me to public service and its role in fraud prevention and detection. From the reports of many Royal Commissioners and their cousins, the Special Prosecutors, we hear complaints of the so called "territorial imperative". Baldly, as all Commonwealth departments are in competition with each other in terms of the recognition of efficiency and ability, the suggestion is that both corporate and individual ambition within departments creates an atmosphere of striving to present the best possible picture externally, together with the suppression of criticism both

* Chris Eaton is National Secretary, Australian Federal Police Association. Paper read to RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, 2 May 1988.

internally and externally. Undoubtedly this has occurred, and undoubtedly will continue to occur.

The real test then is how you minimise, or even more laudably, eliminate the impact of the "territorial imperative" on government income and spending. In this regard, the AFP have a major role. However, like the vast majority of crime, police rely on someone complaining about something to alert them to investigate. While there are specific exceptions in the case of "organised crime targetting", in the case of fraud against government departments, there are agreed processes and procedures whereby the AFP are requested to investigate a matter.

But as can be seen, this depends on two things: firstly that the department identifies the problem; and, secondly, that they are willing to advise the AFP, which is an organisation outside their department and with no loyalty tie to it.

For some considerable time the organisation that I work for, the Australian Federal Police Association (AFPA), has argued that the Commonwealth government's approach to fraud is fragmented and unprofessional, and hence inadequate. The logical extension of this argument is that considerable fraud exists undetected, and some that is detected is not dealt with appropriately.

For some considerable time the organisation that I work for, the Australian Federal Police Association (AFPA), has argued that the Commonwealth government's approach to fraud is fragmented and unprofessional, and hence inadequate. The logical extension of this argument is that considerable fraud exists undetected, and some that is detected is not dealt with appropriately.

The history of official AFP advice to government that it was unable to deal adequately with the level of identified fraud, and I stress "identified fraud", commenced in 1984 with the report of the then Commissioner of the AFP, Ron Grey. His confidential report, "The Cost of Efficient Policing", stated that due in the main to resource deficiencies, the AFP just could not cope with the level of identified federal crime, including fraud against the Commonwealth.

The then Special Minister of State, Mick Young, on advice, rejected that report, and called for a joint inquiry by the AFP and his own department into the accuracy of what Grey had said. That reported in late 1985, and confirmed the Grey report. Fairly obviously it did not say what was wanted, so Mick Young, on advice, rejected this report also, and called for a third report, this time on the "true levels of fraud". Report number three concluded that fraud against the Commonwealth government was of the level of $4 billion annually. This report has been suppressed ever since, having never seen the light of day, despite considerable pressure on the government to produce it.

I am reminded of Sir Humphrey Appleby in the series *Yes Minister*, when he was discussing with the minister, Jim Hacker, the danger of an unwanted departmental report. In his usual indignant way he said:

> Suppression is the instrument of totalitarian dictatorships. You can't do that in a free country. We would merely take a democratic decision not to publish it.

Mick Young, or at least his advisers, watched that show, and the tragic farce played itself out yet again in reality.

The Government's answer to the clamour for release of this report, which must have been seen as damaging, was I suppose all too bureaucratically logical, *to call for yet another report.* Report number four, "Review of Systems for Dealing with Fraud on the Commonwealth", reported in March 1987, and Attorney-General Bowen has forcefully stated that this will be the *last* report on fraud. One can, I suppose, understand why.

Nevertheless this report is compelling reading, and an ornament on how to say so little with so much. But one only has to look at the seniority of the public service Steering Committee members to imagine the labours of the poor devils who were the Working Party. It is a classic example of having the reluctant physician examining himself, and giving himself a clean bill of health, save for a few boils on the posterior. But, I suppose, if you call for reports often enough, sooner or later you are bound to get one that will suit you.

I quote from a letter in August 1986 from the office of the Special Minister of State to the AFP Ministerial Liaison Officer, seeking reponse details for "Possible Parliamentary Questions":

> The proposed PPQ on the fraud study should be positive rather than defensive and dazzle the questioner with science.

This cynical approach to what is a critical issue merely highlights how one can slip so easily in trivialising when one works for the parliamentary circus.

Nevertheless, shortly after Mick Young called for this last report, he had made two telling observations: "Fraud prevention by departments is hampered by a lack of accurate information"; and "Figures ranging from $4 billion a year to as high as $30 billion have been cited." He went on to say that "these figures could be exaggerated. The simple fact is that we just don't know". The last report, number four, was specifically directed away from considering the quantum of fraud by its terms of reference. So conclusively, either the government still does not know and does not want to know, or it has accepted the $4 billion conclusion of the suppressed report.

From our perspective, then, several things emerge:

- The level of fraud against the Commonwealth is a major concern.

- The current procedures for dealing with it are fragmented and inadequate.
- There seems little political or bureaucratic will to deal with a law enforcement problem in a law enforcement way.

Existing procedures are inadequate because they seek to apply a bureaucratic solution to a law enforcement problem. The much touted "National Identity Card", and now proposed use of the taxation number in its stead, are examples of a search for a panacea, with the added advantage of solving a problem by creating still more departmental growth. While police generally support a national identity system, when it comes to law enforcement, there is really no substitute for hard work, and someone will still have to break away from the computer terminals and do it.

When we address ourselves to the level of Commonwealth government fraud, we are not talking about hundreds of thousands of ordinary Australians ripping off the government. We are talking about major and organised crime, corruption and waste. The statutory secrecy provision, backed up by self-interested departmental silence, are a shocking and shameful impediment to law enforcement.

Police, and the AFP in particular, operate on information. We call this intelligence, and so much intelligence exists in government departments, but it is unconnected and never provided to the AFP in anything but a fortuitous way. We need a co-ordinated, regular and absolute exchange of information from all government departments to the AFP.

Additionally, there is no law enforcement audit of individual departmental actions in preventing and detecting fraud, except by the departments of themselves. An AFP role in a process such as this would ensure performance was standardised and investigational quality controlled. There will no doubt be some who will claim that the recently created "Fraud Control Committee" will provide the appropriate mechanism for this, but that committee has little law enforcement input, being controlled by the very departments who would stand to lose the most by criticism. The sad fact is that self-interest and power retention will almost certainly prevent any effective results from this committee.

When we address ourselves to the level of Commonwealth government fraud, we are not talking about hundreds of thousands of ordinary Australians ripping off the government. We are talking about major and organised crime, corruption and waste. The statutory secrecy provision, backed up by self-interested departmental silence, are a shocking and shameful impediment to law enforcement.

This is not your friendly fraud criminal or the smiling face of the infamous tax adviser, Clyne. These are the type of humanity, if you can call them that, who would also deal in drugs and arrange murders. Indeed, they are in so many instances, the self same people. Money is money, which ever way these leaches on society look at it, and it is beholden on us all to apply our wrath to all their activities, not just the more emotive ones.

The future will judge us all in this, but as of now the judgment will not be good.

Car Fraud Owner "Hurt Community"

Attempts to claim insurance by fraud was a crime against the whole community, a Mollymook man was told when he appeared in Nowra Local Court yesterday.

Peter George Hughes, 31, shop proprietor of Pangana Cres, pleaded guilty before Magistrate Angela Karpin of aiding and abetting, setting fire to a motor vehicle and making a false statement to police.

The court was told Hughes, assisted by another man, arranged for his car to be stolen so an insurance claim could be made.

"The sort of costs incurred by insurance companies increases the cost of premiums to others and is a crime against the whole community," Mrs Karpin said.

Hughes was fined a total of $2500 and placed on a $2000 bond to be of good behaviour for three years.

— *Illawarra Mercury,* **12 July 1988.**

Minimising Fraud Through Preventive Systems
LESSONS FROM THE CORPORATE SECTOR

*Garry D Dinnie**

Many recent surveys, conducted both here and overseas, suggest that the incidence of corporate fraud is quite extensive. It has also been often found that particular organisations have experienced fraud a number of times, and the sums involved may well be considerable. The types of fraud we are discussing range from small-scale yet persistent frauds perpetrated by individuals exploiting weaknesses in employers' management systems, to major scandals involving many people acting in collusion and resulting in the loss of many millions of dollars, and all types and extents of fraud in between.

while it will never be possible to prevent the occurrence of all fraud, it is nevertheless possible and fairly straight-forward to identify many of the risks to which a particular organisation is exposed. It is then possible to instigate appropriate and effective procedures to provide at least a first level defence as an effective deterrent to fraud. Even this fairly simple type of management initiative would have prevented many of the frauds which I have seen and investigated.

The increasing public importance of fraud in the current environment is typified by one of the major findings and recommendations of the Macdonald Commission of Canada, whose report was released in June 1988. This Commission was charged with reporting on "The Public's Expectations of Audits". Some of the Commission's major recommendations centred on the need for auditors to conduct internal control evaluation and testing procedures properly so that the possibility of non-detection of any fraud of reasonable size (perpetrated by either employees or management) within an organisation being audited is all but eliminated.

This is a most interesting development, as the results of the Commission's deliberations have attempted to make definite proscriptions over an area involving the precise responsibility of the auditor in the detection of fraud and this has been the subject of much debate over the years. One reason that much of this debate has been fairly inconclusive is that there have been very few relevant court cases actually decided in this area. Also, the only really applicable audit standard or practice statement is AUP 16, and this was only issued in 1983. It is essential, however, that all auditors should at least consider the possibility of fraud when planning their audits, whether they be operating in the private or public sectors.

An important matter for consideration is to determine whether the victims of fraud are merely unlucky, or whether most corporate fraud is something that could or should, in fact, be prevented. Now, while it will never be possible to prevent the occurrence of all fraud, it is nevertheless possible and fairly straight-forward to identify many of the risks to which a particular organisation is exposed. It is then possible to instigate appropriate and effective procedures to provide at least a first level defence as an effective deterrent to fraud. Even this fairly simple type of management initiative would have prevented many of the frauds which I have seen and investigated.

A recent detailed survey, conducted by the Institute of Internal Auditors, of a large number of organisations which had experienced fraud revealed that one of the major causes of fraud is directly attributable to management's failure to enforce the organisation's basic system of internal control. This supports the belief of many practitioners involved in the investigation of fraud that businesses which suffer fraud often use systems which do not possess appropriate or adequate controls or the controls in place can easily be evaded. Because each business is different, it may not always be easy to identify the areas of highest risk. However, the way the business operations are conducted can, in itself, be an effective deterrent to fraud. Like most criminals, those who perpetrate frauds will be deterred if the risk of detection is high.

THE NATURE OF FRAUD

Corporate fraud is nothing new – it has existed more or less since the time when corporations were first formed. So, why does it keep re-emerging in the public arena? One reason is that, in addition to the increasing numbers of frauds being carried out, there is a significant growth in the size of individual cases. This makes the whole issue so much more newsworthy. Some years ago, because the physical bulk of large amounts of money was considerable, frauds tended to be relatively small – the amounts were often limited to amounts which could be easily physically moved. Now, with the dramatic increase in the use of computers along with fairly complicated accounting systems and their attendant use of telegraphic transfer of funds, the ease of diverting delivery of goods and so on, the size of each individual fraud has been able to dramatically increase.

* Garry D Dinnie is a Partner of Arthur Young and Company. Text of an address to Australian Institute of Criminology seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CBPA *No 56, September 1988, 104-110.*

In many ways, fraud is similar to other types of theft. For example:

- Easy targets are usually chosen;
- Some individuals are frequent offenders;
- Large crimes are usually carried out by professionals; and
- No matter how much protection is put in place, it can never be 100 percent effective.

However, fraud does differ from the more traditional theft in some important aspects:

- It is usually perpetrated by an employee or some other person doing business with the organisation.
- Many opportunities are created by deficiencies in the way the company operates or controls its business.
- The fraud is often not discovered for a substantial time. When it is, the offender is often identified but often not prosecuted, which is the exact opposite of the situation for many other kinds of theft.

Further, the nature of corporate fraud has undergone significant change over the past few years. Gone are the days of people dipping into the till or surreptitiously taking stock out the back door. As the modern corporation has matured and advanced in step with large scale use of computerisation and other technological changes, so too has corporate fraud capitalised on emerging technology to develop increasingly sophisticated techniques.

Two main developments of the late 1970s and 1980s must be borne in mind continually if we are to understand the current state of corporate crime and thereby be armed to combat it.

Firstly, the emergence of "white collar" crime has seen a change in the level and background of personnel involved. Misappropriation of corporate assets and fraudulent manipulation of reported results is now often perpetrated by those involved in higher levels of management. Such people are typically perceived to be above reproach (at least by their subordinates who are directly involved in many detection procedures) as well as being positioned above most of the controls and procedures which exist. In addition, much of this type of crime is now carried out for reasons other than theft. For example, in today's corporate environment, there is continued pressure on management to succeed – this can often be reflected in pressure to manipulate the company's results to disclose a much more favourable position than is actually the case.

Second, these executives usually have the benefit of a high level of education as well as access to sophisticated tools to aid their endeavours.

Based on the preceding, we can highlight some initial conclusions:

- Perpetrators, to a large degree, come from within the ranks of higher level management and they are often either above most control procedures or find their circumvention fairly easy.
- They are often highly educated and have access to state of the art tools.
- This type of fraud may remain undetected and grow to massive proportions during a considerable length of time.

TYPES OF FRAUD

1. Management Fraud

As mentioned above, because of the changing business environment, combined with the additional pressures placed on management, there is an increasing risk of fraud being perpetrated by those in a management position. This risk relates both to manipulation of the organisation's results, as well as to straight out theft of company assets. Therefore, particularly where senior or sensitive positions are involved, it is important that detailed and independent references be obtained for all new appointees. A person in a senior position will often be able to override internal controls or persuade junior staff that there are pressing reasons why procedures should be ignored in relation to a particular fraudulent transaction.

2. Purchasing Fraud

Purchasing is particularly vulnerable to fraud. An especially difficult area is where frauds involve collusion with third parties. Often a company purchasing officer is ideally placed to commit a fraud, especially if in collusion with a dishonest supplier. Knowing where the risks lie and having effective and efficient internal control practices, with appropriate independent review procedures are vital in prevention of such purchasing frauds.

3. Treasury Fraud

The treasury function in a large organisation always carries a most significant potential risk, not only from ongoing minor frauds, but also from the one-off transaction involving very large sums of money. The controls and review of the operations in the treasury function should be designed to meet these specific risks.

