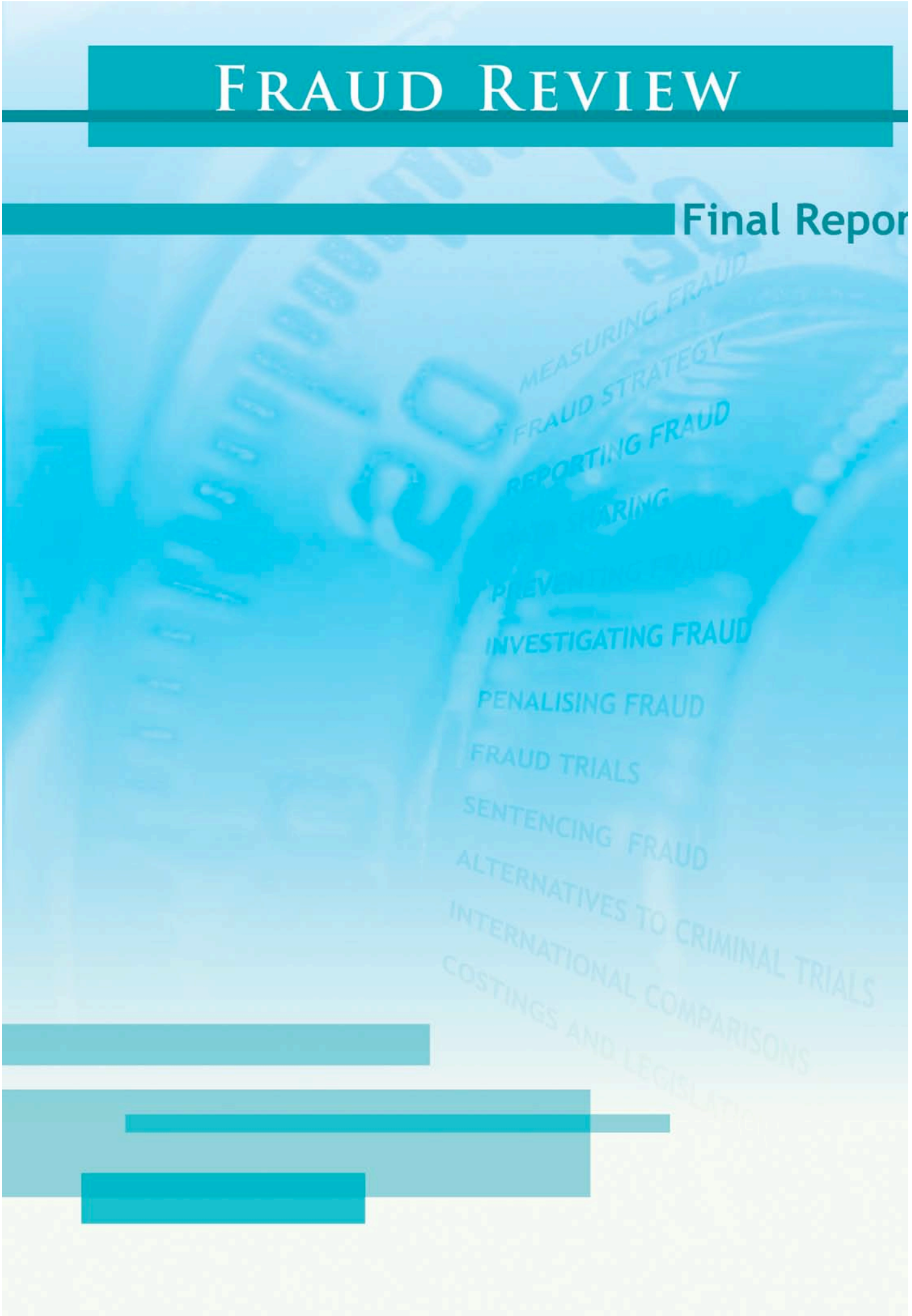
Fraud Review

Final Repor



CONTENTS

		Page
	FOREWORD BY THE ATTORNEY GENERAL	3
	EXECUTIVE SUMMARY	4
CHAPTER 1	INTRODUCTION AND BACKGROUND ……	17
CHAPTER 2	MEASURING FRAUD ……	21
CHAPTER 3	FRAUD STRATEGY ……	41
CHAPTER 4	REPORTING FRAUD ……..	61
CHAPTER 5	DATA SHARING ……..	93
CHAPTER 6	PREVENTING FRAUD ……	118
CHAPTER 7	INVESTIGATING FRAUD ……..	130
CHAPTER 8	PENALISING FRAUD ……..	159
CHAPTER 9	FRAUD TRIALS ……	200
CHAPTER 10	SENTENCING FRAUD ……	226
CHAPTER 11	PLEA BARGAINING…….	252
CHAPTER 12	INTERNATIONAL COMPARISONS …….	275
CHAPTER 13	COSTINGS AND LEGISLATION ……	294
CHAPTER 14	LIST OF RECOMMENDATIONS ……	312
	QUESTIONS FOR CONSULTATION AND HOW TO RESPOND……..	324
	ANNEXES ……	327
	BIBLIOGRAPHY ……	370
	ENDNOTES …….	374

FOREWORD BY THE ATTORNEY GENERAL

In our manifesto in 2005 the government pledged to overhaul laws on fraud and the way that fraud trials are conducted to update them for the 21st century and to make them quicker and more effective.

Fraud is not a victimless crime. Work by the Home Office suggests that fraud may be second only to Class A drug trafficking as a source of harm from crime; and there is evidence that fraud funds terrorism, drugs and people trafficking. This government is pursuing a co-ordinated approach to tackling fraud. We have introduced the Fraud Bill which is currently being considered by Parliament and which will for the first time introduce an offence of fraud. We have pledged to introduce a standalone Bill as soon as parliamentary time allows to allow for non-jury trials in a limited range of serious and complex fraud cases. And we also commissioned this review of fraud which has been reporting to me and the Chief Secretary.

The report we are publishing today is the culmination of nine months hard work by a multi-disciplinary team of officials. I am grateful to those departments and organisations who seconded people to work on this important subject.

An interim report was published in March. The final report has built on that work and it makes a number of wide ranging recommendations which we wish to open up to wider consultation before taking final decisions.

The review is clear that much fraud could be avoided if consumers, businesses, and public sector bodies took elementary precautions and, in appropriate circumstances, exercised sensible scepticism about offers that were obviously too good to be true. Prevention must be the first step we take. But, however strong preventative measures are, they will be insufficient to deal with the major problems created by fraud. The Fraud Review has therefore looked at, and made recommendations on how we measure fraud, how we record the incidence of fraud, how we use that information holistically, how we investigate fraud, and how fraudulent behaviour might appropriately be prosecuted or otherwise dealt with and punished.

Some of the recommendations in the report are challenging. But only by taking a challenging approach to fraud can we hope to provide an effective response to tackle multi-billion pound crime. I hope that a wide range of people will respond to this consultation; and would wish all the recommendations to be considered on their merits and with an open mind.

The consultation period will run until the end of October.

LORD GOLDSMITH

EXECUTIVE SUMMARY

1. We are all victims of fraud. We pay higher prices in shops, higher interest rates on our mortgages, and higher premiums on our insurance policies because of fraud. Tax and benefit fraud means higher taxes. Fraud victims sometimes suffer devastating losses of pensions and life savings, ruining their lives, and honest businesses can be bankrupted by fraudsters.

2. Yet fraud should be one of the easier crimes to prevent. Fraudsters mostly extract money by exploiting carelessness, ignorance or gullibility. Elementary caution and healthy scepticism about offers that look too good to be true would prevent most people becoming victims of fraud. Business and the public sector can protect themselves against fraud by putting in proper systems and controls, but they must make sure that they are implemented and not over ridden. These precautions are not going to stop all fraud; fraudsters will always manage to deceive some people and businesses. But following them should stop most fraud and make tackling the remainder more manageable.

The Fraud Review

3. The Fraud Review was established to recommend ways of reducing fraud and the harm it does to the economy and society. Previous reviews have looked at specific parts of the fraud problem (e.g. the Roskill Commission on fraud trials) but this is the first look at the totality of the problem. Although the details of fiscal and benefit fraud were outside the terms of reference, many of the recommendations are as relevant to these frauds as to fraud against business and the consumer.

The Basic Questions

4. The Fraud Review was asked to consider three questions:

   a) What is the scale of the problem?

b) What is the appropriate role of Government in dealing with fraud?
c) How could resources be spent to maximise value for money across the system?

Scale of the Problem?

5. We cannot answer this question at the moment. There are estimates of some types of fraud (e.g. benefit fraud, credit card fraud, and insurance fraud) where victim organizations measure it. For example, fraud adds around 5% to the cost of the average insurance premium.[1] But most measures of fraud have not been carried out according to a robust methodology, and measure different things, so adding them up to produce an overall total is misleading. Furthermore, many types of fraud, notably against individuals and small businesses, are not recorded and so not measured. In some cases the victim is not even aware that it is going on; other times fraud is classified as "shrinkage" or "bad debt".

6. The Review's first recommendation therefore, is that fraud should be measured on a consistent basis across the economy. A separate study into the "Nature, Extent and Economic Impact of Fraud" commissioned by the Association of Chief Police Officers, Economic Crime Portfolio (ACPO-ECP) is underway and will identify where gaps in measurement occur. The Fraud Report makes recommendations now as to how such work should be carried out in the future. Measurement is fundamental; without better information about the scale and nature of fraud it will be impossible to develop a sensible national strategy for dealing with fraud.

Appropriate Role for Government?

7. The Government has two key roles:

a) Protect public money from fraudsters. That means direct action to deal with fiscal, benefit and procurement fraud where the target is a public

body responsible for taxpayer's money, and making sure adequate systems and controls are in place to prevent internal fraud.

b) Protect consumers and businesses against fraud. That means using the mechanisms of the State such as regulation, law enforcement, criminal justice etc, to prevent, deter, detect, investigate, and punish fraud.

National Fraud Strategy

8. The majority of people consulted during the review felt that the government must formulate a national strategy for dealing with fraud. The strategy should take a 'holistic' approach, focusing efforts and resources where they are likely to be most effective rather than most attention grabbing, and focussing on the causes of fraud as well as dealing with the effects. The strategy will not replace existing strategies but rather to help coordinate ongoing efforts.

9. Such an approach is likely to emphasise upstream action to prevent and deter fraud, such as educating consumers and businesses on how to avoid becoming victims. Despite these efforts fraud will still happen and the strategy will have to set priorities for downstream investigations and effective ways of punishing fraudsters and obtaining justice for victims.

National Fraud Strategic Authority

10. The second key recommendation is that the government should establish a National Fraud Strategic Authority to devise a national strategy for dealing with fraud and ensure that it is implemented. It would not take over any policy or operational responsibilities from existing organizations. It would ensure that their work was coordinated, duplication was eliminated, and gaps addressed. It would also have a role in settling policy conflicts, serve as a centre of expertise to organizations in both private and public sectors that required assistance, and actively promote an anti-fraud culture

throughout society. It would also house the unit established to measure the scale of fraud. It would be staffed by a multi-disciplinary team of experts from both the public and private sectors.

11. The public/private partnership approach is crucial and several other recommendations envisage joint funding and joint staffing of new or existing activities. Much of the existing effort devoted to countering fraud, especially fraud investigations, and much of the expertise in countering it lies in the private sector. It is crucial that this is combined with public sector efforts in a coordinated attack on fraud. There are already successful regional initiatives, such as the North East Fraud Forum that brings together public and private agencies to cooperate to alert consumers and businesses to the fraud risk and help them deal with it. A coordinated national approach is now needed.

Value for Money

12. Maximising value for money will be the job of the National Fraud Strategic Authority and a prerequisite will be proper measurement of the problem. But there are certain recommendations that can be made now that will improve value for money of existing resources.

Reporting Fraud

13. Fraud is massively underreported. Fraud is not a national police priority, so even when reports are taken, little is done with them. Many victims therefore don't report at all. So, the official crime statistics display just the tip of the iceberg, and developing a strategic law enforcement response is impossible because the information to target investigations does not exist.

14. The Fraud Review proposes the establishment of a National Fraud Reporting Centre for businesses and individuals to report fraud. It would receive those reports, analyse them, identify patterns and trends, and provide police and other investigative agencies with information to target

investigations. Every report would help build up a picture about fraud and improve the effectiveness of the overall anti-fraud response. Not all reports may be individually investigated as that would be way beyond the capacity of any police force or law enforcement agency. But the information and intelligence obtained from fraud reports will be used to warn consumers and businesses about fraud risks and contribute towards setting the national anti-fraud strategy and our understanding of how big a threat fraud is to the UK.

15. The NFRC Centre should be a public/private partnership, jointly staffed and financed. This is not just elementary fairness, because the benefits will be shared, or to reduce the burden on the taxpayer It is part of a genuine attempt to tackle fraud on a partnership basis with all participants having a say in the way priorities are set and money is spent. The best guarantee that private sector participants can have of this is to control part of the funding.

Preventing Fraud

16. An ounce of prevention is worth a pound of cure. A sad feature of many frauds is how easily so many of them could have been avoided if the victims had exercised sensible caution about propositions which in retrospect, were obviously too good to be true. Much excellent work is already being done by some organizations to alert businesses and consumers to fraud risks and to stop them falling for scams. These alerts need to be more widely known and much more use could be made of information already held by regulators, law enforcement agencies and businesses to prevent future frauds. An early task for the National Fraud Strategic Authority should be putting together a working group of organizations to mount a public awareness and information campaign. Small investments could pay big dividends.

17. Many organizations and businesses invest heavily in anti-fraud controls and systems. But many do not, probably because of a lack of awareness of

their fraud exposure. For example, a survey of government bodies carried out for this Review by the Treasury revealed that two thirds had no budget for anti-fraud work. All bodies should carry out a risk assessment of their exposure to fraud and consider making appropriate investment to combat it. And the National Fraud Strategic Authority should disseminate examples of best practice.

Investigating Fraud

18. The Interim Report described the rapid and continuing decline in police fraud squad resources outside the City of London. This is not surprising as fraud is not mentioned in the National Policing Plan, as a priority for forces. Yet ample evidence exists of the damage fraud does to individuals, some of whom are vulnerable, businesses, and the national economy. While no comprehensive measure of the size of fraud exists, work on the harm fraud causes to society committed by organized crime suggests that it may be second only to Class A drug trafficking and roughly equal to the harm from people smuggling and people trafficking combined. Reflecting the extent of organized crime involvement in fraud, it has been made the third priority of the Serious and Organized Crime Agency (SOCA) which plans to devote around 10 percent of its resources to tackling fraud. But this addresses only part of the problem. A complementary policing resource must be maintained for frauds which, although not perpetrated by organized criminal networks, nevertheless cause serious damage to the economy and society.

19. The case for major additional investment in fraud investigations will depend on measuring it better and reassessing its place amongst overall policing priorities. Pending the outcome of this work, there are ways of getting better value for money from existing resources. The Fraud Review recommends:

a) That the Home Secretary should consider making combating fraud a policing priority within the National Community Safety (Policing) Plan

and law enforcement agencies encouraged to develop plans which include local performance targets for fraud.

b) Police forces should consider emulating the regional fraud grouping established in the South East; designating a lead force for their area which could provide anti fraud resources and expertise along the lines developed by the City of London Police.

c) Police fraud squad resources should, so far as possible, be ring fenced to stop the current practice in many forces of diverting them into other work as soon as the force has a pressure somewhere else.

d) Additional to fraud squad resources, each police force should develop and maintain appropriate capacity and capability to deal with Level 1 frauds that meet the agreed acceptance criteria and occur at a local Borough Command Unit level.

e) If appropriate in the light of further work on police reform the establishment of a number of Regional Support Centres comprising specialist resources like surveillance and technical services should be considered to provide Fraud Squads with such facilities when needed to support an investigation. At present, fraud squads are regarded as a low priority call on these resources.

f) A National Lead Force should be established based upon the City of London Police Fraud Squad. It would house the National Fraud Reporting Centre and its intelligence and analytical capability. It would also be a centre of excellence for other fraud squads, disseminating best practice, giving advice on complex enquiries in other regions, and assisting with or even directing the most complex of such investigations. The location of this lead force will be dependent upon police restructuring in London.

g) Revised arrangements should be the subject of a "thematic" inspection by Her Majesty's Inspectorate of Justice, Community Safety and Custody within two years of their establishment.

20. The establishment of Regional Support Centres and some of the functions of the National Lead Force would require some additional funding and the Report has assessed the potential costs. The report also sets out a costing for doubling the size of police fraud squads outside London if it was decided to increase the resourcing of fraud investigations now.

21. While there is inevitably a lot of focus on police fraud investigations most cases of fraud are investigated by civilians either employed in or by organizations which have been the victims of fraud or in bodies such as local authorities. Some organizations maintain their own in house capability while others employ specialists such as forensic accountants and private enquiry agencies. There is scope for more public/private partnership, including two way secondments, collaboration on investigations, and the establishment of joint units to investigate certain types of fraud. The Fraud Review considered whether there was scope to "civilianize" fraud investigations still further, given that most of the elements of a fraud enquiry require specialist skills which are not unique to the police. The extreme would be to have police fraud squads staffed entirely by civilians. This is not recommended as there are certain things that only the police can do (e.g. arrest people) and some of the people involved in fraud should only be tackled by investigators with the full range of powers and experience. However, there is certainly scope for more civilian involvement and the report makes some detailed recommendations to increase collaboration.

<u>Fraud Trials</u>

22. The Fraud Review did not revisit the issue of non-jury trials, where the government has already announced its intentions. It did consider the work already underway to improve the effectiveness of fraud trials under current

arrangements. The Fraud Review noted the strong criticism that some commentators have made of the way the disclosure provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) have been interpreted in some instances leading to considerable increases in the cost and length of heavy fraud trials. The Fraud Advisory Panel has recently commented that that the CPIA was unfit for purpose in handling such trials and called for changes.

23. The Attorney-General has only recently issued guidance on how the CPIA should be applied and this, and other recent guidance from the judiciary must be given a chance to work. However, there are some additional ideas we recommend for streamlining disclosure procedures and presenting evidence more effectively, suggested to us by Court practitioners. In particular, we recommend that successful case management in complex cases can only be achieved if both the prosecution and the defence play a full part in identifying issues and facts in dispute. A further move towards formal "pleadings" in fraud and other costly and complex criminal cases should be made. In addition, the continued suitability of the CPIA for complex fraud trials should be reviewed again in 2008.

Fraud Sentences

24. The average sentence after conviction in a case brought by the Serious Fraud Office (where by definition the fraud involves at least £1 million) is three years imprisonment. This is well below the sentence that would be given for another acquisitive crime of a similar value. This is the case for all levels of fraud. Low sentences are insulting to victims and send out a message that stealing money through deception is somehow more acceptable than stealing in other ways. Part of the problem is that the maximum sentence for fraud is only 10 years, while the maximum sentence for money laundering, a crime with some of the same characteristics, is 14 years. The Review recommends the maximum sentence for both should be aligned at 14 years.

25. There are currently no specific guidelines to the courts about fraud sentences. The Fraud Review further recommends that when the Fraud Bill becomes law, the Sentencing Guidelines Council should be invited to issue guidance on the appropriate penalty for fraud.

Wider Sentencing Powers

26. The Fraud Review conducted a small survey of fraud victims to gauge what victims' priorities were when it came to dealing with fraudsters. While they wanted the fraudster punished, a higher priority was given to protecting the public against future frauds and getting victims' money back. There are mechanisms for achieving those results but they are dotted around the regulatory, disciplinary and criminal justice systems in a rather haphazard way, which means they do not always get applied when they should or they are not applied quickly enough.

27. Lord Justice Auld made recommendations in 2001 for dealing with some of these issues. The Fraud Review makes recommendations for extending the sentencing options available to the court, and in appropriate cases consolidating various types of proceedings around a single hearing so that all aspects of a fraud may be dealt with in one place.

28. The Fraud Review also recommends that serious fraud cases and associated proceedings should be dealt with in a more co-ordinated way, by establishing a Financial Court jurisdiction. This would not be a new institution as such, requiring new judges or new buildings. Instead it would involve extending the jurisdiction of the High Court to create a "virtual" court sitting in existing courtrooms and using a specialist cadre of judges who have experience of and familiarity with financial issues and well developed case management skills. They would be drawn not just as now from Crown Court judges (with a High Court judge taking an occasional fraud case), but also from amongst High Court judges: from the Commercial Court, its Mercantile judges and possibly even from the Chancery Division. These judges have experience of commercial and financial cases and can bring to

bear the rather brisker approach of the civil courts. They would not have an unremitting diet of fraud cases.

29. This model is closely based on the existing constitution of the Queen's Bench Division of the High Court, which encompasses the Commercial Court, the Technology and Construction Court and the Admiralty Court. Consideration will need to be given to the appointment of a 'Judge in Charge' (similar to the designated civil judges) or to other co-ordinating mechanisms for managing the cases assigned to the Financial Court.

Plea Bargains

30. The Fraud Review's final recommendation is that in view of the sheer scale of some fraud investigations and trials, more alternatives to full scale criminal trials should be available. A plea bargain involves an agreement between prosecution and defence, involving both a guilty admission to a particular charge(s) and a sentence recommendation to the court. Ninety five percent of criminal cases in the USA, including fraud cases, are settled this way. They avoid the cost and time of a full scale trial and can involve penalties that involve restitution to victims and protection of the public as well as punishment of the fraudster.

31. This is not fraudsters "buying their way" out of justice. In plea bargains, the fraudster must admit guilt, accept a criminal record, and sometimes serve time in jail. Often the plea bargain will result in better and faster victim restitution than awaiting the outcome of a criminal trial. All plea bargains would be reviewed by a judge who could refuse to abide by it if it was considered to be inappropriate. But the interests of justice and, in particular, the needs of the victim can often be better met by a speedy disposition of a case in which the requirements of public protection and victim restitution are met rather than by costly and lengthy proceedings with a doubtful outcome for everyone. We therefore recommend that a plea bargaining framework should be devised for the guidance of prosecutors and defence representatives.

32. In considering other options we noted the provisions in the Criminal Justice Act 2003 for conditional cautions. They do not involve a criminal conviction but the perpetrator has to admit guilt, accept a caution and make restitution. Something similar may be suitable for small scale frauds where the proceeds are small, or for cases where the defendant is a company or organization rather than an individual and where the penalty will necessarily be a financial one in any event as there is no natural person to punish. This would clearly not be appropriate for serious fraudsters.

Costs and Benefits

33. Overall, the proposals should save considerable amounts of public and private money. Certain recommendations, notably the National Fraud Strategic Authority, National Fraud Reporting Centre and the National Lead Force will cost money. The costs are estimated at between £13 and £27 million a year, depending upon where Regional Support Centres are established to provide technical and specialist support to police fraud squads and how many. (Doubling the size of fraud squads outside London would cost another £14.5 million a year. The cost to the tax payer should be offset by contribution of £5 million from the private sector towards some of these new activities.)

34. Other recommendations, notably those aimed at reducing the length of fraud trials or avoiding them altogether have the potential to save substantial amounts of money on court, prosecution and legal aid costs. It is hard to estimate these savings but on certain assumptions they could amount to as much as £50 million a year.

35. However the most important benefits will be the reduced fraud losses throughout the economy from the proposals. The greater scope for data sharing and data matching created by the National Fraud Reporting Centre will generate substantial savings for both the private and public sector. We have not been able accurately to forecast these savings but all previous

exercises of this nature have yielded savings that are a high multiple of their costs. For example, the proposed extension of the National Fraud Initiative data sharing exercise run by the Audit Commission is estimated to generate savings of £280 million for an investment of £2 million, a ratio of 140 to 1. A modest estimate of the further savings from wider data sharing exercises could be several hundred millions a year for both government and business.

Legislative Implications

36. Extending wider sentencing powers to the Crown Court and the recommendation to increase the maximum prison sentence for fraud to 14 years will require legislation. Increasing data sharing and penalties for wilful misuse of data will require legislation but these are already being taken forward by other departments.

Conclusion

37. The recommendations in this report are designed to provide a comprehensive package to tackle fraud in the UK. The recommendations and associated costs should be viewed in the overall context of fraud, which although we cannot yet make accurate estimates, costs the UK economy many billions of pounds each year. The main benefits of implementing the recommendations will be a reduction in fraud and the harm it does to the economy and society, an improvement in the way victims are compensated, and improved confidence in the criminal justice system.

CHAPTER 1 INTRODUCTION AND BACKGROUND

1 Terms of Reference

1.1 The government announced the review to Parliament on 27 October 2005. The terms of reference are attached. The broad mandate was to review the arrangements for dealing with fraud with the aim of reducing the amount of fraud and the damage that it causes to the economy and society. The review is to report jointly to the Chief Secretary and Attorney-General. The target date to report was late spring 2006.