4. Computer Fraud

There has been an increasingly widespread use of computers in most organisations over the past few years. These range from personal computers in the smallest as well as largest businesses, to the large mainframe computers utilising wide ranging networks and complicated data base systems.

What this has meant to the organisation's system of internal control is that many controls are now centralised in one portion of the overall system and are therefore potentially easier to circumvent. In addition, the very nature of today's computer systems have eliminated many of the previously available manual style controls. Specificially, today's systems provide direct on-line input and transaction

initiation to a multitude of end users, without any review or authorisation procedures other than some form of password control. This does not, of course, have to result in a lessening of overall internal control – in fact, if properly thought out, there is the opportunity to dramatically improve control.

If a well thought out and positive system of internal control is in force to deal with all facets of the company's information processing, including the computer systems, the likelihood of fraud is significantly diminished.

Even the most diligently executed financial audit is not a guarantee that fraud does not exist in the organisation. One reason for this is that financial audits are performed on a sampling basis — audit costs would otherwise become prohibitive.

Specific types of computer fraud include, but are not limited to, the following areas of manipulation:

- Input or transaction data
- Output or system results
- Application programs
- Data files
- Computer operations
- Communications
- System software; and
- Computer hardware.

Loss to an organisation through fraud can arise in many ways and some specific examples include:

- Theft of cheques, both coming into and going out of the organisation and the use of dummy bank accounts with similar names to the original payees
- Theft of assets
- Collusion with customers
- Short deliveries of goods, either for goods received or being shipped for sale
- Interference with Creditors' and Debtors' ledgers
- Sale of company assets at deflated prices
- Own account trading by employees
- Frauds involving commission payments
- Expense frauds
- Fictitious overtime or fictitious employees
- Loss of information, theft of customer lists, business plans or other business secrets such as computer software; and
- Manipulation of information to improve apparent company performance.

Management clearly has a difficult balance to strike between installing controls which are so comprehensive that fraud becomes almost impossible, but the organisation has great difficulty in functioning effectively and keeping overheads to a sensible level. The solution of this dilemma is not straight forward but the problem is eminently soluble.

WHAT TYPE OF PERSON IS LIKELY TO COMMIT FRAUD?

Recent studies, both formal and informal, have indicated that there are several definite factors which describe the likely white collar criminal. Typically, these people are likely:

- to live obviously beyond their means
- to possess an inordinately high desire for personal gain
- to have a high level of personal debt
- to enjoy a very close personal relationship with customers or suppliers
- to feel generally their salary is not commensurate with their responsibilities
- to possess a wheeler-dealer attitude
- to treat as a challenge the controls in the system
- to be subject to excessive gambling habits; and/or
- to suffer significant family or peer pressure.

While these characteristics are fairly general and, as expected, very difficult to assess or monitor, they do provide us with a starting point in the identification of potential perpetrators.

WHAT ARE THE RESPONSIBILITIES OF THE EXTERNAL AUDITOR?

Many people believe that it is clearly the responsibility of the auditor to detect and report fraud. However, an external audit is intended for one main purpose and that is to express an independent opinion on the "truth and fairness" of a company's financial statements. Even the most diligently executed financial audit is not a guarantee that fraud does not exist in the organisation. One reason for this is that financial audits are performed on a sampling basis – audit costs would otherwise become prohibitive.

The public accountant's liability to third parties and shareholders is a complex area and derives from common law. Liability for negligence often means a failure to

conduct an audit in accordance with generally accepted auditing standards and these standards do not typically require fraud detection as a primary audit objective. As noted above, the only pronouncement applicable in this country is AUP 16 and this mainly places a responsibility on the auditor to plan the audit properly so material fraud may reasonably be expected to be discovered.

WHAT ARE THE RESPONSIBILITIES OF THE INTERNAL AUDITOR?

In general terms, fraud discovered by internal auditors usually tends to involve lower management levels within an organisation. This is in part because senior management are in the position of being able to over-ride or bypass controls and often their specific activities are not, in fact, subjected to audit review and evaluation. So who within an organisation is able and responsible for the detection of fraud?

Accountants in public practice mostly hold the view that the primary responsibility for fraud detection rests with internal audit, as they know the organisation best and understand its systems and practices much better than the external auditor ever could.

Internal auditors understandably see this issue somewhat differently. They generally believe that their primary objectives do not include fraud detection as such – their responsibility is to detect it only incidentally. It may be argued that you will rarely succeed in achieving a specific result if that result is not one of your primary objectives.

Therefore, at the current time, it is my view that the primary responsibility for fraud detection lies with management. This is essentially because the overall responsibility for the organisation's controls and financial results rests with them – it is primarily their responsibility to set in place effective systems and to operate the business to meet its objectives.

IS A SOUND SYSTEM OF INTERNAL CONTROL SUFFICIENT?

Historically, systems of internal control have predominantly focused on detective control procedures, naturally combined with certain preventative control procedures, to overcome fraud.

Many frauds may, however, remain undetected for considerable periods of time, thereby allowing their effects to continually accumulate. By the time they are discovered, millions of dollars of company assets may have been diverted and be otherwise unrecoverable.

Accordingly, given the gravity of these ramifications, primary reliance on controls of a detective nature is no longer necessarily adequate to the task. It is essential that companies supplement their existing procedures with appropriate and comprehensive preventative controls. Now, more than ever, the axiom "prevention is better than cure" becomes a motto to which we should adhere.

WHAT PREVENTATIVE CONTROLS SHOULD BE EMPLOYED?

Several areas of improvement in controls are available to enhance an organisation's capacity to prevent corporate crime.

Firstly, specific aspects of internal control can be examined and strengthened in those areas which allow prevention of misappropriation rather than detection after the fact. Of crucial importance is the segregation of custodianship of assets from the systems which generate their transferral. For many companies, readily marketable assets will involve cash, securities and inventories. These assets, at a minimum, should be subject to such independent custodianship.

Second, supervisory overviews can play a much more important role in the prevention of corporate crime. Such overviews include greater direct executive supervision, along with closer monitoring of budget/actual performance and asset levels.

Instituting such procedures, whilst allowing for an improvement in the ability of the company to detect corporate crime also provides an effective tool for dissuading potential criminals where such procedures are communicated to all levels of staff, and are perceived to be effective in the prompt detection of any abnormalities.

WHAT CAN MANAGEMENT DO TO FIGHT FRAUD?

Major factors motivating frauds are pressures on employees combined with perceived opportunities. In line with this, it is often the existence of organisational weaknesses that provide the necessary real or perceived opportunity. The most common weaknesses are that the organisation:

- Places too much trust in employees.
- Lacks proper authorisation procedures.
- Does not require disclosure of personal income or interests.
- Lacks an adequate separation of transaction authority from custody of assets.
- Does not conduct independent performance checks.
- Lacks adequate attention to detail in the processing of transactions.
- Lacks an adequate separation of asset custody from their accounting.
- Lacks an adequate separation of accounting duties.
- Lacks clear lines of authority.
- Does not require a statement of an employee's lack of conflict; and
- Does not possess adequate documents and records to run the business properly.

The main mechanism available to enhance the ability of an organisation to detect corporate crime is a sound system of internal control. Long established procedures such as:

- Segregation of duties;
- Reconciliation of account balances; and
- Examination of transactions in risk sensitive accounts,

must be reviewed to ensure they are still sufficient to accommodate the changing environment.

The first and most important thing is the organisational tone set from the top. A sloppy attitude to control does not go unnoticed by other employees, and will encourage fraud if the risk of detection appears low. Directors and senior management have a responsibility to ensure good practice. They must set an example in creating a culture and corporate integrity.

SET AN EXAMPLE

The first and most important thing is the organisational tone set from the top. A sloppy attitude to control does not go unnoticed by other employees, and will encourage fraud if the risk of detection appears low. Directors and senior management have a responsibility to ensure good practice. They must set an example in creating a culture and corporate integrity. Good housekeeping, good financial controls and reliable and prompt management information are all important aspects of this culture.

PROMOTE A CLEAR ANTI-FRAUD POLICY

The board of directors should also ensure there is an effective and well published anti-fraud policy, dealing with:

- A published policy of "Corporate Integrity";
- Published guidelines on receiving and giving entertainment and gifts and commissions to third parties;
- Well defined and clear procedures for:
  - reporting instances of fraud to the board,
  - investigation of suspected fraud,
  - dismissal and prosecution of perpetrators,
  - recovery of losses, and
  - references for employees dismissed in connection with frauds;
- Defined responsibilities of the board of directors including effective oversight of the anti-fraud policy and compliance with it;
- Relevant responsibilities for non-executive directors and the audit committee;
- Relevant responsibilities and reporting lines for internal audit.

KNOW THE RISKS AND OPERATE EFFECTIVE CONTROLS

The controls need to match the requirements of the business. What is suitable for a stockbroker with a large private client base is different from what is needed for a manufacturer of industrial machinery. Moreover, the "control environment" should allow creative action and entrepreneurial behaviour which lead to growth of the business. The controls should be based on knowing the risks, after a thorough and realistic assessment of the business and the ways in which fraud could take place. It will usually be necessary to consider:

Risks to assets – where money can enter or leave the organisation, for example, the loss of existing assets or the payment of fictitious liabilities.

Risks to sensitive information – whether computer based, or other information on matters such as customer details, contract terms, or bids and tenders.

Risks to published information – such as manipulation of company accounts or insider trading through premature release of "price sensitive" information.

Entry controls – the defences which should prevent or, at least, deter white collar criminals entering your organisation, whether as employees, temporary staff, suppliers, customers or visitors, will usually include:

- Checking references of employees thoroughly, not just most recent employment (particularly where the appointment involved gives access to sensitive information or to the assets of the business);
- Limiting and controlling the use of temporary staff;
- Taking proper business references on suppliers and customers; and
- Ensuring physical security in high risk areas.

Internal controls – the defences which should ensure that the resources of the business are used properly in pursuit of its objectives will vary from simple rechecking of the work of others, through a variety of procedures, to the review of management information. They will usually include:

- Realistic budgets being subjected to rigorous review and subsequent detailed comparisons with actual expenditure
- Expenditure authorisation
- Cash management procedures
- Security of cheque books, payment systems and postage
- Prompt billing and follow up of non-payments

- Review of non-routine payments
- Implementation of extensive controls over computing activities
- Segregation and, where practicable, rotation of duties
- Ensuring staff take their full allocation of holidays; and
- Personnel reviews to highlight individual financial risks.

Cost is often given as a reason for removing internal controls such as these, and management must ensure that the controls are in a reasonable relationship to the risks involved. However, cost is a poor excuse if those risks have not been realistically assessed.

Internal control enforcement – the operation of internal controls is the responsibility of management. An approach which ensures that management check employees' work and in which the checks are unpredictable, but not infrequent, encourages adherence to laid down procedures.

A well-organised internal audit effort is a major weapon in the discouragement of fraud through tighter internal control. Internal Audit should have clear objectives and clear reporting arrangements. They need to have appropriate skills, training and experience, including computer skills. They should be able to ensure that action is taken to improve efficiency and control.

FOLLOW UP WARNING SIGNS

Management should be on guard whenever there are unanswered questions in respect of results of the function of internal controls – especially if it is "not convenient" to make a review. These symptoms should be followed to their rightful conclusion. Loose ends are often tell tale signs of something untoward. As well, it is necessary to be alert to apparently minor errors or discrepancies, as these may often be a clue to a much greater or widespread problem.

HAVE A DISCOVERY PLAN

Dealing with a substantial fraud will inevitably be unpleasant, highly disruptive of the time and attention of senior management and, indeed, of the rest of the business. It will almost always hopefully be a "one-off" experience and, within most organisations, experience with dealing with such matters is limited.

When things go wrong, management can act decisively and quickly to minimise the damage to the business if it has a discovery plan which sets out a clear guide on what to do.

The discovery plan need not be complex, but should cover:

- Suspensions of suspected employees and ensuring that they are not able to cause further loss or destroy evidence of what has been done;
- Preservation and presentation of evidence of what the fraud was and how it was committed;
- Retrieval of keys, changing locks, computer passwords;
- Removal of bank, computer and security authorisations;
- Investigation to determine:
  - how much has been lost?
  - how was the fraud detected?
  - what controls were avoided?
  - why did management not find it earlier?
  - what other losses are there?
  - what can be learnt from the episode?
  - what should be done to prevent reoccurrence?
- Reporting
  - to the police,
  - to the relevant regulatory authorities/trade associations;
- Recovering the loss
  - through insurance, where applicable;
  - by civil action against the offender;
- Public relations, what to say to the press, TV and radio, to employees, customers, suppliers, bankers and shareholders, and who will say it and deal with queries.

There is usually a reluctance to publicise what is an internal, distasteful affair. The organisation may feel that publicity will show up weaknesses in the whole management, rather than one unfortunate episode. If management do not act rigorously, the company is open to future fraud because of damage to the "corporate integrity" policy. Research shows the criminals go on to repeat their crimes, but usually they get bigger and harder to detect.

The reporting of fraud is often the most difficult issue, in practical terms, for an organisation to tackle. The survey which Arthur Young carried out showed that no company interviewed prosecuted every fraud, not even every serious fraud.

There is usually a reluctance to publicise what is an internal, distasteful affair. The organisation may feel that publicity will show up weaknesses in the whole management, rather than one unfortunate episode. If management do not act rigorously, the company is open to future fraud because of damage to the "corporate integrity" policy. Research shows the criminals go on to repeat their crimes, but usually they get bigger and harder to detect.

LOOK AT THE SITUATION REGULARLY

Though there are stages in the life of a business when it is more exposed to the risk of fraud than at other times, these are exactly the occasions when management has its hands full with other problems. For example, during time of rapid growth; when there has been a merger or reorganisation and management are not quite sure about the controls in the new or merged entity they have acquired; or during a period of decline, when morale may be low and management is fighting to save the business. Another situation of high risk is when remote operations are involved and management continually relies on financial and management information from those operations.

By being pro-active rather than reactive in subjecting an organisation to regular anti-fraud examinations and by investigating thoroughly whenever there is an unanswered question, an organisation can reduce the risk of being caught off balance by having to deal with fraud.