1.2 At an early stage it was decided:

- To focus on England and Wales; and
- To exclude fiscal and benefit fraud.

1.3 However, there have been a few contacts with people and organizations in Scotland and Northern Ireland and it is recommended that the new arrangements proposed in the report for a national fraud strategy and for reporting fraud should extend to the entire United Kingdom. Similarly these proposals would also cover fiscal and benefit fraud and representatives of HM Revenue and Customs and the Department for Work and Pensions have been involved in our work.

Organization and Governance of the Review

1.4 The review has been conducted by a small core team of officials drawn from Whitehall departments augmented by people experienced in dealing with various aspects of fraud drawn from the National Health Counter Fraud Service, City of London Police, Serious Fraud Office, the Home Office and Crown Prosecution Service. We thank these organizations for providing their staff to the review. We also thank the Financial Services Authority who provided the accommodation from which the review was conducted.

1.5 To provide strategic direction a Steering Group was established to oversee the review chaired by Jenny Rowe (Director of Policy and Resources, Office of the Attorney-General). It also comprised representatives from HM Treasury, Home Office, Department of Constitutional Affairs, Serious Fraud Office, Crown Prosecution Service, Department of Trade and Industry, City of London Police, Department of Health and the Financial Services Authority. Ros Wright, who chairs the Fraud Advisory Panel and is an ex Director of the Serious Fraud Office participated as a full member of the Steering Group in a personal capacity.

Progress of Review

1.6 The first phase of the review carried out between October 2005 and January 2006 was a fact finding exercise. An Interim Report of these findings was published in March which:

- Analysed the problems in tackling fraud;
- Assessed the effectiveness of the response to fraud; and
- Suggested a number of issues for the second phase of the review to study in order to identify options for change and recommendations.

1.7 This final report is mainly about the findings of these studies and should be read in conjunction with the Interim Report which sets out the details of the earlier fact finding exercise. However, the Final Report also summarises these findings in the relevant chapter and can be read as a self contained piece.

Approach

1.8 The limited timescale of the review did not permit a comprehensive evaluation of the issue and this was never the intention when it was commissioned. Instead, the Fraud Review Team concentrated upon

identifying the major problems in the current arrangements and then suggesting practical ways of dealing with them. Many of the recommendations in this report have not been subject to fully worked through business cases and the costings provided are approximate rather than detailed. The objective has been to set them out in sufficient detail that decisions of principle on whether to adopt them (or some variant of them) can be made. Further work on detailed implementation would then be needed.

1.9 The Fraud Review Team did not revisit any issues which were the subject of other reviews or being dealt with in another context. So there is no new discussion of issues such as Police force restructuring, non-jury fraud trials, or reforming legal aid procurement. However, where recommendations made by the Fraud Review have implications in these areas they are pointed out.

1.10 Two pieces of external work were commissioned. The Central Office of Information provided a study of call centres which is incorporated into the chapter on fraud reporting. A report was commissioned from Professor Michael Levi of Cardiff University into the pattern of fraud sentencing whose results are reported in the chapter on fraud sentencing. In addition, we kept in close contact with Professor Levi and the research team currently preparing a separate report on the "Nature, Scale and Economic Cost of Fraud" for the Association of Chief Police Officers, Economic Crime Portfolio (ACPO-ECP) and its early findings have influenced the chapter on fraud measurement.

1.11 However, the majority of our information and analysis has come from a series of extremely productive meetings and seminars with a very wide range of individuals and organizations drawn from both the public and private sectors who provided their time and expertise freely to us. We express our gratitude to them as well.

Next Steps

1.12 The options and recommendations in this report will now be considered in the context of the 2007 Comprehensive Spending Review. As we said in the Interim Report, the key consideration in assessing them should be whether they make a useful contribution towards reducing fraud and the amount of harm that fraud causes to the economy and society.

CHAPTER 2 MEASURING FRAUD

2 SUMMARY

- There are no reliable estimates of the cost of fraud to the economy as a whole.

- There are numerous estimates of some types of fraud and some attempts at an overall measurement. But as each uses different measures and definitions of fraud, the findings cannot be aggregated or compared in any statistically valid way.

- There is currently no agreed definition of fraud and few exercises which measure fraud using robust methodologies;

- The Fraud Bill will create a legal definition of fraud and, together with proposed improvements in the Home Office Counting Rules, should make reporting and recording fraud easier;

- But the picture will still be incomplete, as unreported and unrecognized frauds pose a challenge to current measurement techniques. A comprehensive measurement exercise must:

    - Record properly all known and reported fraud;
    - Increase the reporting of known but unreported fraud;
    - Expose and better estimate undiscovered fraud.

- The cost of fraud goes well beyond fraud losses, and the harm fraud causes to victims and the economy should be included in any measurement;

- The current ACPO study into the "Nature, Extent and Economic Impact of Fraud" is considering how fraud is currently measured and how to

improve it in areas where the methodology is weak or no measurement exists;

- A new unit should be set up as part of a strategic solution in order to carry out measurement exercises across the economy, and build on the results contained here and in the ACPO study;

- Initially it would comprise 13 people at a cost of £450,000 which would enable it to carry out four exercises in the first year. Its long term aim should be to embed quality fraud measurement exercises into other organisations and sectors. It should be reviewed after the first year of operation;

- Improved measures of fraud will improve Home Office work to understand the comparative harm of fraud;

- Although significant caveats apply, this work indicates that quantified non-excise fraud committed by organised criminals is second only to Class A drug trafficking as a cause of harm and is approximately as harmful as people smuggling and people trafficking combined.

Introduction

2.1 This chapter presents a summary of findings on the scale and nature of fraud. Because fraud is *not accurately or consistently measured* the main recommendation concerns the need to create and apply a robust measurement methodology, rather than analysis of where the UK economy is vulnerable to fraud.

2.2 The chapter discusses the issues arising around measuring fraud accurately. It examines the problems of measuring fraud, including what constitutes fraud, and what mechanisms currently exist to measure fraud. The chapter concludes by proposing how fraud should be measured and

recommending a programme of measurement exercises to provide the information currently lacking to levels of accuracy that can be used within the decision making process.

Defining and Measuring the Costs of Fraud

2.3 The problems of measuring fraud fall into two categories:

- Having clear definitions of what constitutes fraud; and
- Having robust and transparent mechanisms for measuring fraud.

Definitions

2.4 There is, at time of writing this report, no single criminal legal definition of fraud in England and Wales. There is a generally held view that fraud is *causing loss or making a gain at the expense of someone by deception and dishonest means*. But the absence of a legal definition of fraud has seriously hampered the objective measurement of fraud. With no single legal definition, a range of descriptions of what behaviour constitutes fraud have been used in measurement exercises across different sectors, contributing to the range of figures for 'fraud' which we find today.

2.5 Fraudulent activity manifests itself in many different ways (and therefore lends itself to different sub-categorisation in the way other crimes do not). But with no basic definition, there is room for interpretation as to what constitutes fraud. In English law, fraudulent behaviour encompasses a variety of offences such as:

- All offences of theft under the Theft Act 1968 that involve deception;[2]
- Forgery and counterfeiting offences;
- Documentary frauds such as false accounting;
- Insider dealing;

- Publishing of false documentation;
- Individual cartel offences;
- Offences under the Financial Services and Markets Act relating to misleading statements and practices;
- Fraud offences under the Companies and Insolvency Acts;
- Conspiracy to defraud.

2.6 Work undertaken by the Law Commission[3] prompted the Home Office to introduce the Fraud Bill which is now before Parliament. The bill will, for the first time, define fraud in English law. The definition of fraud in the bill falls into three parts, which are reproduced below.

2. Fraud by false representation

(1) A person is in breach of this section if he:

(a) dishonestly makes a false representation, and

(b) intends, by making the representation:

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if:

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of:

(a) the person making the representation, or

(b) any other person.

(4) A representation may be express or implied.

(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

3. Fraud by failing to disclose information

A person is in breach of this section if he:

(a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and

(b) intends, by failing to disclose the information:

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

4. Fraud by abuse of position

(1) A person is in breach of this section if he:

(a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,

(b) dishonestly abuses that position, and

(c) intends, by means of the abuse of that position:

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss.

(2) A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.[4]

2.7 Legal definitions provide the basis for measuring crime in the official crime statistics. The new criminal definition of fraud will provide a basis for better classifying fraud within the criminal justice system. This rationalisation of the law is welcome, but even this definition of fraud will not provide the basis for a comprehensive measurement; certain types of fraud will continue to be prosecuted under other legislation (e.g. Companies Act,).

2.8 There are also definitions of fraud contained outside legislation such as in professional standards, e.g. International Accountancy Rules which are applied in the UK and define fraud for auditing purposes.[5] Because fraud can span the 'grey area' from being an outright criminal offence to being the result of poor business management, ignorance or even sharp business practice, it will always have supplementary and wider definitions than those in law. This blurring of what constitutes fraud will continue to make fraud hard to define and measure.

2.9 Measuring fraud in the economy will therefore require looking at more sources and definitions than the criminal law definition. Work commissioned by the Association of Chief Police Officers (ACPO) to research the scale, nature and extent of fraud is using definitions based upon victims and modus operandi rather than a legal definition. However, it should be possible, at least partially, to reconcile these differences because there are areas of commonality between crime statistics (which are based on legal categories) and typologies (which often mirror modus operandi and are useful information for police and investigatory purposes).

2.10 Having a practical legal definition of fraud which can lead to a simplified or more consistent recording of fraud will certainly make it easier to define fraud in the context of criminal statistics. But alone, it will not solve the problem of measuring the occurrence and cost of fraud across the economy. Any measurement must be based on a rigorous methodology, and there are few such exercises in the UK today.

Mechanisms for Measuring Fraud

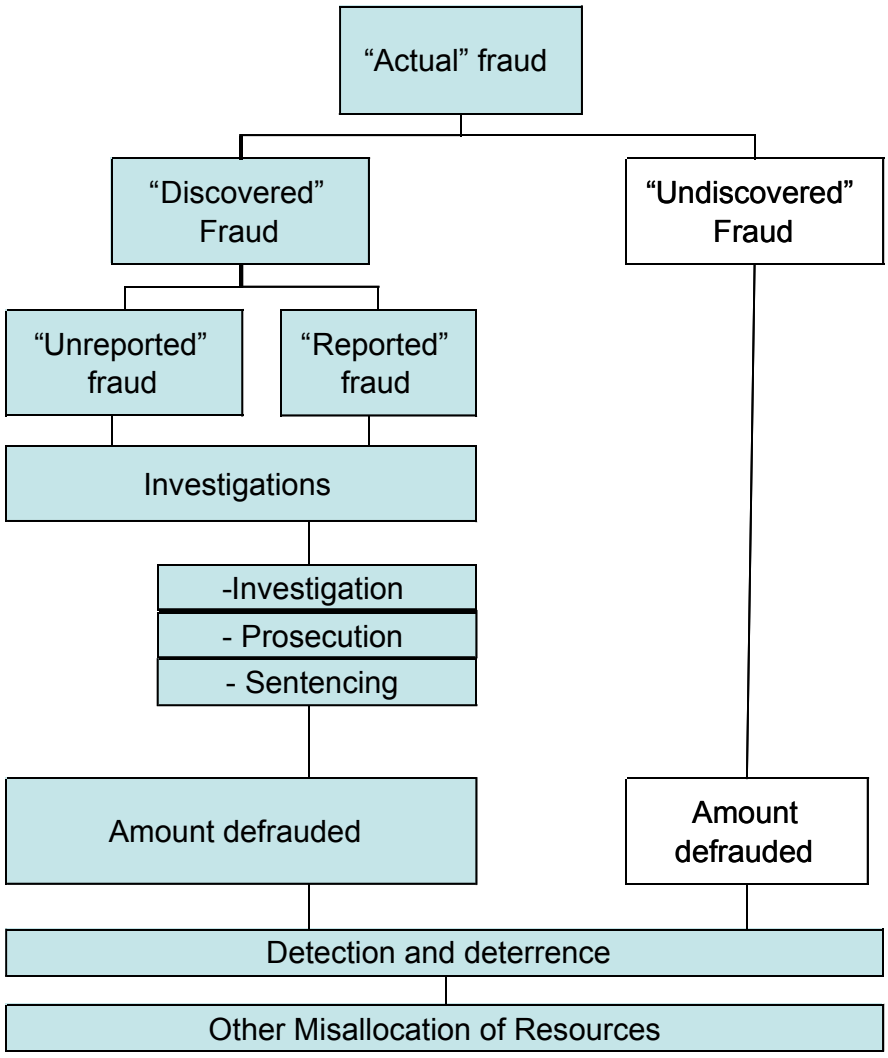
2.11 The NERA study[6] on fraud (published in 2000) summarised the measurement problem in the conceptual model reproduced in figure 1. There are three parts to measuring fraud:

a) Identifying "reported" or known fraud; which is currently a small proportion of the total;

b) Identifying known but "unreported" frauds which can better inform our understanding;

c) Pushing back the boundaries of "undiscovered" fraud; fraud which is not reported because it is not even recognised.

Figure 1. NERA Analytical Framework



2.12 A proper measurement exercise must therefore record properly all reported fraud, increase the reporting of known frauds which are not currently reported, and find ways to better detect and expose undiscovered fraud. One author on the subject claims that only 20 percent of fraud is "exposed and public" with a further 40 percent of the total "known but not publicised" and a further 40 percent "undetected".[7] The next section will look at how we currently count known frauds.

Crime Statistics

2.13 The Home Office lays down rules and procedures for counting fraud and other causes, published in the annual Criminal Statistics. The counting

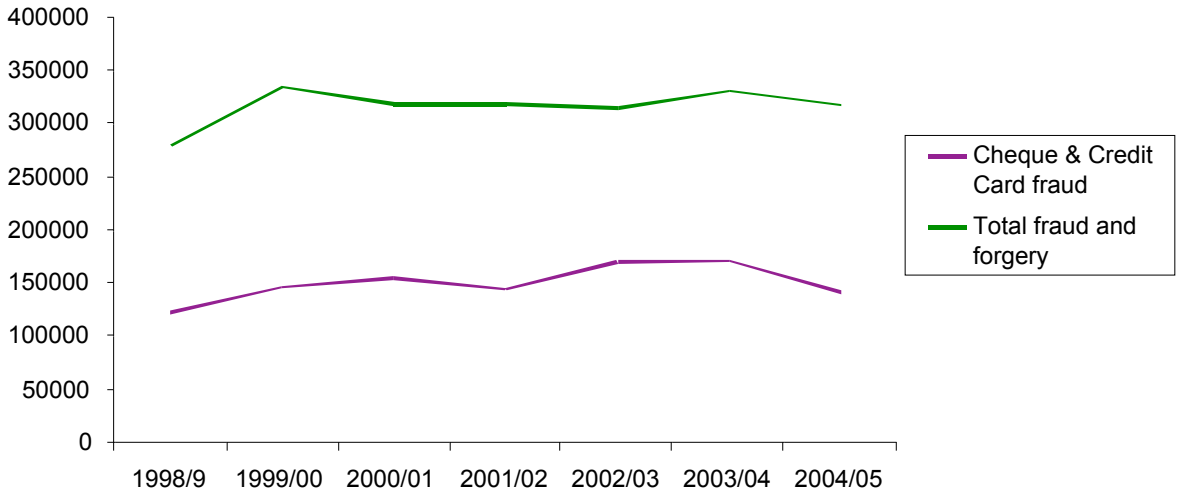
rules for fraud were changed in 1998 and mean that a consistent series of figures only exists from 1998-99.

2.14 There are eight categories of fraud and forgery in the current counting rules. The largest component of fraud is classified as "other fraud" which comprises 35 types of behaviours ranging from the general (conspiracy to defraud, obtaining property by deception) to the very specific (purporting to act as a spiritualistic medium for reward). It accounts for 51 percent of total fraud. Cheque and credit card fraud, accounts for a further 43 percent of the total. Other components with recorded offences in 2004/005 were:

- Forgery (10, 643);
- Vehicle/driver document fraud (5, 434);
- False accounting (531);
- Frauds by company directors (50);
- Offences in bankruptcy (11).

2.15 On this measure the number of offences of fraud peaked in 1999/00 at 334, 773 and fell slightly to 317, 947 in 2004/05. Over the same period the amount of cheque and credit card fraud fell more sharply from 173,857 offences (over half the total) to 120,875 offences (less than 40%). It is estimated that the police only receive reports of 5% of fraudulent credit card transactions.

Figure 2. Fraud and Forgery (Home Office Crime Statistics)



2.16 It is clear that under-reporting of fraud crime is a chronic problem. The difficulties for individuals who are victims, and for businesses to report frauds to the police, are covered in more detail in Chapter 4. The figures as they currently stand do not provide much useful information on the number, occurrence or type of fraud offences.

2.17 A Home Office sub-group of the National Crime Recording Steering Group commissioned an expert from the Metropolitan Police to draw up a new set of Home Office Counting Rules to reform the way the current system works. Consultation with all police forces was undertaken, together with consultation with APACS. Changes to the counting rules centre on rationalising responsibility for recording the crime, and using the statistics collated by APACS to supplement crime statistics. They include:

- Counting one crime per account defrauded, removing the need to record all usages as separate crimes;
- The Home Office will obtain levels of Fraud from Industry (APACS) to represent the true level of plastic card fraud in England and Wales.

2.18 These changes to the fraud statistics, following on from the Fraud Bill, are welcome. However, there are other types of volume frauds which will not be

included in these statistics (such as those frauds against government departments) and which, in order to properly gauge the volume and types of fraud most prevalent, must be encompassed by any measurement regime. Further work is needed to produce consistent recording of such frauds so that all types of fraud can be analysed consistently with published criminal statistics. This is further discussed in chapter 4.

2.19 The British Crime Survey (which is a survey based approach to measuring crime and the perception of crime, and supplements recorded crime statistics) has not in the past included fraud. This is important because not only is the BCS the most comprehensive survey of its kind, but it concerns perceptions of crime. Public concerns over fraud have not been measured or presented to government policy makers in any systematic manner to date. However, some frauds are included in sectoral or other surveys undertaken by the Home Office, the Commercial Victimisation Survey (2004) found that 18% of retailers and 8% of manufacturers had been victims of fraud by outsiders.[8] The 2002/03 British Crime Survey included a module designed to look at various aspects of technology crime which included internet fraud. Results showed that 75% of respondents were worried about the security of using a credit card online.[9]

2.20 The Fraud Review has performed an initial mapping exercise to detail what measures of fraud exist and what methodologies have been used. The results of this research are presented in a table at the end of this report, in Annex A. The conclusions are summarised below.

Statistics from the Public Sector

2.21 Central government departments with major known fraud losses were contacted in relation to their work on measurement; Department for Work and Pensions (DWP), Her Majesty's Revenue and Customs (HMRC), Department of Health (NHS Counter Fraud Service), Ministry of Defence Fraud Analysis Unit (DFAU) and the Foreign and Commonwealth Office

(FCO). Information on these departments is contained in the table reproduced at the end of this chapter.

2.22 The table contains a summary of published material, discussions had with and information sent by contacts. It is not an exhaustive list of methodologies used to measure fraud losses. What the table aims to do is highlight the range of methods used and figures reached as a result. In terms of conclusions it would appear that the DWP, HMRC and NHS are the Government departments with the most robust methodologies for calculating fraud losses. These departments do not look at detected fraud or known losses but instead take a sample of transactions/cases from within a given area of spend i.e. income support or patient pharmaceutical prescriptions and review each case to assess whether the claim was in fact genuine. These figures are then extrapolated out to give a figure for fraud losses within that given area of spend. These are statistically valid results.

2.23 Other departments which measure detected fraud or known losses such as the FCO and the MoD have been gradually improving their counter fraud work by training staff to become Accredited Counter Fraud Specialists and then working on raising awareness of fraud to increase the number of suspicions reported (this does not mean that actual fraud has increased). For example the MoD have a 'something wrong tell us' campaign which has been rolled out amongst all employees.

2.24 The FCO (FCU) carries out a number of pro-active visits to overseas posts every year. Their target is to carry out 15 pro-active visits this financial year. They identify the posts most in need of a pro-active visits based on a range of information (geographical location, history of malpractice, quality of staff, results of previous audits etc). They do identify a number of frauds as a result of these visits by identifying where there are weaknesses in controls and investigating further to see if there is evidence of malpractice.

The most common type of fraud discovered by this means is procurement fraud.

There are numerous Government departments and public bodies which are not included in the table.

Statistics from the Private Sector

2.25 In the private sector we have identified a number of different surveys, which are also included in the table at Annex A. Ernst and Young, PriceWaterHouse Coopers, and Robson Rhodes are probably the best known private surveys, with the first two engaging in global research as well as in the UK. KPMG publishes a 'Fraud Barometer' but the methodology differs significantly, as it monitors not firms, but fraud cases in court where the loss/claim is a value over £100,000. This obviously catches only a proportion of all fraud cases, although is helpful when considering the capacity of the Criminal Justice System to deal with medium and large frauds. BDO Stoy Hayward has published a 'Fraud Track' survey since 2004.

2.26 Our conclusions are mirrored by the emerging findings of the ACPO study. These are that:

- Data are available on commercial fraud from a range of sources and agencies;
- The data…is not routinely collected annually in each survey;
- The sources use different methods; the methods can affect the cost of fraud revealed;
- The surveys cover different sectors and some sectors have better data than others; and,
- The surveys use different categories and definitions of fraudulent behaviour.[10]

ACPO Research

2.27 The Association of Chief Police Officers has commissioned a study on "The nature, extent and economic impact of fraud", which is underway. Its aims are first, to report on the amount and quality of data now available on the costs of fraud and second, to recommend how gaps revealed within this should be addressed. The first part of the work should be available by July 2006 but the second phase will not be completed until later in the year. Recognising the overlap in both projects' terms of reference, the Fraud Review and those undertaking the ACPO research have been working closely together and the outcome of the ACPO work will largely determine the way the Fraud Review recommendations on measurement will be put into effect.

2.28 The ACPO study will generate the following:

- A snapshot of available information about the nature, extent, and cost of fraud to the public and private sectors;

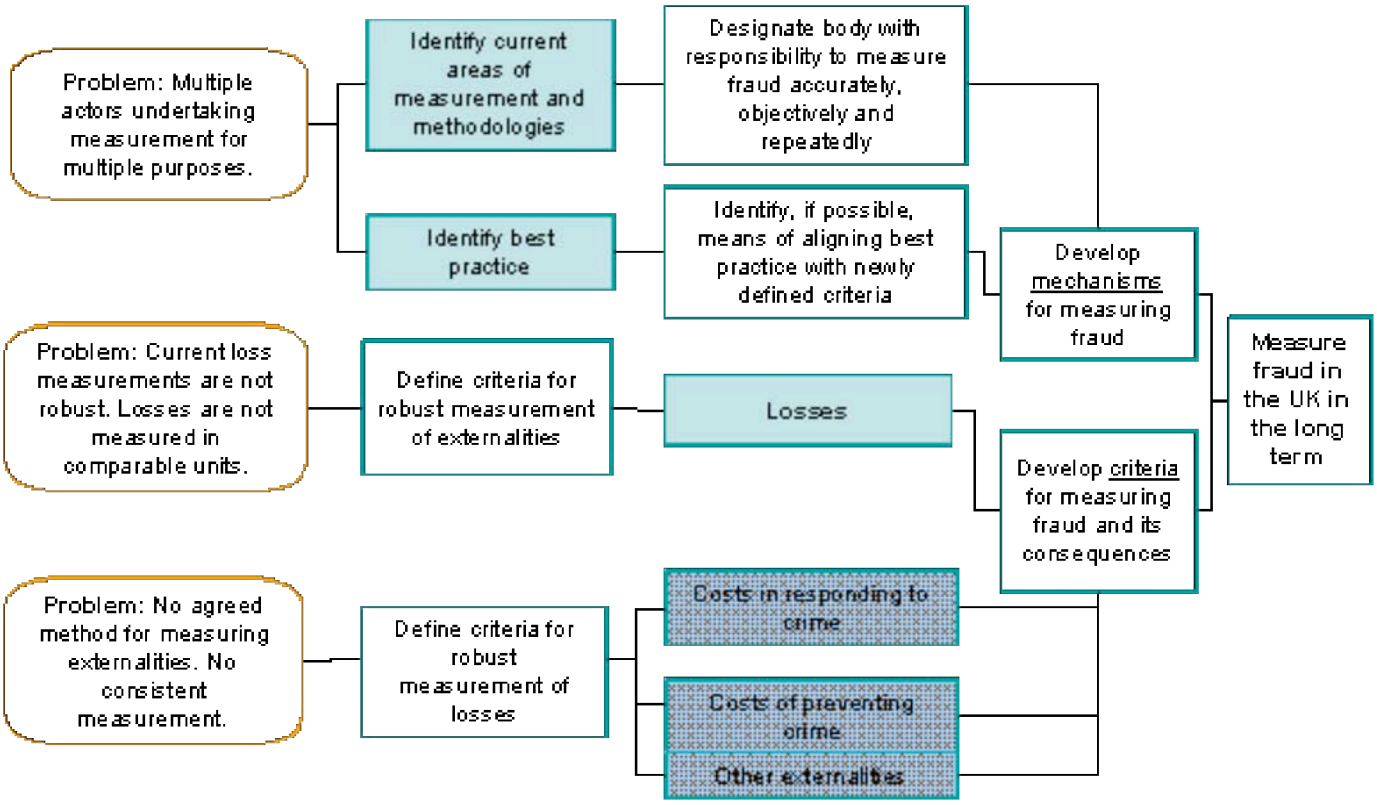
- An assessment of the quality of that data and identification of the major gaps in our knowledge;

- Recommendations as to appropriate strategies to facilitate the comprehensive and consistent recording of data on fraud (i.e. strategies for future data capture).