CONCLUSION

Although the nature and incidence of corporate crime is changing, and, in some ways, the sitaution is worse than ever before, the occurrence of fraud can be minimised by an effective program instituted by management to improve the overall system of internal control. One of the major steps which must be taken within an organisation is at least to recognise that potential fraud is a very real problem in any organisation and the problem must be addressed. All auditors and those in a management position must learn to be a little more sceptical – not to an unreasonable degree, but enough to plan to implement effective procedures properly for the prevention and detection of any material frauds. That is, step one is to improve management awareness.

Alternative Remedies for Fraud

THE RULE OF LAW VERSUS ADMINISTRATIVE REMEDIES

Rick Sarre*

There is no doubt that the time has arrived when society is obliged to re-think its traditional approach to the pursuit and punishment of those who seek to defraud governments. With the costs and the delays attendant upon traditional criminal investigations and the unprecedented escalation in the number of trials, the word "overkill" has entered the parlance of criminal justice commentators when speaking of criminal dispositions. This paper explores the idea that there may be alternative remedies which government agencies may (and do) seek, upon the apprehension or conviction of a person (whether government employee or recipient or user of government services) found acting in a fraudulent manner.

The idea of administrative remedies is here to stay. It may be that these remedies will lead to real savings in terms of dollars spent and hours laboured. But this paper examines some of the draw-backs attendant upon such proposals, and asks whether it is possible for administrative remedies to be applied across the board. Does the ad hoc administrative style of sentencing maintain an acceptable degree of objective consistency and certainty? May we be in danger of throwing the baby of justice out with the bath water of legalism?

* Rick Sarre is a member of the Law Department, School of Business, South Australian College of Advanced Education, Magill, South Australia. Paper presented to Australian Institute of Criminology seminar on "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

CBPA *No 56, September 1988, 110-117.*

THE NOTION OF PUNISHMENT

At the outset I wish to raise the issue of punishment generally. It is all too easy, and too facile, to maintain quite simply that where a person has broken the law, he or she should suffer the prescribed legal consequences.[1] Our accumulated wisdom throughout the ages has taught us how misguided that notion is. We have sought out creative alternatives when it has become apparent that traditional approaches give rise to consequences not in the best interests of society.[2]

Without dwelling on the theoretical aspects of punishment, I wish merely to make the point that our sentencing practices have, with good reason, adopted what is known as a positivist approach to sentencing. That is, we sentence the offender, not the offence. That being the case, we grant our sentencers wide discretionary powers to sentence offenders so that the "best" results occur. But sentencing decisions are not divinely inspired (Zdenkowski 1986:232). Sentencers are reduced to the simple hope that outcomes which are favourable to both the offender and the society result from their deliberations.

It is not the aim of this paper to enter into a full-scale discussion of the accepted aims of punishment and their respective strengths and weaknesses. There are many others who would do more justice to that broad and difficult topic than I would (Walker 1980, 1985; Freiberg 1986:5; Honderich 1984; Zdenkowski 1986; Weatherburn 1983:137, 1988:259; Potas 1984, 1985; Sallmann and Willis 1984:157; Radzinowicz and King 1977:219; ALRC 1987). It is

important, however, to ask the following questions with regard to the disposition of those caught defrauding the government. What will be the effect upon the offender of the adjudication process? What is the aim of the punishment prescribed, both for the offender and for the society generally? What if the punishment prescribed would arguably lead to further acts of the proscribed conduct? What if the process of adjudication and punishment leads to grossly disproportionate costs vis-a-vis the losses actually suffered as a result of the fraud?

I do not raise these questions (nor many others that could be raised) for any reason other than to show that the simple equation: offence = prosecution = punishment is not set in concrete.[3] Our society has been exploring alternative remedies for fraud, outside of the traditional criminal law realm, and with good reason.

But for the moment, let me return to the criminal sentencing process.

There are many considerations that should exercise the mind of the sentencer when pausing to pass sentence. It is not an easy task, nor is it, obviously, a task that avoids disparity of approach and result. Suffice it to say at this stage that professional sentencers (judges and magistrates) have not been able to adopt a uniform and consistent approach to sentencing theory. It is best described as "eclectic", that is, sentences and sanctions are justified according to the premise which seems to best fit the case at hand. Terms such as "retribution", "deterrence", "rehabilitation", "denunciation" and "incapacitation" are tossed around with very little definition and even less sustained public debate, which is rather surprising given that, very often, the aims are quite contradictory. Consistency of approach has, not surprisingly, been just as elusive to parliaments and law reform commissions. The Australian Law Reform Commission noted that even experienced judges "... frequently confess that the longer they perform the task of sentencing, the less confidence they have that they know what they are doing.... Serious, knowledgeable and responsible critics of the system ... chastise the disparities that exist in sentencing and describe the process as a 'random lottery' depending too much on capricious and inconsistent factors and on the personality and the idiosyncratic views of the particular sentencing judge." (ALRC, 1980:3)

It would not be inappropriate for modern society to be creative in the way in which it chooses to determine the fate of the citizens who, it has been deemed, have acted in an anti-social way. The system of sentencing which currently exists within the criminal realm hardly sets itself up as a model worthy of eternal praise. And yet the idea that forcing people through the criminal justice system will instill them with high moral values persists. It behoves a modern society not to persist blindly with practices which arguably run counter to the common weal.

THE ALTERNATIVES: PROSECUTION OR ADMINISTRATIVE SANCTION?

Society has accepted the challenge to seek out creative remedies and the following analysis examines administrative sanctions as an alternative to the traditional sentencing approach.

Simply stated, there are two fundamental strategies for the control of fraud on government, criminal prosecution and administrative action, which, for the purpose of this discussion, includes civil restitution (dealt with later in the paper). There are advantages and disadvantages to both approaches, and it will be valuable to explore them.

One need only examine the extraordinarily poor "success" rate of National Crime Authority investigations and prosecutions (especially when viewed in light of the huge NCA budget) to realise how the pursuit of justice through traditional legal channels is fraught with uncertainty, failures and wasted expense.

PROSECUTION THROUGH THE TRADITIONAL CRIMINAL LAW

Prosecution is the traditional response to a finding of suspected or alleged fraud. It involves a process of pre-trial prosecutorial decisions, negotiations, agreed facts, and then the criminal trial itself. It sets the state against the individual for the determination of responsibility and guilt. It plans for the imposition of sanctions from a rather narrow range of options which centre upon imprisonment. All this involves time. The law is slow and cumbersome. It is crowded with cases. A prosecution may last perhaps as long as two or three years depending upon the complexity of the matter and the level of compliance of defence and prosecution counsel. Peter Cashman (1987:211) reminds us of the so-called "Greek Conspiracy" prosecution which finally wound up in 1986, ten years after the alleged conspiracy, not only without a conviction but with $10 million in compensation payments and possibly in excess of $100 million in civil and criminal legal costs. The enormous costs apply equally for all sides, who become adversaries in every sense of the word. "The strain on the system which this increasing load of business brings is accompanied by the risk of undue haste and hence unfairness to individual accused persons" (Sallmann and Willis 1984:90).

Theoretically, it is not surprising that traditional prosecutions are unlikely to be cost effective as a means of securing compliance with all but the simplest requirements of the law. The English legal system has developed time-honoured principles designed to protect accused persons from unsubstantiated allegations, frame-ups and prejudicial treatment. For that reason the prosecution of fraud has constraints imposed upon the prosecutors by the law. There are requirements, for example, that proof be established "beyond reasonable doubt", and that the burden of proving the charges be upon the prosecution. There are other rules of fairness (often referred to as principles of "due process") which may prove to be a stumbling block for a successful prosecution, including the privilege against self-incrimination, the right to remain silent and the right to elect a jury trial on an indictable offence. One need only examine the extraordinarily poor "success" rate of National Crime Authority investigations and prosecutions (especially when

viewed in light of the huge NCA budget) to realise how the pursuit of justice through traditional legal channels is fraught with uncertainty, failures and wasted expense.

ADVANTAGES AND DISADVANTAGES: SUMMARY

Quite clearly, then, the advantages of the traditional approach are those which follow the so-called "rule of law" in any context: the precedents which allow greater consistency, openness and its attendant fairness, the rules of due process which protect the time-honoured rights of all accused persons to fair investigation and fair trial. The disadvantages are essentially the time and cost factors mentioned above, and the extent to which minor matters are treated as criminal matters, which may label and disillusion the protagonist into further acts of an anti-social nature. There is a wealth of sociological and criminological literature which suggests that, where possible, society ought to be diverting people from the legal process rather than subjecting them to its impersonal and humiliating rigours (Sarre 1984; O'Connor 1982; Zdenkowski 1986:222; Schur 1973; Radzinowicz and King 1977:336; Greenwood 1986). There is pressure to divest the criminal justice system of some of its traditional responsibilities, described by Polk and Alder as "doing good by doing less" (1986:315).

ADMINISTRATIVE REMEDIES

Contrast administrative control. Here the emphasis is upon pro-active rather than reactive regulation. The objective is primarily, though not exclusively, to prevent recurrence of the anti-social conduct by "ad hoc" disciplinary procedures. It seeks to avoid pushing the matter, and the wrong-doer, through the formal legal system. Not only is this designed to save time and expense, it is hoped that by removing the offender from the processes of the criminal justice system, and the attendant "labelling" process, the offender will be less likely to become embittered by the experience, and more likely to move quickly to re-establish him or herself in a productive role. The matter is dealt with as quickly and as expeditiously as possible without the heavy-handed and cumbersome intervention of the adversarial criminal law. Administrative sanctions seek to set and maintain publicised standards. They seek to place in motion strategies, procedures and structures that clarify issues before they become problems. It puts punitive discretion closer to the administration rather than in the hands of detached prosecutorial bodies who are less likely to understand the nuances of the workings of the agency (Grabosky 1987:223).

An example is appropriate. A person has been discovered drawing three welfare cheques under different names. Another person has been detected making long distance calls for friends from his or her position as a telephonist. Rather than invoking the prosecutorial processes, these persons may be asked or required, upon adequate investigation, and in accordance with well-publicised guidelines, to repay the amount of the over-payment with penalties, or in the latter example, be demoted, re-trained or instructed to take leave without pay for a number of days or weeks.

ADMINISTRATIVE REMEDIES IN THE CORPORATE WORLD

A huge amount of material has been prepared on the role of administrative regulation of the private corporate world, a proper examination of which is outside the scope of this paper. It is clear that administrative remedies have been effective in regulating certain conduct of business enterprises, for example, breaches of occupational health and safety regulations, food, environmental and drug and medical irregularities (Clarke 1987:270, 284; Grabosky and Braithwaite 1986). Examples of administrative remedies in such circumstances include the closing down of a plant where unsafe activities are rife and disqualification from government contracts. Other options range from the mild (organisational management reform orders) to the more draconian (licence revocation and company dissolution) (Fisse and Braithwaite 1988; Grabosky and Braithwaite 1986; Braithwaite 1984, 1985; Braithwaite and Fisse 1987). Braithwaite's discussion of self-regulation as a complement to, and not something which should obviate the need for, criminal law enforcement is worth noting (1987:145). The point to be made is that the effectiveness of successful regulation in the corporate world by non-prosecutorial methods highlights the possibilities of effective regulation of fraud on government agencies.

THE ADVANTAGES AND DISADVANTAGES: SUMMARY

The key drawback of this administrative option is that what it gains in expediency, it loses in "due process". That is, without the safeguards provided by the common law requiring, for example, proof beyond reasonable doubt, there is always the risk that "kangaroo" justice would prevail.[4] There are often calls for a return to the system of law and the rigours of prosecution which are perceived to be in decline. Legalists point to the unsatisfactory "... growth of 'bureaucratic-administrative' law, where public policy predominates over individual rights, [where] ... regulation rather than adjudication become[s] the primary form of dispute management" (Freiberg 1986:15).

Proponents of administrative remedies argue, however, that these sanctions are designed primarily to be preventative measures, and thus the chances of contravention are lessened. Furthermore, they argue that the guidelines ought to be so stated as to provide for minimum requirements of basic fairness or "natural justice". "It should be possible to devise publicly agreed to procedures for processing changes in regulations and providing for appeal to outside bodies in the event of sustained disagreements. It is also possible to provide that no sanctions be imposed unless regulations are breached – no retrospective regulation or arbitrary sanctions" (Clarke 1987:289). Finally, they argue that what these remedies lack in due process, they make up in flexibility. What takes place in modern government, they argue, is too complex, technical, transient and esoteric to be effectively enshrined in principles of law (Grabosky 1987:223), which principles are often riddled with a commensurate number of inconsistencies and anomalies.

Another argument in favour of the traditional legal approach is the fact that administrative remedies place the administration of justice well and truly out of the public

eye, when it is well accepted that "justice should not only be done, but manifestly and undoubtedly be seen to be done", to cite Lord Hewart's famous 1923 dictum. Administrative decisions, made in the back rooms of government agencies, are unlikely to be publicly viewed and debated. It is worrisome to many commentators that in the private sector many private firms engage in private justice (such as demotion of an officer caught in fraudulent activities) rather than engage in the laborious and time-consuming task of having the police investigate the conduct, with its attendant bad publicity (Polk and Alder 1986:321). It would be equally worrisome if control by private administrative remedies were to be seen as driving underground the treatment, by the state, of conduct which it is in the public's interests to have revealed (Radzinowicz and King 1977:269). "The particular interests and values of a given [agency] may not coincide with the interests of the community or of other [agencies]" (Sallmann and Willis 1984:93). There is really no answer to this objectiion unless conscious efforts are made to publicise the decisions of administrators in the application of such remedies.

It is very easy to see the administrative alternative to punishment as merely being a "soft option" to the rigours of punishment by the full force of the law. That is, it is very easy to criticise the new initiatives by pointing to the fact that financial constraints are being allowed to determine (read "down-grade") the quality of our justice.