2.29 The ACPO research team do not expect to find better measures of fraud costs than the Fraud Review Team and are very likely to support the Fraud Review recommendations for a proper measurement exercise. Their assessment of existing data quality and recommendations about ways of improving it will complement the work done here in developing future measurement exercises. The flow chart below highlights some of the

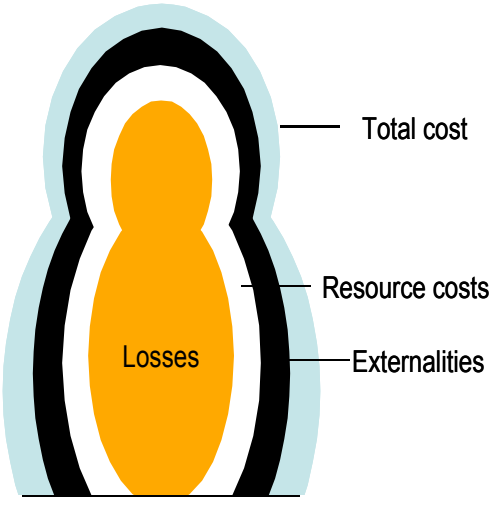
current problems and possible solutions of defining fraud and establishing mechanisms to measure fraud robustly. The boxes in blue represent work that will be undertaken by the ACPO Study. The remaining steps should be performed by the proposed measurement unit.

Figure 3. Better Measuring Fraud



Economics of Fraud

2.30 When measuring fraud, it is important to consider not just fraud losses but the harm caused by fraud.



2.31 At the core of every fraud is a loss. Measurement of fraud must therefore begin by accurately identifying the actual losses to fraud suffered by the individual, organisation or

business. This is difficult. Aside from the problem of recording fraud properly, 'unknown fraud' distorts the picture. A business or individual may not be aware that they have been defrauded. Or, they may be aware they have lost money but do not regard the loss as a fraud but as a bad debt or an operating cost. Accurately identifying losses is the first step towards building a larger picture of fraud.

2.32 Also relevant to assessing the cost to the economy of dealing with fraud are the resource costs and externalities. The resource costs are the costs of responding to fraud such as the cost of investigations, prosecutions and measures taken to prevent fraud. In the public sector they include the cost of Police, prosecutors and building anti-fraud processes into the tax and benefit systems. The same sorts of costs arise in the private sector, for example, financial institutions investing in technology such as chip and pin to defeat fraudsters.

2.33 Externalities are costs or benefits from activities which affect behaviour but are not fully reflected in prices. The reluctance of some people to use the Internet for financial transactions because of fear of fraud even though they would save money on the transaction by doing so is an example of an externality.

2.34 Most of the focus is on fraud losses because they are the immediate consequence of fraud and represent the proceeds of crime. However, the resource costs and externalities also need to be considered when assessing the cost of fraud to the economy. Compiling a measure of resource costs is not technically difficult although the very large number of organizations and businesses involved in dealing with fraud will mean that obtaining a comprehensive measure will be a lengthy process. Measuring externalities is the most challenging from a methodological view point but they should at least be identified, even if they cannot be quantified.

Harms

2.35 The Home Office in an effort to understand the wider costs of organised crime, is estimating a 'snapshot' total of the economic and social costs (or 'harms') of a range of organised crimes. This exercise, along with a range of other factors, has fed into an assessment of SOCA priorities. The study estimates not only the direct fraud losses (the largest element), but costs of undertaking preventive measures, administrative costs, and costs to the criminal justice system.

2.36 Given the focus on organised crime, not all types of fraud have been assessed, and a conservative approach has been taken in determining which frauds are considered 'organised'.

2.37 The initial finding is that in 2003 organised non-excise fraud was the second highest cause of harm after Class A drug trafficking, with the quantified harms being approximately the same as people smuggling and people trafficking combined. However, significant caveats are attached to these estimates, with the level of harms of each of these crimes being almost certainly underestimated. It will not be possible to assess the true harm of fraud until there is a fuller picture of total fraud losses, which brings us back to the need for a proper measurement exercise.

Performance Measurement

2.38 In addition to measuring the extent of fraud, it will be necessary to measure the success or failure of actions taken to reduce the overall problem. The public sector has a regime of Public Service Agreements (PSA) and Key Performance Indicators (KPIs) which are used to assess the effectiveness of government policies. We have already seen that there is a wide variation in departmental investment in anti-fraud activities. There is an opportunity, in developing more sophisticated measurement of fraud, to integrate

measurements which can be used to inform what is a proportionate and efficient use of resources to tackle fraud.

2.39 One way of doing this is to measure losses repeatedly, producing consistently accurate figures. These can be used to show progress being made in reducing losses by action taken. This way of demonstrating progress – proven reductions in losses to spending or income - can be a key performance indicator for anti-fraud action. This can be set alongside and validate other ongoing activity-based performance indicators.

2.40 In recent years work has been completed in two significant areas of government spending; the Department of Work and Pensions and the National Health Service on statistically valid exercises to measure fraud losses. The essential elements of this work have been to take representative samples within areas of spending in order to determine losses to fraud within the sample, and to extrapolate from these figures to estimate overall losses within and area of spending. Exercises are repeated in order to capture the results of anti-fraud work in reducing losses.

2.41 It is therefore possible for a quantitative strategic anti-fraud objective to be devised around reductions in losses within specific timescales, with progress towards these to be demonstrated by repeated measurement exercises. A systematic attempt to create methods for robust measurement of fraud and apply that across the economy will improve our knowledge of areas where measurement is poor or non-existent; in both the public and private sectors.

Limits of Measurement

2.42 There are of course limits to what can be done quickly in terms of such exercises on an economy-wide basis. Not all areas of fraud can be

measured at once and in some areas, data may not be available for sufficiently rigorous sampling and examination to be possible.

2.43 This type of exercise is about measuring losses from all types of fraud within particular areas of spending. It is not a measurement of loss related to a particular type of fraudulent modus operandi across different areas of spending. So the NHS measures losses to the Health Service from fraud but do not separately measure different mechanisms for carrying out the fraud, such as identity theft. While it is important to appreciate how fraud is carried out so as to combat it in future, the most useful measure is the total loss to the organization. Concentrating on a fraud mechanism risks overlooking the big picture and possibly devoting resources to the wrong area of fraud loss. It may also give a misleading indicator of achievement; it would not be an unqualified success if an organization halved its losses from (say) identity fraud if simultaneously losses trebled from (say) misrepresentation of circumstances. Hence the need to measure *total loss within a defined area of spending*.

Conclusions

2.44 Only when there is robust information about the scale and nature of fraud will it become possible to make sound judgements about the priority that fraud should have in the overall fight against crime. The table detailing losses to fraud shows various estimates which all use different methods or measurement. The results of these methods may be useful individually, but cannot be compared or aggregated.

2.45 It will never be possible to measure 100% of fraud; there will always remain undiscovered fraud. But better measurement is crucial to a properly designed and effective strategic response to fraud and to supporting better management of fraud risks.

2.46 The findings of the second stage of the ACPO study due to be available in October 2006, will identify the main deficiencies and gaps in existing data and propose ways of building up a comprehensive national picture of the cost of fraud. Addressing these recommendations will require a dedicated measurement unit composed of specialists. Such a unit would have the task of developing a robust methods for measuring fraud, building on the ACPO report, and carrying out certain measurement exercises itself. The long term aim would be to build up measurement capacity within departments and sectors so that measurement becomes the responsibility of those affected by it.

2.47 Because of the large gaps in fraud measurement there would be scope for a large unit to carry out this task and the size of the unit depends on how quickly the work is required. One approach would be to copy the National Health Service approach and have a unit initially of 13 which in its first year could carry out four major measurement exercises; two in the public sector and two in the private sector. The size of the unit can be reviewed in the light of the first years work.

Cost

2.48 It is estimated that a centrally funded measurement team could deliver four comprehensive measurement exercises per year in different areas of spending.[11] The unit would be part of the National Fraud Strategic Authority discussed in the next chapter, and combined costs will be presented then.

Recommendations

2.49 The recommendations are as follows:

a) A measurement unit should be established within the National Fraud Strategic Authority (NFSA) with a capacity to carry out four measurement exercises during its first year.

b) A programme should be established to measure the national extent of fraud based on a robust measurement methodologies.

CHAPTER 3 FRAUD STRATEGY

"None of us are as smart as all of us"
(Japanese proverb)

3 SUMMARY

- Accurate measurement is an essential precursor for developing a strategy against fraud;

- Currently a lot of organizations have anti-fraud roles but there is no overall coordination of effort, which leads to overlaps and gaps;

- A national strategy would be directed at ensuring the whole was greater, rather than less than, the sum of the parts;

- A national strategy would learn three key lessons from existing best practice:

    - Full participation by and a partnership approach between public and private sector agencies;

    - A close link between policy and operations; and

    - Recognition that "upstream" activity to prevent fraud is as important as "downstream" work to investigate and prosecute fraud;

- Creation of an anti-fraud culture throughout society would be the central tenet of the strategy;

- This would be achieved through effective actions to deter, prevent, detect, investigate, sanction, and provide redress for victims of fraud;

- A model is described to determine the extent to which these actions are performed and then identify gaps in those responses for follow up action;

- The strategy does not have to be delivered through one agency and there are no recommendations for organizational or structural changes;

- The strategy should be the responsibility of a National Fraud Strategy Authority within a central government department but established as a public/private partnership and reporting to a governing body representing the main public and private sector stakeholders;

- The NFSA would have no operational responsibilities but would concentrate on measuring fraud, developing a strategy, assessing performance, and disseminating advice and assistance;

- A Multi Agency Co-ordination Group led by the Chair of ACPO(ECP) should be established to coordinate investigators and enforcement;

- The NFSA would require 50 staff at a cost of around £2 million per year.

Introduction

3.1 The previous chapter established that there is no reliable overall measure of fraud and that individual measures of fraud in different parts of the economy cannot be compared. Without decent measurement, a strategic approach to fraud is impossible. But a strategy is more than a response to statistics. The statistics simply provide a starting point for the key tasks of analysing the source of the problem and devising the most effective response.

Problem

3.2 The Fraud Review Interim Report examined existing arrangements for dealing with fraud, noting particularly the absence of a national anti-fraud strategy. Many government departments and agencies deal with different types of fraud and have different responsibilities for investigating, prosecuting and penalising fraud. For some, it is their sole or major task. For others, it is a small fraction of their work. But there is no mechanism for pulling together the work of the various elements, no mechanism for ensuring that resources are deployed where they are most needed, and no mechanism for considering the effectiveness of the overall response to fraud. There was widespread demand from almost everyone consulted during the first phase of the Fraud Review that the country needed a national strategy for dealing with fraud and it was a government responsibility, working with private sector partners, to devise and implement one.

3.3 This chapter sets out a framework for developing a strategy which can be applied to the fraud problem. It will also discuss the relationship between the strategy, the unit responsible for it, and stakeholders.

Existing Strategies

3.4 Many departments, agencies and organizations engaged in anti-fraud work already have strategies from which they have developed policies and work plans, which are developed from their statutory remits and/or business imperatives and they understandably focus upon how fraud impacts on their own goals. Many of these strategies involve working with other agencies and have been shown to produce results. A good example of joint working is the Economic Crime Strategy for London "Operation Sterling" run by the Metropolitan Police. This is described in the box below:

Operation Sterling

Operation Sterling is the Metropolitan Police Economic Crime Strategy for London. Although owned by the Metropolitan Police it has been developed and delivered with a number of partner agencies in both the public and private sectors. It has three key strands; intelligence, prevention, and enforcement.

Intelligence

A Partnership Intelligence Cell has been established to evaluate the true cost of economic crime to London, exchange information with partner organizations about emerging threats, and target prevention and enforcement opportunities.

Prevention

A "London Fraud Forum" containing a wide range of public and private sector organizations has been established to act as a prevention network in London. A Fraud Alert website has been established to provide advice to the public and business on how to prevent fraud. And specific initiatives have been taken such as establishing a new procedure to prevent dishonest amendments being made to the Companies Register as a precursor to fraud.

Enforcement

Examples of enforcement action under the Sterling umbrella have been cooperation with the Nigerian authorities to disrupt the activities of counterfeiters based in Nigeria, whose counterfeit documents facilitate theft and cheque fraud in the UK.

The success of this example of a strategic approach, pulling together the work of different agencies, shows how the sum of anti-fraud effort can be much greater then the component parts if only they are properly planned and coordinated and makes the case for developing an overall national strategy.

3.5 Several organizations report remarkably similar problems in devising their strategies:

a) Difficult to measure and identify the scale of the problem;
b) Difficult to define fraud; the definition and problems can change for each sector;
c) Dynamic, ever changing therefore response and prevention must be constantly invested in, and linked to intelligence;
d) Lack of law enforcement support; and
e) Barriers to data sharing

3.6 Some organizations have tried to measure the problem and related impacts more accurately as part of their strategic response. The Office of Fair Trading (OFT) work on scams is a good example of a strategy which has put problem measurement at the forefront of its work.

3.7 The strategies of the organizations that the Fraud Review has examined reveal a wide range of approaches. Some, like Operation Sterling, have clear targets and measures to achieve them, but focus on a particular subset of the fraud problem. Others present clear visions of desired outcomes but with no clear pathway for achieving them. Yet others are operationally focussed on what may more appropriately be called policies or work plans without a clear desired outcome. Some strategies focus only on the process of getting organisations to discuss the problem (e.g. by setting up steering groups or panels), but do not provide a strategic vision which the group can work towards or use to prioritise resources.

3.8 Those strategies written by multi-agency groups cover a wider range of actions and show better understanding of the contributions different agencies can make to the problem than those written by single organizations.

3.9 Most strategies are targeted at detection, investigations and sanctions for fraud. Few address underlying systemic weaknesses in operational, legal or policy processes which could be used to prevent future fraud in the first place. Those organizations which did address systemic weaknesses were often not in a position to change the situation and became involved in lobbying actors who could.

3.10 There are three lessons to be learnt when devising a strategy for the whole economy:

a) The strategy should be influenced by the full range of organizations involved in combating fraud;
b) It should clearly link policy and operations; and
c) It should place just as much emphasis on "upstream" activity to prevent and deter fraud happening in the first place as "downstream" action such as investigations and prosecutions to deal with detected fraud.

Strategy

3.11 A strategic process model for tackling fraud has been developed and implemented successfully in the National Health Service – a particularly diverse area of activity generating a very wide variety of financial interactions and, inevitably, a major fraud risk. This diversity means the model is well suited for application to the economy as a whole to develop a national anti-fraud strategy and to consider the associated structures to support it. This model is also in the process of being considered and adopted in other areas within the UK and across the EU.

3.12 The model was developed by experienced counter fraud specialists with a basic set of requirements:

a) The model should present a holistic approach;

b) The framework can be applied to a particular sector, or to a group of sectors;
c) Accurate measurement of fraud is an essential part of understanding the problem;
d) Performance measures linked to accurate measurement are essential and must be tailored to the needs of the sector and the environment in which it operates.

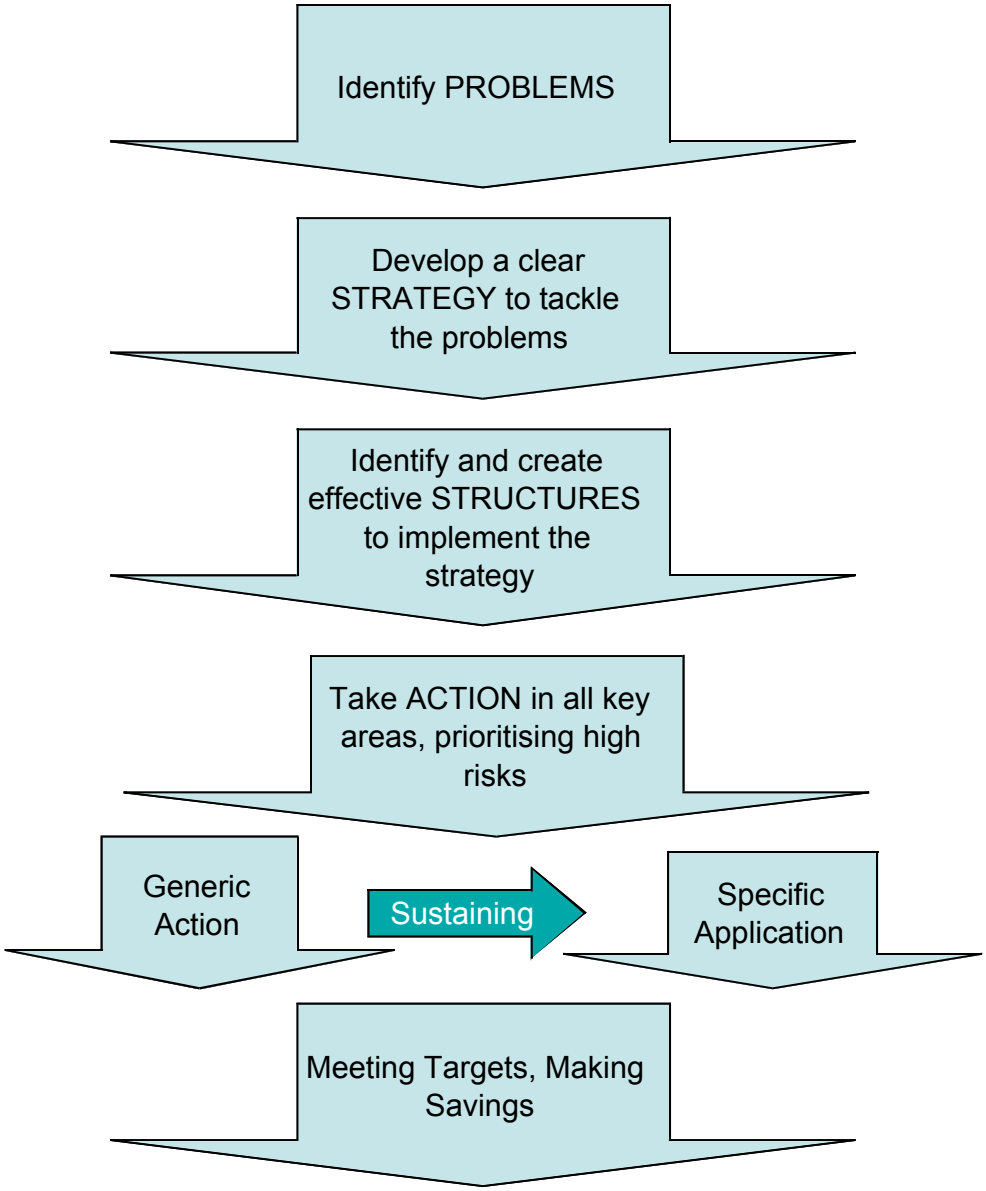
3.13 The strategic process model is as follows:

- Problem: Identify and measure the nature and scale of fraud;
- Strategy: Develop strategic aims for tackling the problem;
- Structure: Create effective structures to implement the strategy;
- Action: Take action in key areas, prioritising high risk areas.

3.14 The Action section of the model encompasses both the generic range of anti-fraud action and specific actions that can be taken within different sectors to address fraud problems. The model also encompasses specific loss reduction targets to be demonstrated by repeated measurement exercises, as described in the previous chapter.

3.15 A strategic response to fraud should present a comprehensive understanding of the nature of fraud; promote development of an anti-fraud culture; deter and prevent fraud; detect and investigate fraud; and ensure that, where fraud is proven, appropriate sanctions and financial redress are applied. These actions are interdependent.

Figure 1. The Process Model



3.16 A national anti-fraud strategy would not replace the need for organizations with responsibility for dealing with fraud to develop their own strategies. The differences in sectoral experiences and different methods for tackling fraud mean a national strategy also requires sectoral policies for tackling fraud. But a national fraud strategy is crucial for ensuring that those individual strategies contribute towards and do not undermine desired national goals. The national strategy *adds value* to these individual strategies by providing a better understanding of what is being done throughout the economy already; a

better assessment of the scale and nature of the problem through more accurate measurement; a co-ordinating function to ensure the various activities are the best way of delivering the national objectives; and a forum for developing and disseminating best practice.

3.17 The very broad range of anti-fraud activities across the public and private sectors and the large numbers of organizations involved in the work means that a lead unit must be located in central government. Nothing less would have the necessary authority to sort out problems. But the broad range of anti-fraud work and numerous organizations with some role in dealing with it means that the lead unit should restrict its involvement to the strategic level.

3.18 The Review Team did briefly consider more radical options such as merging the functions of a number of existing public sector bodies into one all encompassing Fraud Agency running all aspects of work against fraud within the public sector and responsible for drawing up an overall national approach to fraud. This would be one way of bringing policy and operations together and dealing with overlapping responsibilities of different agencies. However, the approach is impractical. Aside from the massive disruption involved in establishing such an organization, there are too many types of fraud and aspects of fraud work requiring specialized knowledge and experience to tackle effectively in one organization. While there might be synergies and economies available in bringing some areas of work together and eliminating duplication, a more effective and proportionate way of dealing with fraud is to develop a more coherent approach by existing organizations. This is best done by coordinating their activities, rather than trying to deliver everything from within one 'super agency'. Consequently we have not developed a Fraud Agency approach and present just one main option for a strategic model and corresponding unit top oversee its implementation. There are, however, choices to be made concerning the functions of the oversight body.

3.19 A central strategic 'authority' should be responsible for identifying, measuring and analyzing problems and determining the best way of dealing with them. Implementation of that strategy will depend on having effective structures and partnerships to deliver those actions. There are three key lessons we identified from current best practice These are:

a) Authority to act;
b) Operations undertaken within a strategic framework;
c) Functions related to skills.

3.20 Having the authority to act is vital as each organisation engaged in fighting fraud must have the authority (and corresponding capacity) to do so. For the most part, this exists; mainly this is an issue of organizations taking fraud seriously and being willing to use powers that they already have more effectively. Any oversight body must have the authority to act to fulfil its functions.

3.21 Policy linked to operations. Many organizations have perfectly good policies for countering fraud but are let down by not implementing them. Others have policies which are not practical given the organizations within which they are supposed to apply. The national strategy should provide enough information and direction that organisations understand their relative role within the framework. It is not possible at a national scale to have a direct link between policy and operations; the Multi-Agency Co-ordination Group detailed later fills this role with regard to the national strategy.

3.22 Functions related to skills should also be self-evident but, in practice, will be complicated given the variety of organizations and the range of skills that need to be deployed.

Action

3.23 The seven areas of generic action shown within the process model are:

a) The creation of an anti-fraud culture;
b) Maximum deterrence of fraud;
c) Successful prevention of fraud which have not been deterred;
d) Prompt detection of fraud which have not been prevented;
e) Professional investigation of allegations or suspicions of fraud;
f) Securing appropriate sanctions against people guilty of fraud;
g) Effective financial redress of money obtained through fraud.

3.24 These objectives support each other. The diagrams in Annex B show relationships between different generic actions. While all organizations should try to address all seven areas there is a balance to be struck between them when addressing fraud problems in a particular area. It is especially important to understand the links between different areas of generic action and to keep under review whether the balance of effort is still right. Effort should not endlessly be put into one or two areas of action without due consideration of its longer term effects, such as the risk of diminishing returns. Examples include keeping under review the balance between reactive investigations and leaning from the results of these investigations to put more work into longer term preventative action.

Specific Action

3.25 The specific mix of generic action in any area of spending or business activity should be determined by those who understand that area and are responsible for setting particular anti-fraud activity targets. Examples might be:

a) An information campaign on deterrence and prevention of frauds (generic), which might be coordinated within a range of financial services (specific);

b) An initiative requiring detailed proof of entitlement in order to prevent fraud (generic) within provision of a government benefit or service (specific);

c) A programme of targeted interventions (generic) designed to penalise frauds in an area of internet-based fraud (specific).

3.26 Applying the process model to the public and private sectors shows the extent of current involvement and reveals gaps that would merit early attention when drawing up a national strategy. For example, most public sector resources aimed at deterring and preventing fraud only focus on areas where the government itself is a victim of fraud. Public authorities capacity to perform investigations, apply sanctions and seek redress, are far more wide ranging than those available to private organizations. The model can be applied to evaluate the response to a particular type of fraud. Again scams can be used as an example. Whilst the OFT has tools available to prevent and detect scams it currently has limited investigative powers (e.g. it cannot undertake covert surveillance of scammers or make covert test purchases of goods) and enforcement action is currently limited to seeking undertakings and court ordered enforcement notices against scammers with no scope for financial penalties or criminal sometimes. These roles and responsibilities may be appropriate given the nature of the organization to which they are entrusted.

Figure 2. Generic Actions Performed by Public Actors and Regulators

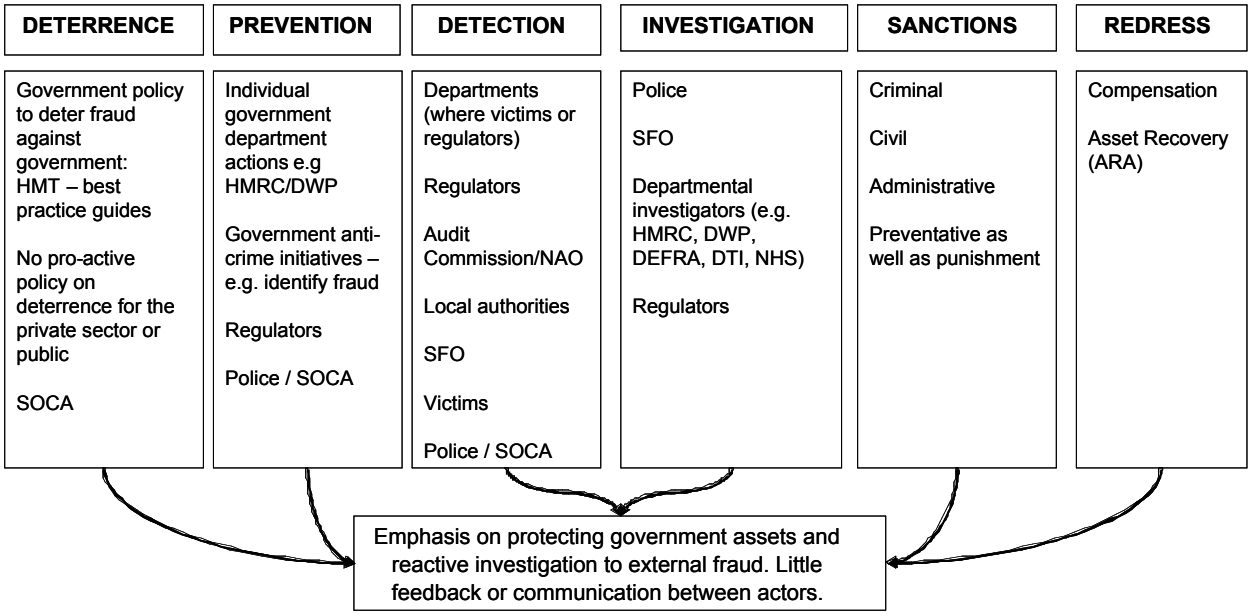
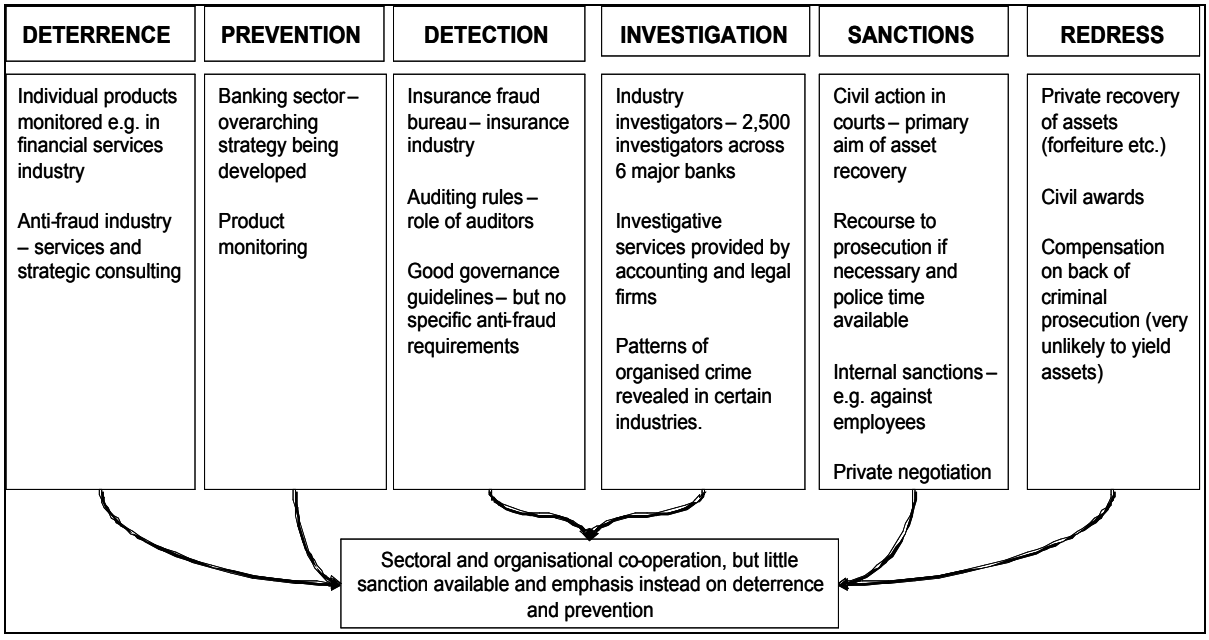


Figure 3. Generic Actions Performed by Private Organisations



Targets

3.27 Understanding fraud problems and having a defined set of strategic aims is essential for developing and prioritising generic and specific action. An organization's whole anti-fraud action programme can be set

out in this way, with corresponding targets. The transparency this provides will allow the organization to determine whether action being taken is really effective and what changes may be needed.

3.28 Targets can be set for both generic and specific action. Generic actions can be the subject of ongoing activity performance indicators, and their application as specific actions measured against targeted reductions in loss or increases in financial redress. Very few public authorities or private sector businesses currently have performance indicators relating to fraud. And it is not possible to show that the sum total of anti-fraud targets, where they exist in the public sector, relates to a declared government position of anti-fraud aims and objectives.

3.29 As an example of what can be achieved through such an approach, the National Health Service in 1998 had no overall position on fraud or dedicated resource to deal with it. Since then, introduction of the model described has resulted in an overall financial benefit of £675 million, with a 54% reduction in overall losses in the area of NHS patient fraud from £171m in 1998/9 to £78m in 2003/04.

Conclusion

3.30 The above model should be the basis for developing a national fraud strategy. Developing it further and implementing it would require the establishment of a central unit, which has been given the working title of the 'National Fraud Strategy Authority' (NFSA). As previously discussed it would not have operational responsibilities. It would have to be located within central government but would need to be a private/public partnership in which the skills of all the various operations could be brought together. The Authority would have the functions in the following table.

Functions of a Strategic Authority	
1.	Oversee the development of the measurement methodology towards the longer term objective of establishing measurement exercises within different government and business sectors.
2.	Management of the fraud measurement exercises recommended in the previous chapter and control of the team carrying these out.
3.	Ownership and development of the national anti-fraud strategy.
4.	Organization of and secretariat responsibilities for the related committee of appropriate stakeholders.
5.	A problem-solving role in respect of overlaps, conflicts or other obstructions to successful anti-fraud work.
6.	Development of anti-fraud and ensuring that they are reflected in the individual performance measures and indicators of operational agencies.
7.	Monitoring of anti-fraud performance and fit with the national strategy.
8.	Regular reporting to stakeholders and to the public of measurement and progress the outcome of monitoring; ensuring that lessons are learnt and influence the future development of the strategy.
9.	Development and implementation of anti-fraud awareness and education initiatives.
10.	The compilation and dissemination of best practice in anti-fraud work.
11.	The identification and nomination of sources of anti-fraud expertise available for those organisations that require training, support or assistance.

3.31 This range of functions would create an agency that would devise a strategy and, while not itself implementing that strategy, ensuring that operational agencies implemented it. In the language of the model it would lead the problem solving and strategy development elements of the model but responsibilities for the structure and action elements would remain the responsibility of those who are currently engaged in anti-fraud work. The need for concentrated effort on fraud measurement and coordination of anti-fraud effort, however, has been

clear for some time; indeed, the 1986 Roskill Report proposed establishing a Fraud Commission with very similar functions.

3.32 Restricting the Authority's responsibilities to this level within the process model means that it is not proposed that the Authority should become directly involved in:

- The policy development of individual departments or business sectors;
- Management of the National Fraud Reporting Centre proposed in the next chapter;
- The collation or development of anti-fraud intelligence;
- Data-sharing work across the public and private sectors;
- The direction of use of resources within individual departments or business sectors;
- Or anti-fraud operational work.

3.33 The Authority would probably comprise four main units, covering measurement (Chapter 1), strategy, prevention and awareness and initially, managing the establishment of the NFSA and the MACG.

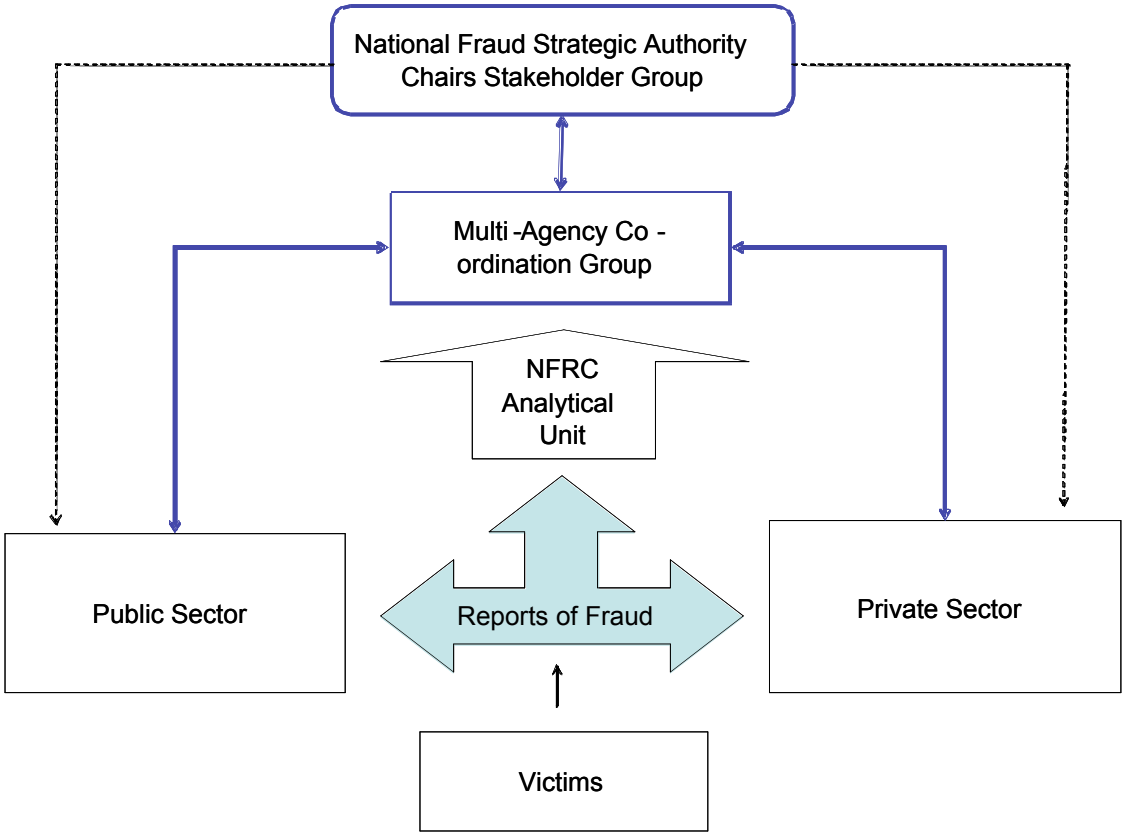
3.34 It is anticipated that the unit would consist of approximately 50 staff members and cost approximately £2m. However, this would to some extent depend on the detailed nature of expected measurement exercises, and the functions agreed for the NFSA. Detailed costs are in Chapter 13.

3.35 It is crucial to establish a clear link between the authority and operational anti-fraud work, including recommendations later in this report regarding a National Fraud Reporting Centre. It is recommended this be done through a more operationally focussed sub-group of the authority. This would be the Multi- Agency Co-ordination Group (MACG).

3.36 The diagram at figure 4 shows how the Strategic Authority, Multi-Agency Co-ordination Group and Fraud Reporting centre would work, and the diagram at figure 5 shows in more detail how other groups would engage in the development of fraud strategy.

3.37 The MACG's main role would be to facilitate anti-fraud work in priority areas designated by the NFSA. In order to do this its membership would be flexible (in order to change according to priority areas). There would, however, likely be a core group of members from law enforcement, government departments and the private sector. The MACG would provide a forum for actors to work together to tackle areas of fraud.

Figure 4.



3.38 It is not envisaged that the MACG would become involved in the usual tasking or allocation of individual fraud investigations. However, the MACG would support the development of responses to fraud by providing a forum where operational matters can be discussed and action plans including actions to increase prevention and deterrence

developed. An example of this model working in practice in operations against a particular type of fraud is described in the box below.

Scams Enforcement Group

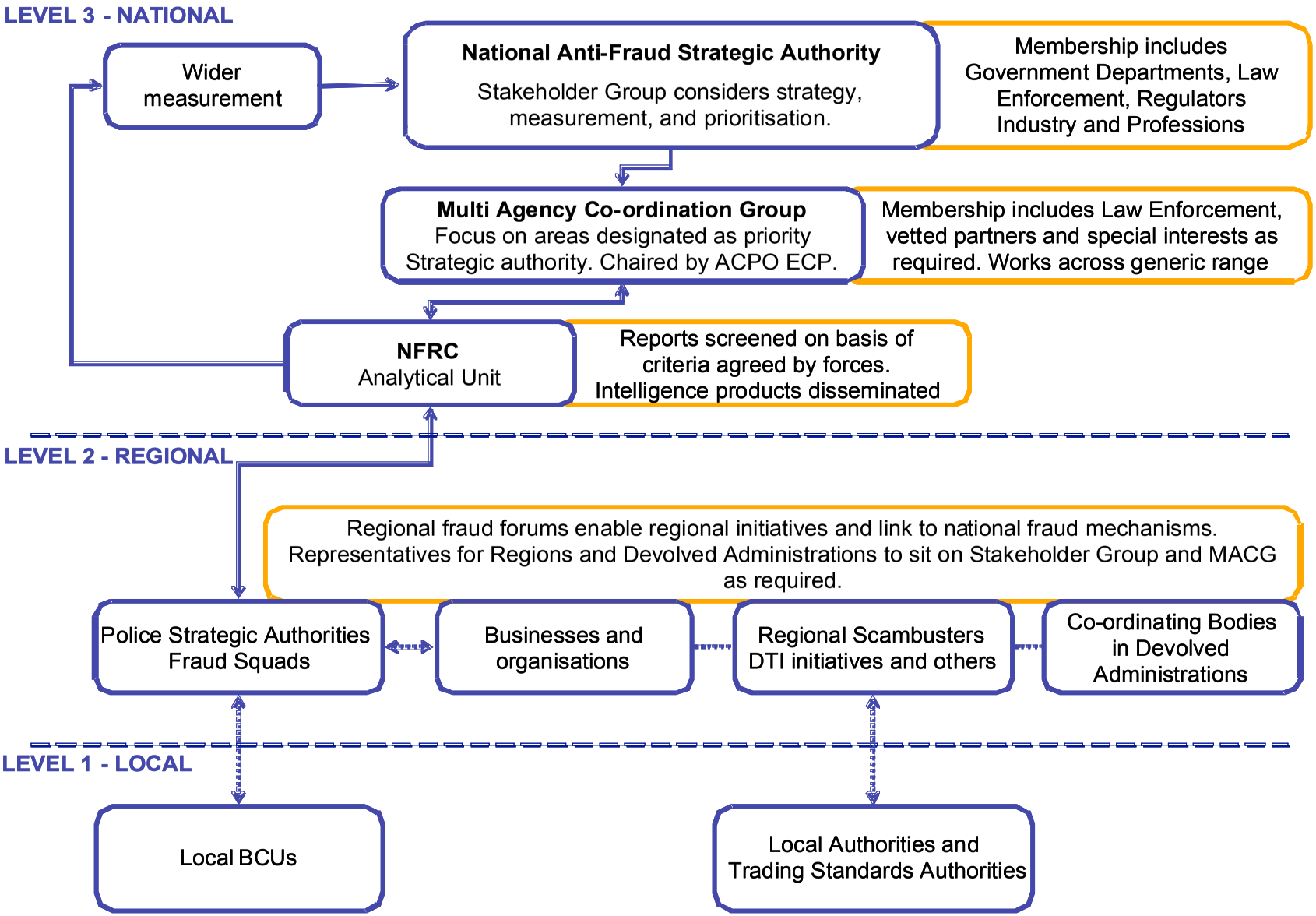
The Scams Enforcement Group brings together relevant enforcement agencies to exchange information and best practice and to coordinate action against scams.

Current membership includes:

- Office of Fair Trading;
- Regional Trading Standards Service representatives;
- Gaming Board;
- Local Authority Coordinators of Regulatory Services;
- Companies Investigations Branch, DTI;
- Law Enforcement;
- ASA;
- Ofcom;
- ICSTIS;
- Royal Canadian Mounted Police.

The OFT receives reports of scams both directly from the public and from partners such as the Trading Standards Service and uses this information to build an intelligence picture of the extent and nature of scams against UK consumers. The cross border nature of a lot of scams means close cooperation with international counterparts is essential to developing an effective response. The Royal Canadian Mounted Police is therefore a member of the Scams Enforcement Group. This intelligence is then disseminated to partners and used to target investigations and preventative work, either by individual agencies or groups of them coming together and forming "task forces" to tackle scams through a variety of prevention, detection and investigation.

Figure 5. Links Between the NFSA, the NFRC and Other Actors



Recommendations

3.39 It is recommended that a new National Fraud Strategic Authority should be established within central government and accountable to Ministers. The NFSA should, amongst other things:

- Develop an umbrella strategy for tackling fraud in the UK;
- Chair a stakeholder committee; set agreed priority areas;
- Undertake measurement exercises and develop measurement mechanisms within other organisations;
- Resolve policy conflicts between actors;
- Monitor anti-fraud performance in the UK; and
- Promote best practice and public awareness of fraud.

3.40 A small committee drawn from potential stakeholders should be established to draw up a blue print for the NFSA.

3.41 A Multi-Agency Co-ordination Group (MACG) should be created as a subordinate group with the responsibility of facilitating operational work on priority areas designated by the NFSA.

3.42 The MACG should be chaired by the Association of Chief Police Officers, Economic Crime Portfolio (ACPO-ECP) who would also be represented on the NFSA Stakeholder Group. Its membership will be flexible and determined on the basis of identified priorities.

CHAPTER 4 REPORTING FRAUD

4 SUMMARY

"Without intelligence the required case for co-operation cannot be adequately made in the first place, the priorities cannot be identified, the threats cannot be tackled, the most impactive opportunities cannot be seized, the activities of agencies cannot be coordinated to the best effect and, above all, we cannot know how well we are doing".[12]

- This chapter sets out problems with the law enforcement's capacity to collect information and intelligence on known or reported frauds, and proposes the creation of a National Fraud Reporting Centre.

- The NFRC would accept reports of fraud from victims and businesses, and would analyse reports to create intelligence products which would inform a strategic and operational response to fraud. It would have some similar functions to the recently created Child Exploitation and Online Protection Centre.

Introduction

4.1 The previous chapters outlined the problems of measuring fraud, and recommend that the Government develop a national anti-fraud strategy based on solid measurements, which could inform policies and operational responses. The strategy is designed to encompass different actors from both the public and private sectors.

4.2 The Review has put the case for improved measurement as a fundamental requirement in developing any strategic response. Collating the right information is crucial not just informing a strategic approach but also a tactical and operational one. The development of 'intelligence led policing' is a good example of how law enforcement has adopted the principles of a strategic response and the Police Service has put in place national frameworks for common standards and approaches in the shape of the National Intelligence

Model. The need to have the right information to hand, and the right processes to develop it has been recognised as crucial in the fight against organised crime; so important in fact, that increasing knowledge and understanding of organised crime is listed as the number one aim of the new Serious and Organised Crime Agency (SOCA).[13]

4.3 This chapter explores how the strategic response to fraud complements the principles of intelligence led policing and how partnership working between the police and other organisations is fundamental to the success of the strategy. It will then go on to make suggestions for improving quality and access to information on fraud to increase shared knowledge and understanding, and recommend the creation of appropriate mechanisms to do so.

4.4 There are a number of interpretations of 'intelligence led policing' in academic and law enforcement circles,[14] and when this review uses the phrase, it does so in its more general application. The following definition is useful and captures the spirit of the Review's approach:

"Intelligence led policing is the application of criminal intelligence analysis as an objective decision making tool in order to facilitate crime reduction and prevention through effective policing strategies and external partnership projects drawn from an evidential base."[15]

4.5 The key areas that 'intelligence led policing' and the national anti-fraud strategy have in common are that they both stress the importance of an evidence base, rely on objective decision making tools or procedures, include prevention of crime as a desired outcome, and require an approach which encourages partnerships beyond law enforcement. When the report refers to a strategic or intelligence led response, these are the principles which are evoked.

4.6 It is perhaps obvious to say that to be part of an efficient and truly intelligent response to fraud, law enforcement engagement must be cast within the

wider context of anti-fraud activity and the police must develop effective partnership engagements with a number of sectors and interests who operate in this area. However, making this co-operation a reality has been a challenge in the past, and will remain so precisely because anti-fraud activities are spread across a huge number of disparate organizations.

4.7 A strategic approach can facilitate the process of bringing together actors with information or intelligence relating to fraud and providing a common approach for making the best use of resources across a diverse range of skill and specialities.

4.8 The following sections will go on to examine what information can be used to develop a better understanding of fraud and how that information is collected.

Knowing the Problem: Dealing with Information and Intelligence Across Sectors

4.9 The difficulties in understanding the nature of the problem we face from fraud, described in detail in the first chapter of this report, has important implications for the strategy. If information on fraud is not properly collected, it becomes difficult to shape the right level of response. If information is not compared between organisations, it becomes difficult to identify the right division of responsibility police and other organisations have in tackling the problem. Above all, if information is not analysed properly it becomes impossible to develop anything resembling an intelligence led solution.

4.10 The role of the police in collecting information and intelligence relevant to fraud is vital. As a protective service, they are the first point of call for victims of crime, and have a duty to accept reports of crime. But police knowledge *does not* present a complete picture of fraudulent activity, and must be complemented by the information held by other organisations such as government departments, local authorities and also the private sector, in order to develop a detailed picture of what is happening. Even so, making the most of police intelligence and information processes regarding fraud is a fundamentally important step towards creating strategic response.

Furthermore, it will be an important tool in effectively shaping the response of partner organisations because of the role it plays within the criminal justice system.

4.11 It may be pertinent here to quickly define what is meant by ‘information’ and ‘intelligence’.[16] 'Information' comes from many sources, but mainly from victims in the form of reports of crime. It can also be collected in the course of routine business or policing activity, for example, processing applications, responding to incidents, undertaking licensing procedures, auditing accounts and so on. Both information and intelligence have a role to play in tackling fraud.

4.12 The ACPO ‘Guidance on Managing Police Information’ classifies 'intelligence' as "information which is subject to a defined evaluation and risk assessment process in order to assist with police decision making" - that is, any information which has been processed for purposes of informing operations or activities. This definition is wide and covers more than traditional ‘intelligence’ which is information which has been collected to inform specific operations or information which has been provided by covert sources or informants. The wider definition could also apply beyond the police to include businesses and government departments, which also collect and process information to produce intelligence, and so is a useful way of labelling those activities.