Furthermore, critics of the administrative remedies point to the fact that without the full force of the law behind the sanctioning process, there will be a lack of deterrent force and, consequently, the incidence of fraud will incline. This is particularly so where there is evidence of large-scale fraudulent behaviour which persists over a long period of time. Of course, the notion of deterrence is fraught with difficulty and anomaly too. The best that can be said is that "[s]ome people are deterrible in some situations from some kinds of behaviour by some degree of subjective probability that they will suffer some sorts of penalty" (Walker 1985:419). Simply stated, it is impossible to say with any degree of certainty that the threat of receiving a "mere" administrative remedy will foster in the minds of the population generally that it will be quite acceptable to engage in fraud. To make that assertion is to ignore the host of other control mechanisms which exist in society outside of the threat of legal sanction. Furthermore such an assertion relies upon the dubious accuracy of the premise that people not only think about the consequences but think about the possibilities of apprehension. In addition, it is based upon the specious assumption that we have mastered all there is to know about human nature. Any debate over the merits of deterrence cannot continue without the debaters first coming to terms with the contradictions posed by the freewill versus determinist lobbyists, and the philosophers such as Rousseau and Hobbes.[5]

THE TRACK RECORD: EXPANDING THE USE OF ADMINISTRATIVE REMEDIES

Medifraud

Medical fraud, particularly through the practice of over-servicing, has concerned the Commonwealth Department of Health for many years (Lanham 1987:376). Draconian prosecution of doctors suspected of fraud may achieve undesirable results. "It is ... of considerable importance that a regulatory regime not have a chilling effect on the provision of adequate medical care; doctors must not be discouraged from providing a medical service when it is warranted" (Grabosky and Braithwaite 1986.155). By the same token, the Department does not want to appear to have an attitude of leniency, and indeed Grabosky and Braithwaite found that in 1984 the Department of Health had set a target of 100 prosecutions per year, a target which has not been reached since then. Nor have they been able to recover from dishonest doctors the $8 million per year spent on the enforcement of the medical benefits scheme.

But those researchers also found a well-entrenched administrative strategy involving counselling and monitoring in cases of suspected over-servicing. A Medical Services Committee of Inquiry could then recommend that the doctor in question be further counselled, reprimanded, his or her name gazetted (or published in the Health Department's Annual Report) and that he or she be required to refund over-payments. Furthermore, the greatest deterrent, arguably, of medifraud investigations is not the threat of criminal penalty, but the threat of disqualification and professional ignominy. Indeed, the use of adverse publicity as an administrative remedy extends to the placing of advertisements in newspapers and requiring the doctor to display a "disqualified" sign in the surgery (Grabosky and Braithwaite 1986:166). To the extent that the professional bodies, the AMA and the various medical colleges are systematically provided with information regarding over-servicing trends and suspect practices, and are consulted concerning steps to be taken to control abuses, there is no doubt that there is encouragement for the medical industry to be self-regulating.

Tax fraud

Tax evasion and, to a lesser extent, tax avoidance are two basic forms of misconduct which the Australian Taxation Office encounters repeatedly. The most widely used regulatory tool of the ATO is the civil penalty, for example the imposition of a penalty tax equal to double the amount of the calculated under-payment. The threat of double tax is a far greater regulatory tool than the threat of conviction. Grabosky and Braithwaite found that the determining feature in the ATO's decision to invoke the legal (criminal or civil) process tends to be that of cost-effectiveness. While prosecution is possible under the *Crimes (Taxation Offences) Act* 1980, it appears to be the case that the involvement of the Director of Public Prosecutions is minor indeed. The collection of payments through the pursuit of civil remedies "... far exceeds any reasonable expectations of financial penalties which might be imposed through the criminal process" (Grabosky and Braithwaite 1986:161).

The ATO encourages self-regulation of tax-payers by the clear dissemination of rulings and information, and by the provisions, introduced in recent years, to allow business tax-payers to self-assess, regulated only by the threat of ex post facto random checks. Tax agents, too, may have their licences suspended in the event of misconduct. And, finally, negotiation is one of the key ways in which the ATO is able

to manage its enormous volume of work. A hard-nosed prosecution policy, rigorously enforced, would submerge the ATO under a sea of paper-work and cost over-runs.

Customs fraud

When the full value of imported goods is not declared, or the correct tariff classification is not used, there will be an underpayment of required duties. The Australian Customs Service Manual contains a set of enforcement guidelines recommending prosecution in the event of listed irregularities including gross negligence and repeated transgressions. But as Grabosky and Braithwaite found, the Customs Service relies heavily upon informal administrative responses to misconduct, for example, the withdrawal of "trust" privileges, or zealous checking of all cargo passing through the hands of the malefactor. Self-regulation is encouraged through the licensing system through a National Customs Agents Licensing and Advisory Committee.

Administrative remedies are certainly most effective where small-time fraud is detected, and detected early. They may not be an appropriate means of dealing with second or subsequent offences.

Social Security fraud

There is no doubt that cheating on welfare is responsible for a considerable drain on welfare funds (Lanham 1987:374). In 1987 the Commonwealth Government, in a report prepared by the office of the Special Minister of State, reviewed its systems for dealing with fraud on government. In the paper it reviewed the possibility of employing administrative remedies to deal with cases of, inter alia, social security fraud. Highlighting the role the administrative remedies would have in identifying and deterring fraud and overpayment of benefits, it identified certain advantages already canvassed: the simplicity, immediacy and directness of operation, the cost benefits, the pro-active role and the flexibility of approach. The Department of Social Security finds within its legislation, the *Social Security Act* 1947, the power to recover overpayments by means of deductions from future entitlements.

But the report recognised a key draw-back with such remedies: that they are only truly effective when the defrauder and the agency have a continuing relationship. Where there is a single transaction, for example, a one-off bogus unemployment benefit claim, the options are not as readily viable. In cases where there is a continuing relationship, "... a service may be refused or deferred, money withheld or reduced ... or privilege withdrawn or suspended." But where services have been terminated or withdrawn, " .. there is no prospect of recovery from future entitlement and little opportunity to threaten a sanction other than legal proceedings" (Australian Government 1987:45).

The government paper recognised other difficulties in applying administrative remedies across the board, notably, for example, where the welfare recipient would suffer great hardship if required to refund overpayments. Or where third parties would be affected, as would be the case if residents of a nursing home were to have entitlements withdrawn, thereby lessening the funding to the nursing home (third party). According to the government report, administrative remedies are less appropriate where large sums of money are involved, although the report does not indicate why traditional criminal law prosecutions would be more appropriate. The burden ought to be specifically on prosecutors to persuade society that prosecution is positively beneficial.

Administrative remedies are certainly most effective where small-time fraud is detected, and detected early. They may not be an appropriate means of dealing with second or subsequent offences. Strangely, the report makes the rather incongruous claim that "[administrative procedures] ... are not an adequate means of dealing with individual instances after they have occurred" (1987:44). Frankly, since that would be, I would have thought, the vast majority of cases, I am astonished that the report considered the use of alternative remedies for fraud at all

The recommendations of the report nevertheless recognise the value of this alternative approach, while reflecting its inherent limitations:

> That, in developing plans and arrangements for fraud control ... agencies which do not already do so consider the use of administrative remedies as a means of dealing with minor instances of fraud and, where necessary, bring forward proposals for appropriate legislation.
>
> That, in order to assist evaluation of the efficiency of resource usage flowing from decisions to adopt administrative remedies in cases involving fraud, appropriate records be maintained of the application and use of such remedies ...

LIMITING THE USE OF ADMINISTRATIVE REMEDIES: THE TELECOM EXPERIENCE

In 1984, Victorian QC, now Supreme Court Justice, Frank Vincent, was asked by the Commonwealth Government to investigate the range and level of offences against the Telecommunications Commission and the remedies proposed by the criminal law (in particular the *Crimes Act*) and under the *Telecommunications Act*, which provides for criminal offences and administrative remedies. The pressing issue at the time was the assistance given to SP bookmakers by Telecom staff. He found that in most cases where Telecom staff had been engaged in criminal behaviour affecting Telecom, criminal prosecutions were avoided and the matters were dealt with internally. Internal discipline included the imposition of small monetary penalties, and the encouragement of resignation. The official policy is contained in Section G7/4/1 of the Standing Instructions:

> In general, Telecom Australia should avoid prosecutions where the case is not of a serious nature and can be satisfactorily resolved in some other way. The emphasis

should be on the prevention of a repetition rather than embarking on prosecution because it appears likely to succeed.

Vincent recognised the difficulties inherent in such a policy. He regarded the above statement as "unfortunately expressed" (Vincent 1984:13.9). By the same token, he did not dismiss the concept of administrative action outright:

> Although it is relatively easy to state that all crime should be prosecuted and all persons detected should be brought before the courts, in fact this has never happened and a very strong argument can be made that indeed it should never happen. I regard the operation of the criminal justice system as being merely one of the devices available to our society to control socially undesirable behaviour. It is clearly not the only device. It is not always the best or most appropriate device and in many situations its stated objectives may be achieved by the operation of other community mechanisms . . . It follows therefore that I do not find anything particularly offensive about the notion that not every person who has been detected in a form of criminal behaviour has been prosecuted before the courts, regardless of the seriousness of that behaviour or the circumstances in which it occurred. (Vincent 1984: 12.25-12.26)

Vincent was convinced that it was possible to have criminal and administrative consequences co-exist in the one matter and in the one organisation. However, he was critical of the way in which Telecom had gone about the task of applying administrative remedies, claiming that it had failed to strike what he referred to as "an appropriate balance" (Vincent 1984:12.27) between prosecutorial and administrative processes. Vincent noted problems of inconsistency, unfairness and caprice within the organisation, and when comparing the potential for variance of policy when dealing with civilians as opposed to officers of the organisation. Furthermore, Vincent was concerned about the possibility that the "sentence" will fail in its denunciatory capacity. If there is evidence of criminal behaviour, he maintained, section 58 of the *Telecommunications Act* (creating criminal offences) ought not be dismissed as an option lest that decision acts "so as to reduce the seriousness of the offence or conceal the criminality of the behaviour" (Vincent 1984:13.13). Concomitantly, Vincent was concerned that the discretion to use administrative remedies is not seen as the total answer for this may create ". . . serious potential for abuse or misguided benevolence such that if offending behaviour by an officer is criminal, but not in Telecom's view 'serious', the matter can legitimately be kept 'in-house' " (1984. 13.20). Hidden away from the public eye, there is the potential problem that matters are inadequately dealt with, accountability becomes impossible and injustices would result.

Vincent concluded his report with a series of recommendations limiting the use of administrative remedies (essentially to minor matters, for example, for offences of dishonesty he set a limit of $5,000) and setting a schedule designed to strike the "balance" which he found lacking. Where there was an argument that the investigation and remedy proposed by Telecom was inadequate or unsatisfactory, Vincent proposed referral of the matter by the Director of Public Prosecutions to the Australian Federal Police for further investigation. There is a difficulty which many may find with this proposal. That is, it may tend to defeat the cost advantages of the administrative process if there is this 2-stage prosecutorial review of the administrative remedy should the DPP think that it is inadequate. Indeed, there is always the danger that the use of administrative remedies will merely toss up a whole new bureaucratic monster, complete with appeal mechanisms and other safeguards. It is incumbent upon those who draft the administrative guidelines that the alternative process does not merely create a re-worked edition of the unsatisfactory predecessor.

REPARATION: RESTITUTION AND COMPENSATION

One of the key administrative remedies is reparation. This involves the paying back of ill-gotten gains either to the persons aggrieved, or, where there are none specifically, the state (Lanham 1987:542). Although in some systems it is tied to the punishment upon conviction, for example, legislation which provides for the confiscation of profits of crime or criminal injuries compensation levies and payments, both at Commonwealth and State level (Lanham 1987:542ff), it may be used in the absence of prosecution. Ian Temby, QC, the Director of Public Prosecutions, notes that during the period July 1985 to June 1987 his office recovered $37.5 million at an operational cost of a mere $5.8 million through successfully pursuing civil remedies from the protagonists of the so-called "bottom-of-the-harbour" tax evasion schemes (Temby 1988, Weinberg 1985:4, 15). Just whether this amounts to administrative remedies or not is a difficult question of definition, for while it avoids the cumbersome prosecutorial realm, it is most often caught up in the intractable civil justice system. Perhaps the best that can be said is that it highlights the existence of a middle ground, indeed, a *sui generis* "grey area" of regulatory enforcement.[6]

The immediate difficulty of the impecuniosity of the offender becomes apparent. How does an agency enforce a civil remedy when the person caught in the fraud is unable to pay? But there are other, perhaps more pressing, difficulties which arise. What if the defrauder made nothing? What if the defrauder was successful, but the losses were insured? What if the defrauder agrees to repay in full in return for no legal or administrative action in relation to the fraud? There is no doubt that administrative or civil remedies would be preferred where there is evidence of reparation. But why should even-handed justice, justice that has at its disposal a range of remedies legal and administrative, deal with these persons any differently from the person who has merely spent the ill-gotten gains and thus can make no reparation in circumstances where the culpability was identical?

IMPRISONMENT

There ought to be, for the sake of completeness, some mention of the ultimate sanction, imprisonment. It is not intended to raise this issue other than to say that it would be entirely inappropriate for imprisonment to be used in response to fraud on government in all but the most serious of cases. "Neither the history of imprisonment nor

contemporary research lends any support to the view that the use of imprisonment leads to the diminution of crime either by way of deterrence or rehabilitation. Imprisonment as a sanction should be used only as a punishment of the last resort" (ALRC 1980:16). None of the studies referred to in this paper disagrees, and yet there is a persistent theme amongst those who are investigating and prosecuting fraud that unless imprisonment is held out as the appropriate punishment, the fight against fraud is in vain. Such a view runs contrary to the evidence (that is, there is little evidence to suggest that the incidence of fraud, fraught as that term is with definitional problems, declines as punishment becomes more draconian), and contrary to recognised theories and philosophies of punishment and deterrence generally. The view ought to be rejected outright.

SUMMARY

The setting up of administrative regulation, or even quasi-legal control, such as that provided by civil remedies such as restitution and compensation, recognises the merits of establishing a body of clear and reasoned guidelines, allowing representation, due process and certainty yet not invoking the formalities of the legal adversarial system. Although it may have a number of disadvantages including inadequate codification, hazy due process and unclear procedures, it does offer advantages (Clarke 1987:290). There is no doubt that even in the legal eyes of a sceptic such as Frank Vincent, there is a place in the criminal justice system for administrative remedies. Not only would they implant into the minds of officers of the government and the minds of those who deal with government agencies that there are certain standards of behaviour and propriety which ought to be adhered to, but they are a practical way of advertising those expectations with a view to prevent future occurrences.

But there is clearly a role for the prosecutorial model as well, for although legalism is said to be "... unwell, it is not yet dead" (Freiberg, 1986:16). Thus, in the final analysis, an amalgamation model is the most likely outcome, that is, a model that uses the legalistic approach where appropriate and the administrative approach where the legal method is inappropriate. May I suggest that the administrative process ought to be considered first until such time as prosecutors decide that the administrative "presumption" has been displaced. May I further suggest that the traditional criteria for opting for the prosecutorial process, namely the scope of the fraud, or the number of protagonists or the amount of money involved, be not the ultimate criteria. Rather, the openness of the enquiry might be a determining factor, or the nature of the defendant's argument, or whether he or she raises a question of critical legal importance and wishes to have the matter dealt with in a criminal court. Perhaps the availability of civil restitution should be a key determining feature. There are many options. At the moment it appears that we resort to legal remedies purely as an act of faith, for, as a society, we have not yet agreed upon the criteria which ought to be used to assess the success or failure of the end product.

It has been, indeed, a brave step for society to launch into this field at all. For it would have been just as easy for society to have retreated behind the rule of law. Fortunately and unfortunately our compassionate zeal and genuine desire for equity as well as expedience has drawn us more and more into a morass of complications. It is to be hoped that we nevertheless continue to accept the challenge to debate the creation of remedies that seek to avoid the legal process and the legal sanction. Indeed, there are some commentators who would seek to have a greater de-legalisation of the entire criminal law, a debate that must continue outside of this paper.

For all of the contingencies that it involves, and difficulties that it poses, the administrative, quasi-legal road must be embraced by us all with confidence and foresight.

Let me add that, ultimately, I am firmly of the belief that if prevention is better than cure, then the preventative spirit is more likely to be engendered within the hearts of a society that is able to meet the needs of its citizenry, rather than one that commands respect merely by fear of punishment.

There will thus need to be greater reliance in our system of legal and administrative justice upon the internal controls deriving from the development of early socialisation skills, and less reliance upon external fear as a form of control. Ian Temby, DPP, has identified something of this trend: "It used to be the case among the self-employed that if you paid your tax in full measure you were considered to be a fool, some sort of romantic ... Nowadays, you don't hear people bragging about the fact that they don't pay tax ... I don't say that people like paying tax, but the general attitude is that, if you don't pay it, you're a freeloader" (Temby 1988:148). It has been said that nineteenth century bush-ranging died out more from a change in community attitudes than as a result of more astute policing or draconian punishment (O'Malley 1979). It is along these lines perhaps that the USA administration has revived the *False Claims Act* 1863, (numbered PL 99-562, 1986) allowing for a private citizen who discovers fraud against the government to sue for damages, a process described by Grabosky as "citizen co-production in fraud control" (Grabosky 1988).

The best results, I believe, will follow a change of community attitude rather than a policy of administrative or legal consequences. For example, in the corporate sector Fisse and Braithwaite aver that it should not merely be the "... optimists who see appeals to corporate social responsibility as the best route to ethical corporate conduct" (1987:245). Being a realist, I do not hope to imagine that those types of community attitudes will be inculcated into our general thinking overnight. It will not occur until such time as every segment of our society believes that we are all able to share the fruits of our plenty, which is sadly, some distance away yet.

ENDNOTES

1. This paper does not deal with the wider definitional questions raised by the term "fraud". It is not an objective term. Much "fraud" is not so defined by law, and would otherwise be termed "good business practice". I will, however, for the sake of expediency, refer to fraud as those activities specifically proscribed by legislation.
2. Often referred to as a positivist response to punishment, these accepted alternatives allow our sentencers to ignore trivial law-breaking, for example, or forgo punishment where there are compelling or over-riding factors, such as the youth of a defendant and the effect of a conviction upon his or her career.

3. Yet this approach is the one consistently adopted by those who call for a "get tough" approach to fraud control. The notion of hanging or transportation to Australia as a response to pick-pocketing was once set in concrete also.
4. There is an argument, on the other hand, that justice and sentencing in the lower courts especially is hardly conducted with a "fully fledged due process of law" (Zdenkowski 1986: 222).
5. Rousseau was of the opinion that humans were basically good but corruptible in some circumstances, while Hobbes, on the other hand, maintained that humans were basically bad, and were only made good by the firm control that the fear of punishment supposedly brings.
6. An area tapped by the USA administration in its False Claims legislation described by Grabosky, 1988.

REFERENCE MATERIALS AND EXTENDED BIBLIOGRAPHY

Australian Capital Territory Administration (1988), *First Report of the ACT Administration on Fraud Control Initiatives*, Canberra, Commonwealth of Australia, March 1988.

Australian Government (1986), "Prosecution Policy of the Commonwealth: Guidelines for the Making of Decisions in the Prosecution Process", Canberra, Australian Government Publishing Service.

Australian Government (1987), Office of the Special Minister of State, "Review of Systems for Dealing with Fraud on the Commonwealth", Canberra, Australian Government Publishing Service (at pp 44 ff "Administrative Remedies").

Australian Law Reform Commission (1980), *Sentencing of Federal Offenders*, Discussion Paper No 15.

Australian Law Reform Commission (1987), *Sentencing: Summary of Discussion Papers 29-31*.

Braithwaite, John (1984), *Corporate Crime in the Pharmaceutical Industry*, London, Routledge & Kegan Paul.

Braithwaite, John (1985), *To Punish or Persuade*, Albany, State University of New York Press.

Braithwaite, John (1985), "Self-Regulation: Internal Compliance Strategies to Prevent Crime by Public Organisations", Peter Grabosky (ed), *Government Illegality*, Canberra, Australian Institute of Criminology Seminar, Proceedings, No 17 at page 145.

Braithwaite, John and Brent Fisse (1987), "Self-Regulation and the Control of Corporate Crime", Clifford Shearing and Philip Stenning (eds), *Private Policing*, Newbury Park, Sage, chapter 9.

Cashman, Peter (1987), "Civil Litigation: Prospects and Problems", Peter Grabosky (ed), *Government Illegality*, Canberra, Australian Institute of Criminology Seminar, Proceedings No 17 at page 207.

Clarke, Michael (1987), "Prosecutorial and Administrative Strategies to Control Business Crimes: Private and Public Roles", Clifford Shearing and Philip Stenning (eds), *Private Policing*, Newbury Park, Sage, Chapter 11.

Fisse, Brent and John Braithwaite (1988), "Accountability and the Control of Corporate Crime: Making the Buck Stop", Mark Findlay and Russell Hogg (eds), *Understanding Crime and Criminal Justice*, Sydney, Law Book Co, chapter 5.

Freiberg, Arie (1986), "Reward Law and Power: Towards a Jurisprudence of the Carrot", Roman Tomasic and Rick Lucas (eds), *Power, Regulation and Resistance: Studies in the Sociology of Law*, Canberra, CCAE Series of Administrative Studies No 8, chapter 2.

Grabosky, Peter (1987), "Concluding Observations on Public Sector Illegality and its Control", Peter Grabosky (ed), *Government Illegality*, Canberra, Australian Institute of Criminology Seminar, Proceedings No 17 at page 219.

Grabosky, Peter (1988), "Citizen Co-Production in Fraud Control", published in this issue of CBPA.

Grabosky, Peter and John Braithwaite (1986), *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*, Melbourne, Oxford University Press, (especially chapter 12).

Greenwood, Bob (1986), "Diversion and the Director of Public Prosecutions", Ron Snashall (ed), *Pre-Trial Diversion for Adult Offenders*, Canberra, Australian Institute of Criminology Seminar, Proceedings No 10 at page 41.

Honderich, Ted (1984), *Punishment: The Supposed Justifications*, Harmondsworth, Penguin.

Lanham David et al (1987), "Restitution and Compensation Orders", *Criminal Fraud*, Sydney, Law Book Co, chapter 19.

O'Connor, Kevin (1982), "Controlling Prosecutions", J Basten et al (eds), *The Criminal Injustice System*, Sydney, Australian Legal Workers Group and Legal Services Bulletin Co-operative at page 151.

O'Malley, Patrick (1979), "Class Conflict, Land and Social Banditry: Bushranging in Nineteenth Century Australia", *26* (3) *Social Problems* 271.

Polk, Kenneth and Christine Alder (1986), "Criminal Justice Reform in Australia", Duncan Chappell and Paul Wilson (eds), *The Australian Criminal Justice System: The Mid-1980s*, North Ryde, Butterworths, chapter 16.

Potas, Ivan (1984), "Measuring Prosecutorial Discretion", Ivan Potas (ed), *Prosecutorial Discretion*, Canberra, Australian Institute of Criminology Seminar Proceedings No 6 at page 35.

Potas, Ivan (1985), "Purpose, Discretion and Sentencing Reform", an unpublished paper delivered at the International Criminal Law Congress, Adelaide.

Radzinowicz, Sir Leon and Joan King (1977), *The Growth of Crime: The International Experience*, Harmondsworth, Penguin.

Sallmann, Peter and John Willis (1984), *Criminal Justice in Australia*, Melbourne, Oxford University Press.

Sarre, Rick (1984), "The Orwellian Connection: a comment upon recent correctional reform literature", *6* (Spring), *Canadian Criminology Forum*, 177.

Schur, E M (1973), *Radical Non-Intervention*, Englewood Cliffs, NJ, Prentice-Hall.

Temby, Ian (1988), Interview with Phil Jarratt, *The Bulletin*, June 7, pp 145-50.

Vincent, Frank (1984), *Review of Matters Affecting the Australian Telecommunications Commission: Report to the Special Minister of State*, AGPS.

Walker, Nigel (1980), *Punishment, Danger and Stigma*, Oxford, Blackwell.

Walker, Nigel (1985), *Sentencing: Theory Law and Practice*, London, Butterworths.

Weatherburn, Don (1983), "Sentencing for What?", Mark Findlay et al (eds), *Issues in Criminal Justice Administration*, North Sydney, George Allen and Unwin, chapter 9.

Weatherburn, Don (1988), "Sentencing Principles and Sentence Choice", Mark Findlay and Russell Hogg (eds), *Understanding Crime and Criminal Justice*, Sydney, Law Book Co, chapter 13.

Weinberg, Mark (1985), "Prosecuting Tax Promoters – A New Growth Industry", an unpublished paper delivered at the International Criminal Law Congress, Adelaide.

Zdenkowski, George (1986), "Sentencing: Problems and Responsibility', in Duncan Chappell and Paul Wilson (eds), *The Australian Criminal Justice System: The Mid-1980s*, North Ryde, Butterworths, chapter 11.

Blowing the Whistle on Fraud in Government

*John McMillan**

Virtually unknown ten years ago, whistleblowing has quickly established itself as a practice that is now both international and respectable. Its international reputation stems in part from the notoriety of some of the whistleblowing folk heroes such as Daniel Ellsberg and Clive Ponting, and from the cinematic portrayal of some other members of the whistleblowing hall of fame, such as Karen Silkwood, Frank Serpico, and Stanley Adams. The respectability of whistleblowing was most firmly established by the enactment in 1978 by the United States Congress, on the proposal of President Jimmy Carter, of what is now popularly known as a "Whistleblowers Protection Act". The influence of that precedent has spread elsewhere – inside the US, where many States have enacted similar legislation; and to other countries as well, where proposals for enactment of comparable guarantees have been made by bodies such as a Canadian Law Reform Commission. Whistleblowing has established itself in other ways too – in the dictionary, in library bibliographies, and in a considerable volume of academic literature that is remarkable for its cross-disciplinary flavour: an extensive literature is now found in disciplines as varied as behavioural psychology, management theory, public administration, civil rights protection, labour or employment law, and law enforcement and fraud detection.[1]

Virtually unknown ten years ago, whistleblowing has quickly established itself as a practice that is now both international and respectable. Its international reputation stems in part from the notoriety of some of the whistleblowing folk heroes such as Daniel Ellsberg and Clive Ponting, and from the cinematic portrayal of some other members of the whistleblowing hall of fame, such as Karen Silkwood, Frank Serpico, and Stanley Adams.

Australia, like other countries, has its well-known whistle blowers, such as Phillip Arantz, Don Witheford, David Berthelsen (and the NSW Police Technical Survey Unit, publishers of "The Age Tapes"). Though the disclosures by each of these have all been treated in the popular media, the practice of whistleblowing has otherwise been the subject of little attention in Australia. Virtually no serious literature on the issue has been published,[2] no sustained attention has ever been given to it by any of the numerous enquiries and reports into fraud and law enforcement that we have had in recent years, and (to my knowledge) no Commonwealth or State parliamentarian has ever sought to be a public champion of the issue.[3] In that context, it may not seem surprising that the Commonwealth's 1987 report on *Review of Systems for Dealing with Fraud on the Commonwealth*[4] had virtually nothing to say about combatting fraud by devices (such as whistleblowing) which rely on enlisting the assistance and information of individuals who otherwise have no responsibility for correcting an abuse.

The issue is, nonetheless, one that is worthy of serious consideration. Those working within an organisation will often be the first – and sometimes the only ones – to know of any illegal or immoral practice committed by or within that organisation. One of the first things to become apparent in any public enquiry into government illegality – whether occurring within the Queensland police force or within the US Defense Department – is that the nature of the scandal has been widely known within the organisation for many years. Usually, too, those official enquiries will highlight individuals who had previously made valiant but unsuccessful attempts within the organisation to correct the abuse, or who had appreciated full well that they would be the first victims should any attempt at disclosure be made.

Often times the price of silencing internal criticism is simply too high. A popular example nowadays is the Challenger disaster, which claimed seven lives, destroyed two billion dollars in hardware, and "punctuated NASA's and America's aura of high-tech invincibility".[5] Subsequent inquiries into that disaster have revealed not only that relevant organisations had ignored the warnings of internal specialists that the flight should not go ahead, but also that those same specialists were later punished for publicly disclosing the fact. Equally, the annals of American whistleblowing now record the millions of dollars that have been saved as a result of whistleblowing disclosures that have corrected automobile design defects, inadequate health inspections, graft and other corruption of public officials.[6]

Later in this paper I shall look at different options that exist (such as hotlines and whistleblowing protection statutes) for facilitating formal disclosure of fraud and illegality. Before doing so, it is necessary to define whistleblowing more precisely, to consider the extent to which unauthorised public interest disclosures are already protected within our legal system, and then look at the legal and other obstacles which those disclosures nevertheless face.