The Role of Information

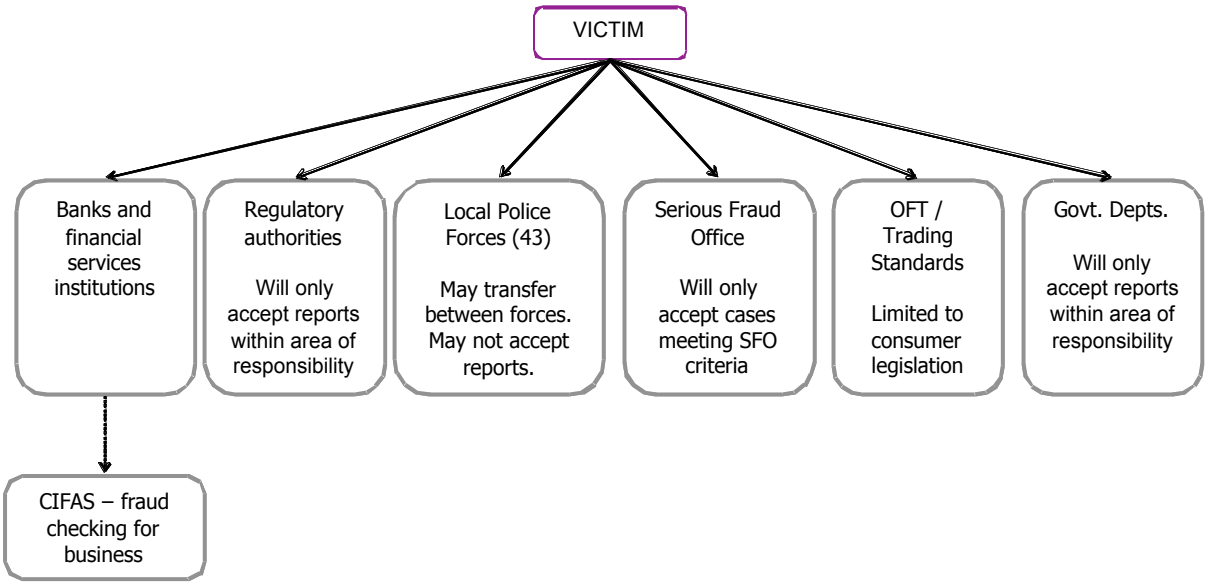
4.13 Reporting fraud and getting a better picture of ‘known’ frauds is an important component of measuring fraud. It is also important because it can directly inform an operational response to fraud.

Reporting Fraud

4.14 There are currently many ways for victims to report fraud, often depending on the nature of the fraud perpetrated against them. The process model at figure 1 shows a simplified flow chart of some of the different ways of reporting

fraud, including to local police forces (of which there are at time of publication still 43, but with police restructuring agreed in some areas).

Figure 1. Current Fraud Reporting Methods



4.15 It is often confusing for victims to know who to report the fraud to, particularly if it crosses geographical or sectoral boundaries. Fraudsters benefit from this lack of continuity of response. Internet fraud is a particularly good example of how a fraud can become difficult to report, and an example is shown in more detail in the box below. An additional problem is that Scotland has a different police reporting and legal system to the rest of the UK. ACPOS and the Scottish Business Crime Centre[17] are already working towards developing a strategic approach to fraud in Scotland. It is important that when developing better cross boundary links and reporting systems, there is some ability to create a truly national intelligence picture through co-operation with devolved administrations.

Fraud: A Challenge to Reporting

A computer is advertised for £2000 on an auction site by Mr. Bogus. Mr. Green successfully bids for it, and transfers his money to the seller. The goods never arrive. Mr. Green makes a complaint to the internet auction company, to the police, and possibly also to trading standards authorities in the area where he lives. As Mr Bogus lives in a different police force area the police are reluctant to accept the report. It is a similar situation with trading standards. Furthermore, if the goods are not worth a large

sum of money, it does not appear to be a significant crime and the police will often not investigate the case, even if they do take a report.

Mr. Bogus remains free to re-advertise the computer and performs the same fraud on an increasing number of victims. The police and trading standards do not identify Mr. Bogus as a repeat offender because the reports of fraud are either not accepted, or appear in different force areas.

Even if complaints from victims manage to get the goods removed from the auction company website, Mr. Bogus may advertise again on another site.

4.16 Some networks exist to allow organisations to share information about reports of fraud. In 1988 the credit industry established CIFAS, a not for profit organisation, to cross reference known frauds and so to flag up where there may be common or repeat instances of fraud. It does not automatically indicate the nature and type of fraud, but its service has proved very effective at allowing businesses to check for fraudulent activity. It now has over 250 member businesses which contribute to it.

4.17 The public sector also has existing networks (such as the FINNET) which act in a similar way, providing a 'dating agency' for organisations to work together to investigate suspected frauds. The Dedicated Cheque and Plastic Card Unit (DCPCU) is also an excellent example of how reports of (plastic card) fraud are being analysed by the police and the Association of Payment and Clearing Services (APACS), even though they are not all 'official' crime reports. These groups are to be commended for the work they do, and the steps they have taken to solve reporting and information exchange difficulties which face public and private sectors today.

4.18 But the fact remains that it is confusing and difficult to report fraud, and even where reporting arrangements exist, they are still only partial in reach. Many reports will therefore 'fall through the gaps' and the vast majority of frauds will

not be reported at all. Only the police have the responsibility to accept reports from victims of any type of crime.

Reporting Fraud to the Police

4.19 The police have a duty to accept reports of crime where the balance of probabilities indicates a crime has been committed, even those which are not committed in their force area.

4.20 A new Code of Conduct for Victims (issued by the cross-departmental Office for Criminal Justice Reform) reiterates the responsibilities of police when accepting and following up on reports of crime, and applies to "any person who has made an allegation to the police, or has had an allegation made on his or her behalf, that they have been directly subject to criminal conduct under the National Crime Recording Standard (NCRS)."[18] Amongst other things, the Code provides for minimum standards of service for victims of crime in England and Wales, including being kept informed of the progress of investigations and the outcomes of prosecutions.

4.21 While they are very technical aspects of how the police function, the National Crime Recording Standard (which determines the duties of police to accept reports) and the Home Office Counting Rules (which determine how those reports are categorised) are important pieces of infrastructure which govern the way we understand and use statistics to analyse crime. National crime statistics are also used to develop government policies on a wide range of issues beyond criminal justice. It is therefore vital to ensure that both the NCRS and HOCR are working effectively with regard to fraud as this will influence not just the criminal justice response, but may also inform regulatory or economic policy. Common complaints arise about the reporting process itself, and the general attitude of police forces towards fraud.

4.22 There is:

- A lack of understanding by the police of exactly what constitutes fraud and how to categorise it;
- A lack of willingness by police forces to accept reports of fraud outright;
- If a fraud has occurred across force boundaries, forces have been known to not accept the report and try to send the victim on to another force.

There is often also (though by no means always):

- A perception that frauds against business are somehow "victimless";
- An attitude that victims of fraud should have done more to protect themselves;
- A pragmatic realisation that fraud is not a policing priority and so is unlikely to get investigated.
- A lack of capacity discouraging police from accepting reports.

4.23 These are only some of the complaints which have been raised with the Review during our consultations. Of course, it is very important to note that reporting and recording of fraud have been difficult to date because fraud has not been a specific criminal offence, and the police response has been affected by this.

4.24 It is also important to stress that there are many innovative police responses to the problems of reporting and sharing information on fraud, such as the creation of Operation Sterling and Fraud Alert by the Metropolitan Police, the North East Fraud Forum by Northumbria Police, and the City of London Police's Fraud Desk.

4.25 However, crime reporting for fraud is clearly sub-optimal. Putting the situation in the wider perspective of crime statistics, a recent Home Office paper notes:

"Data for general crime is valuable at all levels from local to national. It provides information to assist in a variety of matters including: deciding operational response, crime reduction initiatives, and performance by monitoring and priority setting. However, the difficulties created by trying to

apply the current counting rules to fraud has created inconsistencies between forces and under recording that not only fails to deliver the above benefits but also has the potential to corrupt the data provided for general crime. …This is further exacerbated by the low priority level of fraud investigation across England and Wales."[19]

4.26 It is clear that fraud suffers under the current crime reporting arrangements and that this is unhelpful both to police efforts to develop an intelligence led response to fraud and to victims, who are frustrated when reporting a crime.

4.27 The new Fraud Bill will, for the first time in English law, define fraud as a criminal offence. The Home Office has been working on redrawing the definitions within the counting rules, which it is hoped will enable fraud to be more accurately measured within the system.

4.28 This is a step in the right direction. Correcting the reporting rules will ease some of the difficulties faced by police when classifying fraud. However, that alone will not help overcome barriers to reporting created by the dispersed nature and low priority given by police to fraud.

4.29 A second step forward will be solving the problem of reporting fraud to multiple agencies as well as to the police, which will in turn help improve the quality and range of information available so that a better response can be formulated.

4.30 The next section will look at the role the National Intelligence Model can play in organising the information obtained from fraud reports to contribute to police and law enforcement decisions on fraud, and the final section will look into solutions to problems of fraud reporting and developing intelligence products using information from a broad range of sources.

The Role of Intelligence

4.31 The use of criminal intelligence has always been central to policing work, but the way it is managed and used has changed in response new criminal practices and developments in the law. Furthermore, the concept of 'intelligence' has evolved from primarily relating to covert sources and classified information towards the definition given by ACPO at the beginning of this chapter, which is far wider and can apply to any information which has been risk assessed.

4.32 The adoption of the National Intelligence Model (NIM) has aimed to standardise the use of criminal intelligence across England and Wales. The NIM was designed to translate information into a set of products that are used for effective decision making and so assist police in business planning and prioritisation at a number of different geographic levels and seriousness. The levels are broken down as follows:

Level 1. Local crime and disorder, including anti-social behaviour, capable of being managed by local resources.

Level 2. Cross-border issues affecting more than one BCU within a force or affecting another force or regional crime activity and usually requiring additional resources.

Level 3. Serious and organised crime usually operating on a national and international scale requiring identification by proactive means and a response primarily through targeted operations by dedicated units.[20]

4.33 Using the right information at the right time and at the right level is a crucial part of NIM. Part of the NIM process is applying qualifying criteria to define seriousness or cross border issues so that the geographic basis of the levels does not become too rigid or static. This enables the NIM to be a flexible process if applied properly.

4.34 The development of the NIM and the move towards defining ‘intelligence’ as relating to a particular process (and so product) has not, of course, removed

the need for the police to engage in work with covert sources, deal with sensitive information from witnesses, undertake surveillance and engage in what may traditionally be viewed as intelligence gathering activities. There are detailed legal requirements governing law enforcement activity in this area, and their responsibilities to the sources they use.[21] The police have well established procedures to collect and deal with this type of intelligence, and feed it, where appropriate, into the NIM and decision making process.

Informing Strategic Decision Making: Analytical Products

4.35 Making optimal use of intelligence relating to fraud depends not only on being aware of how to collect and handle this intelligence, but on how to apply it to a problem in a way which is useful.

4.36 Another important component of the NIM therefore, is its development of a set of criminal intelligence 'products' which are used for different purposes. The different types of NIM intelligence products are described in the box below. These products are the outcome of an analytical process which is an absolutely vital step in turning information into useful intelligence. This analytical function is currently carried out by law enforcement at different levels, depending on the nature of the criminality. For level 3 criminality, for example, this is the role played by SOCA and other large forces. The capacity to organise, categorise, sift, store and analyse information on fraud at a national level is not a responsibility any law enforcement organisation currently has.

NIM Intelligence Products

Strategic Assessment

The aim of the Strategic Assessment is to identify the medium to long term issues that are apparent or emerging and to determine resource, funding and communications requirements.

Tactical Assessment
The aim of the Tactical Assessment is to identify the short term issues which require attention and to monitor progress on current business in line with the Strategic Assessment

Problem profiles (for hot spots or crime types)
The purpose of the problem profile is to provide an assessment of a specific problem or series of problems which may be criminal, which may pose a threat to public safety, or which may be anti-social in content.

Target profiles (for people or groups)
A target profile is a detailed analysis of an individual or network and should contain sufficient detail to enable a targeted operation or intervention against that person or network.[22]

Handling Intelligence

4.37 The state of intelligence about fraud at different levels varies enormously, and is not least dependent on police forces being actively engaged in fraud investigations. Fraud knowledge at level 1 can be vital (and is where much intelligence collection starts and can develop into level 2) but unless matched with similar information across forces may not put into the correct context.

4.38 The NIM underlines the importance of clear information and strategic decision making. But NIM is equally focused on enabling those decisions to be made at the most appropriate level and to contribute to all levels of police work.

4.39 The NIM also enables the police to handle any problems which may arise during the collection of information and intelligence. Information and intelligence is the lifeblood that feeds the entire NIM process and must be handled effectively. Security and integrity of intelligence is paramount and intelligence databases require robust measures to protect the data held. Input and access rights must be tightly controlled and checking mechanisms need

to be embedded to ensure intelligence is handled correctly. This is most critical when information or intelligence is obtained from a Covert Human Intelligence Source (CHIS), a person providing intelligence covertly and potentially at risk. Law enforcement bodies in the UK have strict guidelines for the handling of data and the management of those supplying intelligence. Intelligence gathered on fraud in this way, either locally or nationally by law enforcement must be treated with the same level of security and concern.

4.40 Information and intelligence on fraud can sometimes be of a highly sensitive nature; either in and of itself, or through links to other types of serious criminality. Fraud has been linked to funding organised crime and terrorism. It is therefore vital the not only is information and intelligence on fraud collected but that it is handled properly.

IMPACT

4.41 The Bichard Inquiry noted that there was "still no common IT system for managing criminal intelligence" and recommended that the Home Office and PITO should work to solve this problem. The IMPACT programme is a Home Office initiative to improve the sharing of intelligence and information across the current 43 police forces. It will match information from 6 major police databases (crime, intelligence, firearms, child protection, custody and domestic violence) with all types of crime, not just fraud.

4.42 The programme will establish common standards for managing information across forces, and offer a range of services to police forces- analysis, alerts and possibly a 24/7 response capability. Current plans are only for interfacing with police organisations. All police forces should continue working to achieve compliance with the IMPACT programme, and the Review supports a proposed pilot to match known frauds from the private sector against police data sets. The results will build on similar exercises and contribute to a better understanding of the relationship between fraud and other crimes.

4.43 IMPACT is, however, primarily a facilitator for communication on an issue, and cannot provide analysis which produces intelligence products on fraud.

Level 3 Criminal Intelligence

4.44 The UK has had a national capacity to gather intelligence about particular crime types, especially serious and organised crime since 1992 in the form of the National Criminal Intelligence Service (NCIS).[23] SOCA (which came into being on 1 April 2006) has retained most of the intelligence functions of NCIS, including the responsibility of receiving and analysing Suspicious Activity Reports (see insert) and developing the strategic assessment of threats to the UK.

4.45 SOCA is designed to work on level 3 crimes, but has a wide scope to work on other crimes and with other law enforcement agencies. It will be devoting 10% of its resources to work on fraud. It is becoming apparent that organised crime is moving into fraud, including revenue fraud, and this will be a major part of the work carried out by SOCA, and other agencies such as Her Majesty's Revenue and Customs (HMRC). However, not all fraud is organised and not all fraud is serious. The mass of unreported fraud is low level. The Review therefore believes that SOCA should be one of the principle beneficiaries of improved intelligence products and reporting of fraud, but that the reporting and intelligence processing of fraud information should be performed by another law enforcement agency.

4.46 On the formation of SOCA, the NCIS intelligence database relating to cheque and plastic card fraud was transferred to the City of London Police. The City's Economic Crime Department have been working with police forces across England and Wales to re-populate the database with fraud intelligence by acting as a national point of contact. Within one month of their initiative being

launched, this exchange of information has led to 5 operations being undertaken against organised gangs involved in plastic card fraud.

The Suspicious Activity Reporting (SARs) Regime

The SARs regime is the process whereby suspicious activity that might indicate money laundering or terrorist financing (and thereby criminal or terrorist activity) is reported to law enforcement in a suspicious activity report. The regime is intended to:

- Reduce the harm caused by crime through intervention opportunities created or aided by the intelligence gained; and
- Increase knowledge and understanding of acquisitive crime, gleaned from the points at which criminal and legitimate activity interact.

The reports are sent to a central collection point where they are stored on an electronic database, whence the individual and collective intelligence value can be extracted; and any resulting intervention opportunities can be identified.

The intelligence contained in the SARs database has a wide range of customers: national and local Law Enforcement Agencies; regulators; policy-makers; as well as the reporters themselves. It can provide them with intelligence and analysis that aids their organisational objectives.

The intelligence contained in the database has potential value in relation to all acquisitive crime, whether serious and organised or low value and high volume crime.

Sir Stephen Lander's recent SARs Review concluded that the success of the regime depended, among other things, on effective communication between all participants, including the reporters, particularly through greater sharing of sensitive intelligence.

4.47 A strategic response to fraud must be informed by the widest range of information available. There is a lot of information already being collected beyond the police, and the police themselves have an important role to play in providing a service to victims of fraud. However:

- Raw information is not being collected because fraud at force level is rarely a priority;

- There is no standard mechanism for being able to allocate fraud cases to the most appropriate organisation to deal with them;

- Intelligence is not being effectively shared across police forces, let alone with other concerned parties;

- Very few police forces are engaged in developing a strategic response to fraud with partners; and

- There is no law enforcement agency tasked with developing strategic assessments of level two and three fraud or contributing to a national anti-fraud strategy.

These problems can be resolved by taking the following steps:

- Improving victim reporting arrangements so consistent reports are accepted nation-wide;

- Identifying other relevant information which is not collected by the police, but which is contained by potential partners (e.g. government departments, banks);

- Establishing principles and conditions of partnership working under a national anti-fraud strategy;

- Creating a mechanism to cross reference police and other reports according to strict criteria and quality control;

- Improving quality of police national intelligence on fraud;

- Creating analytical capacity to perform analysis of information and generate intelligence products; and

- Creating a system to distribute intelligence products to partners.

Options

4.48 There are three immediate ways of increasing our knowledge and understanding of fraud:

- Changing the Home Office Counting Rules.
- Reporting more fraud through existing systems.
- Creating a National Fraud Reporting Centre.

Changing the Home Office Counting Rules

4.49 The role of the Home Office Counting Rules (HOCR) in helping to categorise crimes, allocate them to forces and provide crime statistics for policy makers has been described in the previous 2 chapters, as have the proposals by the Home Office to update the HOCR to take into account the Fraud Bill and crime statistics received through APACS.

4.50 When looking at improving reporting of fraud, therefore, the usual mechanism would be to refine the HOCR and leave current systems and structures in place. However, this suffers from a number of problems:

- Changing the HOCR may make it clearer what should be categorised as fraud, and even perhaps to which force frauds with multiple instances (e.g. credit card fraud) should be allocated.

- But it will not resolve police reluctance to accept report of fraud, nor will the HOCR be able to ensure that fraud reports are analysed or cross referenced in an optimal manner.

- There will remain an analytical deficit when it comes to fraud information and the generation of intelligence products.

- It will also not affect organisations outside the police service, nor will it offer the public an improved police response to fraud.

For these reasons, changes to the HOCR must be welcomed, but are just one step to creating a better understanding of fraud which can contribute to a strategic response.

Reporting More Fraud through Existing Systems

4.51 As also discussed in this and previous chapters, there are systems in place which businesses and the public sector use to share information on reported frauds (such as CIFAS or FINNET). There is potential to expand these systems further to share more reports of fraud, for example, between the public and the private sector. This would increase the pool of reports available for analysis and provide some initial indicators of the prevalence of fraud which could inform business decisions.

4.52 Furthermore, there are developments in some industries to pool information to prevent fraud, for example the insurance industry. These types of exercises are attractive as they offer a mechanism to manage large volumes of information but also undertake analysis to identify frauds. The products of these systems could feed, in a structured way, into a tactical response to fraud through the MACG.

4.53 But there are some shortcomings to such a system:

- There is little analytical capability currently attached to reporting mechanisms; ambiguity over what type of intelligence products they would be able to produce, and who would have access to them;

- There are a number of different analytical and information handling techniques being employed which are not always to a consistently high standard;

- These reporting systems may improve business and/or public sector reporting but they would not solve the problems currently facing victims when trying to report to the police;

- There would be no automatic capacity to pass on analytical products or information to the police, and no link to criminal intelligence; therefore there would be no capacity to inform an intelligence led response.

- Governance, security and audit arrangements would have to be carefully scrutinised so that individual rights and transparency were preserved.

4.54 The Fraud Review therefore believes that while existing systems can contribute to a better understanding of fraud, and can be useful partners within a strategic framework, they will not be able to fulfil the role designated to the police to accept crime reports and to engage in analysis to shape an overarching response for law enforcement and partners.

Create a National Fraud Reporting Centre

4.55 The Fraud Review has explored the option of creating a 'National Fraud Reporting Centre' (NFRC) which will accept reports of fraud from victims across England, Wales and Northern Ireland, and other sources. A National Fraud Reporting Centre would have a certain range of functions and responsibilities. It would:

- Accept crime reports of fraud from across England, Wales and Northern Ireland and relieve police of the burden of accepting reports of fraud;

- Provide a repository for quality controlled reports from other organisations;

- Provide a service to victims by accepting reports of fraud, and fulfil Code of Conduct requirements,

- Contribute through accurate crime reporting to the overall measurement of the scale and nature of fraud in England, Wales and Northern Ireland;

- Provide a service to law enforcement by allocating frauds to the most appropriate body for action on the basis of *criteria agreed with those forces*;

- Provide analytical services to identify trends, patterns and modus operandi;

- Be linked to an intelligence database and have capacity to provide NIM compliant assessments for investigation or proactive targeting by law enforcement and partners;

- Have clear accountability through law enforcement.

4.56 The Fraud Review believes the NFRC offers the optimal range of functionality desired to improve knowledge and understanding of fraud. The following table represents the functions each option would be able to provide.

Table 1: Functionality of Different Options for Improving Reporting Fraud

Functions	HOCR	Existing Systems	NFRC
Accept Police reports of fraud from victims	•	O	•
Accept reports of known fraud from Government Departments	O	O	•
Accept reports of known fraud from businesses	O	•	•
Conform to Home Office Counting Rules and NCRS	•	O	•
Able to allocate cases to police and partners for follow up	•	O	•
Able to perform analysis on reported frauds (trends etc.)	O	O	•
Receive and secure intelligence on fraud	O*	O	•
Cross reference reports and intelligence to produce 'rich' assessments	O	O	•

(* The information would, technically, be held by many different police forces and would not be a product or function of the change in the HOCR.)

How would the NFRC work?

4.57 The NFRC would accept reports of fraud from victims. It could similarly accept reports of fraud from business. It would analyse those reports of fraud, and direct them to police forces on the basis of criteria agreed with those forces. The NFRC should work with industry and other organizations (e.g. DCPCU) to manage and cross reference large volumes of fraud reports. Each stage will be explained in more detail below.

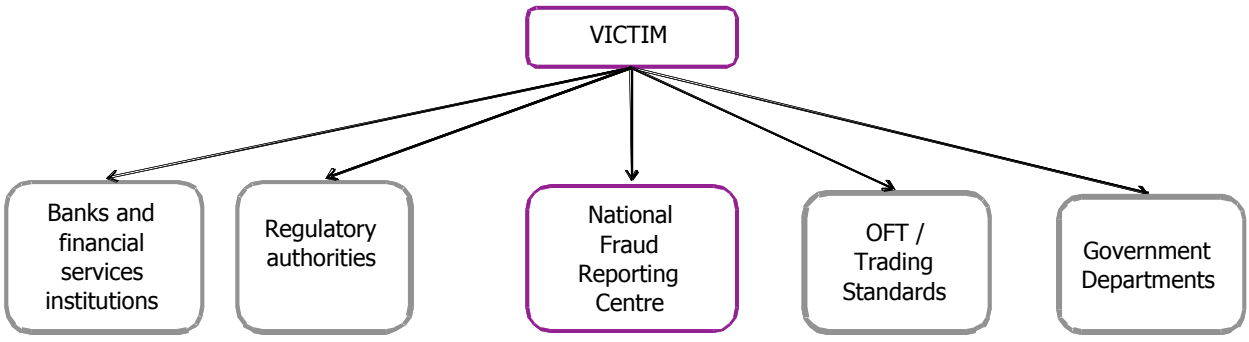
Accepting Reports from Victims

4.58 The NFRC would resolve the problems of accepting police reports detailed above by taking all reports of fraud from England, Wales and Northern Ireland. Victims would be able to contact the centre by telephone or reporting online.

4.59 The acceptance criteria for reports would be based on definitions of fraud in the Fraud Bill, plus agreed offences under other legislation (e.g. Companies Act offences). Where existing reporting arrangements exist for the police, (e.g. the Metropolitan Police's Fraud Alert) these should be incorporated into the NFRC.

4.60 Where existing reporting arrangements exist outside the police, the NFRC should work in partnership with these organisations (e.g. OFT's Scambusters or DWP's fraud hotlines) to ensure that double reporting was kept to a minimum. Victims reporting to the NFRC would be given a crime number and the crimes recorded under HOCR and NCRS.

Figure 2. NFRC, Victims Reporting.



4.61 Improving the accessibility of reporting fraud is designed to better capture known frauds, as discussed in Chapter 2. It is anticipated that this, and the Fraud Bill, will lead to an increase in reports of fraud. Expectations must carefully be managed on two fronts:

- Recording fraud properly is an improvement on the current situation, and increased reporting does not necessarily mean fraud is worse now than in the past; and
- Reporting a fraud will not necessarily result in an individual investigation – but it will contribute to a better overall response to fraud.

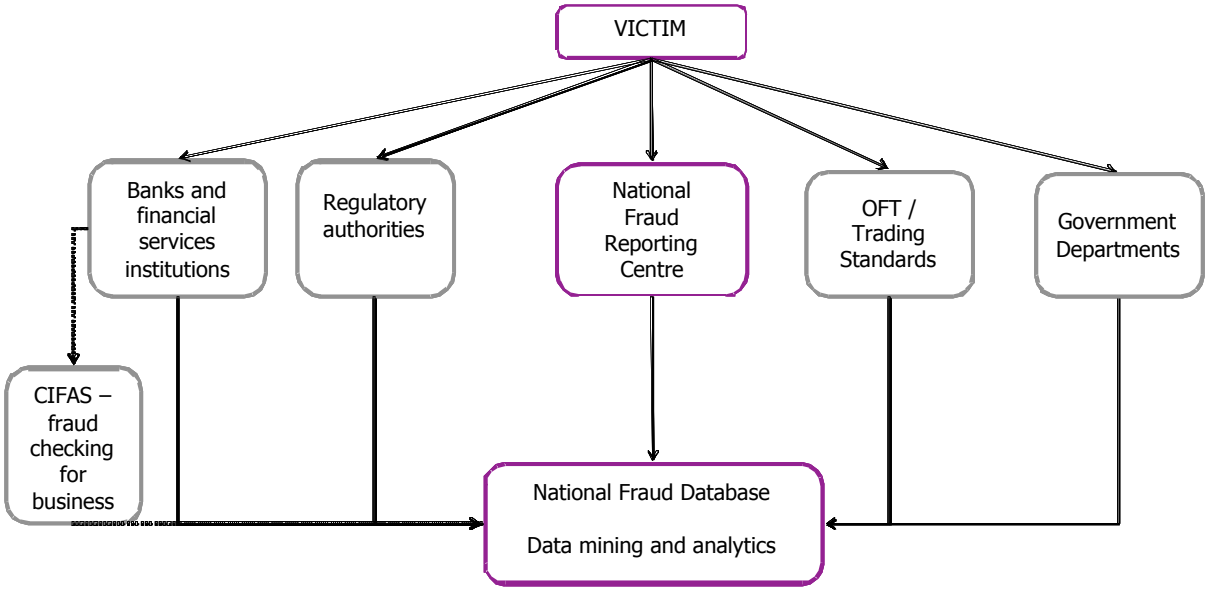
Accepting Reports from Organizations

4.62 As well as accepting reports of fraud from victims, the NFRC should be able to accept volume reporting of frauds from other organisations. These could include government departments and businesses, such as banks.

4.63 All reports would have to be 'quality controlled'; i.e. contributing organisations would have to make reports to an agreed standard and contain a comparable set of basic information in order to make the report useful. Only organisations which had controls in place to ensure the integrity of data, and met agreed standards would be allowed to make such reports. This will not only help the right information to be identified, but will help increase trust across partners.

4.64 There are similarities with the SARs regime, but also important differences. Fraud reporting would come directly from victims, and cover a large range of crime types which would fall outside the definition of 'serious and organised'. Co-operation with the NFRC would also be voluntary, whereas anti-money laundering and terrorist financing regimes are statutory obligations.[24]

Figure 3. NFRC, Business Reporting.



Analysing Reports of Fraud

4.65 It is vital that the NFRC has access to an analytical capacity which it can apply to the raw information reported to it. This will produce the intelligence products and cross reference with crime reports.

4.66 Once categorised and accepted, reports of fraud can be automatically analysed using sophisticated software available today. Programmes exist which can identify volumes and patterns of fraud; reveal links and networks; show trends, and enable specific reports and cases to be developed for further investigation. These will be used to form the basis of intelligence products and packages for onward transmission to partners.

4.67 As the NFRC will also accept reports of known frauds from business and government organisations, reports would be able to be checked across a much larger set of data and yield matches across sectors. Analysis of these matches would enable the NFRC to identify potential patterns of fraud against the public and the private sectors either by victim, by type of fraud (where a similar modus operandi exist), or by perpetrator. In time, this analysis will contribute to better prevention, detection and deterrence of fraud and to best practice in these fields.

4.68 Where necessary, reports can also be cross referenced with the police intelligence. The precise relationship between the NFRC, its information and when it should be linked to police intelligence must be clearly defined because of the sensitivities of using police intelligence. Placing the NFRC within a law enforcement environment will be vital to help manage those sensitivities.

4.69 When analysis identifies frauds, the law enforcement agency running the NFRC should be able to use functionality provided by the IMPACT programme to cross reference those reports with other crime reports. This functionality could also work in the reverse for law enforcement to cross reference other crime with fraud. Our understanding of patterns of criminality will be enhanced by this analysis.

4.70 Finally, the NFRC would also be able identify those frauds which are not related to other frauds, and allocate these as is appropriate for follow up. Its capacity to identify non related frauds will improve over time; the larger the number of incidents which have been reported, the easier it will be to cross reference individual reports to identify relationships with other frauds. The NFRC should be able to identify any links, or their absence, very quickly.

4.71 It is hoped that the NFRC could provide a responsive service to users. Intelligence products could be requested, but the list below presents an example of how certain products might be distributed:

a) Strategic assessments for the National Fraud Strategic Authority and to contribute to the UK Threat Assessment (UKTA);
b) Tactical assessments for partners / law enforcement;
c) Problem profiles for partners / law enforcement;
d) Target profiles for law enforcement.

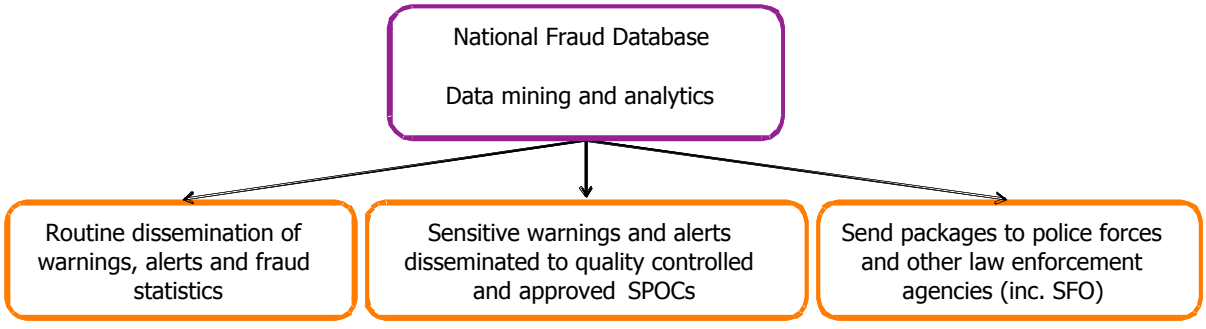
'Fool proofing' mechanisms can be built into the information management processes to update records or re-allocate cases if more reports and evidence emerge over time.[25]

4.72 There are already initiatives within some sectors to perform this type of analytical role for example, the Insurance Fraud Bureau (IFB) which has been established by the insurance sector to tackle the growing threat of organised fraud rings targeting insurance. The comparative advantage of the NFRC would lie in being able to perform these functions across sectors and traditional organisational divides, and offer the security of being within a highly regulated and accountable structure.

Distribution of Cases to Forces and Partner Organisations

4.73 On the basis of this analysis the NFRC would send unrelated level 1 frauds to local forces for follow up as they determined fit. It would also be able to send packages relating to level 2 and 3 frauds which can be sent on to partner forces (including SOCA) as appropriate.

Figure 4. NFRC, Packages and Warnings



4.74 The distribution of packages to appropriate forces is a key function of the NFRC, just as tasking and co-ordination is a key function of the National Intelligence Model. However, allocation of NFRC cases would not remove the capacity of forces or partners to prioritise their own work. The criteria for

onward allocation need to be agreed with partner organisations and reviewed to ensure it was meeting their needs.

4.75 There is a difference between reported crime and performance measures on which police forces are evaluated. It is not envisaged that the NFRC would have any role in monitoring fraud performance of police forces, as this is not its function.

4.76 Detailed partnership agreements would be needed between the NFRC and police forces, departments, agencies and other organisations to ensure consistency of engagement with the NFRC, integrity of data handling to satisfy Data Protection Act and other legal requirements, and provision of feedback to ensure the NFRC could gauge its own efficiency in performing its agreed functions.

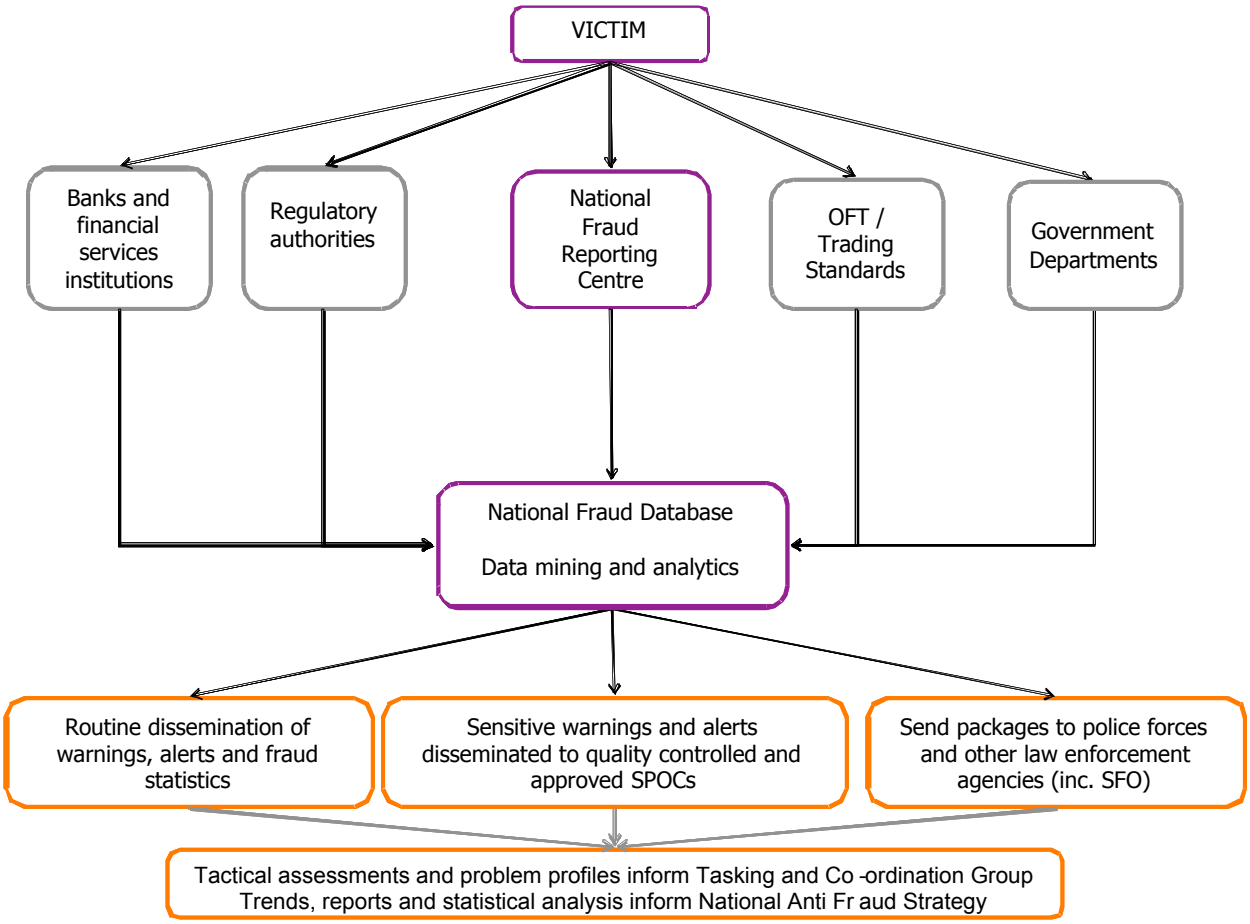
4.77 The NFRC should follow the example set by SOCA in aiming to provide a responsive service to contributing organisations. The NFRC must learn lessons from the previous experiences of law enforcement and seek to ensure that services provided meet expectations.

Inform the Multi Agency Co-ordination Group and the National Fraud Strategic Authority

4.78 The Multi-Agency Co-ordination Group, described in chapter 3, is sub-ordinate to the National Fraud Strategic Authority and supports the development of responses to fraud by providing a forum where more operational matters can be discussed and action plans to tackle problems developed.

4.79 The NFRC should provide aggregate statistics to the measurement team within the NFSA and information on priority areas to the MACG. Membership of the group should in no way prejudice the prioritisation of cases, and can extend beyond the public sector and law enforcement.

Figure 5. The Full Cycle of Reporting Fraud and Producing Assessments



International and National Comparisons

4.80 The idea of using better reporting to inform a response is not new, and the model described above already exists (with variations) in Canada and the USA.

4.81 The Royal Canadian Mounted Police (RCMP) operate the RECOL centre (Reporting Economic Crime Online[26]) which accepts reports of fraud from across state and provincial boundaries, undertakes analysis and packages reports of fraud to send to law enforcement agencies. RECOL is soon to merge with 'Phone busters', which was established as a call centre to accept reports of consumer frauds.

4.82 The Internet Crime Complaints Centre[27] (known as 'IC3') is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Centre. It is specifically designed to accept reports of people who have been defrauded over the internet – a problem which is particularly difficult to solve with geographical reporting arrangements. IC3W provides an analytical function and informs FBI work, and is linked to the National Cyber-Forensics & Training Alliance which tackles internet and high-tech crime.

4.83 RECOL and IC3 both provide the vital link between reporting and analysis, and so are able to provide high quality intelligence products and packages to law enforcement partners.

4.84 The importance of good reporting arrangements is made even more urgent given the increasingly international nature of some types of frauds (e.g. lottery scams). RECOL estimates that roughly 40% of its reports are from people who are based in the USA, but have become victims of scams or frauds operated from within Canada.

4.85 The G8 Law Enforcement Projects Sub-Group (LEPSG), of which the UK is a part, has been discussing the best way to create fraud reporting arrangements in each country and establish co-operation agreements so that international fraud rings can be identified and frustrated. Proposals for a National Fraud Reporting Centre would enable law enforcement in the UK to co-operate directly with other national bodies to prevent fraud.

4.86 Finally, while no such centre exists in the UK to tackle fraud, a national reporting centre has recently been launched to tackle paedophilia and protect children. The Child Exploitation and Online Protection Centre (CEOP) provides a place where children can report abuse, but also provides a vital intelligence function and a single law enforcement point of contact for partner organisations, international law enforcement and victims. This model shows that it is possible to establish such operations in the UK and it is feasible to do so.

Conclusions

4.87 Law enforcement and those who suffer from fraud cannot solve the problem by only maintaining reactive investigations. Even if fraud was a police priority (which it is not), the capacity to engage in reactive investigations is naturally limited. Intelligence led policing, aiming for a strategic solution, is therefore the recommended course of action, and is compatible with the national anti-fraud strategy being recommended by the Review. For law enforcement this means having:

- Access to accurate information and intelligence on fraud;
- Systems and processes in place to manage information and intelligence;
- Systems and processes in place to inform decision making by the appropriate bodies.

4.88 Law enforcement currently has processes to manage information and intelligence but does not have access to complete and accurate information and intelligence on fraud, without which, they cannot properly inform decision making or support action by appropriate bodies.

4.89 It is appropriate that a law enforcement agency take on the role of increased reporting and analysis:

- To ensure law enforcement fulfils its duty of care to victims and those supplying information;
- To ensure governance arrangements are publicly accountable;
- To ensure the continued existence of an ethical framework for data sharing; and
- To ensure prosecutions can be taken forward effectively.

Recommendations

4.90 A National Fraud Reporting Centre (NFRC) should be established for England and Wales, with capacity to link to domestic and international partners.

4.91 The NFRC should accountable through the National Lead (Police) Force (see Rec 37) and jointly staffed by police officers and civilians. It should have a defined relationship with the NFSA and MACG.

4.92 The NFRC should have the capacity to accept crime reports from victims according to the Home Office Counting Rules (HOCR) and the National Crime Reporting Statistics (NCRS). It should be able to take or including businesses and Government departments, Regulators, etc) according

4.93 The NFRC should work with police forces to agree criteria for screening and allocation of cases to forces. These criteria should be reviewed on a regular basis (e.g. annual or bi-annual).

4.94 The NFRC should be compatible with the IMPACT programme and searchable by police forces, and its analytical services responsive to police needs.

4.95 The NFRC should identify trusted partners in different sectors and establish working relationships with them to identify how information on known fraudsters can be shared efficiently to prevent and detect fraud.

4.96 The NFRC should analyse reports to provide strategic, tactical and other assessments to the police and partner organisations. Strategic assessment would pass to the NFSA and inform the United Kingdom Threat Assessment (UKTA). Tactical assessments would inform an operational response.

CHAPTER 5 DATA SHARING

5 Introduction

5.1 This chapter will look at barriers to data sharing and suggests that existing legal powers to share data should be better used and understood and that where necessary changes to legislative gateways should be considered to share more information for the purposes of preventing and detecting crime. This data sharing should, however, take place in a properly structured, accountable and auditable manner in order to balance the privacy rights of individuals. Two examples of the scope for improving data sharing are explored; the National Fraud Initiative by the Audit Commission; increasing access to deceased data. The IMPACT programme being undertaken by the police has already been discussed in chapter four, but is an initiative which can increase data sharing within the police.

Problem

5.2 In the previous chapter the Review discussed proposals to develop better information sharing to prevent fraud, and to allow for proactive and preventative work to be undertaken to reduce vulnerability to fraud in the long term. At the heart of these proposals lies the principle that sharing the right information with the right people can improve the quality of response to a particular problem. The right information may be spread across a number of different organisations. This chapter will address some of the considerations surrounding increased data sharing, and how this can be done in a way which both protects the individual's right to privacy, but balances that against the public interest in fighting crime.

5.3 There are a large number of public sector bodies, which, in the course of performing their duties, acquire information from people who use their services. Local authorities, Jobcentre Plus offices, revenue collecting agencies, driving licence and passport agencies, police and courts all collect information in order to perform their functions. Clearly, not all of these organisations collect this

information in order to prevent or detect crime, but the information may be useful for these purposes nonetheless.

5.4 Furthermore, many of these public bodies are vulnerable to fraud. Fraud against the public sector has a direct impact upon the provision of public services to the citizen; whether it is by taking money away from legitimate claimants; avoiding paying it in tax in the first place or by promising services which are then not delivered. The information collected in the course of their duties can therefore be legitimately used to tackle fraud against the organisation.

5.5 But as fraudsters will often target any weak link, they will often commit fraud against many different departments, agencies or businesses at the same time. Alone, bodies can take actions to strengthen their anti-fraud measures and prevent some attacks using the information they have at hand. But by sharing information on known frauds between bodies, the wider extent of criminality be revealed, investigated and prosecuted, and frauds against other public and private sector organisations can be prevented.

5.6 When fraudsters have been identified, sharing personal details such as names, addresses or dates of birth is necessary for the purposes of investigating, preventing and detecting crime, primarily because this is the only information which will be comparable across many different types of organisation. This is possible under the Data Protection Act 1998 (DPA). But given public concerns over this being misused, it is paramount that information used to tackle fraud is shared in a structured and accountable way. Increased data sharing to combat crime should be balanced by increased penalties for those who deliberately misuse data to perpetrate crime and fraud.

5.7 Increasing the efficiency of fraud prevention by increasing data-sharing means removing barriers to areas where data sharing can be shown to add value and prevent crime. Fraud is such an area. It will not mean that data will be shared where no clear crime prevention or business case exists.

5.8 Sharing anonymous trend information or statistics (e.g. fraud losses) is an important part of fraud prevention as information relating to trends and occurrence etc helps develop an evidence based solution. But it is not currently done as much as it could be, even though it presents less of a challenge to privacy (because it is by its nature abstract and non sensitive information).

5.9 There are a large number of databases which retain information which could be of used to identify patterns of fraud or known fraudsters. When fraud is identified within one dataset it is possible to highlight frauds which may not yet have come to light, or to confirm patterns of fraud against different victims if these results can be shared with other data sets.

5.10 There are more than thirty projects currently underway with the aim of increasing data sharing in the public sector.[28] The Government has established a Cabinet Committee (MISC31) which has the role of developing a data sharing strategy for Government with a view to improving service delivery. While this is also clearly wider than fraud or crime prevention, MISC 31 should note the recommendations of this Review.

Potential Savings

5.11 Data matching has already been seen to identify millions of pounds in losses to the public sector. The National Fraud Initiative (NFI) run by the Audit Commission has identified £111million of savings in 2004/5. This information can prevent repeat offences, help recoup costs and decrease vulnerability to future frauds. Using data to identify and prevent fraud is also taking place in the private sector. The insurance industry is investing money in an industry database to identify claimant fraud. They have estimated likely savings of at least £50million per annum.[29]

5.12 Identifying fraud is only the first step to fighting it. This information can be used (as discussed in the chapter on fraud reporting) to prevent future potential fraud by recognising fraudulent applications for loans, for example; to identify frauds which have already taken place, and allow action to recoup costs and/or take

prosecutions; and to show trends and new types of fraud which will allow preventative action to be taken.

5.13 Public organisations are not always under an explicit duty to assist in the prevention or detection of crime,[30] which will often negatively affect decisions on funding anti-fraud systems. Some government departments are well equipped to deal with the threat from fraud (e.g. DWP) others less so (e.g. local authorities). This means the response is patchy and inconsistent and that economies of scale cannot be exploited when tackling fraud.

5.14 Even where tackling fraud and preventing crime may be considered to be a core function of a public body (e.g. the police) funding arrangements can still present problems in for national solutions; a point clearly made by the Bichard Inquiry in reference to the development of national police IT systems.[31]

5.15 The Review understands that investment in anti-fraud systems and data sharing must be proven. However, with potential savings and returns comparable to the IFB or NFI, there should be a cross government commitment to support data sharing initiatives in the wider public interest.

5.16 In the private sector, it is clearly the responsibility of each business to decide whether it wants to invest in fraud prevention or not, and data sharing is one such investment. However, there are persuasive economic arguments which support putting in place both anti-fraud systems, and that information exchange is not a threat to competitiveness. The insurance industry has demonstrated precisely this by pooling its claims data and identifying fraud across a number of businesses.

Protecting the Integrity of Data

Data sharing should always:

- Use relevant and accurate information.
- Process data in an agreed and auditable manner.

- Protect data.

This will help ensure:

- The effectiveness of action taken on the basis of information shared.
- Ensure data is not shared where there is no need.
- Protect against data being stolen or misused.

5.17 Ensuring that data is accurate and stored correctly are core provisions of the Data Protection Act. Government and public authorities must endeavour that all data kept by them is accurate and up to date. In addition to being a core responsibility of the DPA, regular checking of the accuracy of data can help reduce the risk of fraud and error.

5.18 The risks to personal information being stolen and misused – from departments, banks, or other organisations are increasing. Organised crime is known to be targeting call centre employees for access to data, and insider fraud is beginning to be recognised as a serious problem.[32]

5.19 The US has federal and some state legislation which criminalises identity theft.[33] Firms are required to notify victims of breaches of their privacy, and in some states (notably California), are required to publicly declare the theft of personal details. This has not only meant that consumers are made aware much more quickly of any potential breaches of their privacy, but official and non-official statistics of data losses are kept. Figures from the US Federal Trade Commission show "that 4.6 per cent of the adult population aged 18 and over, or nearly 10 million people, had been a victim of identity theft in 2002."[34]

5.20 A recent report by the Information Commissioner[35] recommends that maximum sanctions for the wilful misuse of data under Section 55 of the DPA be increased from a fine to a custodial sentence. The Review supports increased sanctions in cases where data is obtained illegally and wilfully or recklessly misused as the theft of data is a step to committing fraud. The Department for Constitutional

Affairs should work with the proposed National Fraud Strategic Authority to detail best practice for sharing information to prevent fraud.