DEFINING WHISTLEBLOWING

Dictionary references to whistleblowing tend to emphasise a pejorative character that its victims would probably

* John McMillan lectures in the Faculty of Law, The Australian National University. Text of an address to Australian Institute of Criminology Seminar, "Fraud on Government", Surfers Paradise, Queensland, 18-20 July 1988.

applaud; common here is the notion of a person betraying some secret, especially to the authorities. However, the contemporary interest in and definition of the term probably stems from Ralph Nader in 1972, who described it in tendentious language as "an act of a man or woman who believing that the public interest overrides the interest of the organisation he serves, publicly blows the whistle if the organisation is involved in corrupt, illegal, fraudulent, or harmful activity."[7] A more temperate and more commonly used definition stems from the protection given by the US Civil Service Reform Act (discussed below) to an employee "who discloses information he reasonably believes evidences a violation of any law, rule, or regulation, or mismanagement, a gross waste of public funds, an abuse of authority, or a substantial or specific danger to public health or safety." To go yet a step further, other writers (particularly in the field of organisational theory) tend to emphasise the separate existence of a number of elements, common among them being:[8]

- the whistleblower: a current or past employee of an organisation who makes accusations against that organisation;
- the recipient of the complaint: commonly some external body (such as the media, Parliament, or a public enquiry) but sometimes also an internal recipient (such as a more senior officer, or a special internal office created to receive such complaints);
- the complaint: normally that an organisation has practised, tolerated or bears responsibility for some illegal, immoral or unethical conduct which is likely to result in unnecessary harm to third parties; and
- the circumstances of the disclosure: which usually occurs in a way whereby the whistleblower (either intentionally or accidentally) is identified publicly with the complaint, and claims that the principle motive for the disclosure was to advance the public interest.

LEGAL PROTECTION OF INDIVIDUALS WHO REPORT FRAUD

There are many ways in which or legal system encourages individuals to assist in the detection of unlawful behaviour, and also protects those who do so against any reprisal or victimisation. In the administration of the law generally, the police and other government departments routinely rely on informers for information which assists in the efficient enforcement of criminal, taxation, immigration, social security, corporate and other laws. This assistance is formalised at times, by such things as financial rewards, neighbourhood watch schemes, witness protection units, and even government publicity campaigns to encourage dobbing (for example, on drugs). In some Australian jurisdictions we also have the old common law offence, misprision of felony, which imposes a duty on every person to disclose to the authorities any knowledge which he or she has about the commission of a felony by another; breach of that duty is itself a criminal offence which can lead to fine or imprisonment, even though the offender is in no way actively involved in the felony of which he or she has knowledge.[9]

There are now also many legislative schemes which not only facilitate complaints by people about government breaches of legal or ethical standards but which also protect those complainants against any harassment or intimidation: see for example the *Ombudsman Act* 1976, the *Human Rights and Equal Opportunity Act* 1986, and the *Royal Commissions Act* 1902.

Similar protection against adverse consequences has also been developed by the common law. For example, it is a contempt of court to victimise or intimidate a party or a witness in judicial proceedings.[10] The concept of contempt also operates in the parliamentary forum, to preclude victimisation or obstruction of witnesses to parliamentary inquiries.[11] Equally, a person who has disclosed evidence of another's wrongdoing (particularly to the authorities) may have a number of public interest defences to an action for defamation – for example, truth or justification, where the disclosure was true: and, even where the disclosure was false, by the defences of fair comment on a matter of public interest, absolute privilege for statements made in the course of parliamentary or judicial proceedings, or qualified privilege for a communication of information between persons who had a relevant legal, moral or social interest or duty in communicating with each other.

It is not the main object of any of those principles to encourage or protect whistleblowing, but there are many instances nonetheless in which that has occurred. There is, for example, the case of David Berthelsen, about whom the House of Representatives Privileges Committee made a recommendation that the Public Service Board take steps to restore his career prospects that had been damaged after he gave evidence to a parliamentary committee concerning financial mismanagement in the Defence Department.[12]

There is one area where the law comes close to recognising a "whistleblower's defence".[13] The common law imposes on employees a number of obligations towards their employer, chiefly the duties of loyalty (for example, to work diligently, skilfully and honestly for the employer), of good faith (for example, to avoid any private conflict of interest), and the duty of confidentiality (to keep certain information confidential). Breach by the employee of any of those duties can be actionable in a number of ways, including dismissal of the employee, liability of the employee for damages, or an enforceable restraint by the employer on behaviour such as a threatened disclosure of information. One of the important exceptions to the common law duty of confidentiality, sometimes called "the whistleblower's" exception, is that an employee is excused where he or she releases to the public or to the proper authorities information that evidences wrong doing by the employer that ought, in the public interest, be disclosed. In general terms, this defence will often mean that no action can be taken against an employee for disclosing iniquity, such as a crime or fraud. One writer has described the defence as follows:

> The defence of just cause or excuse is potentially applicable to the disclosure of information concerning any crime or civil wrong, whether committed or in contemplation. But, in each case, the public interest must be borne in mind. It is difficult to conceive of any circumstances in which it will not be in the public interest to disclose information about past or proposed

crimes. Similarly, the disclosure of proposed civil wrongs would always seem to be in the public interest since society has an interest in ensuring that its laws, whether civil or criminal, are respected.[14]

An instance in which the defence is recognised was where an employee had disclosed that his employer's high retail prices were not, as the employer claimed publicly, due to an employment tax, but due instead to an unlawful price fixing agreement between that employer and other firms.[15] The public interest defence was also applied by Mr Justice Kirby of the NSW Court of Appeal in the *Spycatcher* case. His Honour held that the public interest of Australia justified the disclosure of the matters in *Spycatcher*, by reason of the bearing which those disclosures had on the history of ASIO, "and the relevance of those disclosures to the defences which this country should build against similar treason, deception and error."[16]

The significance of this defence is that it is based squarely on a judicial assessment of the public interest. In the context of defining the important duty which an employer can rightfully demand of an employee, the courts have recognised nonetheless that the public interest should permit, by way of a balance, that an employee can in the right circumstances unilaterally determine to breach that duty, by disclosing secrets of the employer without any authorisation so to do.

The same public interest emphasis on disclosure of executive or corporate illegality is found in other principles in our legal system. For example, the doctrine of confidence discussed above can be employed to restrain not only information disclosed by an employee, but also any disclosure by a third party who may have obtained information improperly or surrepticiously (for example, by a leak). Here again, however, the courts will not restrain disclosure of government information unless disclosure is likely to injure the public interest. The strength of the public interest in disclosure was best illustrated in the *Defence Papers* case, in which the Government could not restrain by the use of this doctrine the disclosure of classified documents relating to Australia's defence and foreign policy in South East Asia. As Mason J commented, "it is unacceptable, in a democratic society, that there should be a restraint on the publication of information relating to government where the only vice of that information is that it enables the public to discuss, review and criticise government action".[17] That same public interest in disclosure has now been entrenched more broadly and more firmly in the *Freedom of Information Act* 1982.

Some implicit condonation of whisteblowing might also be extracted from the decision of the High Court in the *Sheraton Hotel* case. The Court refused to restrain the Commonwealth from handing to the Victorian law enforcement authorities the names of the ASIS officers who participated in the events at the Sheraton. That is, the Executive itself was not restrained from disclosing to the police the identity of law breakers. A comment of the Chief Justice, Sir Harry Gibbs, is also apposite: "it is fundamental to our legal system that the executive has no power to authorise a breach of the law and that it is no excuse for an offender to say that he acted under the orders of a superior officer."[18]

LEGAL AND INSTITUTIONAL OBSTACLES TO PUBLIC INTEREST DISCLOSURES

If whistleblowing is respected by our legal system in so many ways, why then are whistleblowers such a persecuted class? The answer is for most purposes a simple one. Whilst the whistleblower demonstrates a concern for and a loyalty to the welfare of the public and the state in general, the whistleblower is usually demonstrating as well a disloyalty to an organisation in which he or she is employed. It is in the nature of organisations in our society, whether they belong to the public or the private sector, that the first loyalty which they demand of all employees is to the organisation itself. The capacity to enforce that loyalty is immense. Whilst a court may be able to restrain overt intimidation by the organisation (such as a dismissal order), a court can often do little to erect a protective shield that accompanies the employee every minute of the day. What eventually breaks many whistleblowers is the aversion and subtle abuse which they suffer, the transfer to a menial position, the exacting scrutiny of their time sheets and other work records, the demanding nature of the orders given to them, and the constant threat of demotion or dismissal for some unrelated misdemeanour. Where the employer is a government agency there are in addition a great many legal and administrative weapons that can be used in retaliation. Philip Arantz, for example, was referred immediately for psychological assessment and treatment. Daniel Ellsberg and Don Witheford were not prosecuted for whistleblowing or for unauthorised disclosure, but for unlawful possession of government documents.

Quite simply, organisations like the state have established a vast superstructure of principles that can suppress internal dissent and disharmony. In Commonwealth legislation alone there are as many as 150 different secrecy provisions which penalise the unauthorised disclosure of information. The most ubiquitous in effect is section 70 of the *Crimes Act* 1914, which imposes a 2-year prison sentence for any unauthorised disclosure of information acquired by a current or a former Commonwealth employee. Questions of motive, purpose and justification for the disclosure provide no defence to this blanket offence. It is indeed an interesting reflection of the Government's values that the disclosure of information often attracts more serious criminal penalities than the unlawful conduct in respect of which the information was collected by government!

In the Commonwealth's *Guidelines on Official Conduct of Commonwealth Public Servants* (1987), there is the same emphasis on keeping the lid on internal dissent or disagreement. For example, a Departmental Secretary who believes that a minister's instruction is illegal or unethical is counselled to raise the matter orally or in writing with the minister and as an ultimate (and "extreme step") seek to have the disagreement brought before the Prime Minister.[19] The *Guidelines for Official Witnesses Before Parliamentary Committees*[20] also stress that it will be for a minister or agency head to decide which official is the most appropriate to provide the information sought for an agency. Implicit too in those Guidelines is that the official's evidence should not embarrass in any way a minister or the government.

There are other ways too in which our legal system threatens the security of whistleblowers. For example, where there

are substantive proceedings already before a court, different legal processes (such as subpoenas and contempt of court) can be used to compel, either directly or indirectly, the disclosure of a journalist's sources. By dint of this manouvre a British civil servant, Sarah Tisdall, was sentenced to six month's imprisonment for anonymously leaking to *The Guardian* a defence document about ministerial tactics involved in parliamentary and public statements about the installation of nuclear weapons at a Royal Air Force base.[21] Equally, even the utility and sanctity of the public interest defences referred to earlier are fragile in the light of some judicial statements which warn that the official who discloses in breach of an obligation of confidence bears a heavy onus of establishing the facts on which he or she relies to be relieved of the confidential obligation.[22]

Lastly, if one is to draw a comparison between our legal and institutional framework and the whistleblowing protection schemes discussed later, many other points of difference are revealed which show clearly the starkly different bias inherent in each system. One of the chief objectives of a whistleblowing protection scheme is to establish a clear procedure by which a complaint of illegal or unethical behaviour can be raised internally, often with a view to averting the need for public disclosure. The Commonwealth's *Guidelines* for public servants, by contrast, contain no similar procedure. Overall their purpose, instead, seems to be to preserve the integrity of the organisational structure against criticism or embarrassment. Equally, it is a feature of whistleblowing legislation to establish an independent or protective office, which has an explicit mandate to safeguard the interests of an individual whistleblower. In our system, by contrast, a whistleblower would most likely rely for protection on the very officers whose behaviour may be the subject of criticism. Lastly, the whistleblowing legislation recognises that in some instances the just and equitable solution is to compensate a whistleblower (often financially) for the damage suffered as a result of taking steps to protect the public interest. No similar notion can be identified in our system.

WHISTLEBLOWER PROTECTION MECHANISMS

The United States has undoubtedly led the way in establishing general legal protection for whistleblowers.[23] Initially the protection was constitutional: from 1968 onwards the Supreme Court established that the First Amendment right to freedom of speech protects federal government employees who express public dissent, provided that internal administrative remedies are first used where these are available. All employees, in both the public and the private sector, now gain a similar protection by reason of court decisions in a large number of States, that the traditional common law right of an employer to fire-at-will is tempered by a public policy exception: a person cannot lawfully be dismissed for a reason that would undermine a firmly established principle of public policy, for example, that the employee was defending public health or safety, or was acting conformably with the requirements of a professional code of ethics).

This protection has been strengthened in the last decade by the enactment of a large number of whistleblower protection statutes. These exist in as many as thirteen States. At the federal level, upward of thirty different statutes have been enacted which protect both public and private sector employees who disclose potential violations of laws in areas as diverse as environmental protection, mine safety, labour regulation, health and safety standards, transport safety, and civil rights.

The most renowned of the statutes, however, and the one which paved the way for most others, was the *Civil Service Reform Act* of 1978.[24] This Act was prompted by a number of concerns – the Watergate exposures of abuse of civil service principles, an acceptance that whistleblowing can have a desirable effect in containing government fraud and mismanagement, a desire to introduce a more appropriate balance into the ethical foundations of the civil service, and a realisation that whistleblowers were, as a class, unjustly persecuted. Overall the Act represents a genuine attempt to protect whistleblowers by balancing their interests against a number of other considerations – among them, that the civil service can legitimately expect loyalty from its employees, that persons in positions of trust should normally honour that trust, and that whistle-blowing can sometimes be wrongheaded, ill-informed, or actuated by malevolence or improper motives.

The main principles of the Act are as follows:

- The protection of the Act extends to any federal employee who discloses information which he or she reasonably believes evidences a violation of any law, rule, or regulation; mismanagement; abuse of authority; a gross waste of funds; or a substantial or specific danger to public health or safety.
- Administration of the scheme rests primarily with the Office of the Special Counsel (OSC), who discharges a unique range of quite different functions – investigating allegations of reprisal against employees, preventing further retaliation against employees, prosecuting managerial personnel who have victimised a whistle-blower, determining whether relief of some kind should be made to an employee, and acting as an early warning system by screening potential whistleblowing disclosures and ordering agencies to investigate those allegations which have merit.
- Some of these functions of the OSC are discharged through another agency, the Merit Systems Protection Board, which determines all actions for compensatory or corrective relief for a whistleblower that have been instituted by the OSC, together with any stay orders sought by the OSC.
- To gain statutory protection, a whistleblower is not obliged to report an allegation directly to the OSC as opposed to making a public disclosure, but more extensive protection exists where the OSC channel is used. Specifically, to gain protection for direct public disclosures, the employee has the onus of proving that he or she "reasonably believes" the substance of the allegation. Where the allegation is made to the OSC, the investigatory procedures of that office are meant to substantiate or disprove the allegation.