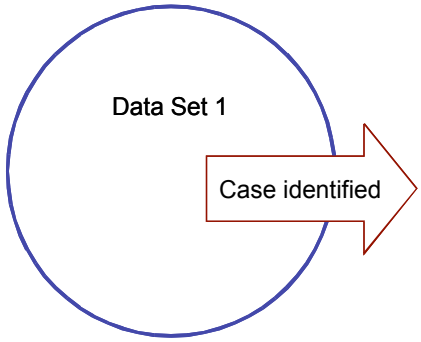
5.21 But the Government must endeavour to make sure those increased sanctions do not create a perverse incentive for organisations not to share data at all, and to balance the requirements on organisations to protect their data with their capacity to share that data to prevent crime. Given the climate of caution which currently applies to the Data Protection Act, standing alone, and without proper explanation and contextualisation, this amendment would, the Review thinks, risk reinforcing current operating practices, which we have found are restrictive. This work should be informed by consultation with the Information Commissioner.

Ways of Identifying and Sharing Data on Fraud

5.22 The previous chapter examined how reporting fraud can be improved, and this chapter will clarify some of the mechanisms for identifying fraud and how those mechanisms can improve understanding of fraud. These have been represented by diagrams to ease understanding.[36]

5.23 Fraud can be identified on an individual basis. A suspected fraudster is identified (by person in a bank, or in a government department for example) and information surrounding that case is then pursued in the course of an investigation. Some of the provisions of the Data Protection Act (including the second data protection principle and the right of subject access) do not apply where this occurs under Section 29 of the DPA.

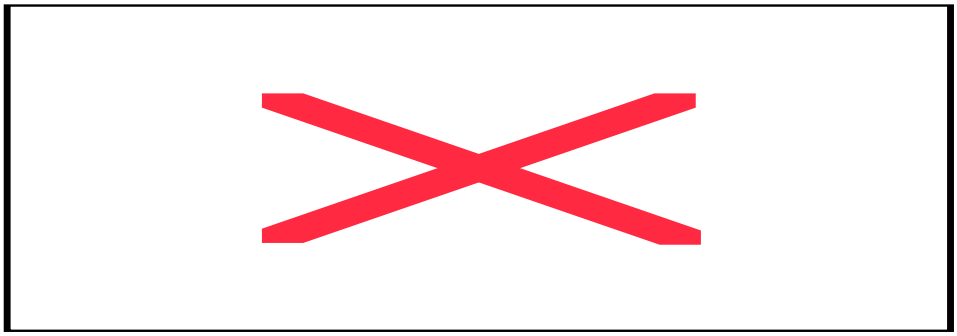
Figure 1. Case By Case Identification



5.24 However, not all frauds will be identified this way, partly because of the sheer volume of cases which happen, and the capacity of staff to identify them.

5.25 The second commonly used method for exposing fraud is by data matching. This is where two separate data sets with comparable information (i.e. both contain the same types of information, for example names) are cross referenced to produce matches. These data sets would typically be for mutually exclusive purposes which can reveal where entitlements are being incorrectly granted; e.g. pension claims and deceased data. This method employs bulk data sharing to match whole data sets.

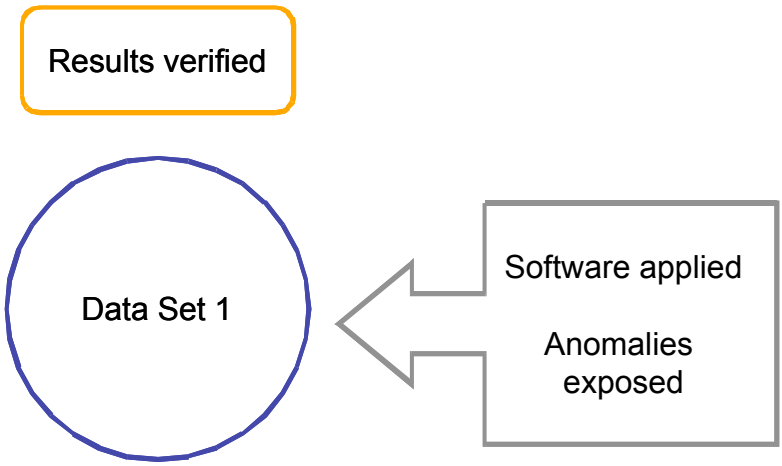
Figure 2. Data Matching



5.26 While data matching enables comparative data to be matched, exposing fraud depends on comparing the right data sets. Furthermore, it only shows basic links between data types and does not automatically identify networks or patterns of fraud.

5.27 Data mining uses more advanced software to analyse data in a number of ways. It can be used within data sets to expose fraud, and is particularly useful when there are many variables within a data set or the sheer volume of data means that automated analysis is necessary. For example, banks use software to identify unusual spending patterns on bank accounts, despite having millions of transactions every day, and possibly hundreds on each account.

Figure 3. Data Mining



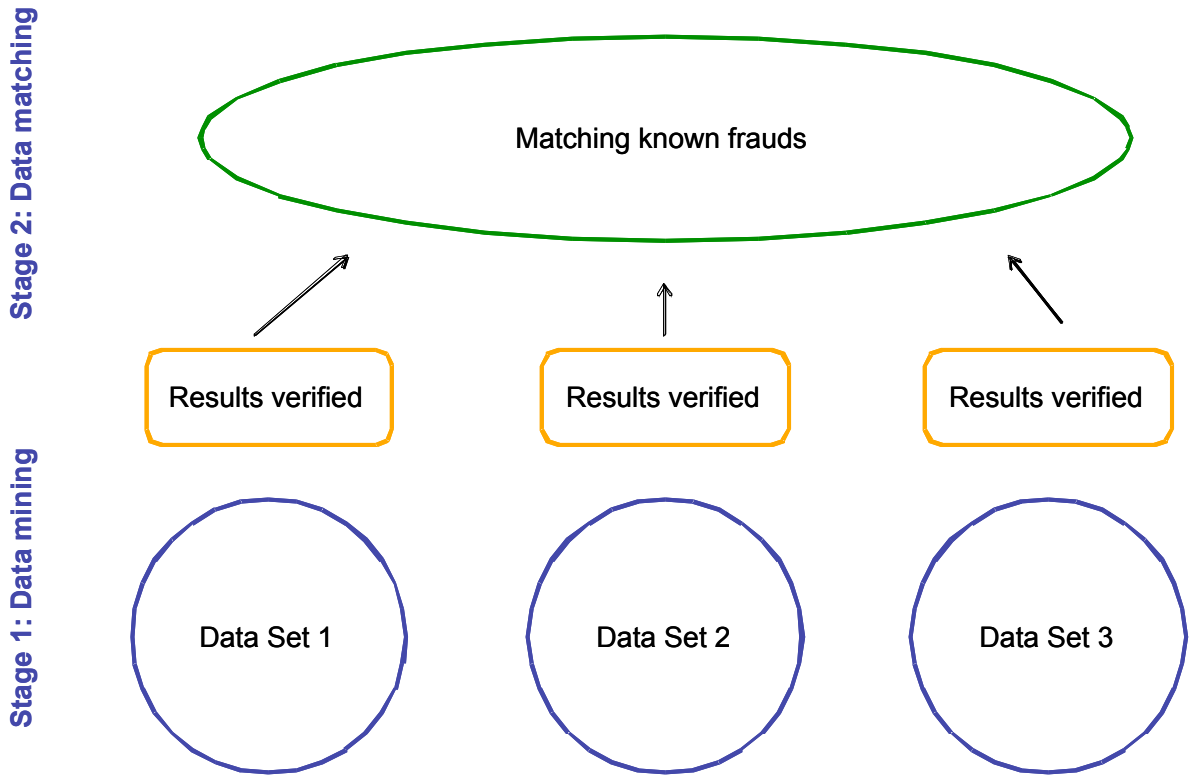
5.28 It is possible to data mine across data sets, particularly where organisations have merged but are performing the same tasks (e.g. insurance companies) with those data sets.

5.29 Finally, it is possible to use a combination of the two methods to search for, identify and refine possible frauds across different data sets. One possible suggestion is that each organisation can data mine its own data to identify frauds, and verify their status as such. These reports can then be matched to expose links to other organisations and patterns of criminality (see Figure 4).

5.30 Reducing the number of times data is shared for the same purpose can reduce the opportunities for data to be intercepted or misused, and will increase the likelihood that systems and controls for protecting that data can be more effectively scrutinised.

5.31 The Data Protection Act is a very important piece of legislation, but one which is not clearly understood, and which is often used as an excuse for not sharing data. In reality, conflicting priorities for the department can mean that there are other overriding concerns than tackling crime; technical and cultural barriers also often emerge, but are rarely legitimate reasons for not sharing data.

Figure 4. A Combined Approach



The Data Protection Act

5.32 The DPA regulates the processing of personal data and provides a framework where data can be shared in order to protect the rights of the citizen. There is an exemption to sharing data in order to prevent or detect crime. Section 29 states that if one relevant condition of schedule 2 (and sometime also a condition of schedule 3) are met the first data protection principle does not apply to personal data processed for any of the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders; or
- The assessment or collection of any tax or duty or of any imposition of a similar nature.[37]

5.33 These, and other sections in the DPA, [38] allow a wide range of activities and data sharing for the purposes of preventing and detecting crime. Unfortunately, the extent of the reach of this exemption is subject to conflicting legal interpretations.

The main perceived problems and solutions currently facing the interpretation and efficient application of the DPA the Fraud Review has found are the principle of consent; 'case by case' decision making; and civil and criminal distinctions.

5.34 There is a lack of clarity about how far data can be re-distributed after analysis, and what legal requirements this may need from the private sector, public sector and law enforcement.

The Principle of Consent

5.35 It is a requirement of the DPA that when collecting personal information, the data controller makes clear to the individual concerned who the data controller is, and what the information will be used for. This often takes the form of a clause or statement to which the subject must agree before accessing services or goods. If the data controller does not clearly state that the information provided may be used for the purposes of crime prevention or identifying financial malpractice (inside or outside the organisation), then they may feel constrained as to how far they can use or share that data for those purposes, even though the DPA itself does not prohibit sharing information for these purposes. Even private sector organisations do not always have to rely on consent to process data: the only DPA requirement is that at least one Schedule One condition is met (indeed, the Information Commissioner's Legal Guidance on the DPA cautions against a reliance on consent where it is not absolutely necessary.[39]) Nonetheless, given the importance of sharing information to prevent crime, organisations which already do gain consent to share or process data should explore adding crime prevention to any terms of consent they already offer.

5.36 However, it is important to note that public sector organisations (including Government Departments) often do not require consent to process or share data and consent is therefore currently not routinely collected. Government Departments and public bodies are under an obligation to provide services to citizens and, unlike banks for example, cannot withhold services if consent to data processing is not given. Introducing a requirement for citizens to consent to their data being used either for specific purposes or to prevent and detect crime

by public bodies (for example, DWP) would place unreasonably and costly burdens on information management systems and create duplicate systems.

5.37 Once data has been processed and frauds identified, there is the question of what happens to that information. In order for fraud to be properly tackled and effectively managed, that information may have to be passed either back to the organisations who submitted the data in the first place or onto other bodies, for example regulators, or even the police. There is confusion amongst practitioners as to how consent allows this processed information to be distributed more widely.

'Case by Case' Evaluation

5.38 There are current limitations on the capacity of organisations to share data between each other in a more automated fashion than at present. This is because data sharing must be proportionate, and being proportionate has been interpreted so that each act of data sharing should be evaluated on an individual basis. However, multiple records at one time can massively increase the efficiency of systems to identify patterns or links between data for further analysis, and impose a lesser burden on organisations. For example, data mining can compare thousands of records and transactions and identify suspicious activity very quickly. This technique is already commonly used within data sets; banks may mine their own data sets to expose irregular credit card use.

5.39 It should be noted that 'case by case' does not mean that data sharing is restricted to information on one person or data subject. It can be done at the level of an individual operation or exercise (which may involve large numbers of individuals). As long as the operation or exercise is properly structured and conducted, and is necessary to significantly aid fraud prevention and detection, it should not breach the provisions of the DPA.

5.40 The individual is not adversely affected by the process itself, and conclusions drawn from that process can be further investigated. It is essentially, a sophisticated way of sifting huge amounts of information to expose areas where

investigating authorities should direct their efforts. Alone it does not, cannot and should not mean that services are not provided or the citizen adversely affected.

5.41 The Review believes it should be possible to put in place systems which allow cases to be automatically identified and then verified, to be shared more widely to confirm if they are linked to other frauds, as shown in figure 4 above. These automated processes should not be considered disproportionate given the volume of data (sometime millions of records) which have to be managed to identify and prevent fraud.

The Criminal/Civil Distinction

5.42 The Review has found, through talking to practitioners in both the public and private sector, that Section 29 (3) has sometimes been interpreted to apply only to criminal offences, and not frauds which are being sanctioned by civil means. If this is a common practice, it will present difficulties to organisations attempting to investigate fraudsters because it can be difficult to tell, at the start of an investigation, whether civil or criminal charges, or both, are going to be the outcome of the investigation. Departments, regulators and other bodies can pursue both criminal and civil sanctions, and fraud can lie in the grey area between civil and criminal transgressions. However, the Data Protection Act does allow data sharing if certain circumstances are met as already discussed, and this means that it may not always be necessary to rely on the crime specific exemptions within Section 29. Further circumstances are found in the Data Protection (Processing of Sensitive Personal Data) Order 2000,[40] which explains further conditions under which information can be shared. Unfortunately, these conditions are rarely applied and the default position for many organisations is to not share data at all.

Legislative Gateways

5.43 Legislative gateways regulate the exchange of information between some public bodies by allowing information to be exchanged for certain purposes. Government agencies which are established in statute have less flexibility to

share data where they not given express legislative powers to do so. Other government departments may be able to rely on common law or implied statutory powers to facilitate data sharing.[41]

5.44 Examples of gateways include:

- Section 115 of the Crime and Disorder Act 1998 enables disclosure of information to relevant authorities if they are expedient for the purposes of the act (e.g. police to local authorities).

- Social Security Administration Act 1992 sections 121E – 122 allows the transfer of information from HMRC to DWP for the purposes of preventing fraud and social security offences. It also provides the gateway which underpins the DWP Longitudinal Study – which is used for research and some limited operational purposes.

5.45 A large number of gateways exist for many different purposes and by no means do they all relate to crime prevention. The patchwork of gateways not only means that sharing information (which may be used for exactly the same purposes in one recipient as another) is limited, but that it is difficult for staff and even citizens to know what information is shared with whom. As a recent report by the Council for Science and Technology commented; "There is… a very substantial range of guidance, protocols and agreements between organisations about data-sharing arrangements in specific circumstances which often complicate rather than simplify the overall situation."[42]

5.46 There are still limitations on government organisations capacity to share information about fraud, because the gateways they have are not wide enough; do not specify the right institutions, or data sharing suddenly becomes imperative in an areas which was not envisaged by the enabling legislation.

5.47 There has been, in recent years, a tendency to favour the creation and use of legislative gateways above either implied or common law power to share data unless it is expressly prohibited by statute. Departments should rely on common

law or implied powers to share data in the first instance, and only if that is not possible look to ensuring their gateways give them the capacity to share data to prevent and detect crime.

5.48 The Serious and Organised Crime Agency has deliberately been given wide legislative gateways which enable it to proactively share data with partners for a number of reasons, and which also places the police under a duty to provide SOCA with information which may be relevant to its activities. This is a positive step forward which shows that the government has recognised that a capacity to share information should not be a hindrance when tackling crime. But it does not follow that SOCA can be a conduit for exchanging information on all types of crime, including fraud, as this would place a large burden on SOCA, and not necessarily meet the needs of those organisations who want to share more information (e.g. those which have little match with serious or organised crime).

5.49 Of course, for those departments created (and therefore limited) by statute, their capacity to share data may be limited to pursuing a set of core purposes. Acting beyond their vires could have serious legal consequences, and departments are naturally concerned that they protect their core business and reputation. This can result in data not being shared. For example, the Inland Revenue always adhered to a primary principle of confidentiality in tax matters, which took precedence over all other considerations. This meant that for a long time it did not share tax data with other investigatory agencies, which has since been remedied.

5.50 Preventing and investigating crime can be argued to be a fundamental responsibility of the public sector, it is a non-competitive issue and departments should co-operate with each other and law enforcement at all times. If this principle were more generally acknowledged, gateways could and should be realigned to facilitate data sharing to prevent, detect and investigate crime.

State of Data

5.51 There are two technical issues which lead to reluctance to share data, but both of these can be overcome if organisations are willing to invest expertise and time in them. The first is that the quality of data held is not always up to date or accurate; and the second is that this data is held on many different databases with different operating systems and types of information.

5.52 Organisations may be reluctant to share information which they suspect is not accurate. Increasing data sharing would provides a continuing incentive to maintain quality data, which in itself can result in benefits to an organisation by reducing the risk of error and fraud.

5.53 The development of new software, powerful search engines and concept recognition technology is helping to overcome difficulties previously presented by data being held in different systems and formats. The development of IT systems, organisational mergers, different business needs and so on all mean that often organisations may be working with multiple different computer systems. Enabling data to be exchanged has in the past required (and may still require) the creation of new information management systems. But technological developments do mean that it is cheaper and easier to compare information across these different systems using advance searching software and this should be explored as a way of resolving outstanding issues with technical legacies.

Public Opinion

5.54 A recent survey by the Information Commissioner revealed that preventing crime remains the public's number one concern, and protecting personal data their third priority.

Table 1. Concerns with Issues of Social Importance: Information Commissioners Survey[43]

Concerns with issues of social importance		
Concerned	**2004**	**2005**
Preventing crime	85%	88%
Improving standards in education	76%	84%
Protecting people's personal information	70%	83%
The National Health Service	78%	83%
Equal rights for everyone	69%	81%
Protecting freedom of speech	67%	80%
National security	71%	78%
Environmental issues	66%	74%

5.55 People appear to have a high degree of confidence in the Police and financial sector handling their data, but a lower degree of confidence in government departments. Tackling fraud is regularly mentioned in public surveys as one of the positive reasons for data sharing.[44]

5.56 Recent problems with incorrect data being held by government (for example, the Criminal Records Bureau), and stolen personal details being used to perpetrate tax credits fraud mean it is of paramount importance that there is confidence in the information and systems used to share that information when tackling fraud. It is essential for wider trust in government that a reputation for handling data with the highest integrity and security is maintained. Instances of fraud can be very damaging to the reputation of government departments and trust in the criminal justice system.

Options

5.57 There is a risk that failing to share data or know what information is available can lead to poorer services being offered, and in extreme cases, endanger lives. The Bichard Inquiry showed how a failure to store data correctly and to share intelligence led to serious reduction in the capacity of the police and social services to offer protection against harm.

5.58 Fraud certainly does not often have as dramatic an impact on people's lives as other violent crimes (although it can in high value cases, and suicides have occurred as a result of fraud). But when fraud occurs in high volumes it can certainly undermine public service delivery and trust in government. The Review is firmly of the opinion that increased data sharing is not only possible, but that it will yield enormous benefits. The Home Office have explored the benefits of public and private sector organisations sharing information to reduce fraud by undertaking a data matching exercise between data held on CIFAS and data held in each of the organisations DWP, DVLA, HMRC and UKPS (now Identity and Passport Service). Initial results showed a high level of matching and further investigation is ongoing to establish the relative cost and benefits to public/private sector organisations.

Current Initiatives to Improve Sharing Data

5.59 There are many example of good practice in data sharing in both the public and private sectors; the Insurance Fraud Bureau is just one of them. However, there are two major initiatives to improve data sharing which the Fraud Review supports the development of. These are:

- The National Fraud Initiative.
- Increasing access to deceased data

The National Fraud Initiative

5.60 The National Fraud Initiative is an existing programme run by the Audit Commission, but the Audit Commission would like it to be expanded. The NFI takes data from local authorities, payroll records, the NHS and other audited customers, student grants, pensions and a number of other data sets. It performs a data match between records to identify frauds, very much along the lines described earlier in the chapter but with a number of data sets. As the relevant legislation contains a statutory power to require the sharing of data, it removes many DPA uncertainties.

5.61 In 2006 the NFI has identified frauds which cost the taxpayer £111 million pounds. The frauds identified have increased significantly since the NFI started, and increased as their access to more data has also increased. The Audit Commission is seeking to extend its capacity to match data to the following areas:

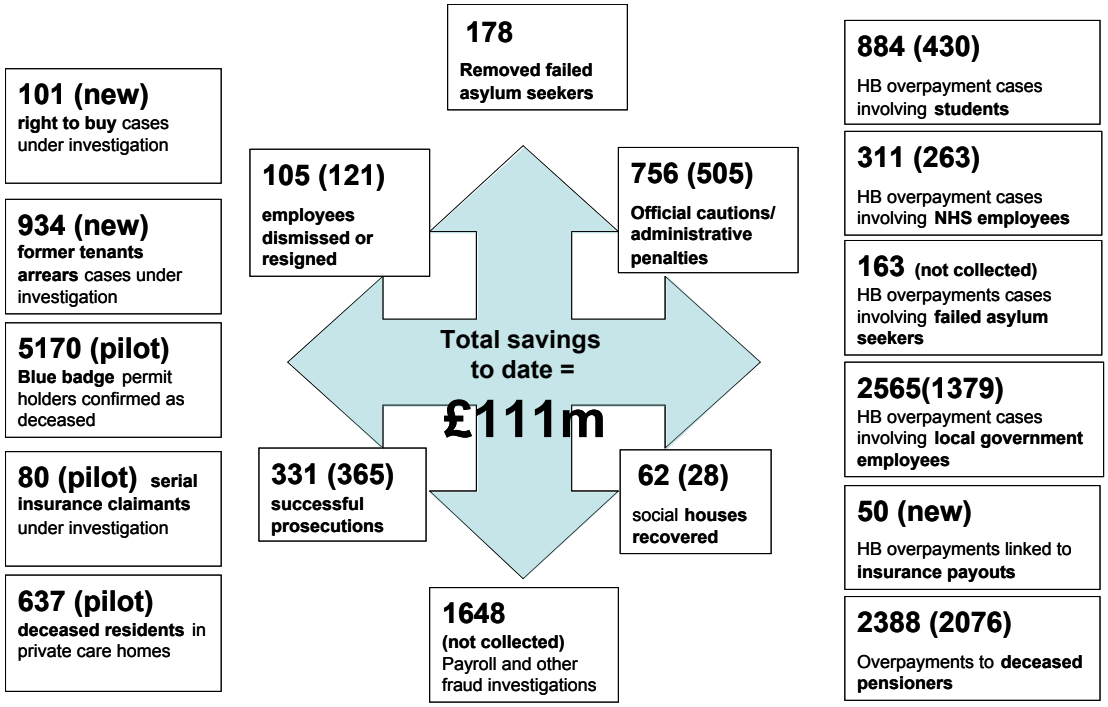
- Cross border matching.
- Mortgage records.
- Central government and private sector pension records.
- Central government and private sector payroll.
- Foundation trusts.
- Housing associations.
- Former tenants arrears.
- Outsourced services.
- Insurance.

5.62 The Audit Commission are currently seeking the extension of their capacity to match data; this may require legislative changes.

5.63 The Audit Commission has now included tackling fraud in its Best Value Indicators for public authorities but this is dependent on them using the NFI. Huge amounts of data identifying fraudsters are identified by the NFI and sent to authorities to deal with but there is often a very limited capacity in those bodies to investigate or prosecute these frauds. The Audit Commission, and other audit

bodies (the National Audit Office) should be proactively engaged in improving wider fraud prevention financial systems and controls, capacity to respond etc, and not just focus on investing effort into a reaction to fraud.

Figure 5. Frauds Identified by the National Fraud Initiative 2004/5



Increasing Access to data on deceased persons

5.64 Increasing access to data on deceased persons means increasing the speed at which information concerning the identities and details of deceased persons are transmitted to service providers in the public sector (e.g. DWP) and service providers in the private sector (e.g. banks). Fraudsters have been known to use the identities of the deceased to continue to claim benefits or services in their names. Some also use the identities of deceased people not just to continue a claim which was previously legitimate, but to perpetrate new types of fraud.

5.65 There is currently a reasonably quick turnaround between the information being transmitted from Office for National Statistics/General Registrars Office (ONS/GRO (who collate the information) to DWP, but a rather longer delay in

transmitting the same information to the private sector. This means fraud, errors in payment and bad debt all result from inefficient systems, and providing this information swiftly would result in savings – not to mention saving families from the trauma of realising a relatives details may have been misused.

5.66 Information relating to deceased persons is not restricted by the Data Protection Act. Changing the ONS vires to share this information is necessary. The Home Office are working with ONS to find a suitable legislative vehicle to enable ONS powers to share death registration information with Police, other law enforcement agencies (e.g. SOCA) and other designated public/private sector organisations for the purposes of prevention, detection, investigation or prosecution of offences. An amendment to the Police and Justice Bill was introduced at report stage to provide legislation for the Registrars General for England, Wales and Northern Ireland. Under the current timetable, Royal Assent is expected in November 2006 with the GROs working towards being able to make data available in summer 2007. The Registrar General for Scotland will have powers to release data under the Local Electoral Administration and Registration Services (Scotland) Bill which is currently before the Scottish Parliament.