It has to be said that hardly any commentator has rated this particular whistleblowing protection scheme to be a

success, with some going so far as to say that it "has disintegrated into an effective weapon against the intended beneficiaries".[25] Instances have in fact been reported in which an early warning disclosure made by a potential whistleblower was then used both by the OSC and by the agency to persecute that person! More generally, until 1986 there were only four instances in which appellants before the Board had prevailed in relying on the whistleblower defence; the OSC had turned down 99 percent of whistleblower cases without attempting any disciplinary or corrective action; and in 1983, 23 percent of those who blew the whistle reported actually suffering reprisal.

Legislative protection of whistleblowers is in no way the only method, or even the most effective method, for combatting government fraud. Other practices or institutions have a demonstrated record of achievement in this respect: the list includes internal auditing, effective policing, public inquiries, parliamentary questions, investigative journalism and, probably the simplest method of all, the time-hallowed "leak".

A study of some early figures under State legislation yields similar statistics.[26] Whistleblowers show an equal preference for resorting to their common law rights, both in the States which have no whistleblowing statutes, as well as in those which offer the statutory alternative. This has lead some writers to conclude that the whistleblowing statutes are no more effective in encouraging whistleblowing or in providing protection for whistleblowers than is the common law.

This experience at both the State and federal level has lead some writers to suggest that it would be better not to have whistleblowing protection statutes. More protection would be gained by developing the constitutional and common law guarantees referred to earlier, or by devising administrative and ethical practices that would allow fraud to be revealed and restrained.

The preponderance of commentators do, however, still affirm their faith in whistleblowing legislation. Even if its achievement is largely symbolic – affirming the conscientious right of individuals to dissociate themselves publicly from fraud and illegality in an organisation – the legislative endeavour is still seen to be a worthwhile one. Perhaps also one can credit the unsuccessful 1978 US Act with sparking the extraordinary attention given to this issue in the last decade that has lead to a general acceptance of the practice of whistleblowing. Another important development in the US which followed the 1978 Act was the adoption by a majority of professional societies of principles espousing whistleblowing within their codes of ethics.

It is perhaps relevant too that most of the blame in the US for the failure of the 1978 Act has been attributed largely to the performance of the individuals who have occupied the Office of Special Counsel (particularly those appointed by President Reagan). Most of the discussion has thus focussed on reform options. Extensive hearings were held by US congressional committees in 1987 with a view to strengthening the legislative scheme. (The outcome of that process was not available at the time of writing this paper.)

Support for the US model is contained also in a recent report of the Ontario Law Reform Commission.[27] The Commission proposed a modified version of the US counterpart. Statutory protection would be available to whistleblowers who raised their concerns with an independent Special Counsel. The Counsel's main function would be to ensure the proper investigation of the allegations (and not, for example, to act essentially as a private solicitor representing the interests of the whistleblower). In addition, the Commission proposed that the investigation file on each complaint which substantiated evidence of government wrongdoing should ordinarily be available for public inspection.

There is a range of other and quite different protective options that should be examined also. For example, worthy of consideration is a proposal made by the English Law Reform Commission in 1981. It recommended that the action for breach of confidence be regulated exclusively by statute, which should require a plaintiff to establish that the public interest involved in upholding the confidentiality of information outweighed any public interest which, on the defendant's evidence, justified the disclosure of that information.[28]

WHISTLEBLOWING IN CONTEXT

Legislative protection of whistleblowers is in no way the only method, or even the most effective method, for combatting government fraud. Other practices or institutions have a demonstrated record of achievement in this respect: the list includes internal auditing, effective policing, public inquiries, parliamentary questions, investigative journalism and, probably the simplest method of all, the time-hallowed "leak".

It is worth noting also another US innovation which relies on voluntary public assistance, the Fraud Hotline.[29] This was established administratively within the General Accounting Office in 1979; it is essentially a method of institutionalising those procedures which exist informally in most other countries for enlisting public assistance in the detection of fraud and illegality. It centres on a nationwide, toll-free Hotline, which receives information from any person concerning fraud, waste, or mismanagement by or within the federal government. After filtering, the allegations are referred by the GAO to the appropriate investigations unit within the relevant federal agency; if no such unit exists, the GAO conducts the investigation. It is ultimately for the GAO to review whether an allegation has been investigated properly, and whether any appropriate law enforcement action has been taken.

The statistical record of the Hotline attests to its success. In the first eight years over 87,000 calls were received, resulting in 13,109 cases warranting further review. Of those, 70 percent were received from anonymous sources, and 26 percent from federal employees. Of those reviewable

allegations, 42 percent concerned the actions of federal employees (for example, work hour abuse, improper use of government property, unlawful behaviour, conflict of interest, bribery or fraud); 19 percent concerned federal contractors or grantee organisations (for example, improper use of government funds, medical fraud, theft, and provision of false information); and 39 percent concerned individuals (for example, welfare fraud or tax cheating). In 19 percent of the investigated cases the allegation was substantiated or preventive action was taken, including 240 cases in which criminal or civil proceedings were instituted. The GAO has made a conservative minimum estimate that millions of dollars in waste and abuse have been averted. Beyond that the GAO feels there have been considerable potential savings by reason of the steps taken to prevent or deter waste in the future.

Hotlines and other innovations need not, however, be treated as an alternative to whistleblowing protection. All the devices have in common the objective of enlisting public assistance in combatting government fraud, but thereafter the objectives diverge. In particular, formal protection of whistleblowers can be justified quite separately by a much broader spectrum of considerations.

There is in the first place the open government imperative. The Ontario Law Reform Commission, in support of its whistleblowing proposals, stated that it could not see how, in a contemporary climate of openness, a government could any longer invoke the principle of confidentiality to cover up serious government wrongdoing. Public awareness of government activity was seen to be an essential means of monitoring that activity and of holding the government accountable for its actions.

Mr Justice Kirby has recently expressed a similar sentiment:

> Obviously, people in positions of trust should normally keep the secrets of that trust. Equally clearly, it cannot be left to individual employees to be the final arbiters of the public interest that would excuse disclosure. Likewise, it cannot be left exclusively to the holders of the secrets. They may be blinded by self-interest, tradition or the covering up of wrongdoing – so that they do not see where the true public interest lies. That is why, in the end, the responsibility of judging whether the "whistleblower" was justified, lies with the courts.[30]

Finally, the ethical dilemma that motivates many whistleblowers cannot be ignored. The genuine whistleblower is a person who believes as a matter of conscience that loyalty to an organisation or institution must be subordinate to loyalty to society or the state itself. Employment in an organisation should not entail as a necessary consequence that a person is compelled by an employer to accept complicity in all activities which that employer has decided to pursue or to conceal. Our society should be civilised enough to protect those who are led by conscience to place pursuit of the public interest ahead of career or personal interests.

ENDNOTES

1. Besides the references given elsewhere in these notes, see also the extensive bibliographies attached to the following references: F Elliston et al, *Whistleblowing: Managing Dissent in the Workplace*, Praeger; J W Graham, "Principled Organizational Dissent: A Theoretical Essay", in L Cummings (ed), *Research in Organizational Behaviour*, 1987, Vol 9, 1; and J P Near and M P Miceli, "Whistleblowers in Organizations: Dissidents or Reformers?", in Cummings, ibid, Vol 8, at 321.
2. For some treatment of the issue, see D Johnson, "Justice for Whistleblowers? The Phillip Arantz Case", 11 *LSB* 45; J McMillan, "Whistleblowing", in P Grabosky (ed), *Government Illegality*, Aust Inst Crimin, 1987. Now see also G E Caiden and J A Truelson, "Whistleblower Protection in the USA" (1988) 67 AJPA 119.
3. Though the Australian Democrats proposed in 1985 that Parliament examine the issue, by the medium of a Select Committee on Public Servants' Rights in Relation to Exposing Breaches of the Law (1985 Senate Hansard 22.5.85, p 2292). For other parliamentary references see Senate Hansard 13.10.83, p 1562 (Senator Primmer), referring to an ACOA submission to the Reid Review of Commonwealth Administration, proposing the adoption of whistleblower protections in Australia; and at the time of writing Mr John Hatton MLA was formally proposing such legislation in NSW in a submission to the NSW Government.
4. Parl Paper No 297/1987.
5. "Whistleblower", *Life*, March 1988, 17.
6. For example, see R Nader et al, *Whistleblowing*, Grossman, Bantam, 1972; W McGowan, "The Whistleblower's Hall of Fame" (1985) *Business and Society Review*, 31.
7. R Nader, "An Anatomy of Whistleblowing", in Nader, ibid, at p 1.
8. See, for example, the discussion by T M Dworkin and J P Near, "Whistleblowing Statutes: Are They Working" (1987) 25 Am Bus L J 241, 243; N M Rongine, "Toward a Coherent Legal Response to the Public Policy Dilemma Posed by Whistleblowing" (1985) 23 Am Bus L J 281, 282.
9. See J W C Turner, *Kenny's Outlines of Criminal Law* (19th ed, 1966), 405. The offence no longer exists in those jurisidictions which have abolished felonies.
10. *Attorney-General v Butterworth* [1963] 1 QB 696.
11. J A Pettifer (ed), *House of Representatives Practice* (1981) at 657.
12. Pettifer, ibid, at 658.
13. For more detail, see Ontario Law Reform Commission, *Political Activity, Public Comment and Disclosure by Crown Employees* (1986) 51-70; and Y Cripps, *The Legal Implications of Disclosure in the Public Interest* (1986) ch 2.
14. Gurry, *Breach of Confidence* (1984) 334.
15. *Initial Services Ltd v Putterill* [1968] 1 QB 396.
16. *A-G (UK v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86, 170.
17. *Commonwealth v John Fairfax and Sons Ltd* (1981) 32 ALR 485, 492-3.
18. *A v Hayden (No 2)* (1984) 59 ALJR 6, at 7.
19. Public Service Board, *Guidelines on Official Conduct of Commonwealth Public Servants*, AGPS, 1987, 4, 5.
20. Published as Appendix A to *Guidelines*, ibid.
21. Discussed in Y Cripps, "Protection from Adverse Treatment by Employers: A Review of the Position of Employees who Disclose Information in the Belief that Disclosure is in the Public Interest" (1985) 101 LQR 506.
22. For example, *A v Hayden (No 2)* (1984) 59 ALJR 6, at 9, and *Schering Chemicals Ltd v Falkman Ltd* [1981] 2 WLR 848, at 869.
23. For more detail, see for example, S M Kohn and M D Kohn, "An Overview of Federal and State Whistleblower Protections" (1986) 4 Antioch LJ 99.
24. 5 USC No 2303 (b)(8), see, for example, R G Vaughan, "Statutory Protection of Whistleblowers in the Federal Executive Branch" (1982) U of Ill L Rev 615, and T M Devine and D G Aplin, "Abuse of Authority: the Office of the Special Counsel and Whistleblower Protection" (1986) 4 Antioch L J 5.
25. Devine, ibid, at 6.
26. See Dworkin, supra note 8.
27. Ontario Law Reform Commission, supra note 13.
28. Discussed in Cripps, supra note 13, at Ch 14.
29. US General Accounting Office, *8-Year GAO Fraud Hotline Summary* (1987).
30. Book review (1988) 62 ALJ 397.

Citizen Co-Production in Fraud Control

*P N Grabosky**

That we are living in an age of fiscal austerity is hardly news to any public servant today. But within this climate of belt-tightening, we are confronted with the growing awareness that revenue loss due to fraud, waste and inefficiency has reached proportions deemed intolerable by governments and oppositions alike. The next few pages will discuss how public administrators can enlist the support of the general public to combat fraud against the government.

revenue loss due to fraud, waste and inefficiency has reached proportions deemed intolerable by governments and oppositions alike.

The concept which I would like to introduce is that of citizen co-production. To complement the various fraud control initiatives that are mounted within government agencies, members of the general public may themselves contribute to the battle against revenue loss by producing fraud control services. These services, moreover, are what is termed "off-budget" – that is, they entail no cost to the public treasury. I shall illustrate my argument with an example which is hardly novel. Indeed, it dates back 125 years, with roots half a millenium older than that.

But first, let me cite some contemporary examples of citizen co-production in Australia from other domains of law enforcement. The first, and perhaps the most familiar, is the ubiquitous Neighbourhood Watch. When it is operating successfully, the eyes and ears of neighbourhood watch participants provide surveillance services that would cost thousands of dollars if delivered by police or private security agents.

Another example can be drawn from occupational health and safety regulation in Victoria. There, the institution of elected worker safety representatives complements the government inspectorate (Braithwaite, Grabosky and Fisse, 1986). Safety representatives may demand access to inspect any part of the workplace or company records relating to health and safety. They are empowered to issue provisional improvement notices when they discover a workplace hazard. These notices have the force of law, pending abatement of the hazard in question or authoritative determination by a government inspector. Breach of such a notice renders one liable to prosecution. Regulatory vigilance in the Victorian workplace is thus enhanced far beyond the degree which could otherwise be provided by a government inspectorate.

Other examples of public involvement in the regulatory process include the use of volunteers to monitor beach erosion and to submit regular reports to the Queensland Beach Protection Authority; the use of voluntary wardens in South Australia to watch over historic shipwrecks, and the use by the New South Wales Department of Consumer Affairs of a network of volunteers from the consumer movement to discover hazardous products on the market (Grabosky and Braithwaite, 1986).

In our research on regulatory enforcement in Australia, John Braithwaite and I found a few examples of regulatory agencies which encouraged citizens to protect their interests through civil litigation. One agency, the Victorian Environment Protection Authority, was actually prepared to make funds available for the legal assistance to private plaintiffs in environmental litigation.

But what of citizen co-production in combating fraud against the government? For this, let us go back 125 years to a far away place.

During the Civil War in the United States, the federal bureaucracy bore no resemblance to its counterpart today. There was no Federal Bureau of Investigation, and little in the way of fraud control apparatus. At the same time, support for the war effort was not uniformly enthusiastic. Whilst many fought and died bravely to save the Union, others were able to avoid conscription by purchasing the services of a stand-in. Others still rioted. Purveyors of provisions and equipment to the Grand Army of the Republic were also inclined to cut corners from time to time. Cases purporting to contain gunpowder which were opened on the battlefield were found to contain sawdust. Useless muskets were sold to the government at eight times their value. In 1861 one thousand mules were purchased by the Army at $119 each. Some were diseased, others were blind, almost all were useless.

In the face of such abuses, and mindful of the lack of investigative resources within the government, the United States Congress enacted the *False Claims Act* 1863. The legislation was noteworthy in two respects. First, it was a civil and not a criminal statute, intended to be remedial rather than punitive. It provided for double damages, that is, twice the amount falsely claimed, plus a civil fine of $2000. The standard of proof required was civil, on the balance of probabilities, rather than the more formidable criminal standard.

Second, the statute provided for private actions, actually authorising citizens to sue on behalf of the government, and to share in any recovery of defrauded funds. These so called *qui tam* provisions (Latin for "who as well", that is, who

* Peter N Grabosky, PhD, is Senior Criminologist, Australian Institute of Criminology. Text of an address to 1988 RAIPA (ACT Division) Autumn Seminar on "Ethics, Fraud and Public Administration", University House, The Australian National University, Canberra, 2 May 1988.

CB PA *No 56, September 1988, 124-127.*

sues for the state as well as for him or herself (see Fisse and Braithwaite, 1983, 251-254)), allowed a succesful citizen plaintiff to recover up to 50 percent of moneys eventually recovered by government. Lest it appear that I am suggesting that *qui tam* suits are an American invention, I readily concede their roots in the law of fourteenth century England.

For reasons which are not entirely clear, the *False Claims Act* fell into disuse for the best part of a century. Then, during the Second World War, a case brought under the Act resulted in decision of the United States Supreme Court (US ex rel Marcus v Hess 317 US 537 (1943)) which invited widespread abuse of the statute. In that case, the Court held that a person could sue under the *False Claims Act* on behalf of the United States Government even though the action was based solely on information acquired from the government itself. The decision thus invited citizens to ride piggyback on any government fraud investigation. The United States Congress promptly amended the Act to prevent any suits based on information the government had when the action was brought, and limited the damages available to a private plaintiff in cases joined by the government to 10 percent of monies recovered – with no guarantee of any recovery. Thus emasculated, the *False Claims Act* lay all but forgotten until the Reagan administration.

Among the events of the 1980s which precipitated a revival of the *False Claims Act* were the egregious abuses by US Defense contractors. Tales of $300 toilet seats, $5,000 coffee urns, and kennel fees for the family dog of one executive being added to the account for a nuclear submarine contract, engendered media ridicule and not inconsiderable public indignation. The problem was by no means limited to defense procurement (Eagleton and Shapiro, 1983). Given the Reagan administration's pontifications about the necessity for fiscal restraint, the Congress of the United States decided to revitalise the *False Claims Act.*

As amended in 1986, the legislation (PL 99-562) incorporates the following:

1. allows a private citizen who discovers fraud against the government to sue for damages;

2. provides for an award of triple the damages sustained by the government;

3. provides for a maximum civil fine of $10,000;

4. guarantees the private citizen who initiates the suit, a proportion of the damage award – between 15 percent and 25 percent if the government enters the case; if the government does not enter the suit, the successful private plaintiff can receive between 25 percent and 30 percent of damages. (Awards are at the discretion of the presiding judge, based on his or her assessment of the citizen's contribution to the litigation);

5. requires the defendant to pay the legal expenses of a successful private plaintiff;

6. protects private plaintiffs from harassment, dismissal, demotion or suspension by their employer. These whistleblower protection provisions are tremendously important, as they help overcome what had been a significant impediment to the disclosure of fraudulent practices – that is, victimisation of the complainant. They apply to "any employee who is discharged, demoted, suspended, threatened, harassed, or in any other matter discriminated against in the terms and conditions of employment by his or her employer because of lawful acts done by the employee on behalf of the employee or others in furtherance of an action under this section, including investigation". Remedies available to a victimised employee include reinstatement with the same seniority the employee would have had – but for the discrimination; two times the amount of back pay; interest on the back pay; compensation for any damages sustained as the result of discrimination, including litigation costs and attorney's fees. It also provides for the possibility of punitive damages.

The most vociferous opponents of the new False Claims legislation were, not surprisingly, the nation's defense contractors. Among the reservations voiced by critics of the *False Claims Act* were:

1. that it is an invitation to frivolous or vexatious litigation, false allegations, politically motivated action, or retaliatory behaviour by disgruntled employees;

2. that it appeals to the baser motives of the public by inviting "bounty hunting";

3. that it invites parastical behaviours such as joining a suit that has already been or would otherwise be brought by the government;

4. that it has the potential of prejudicing a concurrent criminal investigation, or otherwise interfering with steps taken by the government to recover the ill-gotten gains.

Closer inspection, however, reveals these objections to be ill-founded. There are ample safeguards in United States law to protect against frivolous or vexatious litigation. Those lawyers acting on a contingent fee basic (if they lose, they get nothing; if they win, they get a percentage of the damages – usually one third) would be disinclined to waste their time on a lost cause. US Federal Courts have ample powers to dismiss frivolous complaints. A vexatious plaintiff who has both the inclination and the means to bankroll a frivolous lawsuit nonetheless, runs the risk of being thrown out of court (figuratively speaking) by a federal judge. Legal practitioners are also vulnerable to negative sanctions for abuse of process.

The "bounty hunting" objection may be countered by the argument that citizens who provide valuable, indeed, often crucial investigative assistance to the government are entitled to modest compensation for their efforts. Many will expend considerable time and energy in developing their case. For some, the experience will be emotionally costly if it entails a conflict of loyalties to employer and to one's nation. Moreover, the citizen's reward is but a fraction of the total damages. At least 70 percent of all monies eventually recovered will go to the government. The risk of parasitical litigation is neutralised by the ability of the federal courts to dismiss a *qui tam* complaint if the citizen

plaintiff's allegations relate to matters which were previously the subject of hearings, investigations, or media coverage.

The risk of prejudicing parallel criminal proceedings is controlled by the requirement that the citizen plaintiff's action be filed initially under seal in court, and only served on the Attorney General in Washington. It remains under seal for at least 60 days (subject to extension for good cause) before being served on the defendant. The purpose of this provision is to permit the government to conduct its own investigation without indicating to the defendant that such an investigation is underway.

Cynics might suggest that agencies of government are not always lightning fast in their responsiveness to problems, often preferring to deny them, or minimise them. Bureaucrats prefer to control their own case loads, and dislike pressure being brought to bear against them. In general, bureaucratic inertia is more noticeable when it comes to pursuing powerful interests. Whether this criticism applies to the fraud control efforts of Australian federal bureaucracies is a question best answered by persons wiser than I.

In the event that the government chooses to proceed with criminal charges, it may request that civil proceedings be stayed, so as not to prejudice the criminal case.

In the event that the federal government joins the action, the risk of disruptive, repetitious or harassing behaviour on the part of the citizen plaintiff is minimised by the power of the court to make specific findings to that effect, and thereby limit the private plaintiff's participation in the suit.

Is it not interesting that a concept devised over 125 years ago would be consistent with contemporary values of public administration?

The government simply does not have the resources necessary to police fraud thoroughly. As an alternative to expanding an already massive enforcement apparatus, the *False Claims Act* provides market incentives to encourage private individuals to produce services that would otherwise be delivered at public expense. The *False Claims Act* does not add one person to the bureaucracy, nor does it impose one extra dollar of cost upon the nation's taxpayers. It is entirely consistent with the principles of privatisation and deregulation which governments throughout Australia have embraced with such enthusiasm.

Cynics might suggest that agencies of government are not always lightning fast in their responsiveness to problems, often preferring to deny them, or minimise them. Bureaucrats prefer to control their own case loads, and dislike pressure being brought to bear against them. In general, bureaucratic inertia is more noticeable when it comes to pursuing powerful interests. Whether this criticism applies to the fraud control efforts of Australian federal bureaucracies is a question best answered by persons wiser than I. But consider that under the *False Claims Act*, once a private citizen mobilises the law, there is a stimulus to government action. The government is no longer able to ignore the allegations for political or administrative reasons. Excuses such as lack of resources or low priority carry much less weight.

But False Claims litigation should not be looked upon as a challenge to the authority of government. Rather, it is the basis for a partnership between the citizen and the state. It encourages people on the front lines to come forward with information that might not otherwise be available to investigative authorities.

By the end of 1987 some 10 cases brought under the US *False Claims Act* had been publicly disclosed. Targets of the actions were defense contractors, and medical practitioners accused of defrauding the medicare system.

At least three false claims suits were pending against Northrop Corporation, a large defense contractor. In one of these, two former employees filed suit in October 1986 claiming that the company knowingly used defective parts in producing MX missile guidance equipment. The US Justice Department declined to join the plaintiffs' case, and filed a motion for dismissal, arguing that the employees' case was substantially based on information previously known by the government. In an unrelated action brought in August 1987, the government had sued Northrop for allegedly falsifying test data. A federal judge dismissed the employees' suit early in April.

The new era of false claims litigation has begun. Only time will tell how well this time-honoured tool of fraud control works in practice. Whether Australian governments are sufficiently troubled by fraud to consider adopting it remains to be seen.

Lest there be any uncertainty about what I am arguing here, allow me most emphatically to declare that I am *not* suggesting that false claims litigation is *the* solution to the problem of fraud against the government. Even if it were to be seen to be functioning well, false claims litigation is not a panacea or magic bullet. To place all of one's fraud control eggs in the basket of false claims litigation would be ill-conceived public policy.

The ideal fraud control policy would consist of multiple overlapping countermeasures. These would include both rigorous internal controls, backed up by vigilant institutions of external oversight (Grabosky, forthcoming).

The need for internal mechanisms of control should be obvious. Whether a government agency is in the business of collecting revenue, dispensing benefits, or purchasing goods and services, management information systems should permit the systematic monitoring of its transactions.

This in fact is mandated by law in the United States. There, the *Federal Managers Financial Integrity Act* requires agency heads personally to certify that their agency's

internal control systems are sound; if not, they are required to explain the corrective measures to be taken. The degree to which an organisation takes fraud control seriously may be reflected in the size and prestige of its internal audit division. If I might propose a simple index of the extent to which an agency is committed to fraud control, consider the ratio of the size of an agency's internal audit division to the size of its public relations apparatus.

Fraud control also requires leadership. Ralph Nader once said that corporations, like fish, rot from the head down. The same could be said of public sector agencies. Public sector managers, as do their private sector counterparts (Clinard 1983), create a moral climate which influences the values and the behaviour of those who work for them. The executive with a half-hearted commitment to fraud control is unlikely to inspire a different orientation in his or her workforce.

Internal controls and exemplary management practices must also be reinforced by institutions of external oversight. In addition to such formal agencies as audit offices and parliamentary public accounts committees, external oversight can be provided by a vigilant citizenry. One opportunity for citizen co-production of fraud control services was noted above. In addition to false claims litigation, the risk of exposure by a vigorous and critical press can induce many senior managers to reinforce their control procedures. Implicit in this desideratum are the following essentials: a diverse media; freedom of information; and whistleblower protection. But these must be the subject of future papers, and indeed, of future seminars. My purpose in this essay has been to introduce the concept of citizen co-production and to acquaint the reader with the basics of false claims litigation. More grist for the fraud control mill.

REFERENCES

Braithwaite, John, Grabosky, Peter and Fisse, Brent, *Occupational Health and Safety Enforcement Guidelines: A Report to the Victorian Department of Labour*, Melbourne, Department of Labour, 1986.

Clinard, Marshall, *Corporate Ethics and Crime*, Beverly Hills, Sage Publications, 1983.

Eagleton, Thomas and Shapiro, Ira (1983), "Federal Fraud Waste and Abuse: Causes and Responses", *Government Accountants Journal*, (Summer), 1-8.

Fisse, Brent and Braithwaite, John (1983), *The Impact of Publicity on Corporate Offenders*, Albany, State University of New York Press.

Grabosky, Peter and Braithwaite, John (1986), *Of Manners Gentle: Enforcement Strategies of Australian Business Regulatory Agencies*, Melbourne, Oxford University Press.

Grabosky, Peter, *Wayward Governance: Illegality and its Control in the Public Sector* (forthcoming).

Interview with John R Phillips, Co-director of the Center for Law in the Public Interest, Los Angeles, California, *Corporate Crime Reporter*, November 9, 1987, 5-12.

United States Congress, House of Representatives, Committee on the Judiciary, Subcommittee on Administrative Law and Governmental Relations, *False Claims Act Amendments, Hearings*, US Government Printing Office, Washington, 1986.

What do you want from a computer company, a hardware vendor or a partner?

If all you were looking for in a computer system was the hardware, it would be hard to go past a company like IBM.

Simply because the IBM range of products is so varied and technologically advanced.

In the past year alone, IBM has introduced more than 700 new products including enhancements to the largest and most powerful 3090 processors, a new mid-range family, the 9370, and more recently, the Personal System/2.

But this is really only half the argument for choosing IBM.

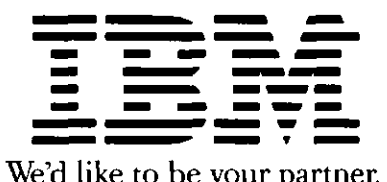
The other half is intangible and something that's difficult to put a price on.

At IBM, we consider the relationship between our customers and ourselves as being every bit as important as the hardware we sell.

Thus our goal is to work together to achieve a common objective, the success of our customer's organisations. To the point where the relationship becomes a partnership.

This is achieved by following three basic beliefs. Respect for the individual, excellence in everything we do, and providing the best customer service.

If you're in the market for a computer system, we strongly suggest you look to the company that's going to provide you with a lot more than just a system.



We'd like to be your partner.

Magnus Nankervis & Curl/IBM/6463   IBM Australia Ltd (Incorporated in NSW)