Conclusions and Costs

5.67 In order to be able to tackle fraud effectively, to inform a strategic response and engage in preventative work which could save hundred of millions of pounds, data sharing on frauds must be increased. However, it must also be increased in a controlled, auditable and accountable manner which clearly protects the data and does not infringe upon the privacy rights of the individual.

5.68 The Review has explored the following issues:

- Increasing data sharing of known frauds between public bodies;
- Increasing the data sharing of known frauds between public and private bodies (who have quality controlled processes) through the analytical capacity of the NFRC, which is located within law enforcement;

- Increasing the scope of the NFI to identify frauds by increasing access to data sets; and
- Allowing access to data on deceased persons to prevent fraudulent use of their details.

Recommendations

5.69 The Cabinet Committee MISC 31 should consider the recommendations of this Review with a view to increasing data sharing to prevent fraud.

5.70 Organisations which already gain consent to share or process data should explore adding crime prevention to any terms of consent they already offer, and the Government should support them in doing so.

5.71 The Department for Constitutional Affairs (DCA) should work with the proposed National Fraud Strategic Authority to co-ordinate the development of government wide guidance on data sharing to prevent fraud. The guidance should be developed in consultation with the Information Commissioner.

5.72 Public authorities should give the common law position on data sharing primacy and where legislative gateways exist, they should be widened if necessary to increase data sharing to prevent fraud.

5.73 Matching multiple data sets should be encouraged as part of a process of pursuing suspected frauds, and the proceeds of information matching be used to pursue crime.

5.74 The remit of the National Fraud Initiative (NFI) should be widened across more public sector authorities and the Audit Commission and National Audit Office should play an active role in developing anti-fraud measures in the public sector.

5.75 Data on deceased persons should be released as quickly and efficiently as possible to the public domain.

CHAPTER 6 PREVENTING FRAUD

6 SUMMARY

"Investor protection starts with the investor … there is simply no substitute for a person's awareness and wariness."[45]

- Fraud is largely a preventable offence. It usually happens because the trust of individuals or businesses is abused: violence or coercion is seldom involved. The victim's attitude and co-operation are the keys to a successful fraud.

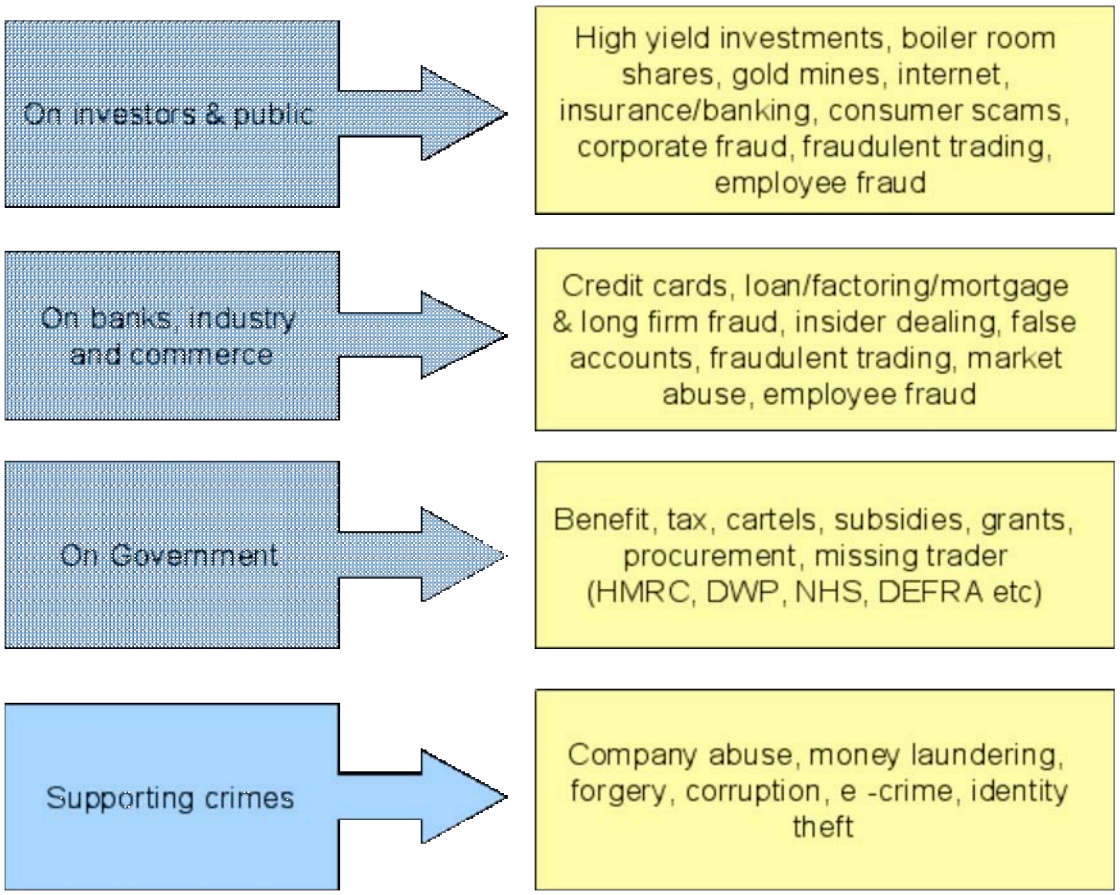
- There is some excellent work already being done to protect consumers and individual victims from fraud. It is one of the functions of the National Fraud Strategic Authority to promote awareness and best practice. This chapter draws out just how this might be done.

- The patterns and trends detected through the NFRC and other measurement exercises will, when combined with information already available from organisations such as APACS, provide a rich source of information on which preventative measures can be taken.

- Preventative action can be a success story for the consumer too; awareness campaigns have contributed to a 57% fall in domestic burglary over the past 10 years and have substantially reduced Nigerian advance fee frauds as well.

- Public authorities must protect their budgets and taxpayers money from fraud and error. To this end they should reinvigorate fraud measurement and risk assessments in their financial processes in order to better assess the scale of fraud, risks face from fraud, and reduce losses to fraud.

The Problem: Types of Fraud & Victims



6.1 The diagram above shows common 'groups' of victims and the type of fraud perpetrated upon them. It points to ways in which fraud can be reduced by increasing :

a) Individual caution

Informed and proactive consumers who are prepared to perform a number of simple checks when carrying out financial transactions are the best defence against fraud. They can be helped by having clear and accessible information available to them, and timely and well publicised warnings of fraud types.

Businesses and the public sector can benefit from warnings and information too, as they can be consumers of products. More detailed information on new frauds in their sector and crucially, how each fraud is being or has been committed can be incredibly helpful.

b) Best practice in internal controls

Business and the public sector though, can also take steps to improve the systems and controls they have in place to prevent and deter fraud. Good practice in financial controls, auditing and procurement are obvious areas where organisations, particularly large ones, need to and can protect their interests.

Awareness Raising

Case Studies from Operation Sterling

(1) Roger bid for a digital camera on an internet auction site, only to be outbid. He then received an e mail from someone purporting to be from the auction site, telling him he could still purchase the camera. Roger sent £355 via the specified money transfer company and e mailed the fraudster for details of the camera despatch. He received an automatic message saying the address did not exist. He never got his camera.

(2) A 73 year old lady entertained herself by entering competitions. She received a call informing her that she had won £195,000 and asking for cash for security, delivery and government charges. During several calls the victim was persuaded to send a total of £21,830 via a money transfer service and she had heard no more from the fraudster.

6.2 Potential victims, regulators and law enforcement all have a part to play in fraud prevention.

6.3 Raising awareness enables potential victims to protect themselves and deter fraudsters. There is no incompatibility between raising awareness and investigating fraud; indeed, increased publicity around a particular fraud type can often result in more information on cases. Information can immediately be used in training and by industry in targeting prevention efforts or designing systems. Reliable measures of impact will enable organizations to justify (or abandon) particular actions or systems.

A Strategic Success Story

Domestic burglary has fallen by 57% in 10 years[46]. Why?

- Reducing it has been one of the Home Office's principal aims since the mid 1990s.
- Robust statistics are kept on the offence by Police and Insurance companies, which have informed public awareness campaigns ("domestic burglary offences represent 10% of all recorded crime").
- Enabled resources to be precisely targeted (2001 Neighbourhood renewal: National strategy action plan).
- Partnerships have been formed and incentivised (Crime & Disorder reduction partnerships, Local Public Service Agreements).
- Action has been monitored (Crime Reduction Directors in each region).
- Targets have been set (25% reduction by 2005/6).
- Very specific actions have been identified (using the DNA database, identifying repeat offenders).
- Increased deterrent penalties including minimum custodial sentences are part of the strategy (Powers of Criminal Courts (Sentencing) Act 2000)

6.4 The OFT has a detailed strategy set out in its 2006-2007 Annual Plan. This includes the innovative "Scambusters" campaign and the Scams Enforcement Group, which involves Local Authority Trading Standards (TS) offices, public and private sector representatives and even overseas law enforcement in a "virtual" task force. The OFT is also taking over and integrating the DTI Consumer Direct service, and new EU standards[47] in consumer protection

and regulatory co-operation will give OFT and DTI an even greater opportunity for action and publicity in this sector. The OFT now offers regular training and disseminates best practice to Trading Standards Officers.

6.5 The FSA plays a dual role, as a designated consumer enforcer[48] (Enterprise Act 2002), but also as a regulator ensuring that the regulated sector manages their financial crime risks appropriately.[49]

6.6 The FSA and the OFT working together could become a very powerful force in promoting fraud awareness and prevention. The “instant” warnings issued by the FSA in May 2006 to industry (on the Cheshire Building Society scam) and to the general public (on boiler room share sales) show how effective these can be.

6.7 Government Departments can also benefit from raising awareness of the public to help prevent fraud against the State. The DWP has run a high profile campaign to encourage awareness of the impact of benefit fraud, and increase deterrence and detection. The national benefit fraud hotline received over 200,000 calls last year alone.

6.8 Existing initiatives do exist outside government and regulators though, and the recent introduction of Chip and PIN has raised consumer awareness of fraud significantly. APACS operate a public warning website called 'bank safe on line', and advice can be found from other sources. Industry associations such as the Association of British Insurers (ABI), APACS, and the British Bankers Association (BBA) have shown themselves willing to share generic fraud experiences with competitors and the general public, e.g. recent publicity given to “staged car crashes”. [50]

6.9 Regulated firms could include warnings in their literature and might be willing to include them in their own press advertisements and premises. They are almost as much the losers as the victims, who might have placed their funds in legal investments to more mutual benefit.

6.10 However, given that each type of organization reaches different sectors of the population, there is a great deal of opportunity for improving co-ordinated and targeted messages on anti-fraud themes. In particular, raising awareness of the international nature of some frauds may involve partnerships with organisations in different countries.

6.11 The “warning blitz “has proved its worth in the case of the notorious Nigerian 419 frauds. Deliberate joint efforts by the police (including providing for some years a special hotline and website) and the press have made the 419 a subject of scepticism. A number of prosecutions received good publicity and provoked some local action in Nigeria to close down PO boxes and seize accounts. A few may still fall for the scam, but there has been an appreciable reduction in incidents.

6.12 But warnings and campaigns need constant updating and refreshing. The press, though very fraud aware, need to be kept informed of frauds and their impact and the public need to be persuaded to make use of regulators’ websites and open source information to check credentials.

A Role for the NFSA

6.13 Preventive work will need to concentrate in assembling and providing (packaging) the information which the NFSA has access to, both from a NFRC and from other sources such as SARs. The NFSA is then best placed to make the maximum information accessible, including:

- Targeting messages to vulnerable business sectors, people or geographical areas;

- Identifying and providing information on best practice to solve current problems/prevent them happening again; and

- Identifying and providing links to overseas organisations and websites in the case of frauds perpetrated across borders.

6.14 This strategy was recommended in the report Improving the Response to Fraud Part 2, and there is plenty of scope for sector related or local initiatives here - such as the impressive work being done regionally by such networks as the North East Fraud Forum, though they would inevitably benefit from feeding into an overall national strategy and being able to measure their impact on fraud activity.

Preventing Frauds through good Systems and Controls in the Public Sector

6.15 Public bodies are vulnerable to internal and external fraud. Responses to both types of fraud will differ; but vulnerabilities to fraud should be better identified and then better mitigated by the public sector. The onus on preventing and detecting fraud should be supported within senior management, particularly finance and budget units of public bodies, but should also be stressed as a responsibility for all within the organisation, especially those in the front line of providing services.

- Internal Fraud. Fraud committed by staff against an organisation, can and should be controlled with good systems and controls (for example, on travel expenses) and detected either by staff or financial management systems.

- External Fraud. Fraud committed against the organisation by an outside actor, is more difficult to identify and to resolve. However, products and processes can still be 'fraud proofed' and such proofing of systems should be encouraged at the earliest stages of product or policy development.

6.16 Where a fraud risk will nonetheless continue to exist, proportionate investment should be made in identifying and responding to any fraud which does occur. For example, lottery grants awarded by the Department for Culture, Media and Sport will be inherently vulnerable to fraudulent applications, but clearly they should continue to be made, and the DCMS has taken sensible and proportionate steps to mitigate those risks.

6.17 The National Audit Office has provided a number of useful guidelines on tackling external fraud. As discuss in the measurement chapter, "assessing the loss from fraud is an important first step in developing a strategy for tackling external fraud".[51]

6.18 Once that loss is known, it must be dealt with – and these decisions often lack a clear framework for action. "A major obstacle to developing a fraud response is the absence of a clear assessment of what might constitute an acceptable level of the risk of fraud. From a purely financial point of view, a decision about the level of acceptable risk would be determined based on the scale of potential loss and the cost of preventative and detective controls."[52]

6.19 It is our view that the public sector should take a zero tolerance approach to fraud – that is, where the known losses to, and risks of, fraud outweigh the costs of preventing and detecting that fraud, then action should be taken. Public authorities who are victims of fraud have an incentive to protect their budgets and address their own weaknesses, but public money should be safeguarded from fraud.

6.20 In order to aid this process, public authorities should consider mainstreaming fraud measurement and risk assessments in financial planning, and the National Audit Office and the Audit Commission should audit public bodies on the strength of their anti-fraud controls. Many organisations have already put in place fraud management strategies, and there is a growing body of good practice. But often front line staff are not aware of fraud risks and do not feel responsible for tackling it. Examples are given to illustrate only what can be done; and perhaps copied in the public-private arena. The NHS has a sophisticated programme for raising and maintaining internal fraud awareness amongst its staff and contractors.

Public Sector Spending on Fraud

6.21 As part of the Fraud Review, research was undertaken to find out what statistics were held and produced by Government departments on losses to fraud, with a view to better informing any measurement exercise on losses and resource costs. The Review was unable to replicate this for the private sector.

6.22 This research was carried out with the help of HM Treasury (Assurance, Control and Risk Department). A questionnaire was sent to Finance Directors of all government departments with a request that they cascade to agencies and NDPBs. 111 responses were received.[53] The questionnaire is attached at Annex C. Due to time constraints, an initial analysis was undertaken, in particular looking at what losses were experienced and how losses were measured.

6.23 This initial analysis revealed that there is no standard robust methodology for evaluating losses to each department as a result of fraud. Methods of calculating losses vary greatly, which the Review concludes further weakens the ability of government to establish a clear figure of the amount of fraud lost in government departments.

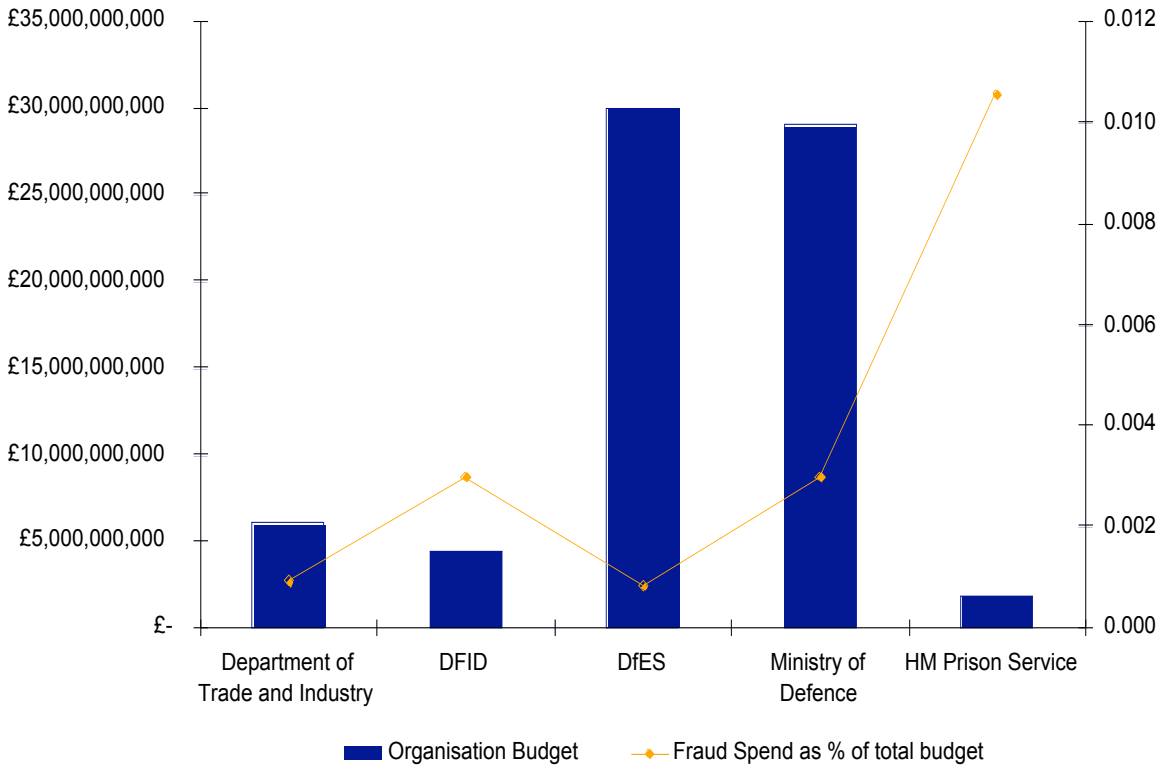
6.24 Each department was asked to identify their total budget and the risk faced from fraud. The level of risk faced by departments will, of course, vary depending on what budgets are allocated for. More than two-thirds of all types of government bodies involved in the survey have no budget for anti-fraud activities, or spend 'nil' amounts of their budget on fraud.

6.25 Approximately one in five of all respondents acknowledged that anti fraud activities are incorporated into their other budgets (for example their Internal Auditing or Professional Standards budgets) but they have no specified budget for fraud-related work or way of knowing how much they spend on this work.

6.26 The bodies that do budget gave tremendously varied figures on how much they budget for anti-fraud activities, irrelevant of the type of agency or size of

its annual budget. The graph below demonstrates this; comparing organisational budgets with amounts spent on fraud activities (where specified). Even taking into account that this does not account for different levels of risk, it is clear that there is no consistency or established approach in budgeting for anti fraud activities in UK government bodies.

Figure 1. Departmental Spend on Fraud Activities



Preventing Fraud through Systems and Controls in the Private Sector

6.27 The ICAEW and international auditing regulations set auditing standards for the industry which are designed to reflect best practice in anti-fraud systems. British industry has invested heavily in fraud prevention, in particular in the financial services sector; accounting and IT firms offer sophisticated services to this end. Internet banking and payment services have developed (and continue to develop) robust systems to counter threats. Efforts and expenditure are redoubled with every new assault.

6.28 Information enabling firms to target efforts on pernicious or high risk fraud, providing details of the methods actually used by criminals, should ensure better value for money. Industry associations are keen that their prevention work is recognised, and it is clear that they will participate enthusiastically in anti-fraud partnerships. Mutual information exchange with law enforcement as described chapter 4 can provide real benefits to consumers and businesses.

6.29 There is no UK Government appetite for the Sarbanes-Oxley route to corporate fraud prevention. But, whilst the suggested obligatory Operating and Financial Review has not found supporters; there is nothing to stop us celebrating voluntary efforts in this direction and publicising the work of those companies that choose to invest in fraud (or any crime) prevention.

The Need for a Fraud Prevention Working Group

6.30 A small team to undertake best practice and awareness raising is suggested as part of the National Fraud Strategic Authority. Obviously though, the partnerships described earlier in the chapter will be crucial in terms of co-ordinating messages with like minded actors.

Costs and Legislation

- Warnings need to be kept up to date. Regulators, Industry Associations and Law Enforcement agencies need capacity to disseminate information and warnings, or to include this responsibility in existing job descriptions. The OFT and FSA both include prevention in their current objectives and devote resources to educating and warning the public.

- Industry already fund specific campaigns or to sponsor advertisements or leaflets.

- The National Fraud Strategic Authority along with interested parties will be best placed to seek sponsorship and to place warnings, perhaps within commercial or generic advertising.

- There may be costs associated with public authorities putting in place proper systems and controls to prevent fraud and financial malpractice, or making sure systems already in place work.

Conclusions and Recommendations

The following are the conclusions and recommendations:

6.31 The NFSA and the NFRC should have a direct role in relation to:

- Devising and implementing public anti fraud campaigns and warnings, drawing on generic and case specific information provided by NFRC;

- Liaising with the press for campaigns and case publicity;

- Devising and circulating best practice and advice on systemic fraud prevention within industry and government;

- Co-ordinating and informing the anti fraud awareness training provided to industry by other regional and sectoral groups.

6.32 Public authorities should reinvigorate fraud measurement and risk assessments in their financial processes in order to better assess the scale of fraud, risks face from fraud, and reduce losses to fraud.

6.33 The National Audit Office and the Audit Commission should audit public bodies on the strength of their anti-fraud controls.

CHAPTER 7 INVESTIGATING FRAUD

7 SUMMARY

- The Interim Report noted that fraud was not a national policing priority, and documented the continuing decline in the number, scale and resources of police fraud Squads.

- The exception was the City of London Police, whose fraud squad had doubled since 2002, and had assumed the Regional Lead Force role for fraud investigations in the South East and London.

- The number of officers in police fraud squads in England and Wales has fallen from 589 in 1998 to 416 and even this resource is under threat.

- Large organizations deal with fraud in-house, and the largest frauds are investigated by the Serious Fraud Office. Apart from mass market scams, which the Office of Fair Trading and Trading Standards Service make a priority, much lower and middle ranking fraud against individuals and small businesses are largely uninvestigated.

- The Fraud Review has considered ways of improving the response to fraud through:

    - Adding fraud to the National Policing Plan
    - Increasing police capability;
    - Increasing civilian investigative capacity, and
    - Public/private partnerships.

- Regarding police capacity the review recommends:

    - The Home Secretary should consider making combating fraud a policing priority within the National Community Safety (Policing) Plan and law

enforcement agencies encouraged to develop plans which include local performance targets for fraud.

- Police fraud squad resources should, so far as possible, be ring fenced to stop the current practice in many forces of diverting them into other work as soon as the force has a pressure somewhere else.

- A National Lead Force should be established based upon the City of London Fraud Squad. It would house the National Fraud Reporting Centre and its intelligence and analytical capability. It would also be a centre of excellence for other fraud squads, disseminating best practice, giving advice on complex enquiries in other regions, and assisting with or even directing the most complex of such investigations.

- Additional to fraud squad resources, there should be appropriate capacity and capability to deal with Level 1 frauds that meet the agreed acceptance criteria and occurring at a local Borough Command Unit level.

- If appropriate in the light of police reform, a number of Regional Support Centres (RSCs) comprising specialist resources like surveillance and technical services should be established to provide fraud squads with such facilities when needed to support an investigation. At present, fraud squads are often regarded as a low priority call on these resources.

- These arrangements to be subject to a "thematic" inspection by Her Majesty's Inspectorate of Justice, Community Safety and Custody within two years of their establishment.

- Regarding civilian capacity the Review recommends:

- There is scope for increasing the contribution civilians make to investigating fraud as a supplement to, not as a substitute for, police capacity.

- Most fraud is already investigated by civilians. The development of "accredited investigators" would increase the long term pool of investigators and increase co-operation between police and other organisations.

- Police forces should consider the scope for employing civilians, after appropriate training, as investigators as well as support staff within police fraud squads.

- There is scope for greater public/private partnership working in investigating fraud, either through joint units or joint investigations involving "accredited investigators". A national programme for accrediting investigators based on certifying fraud training courses and expanding existing accreditation services should be implemented.

Introduction

7.1 The Interim Report summarised the existing position on fraud investigations as follows:

a) Reporting and recording of fraud is bureaucratic, inconsistent and not conducive to accurate measurement.

b) Police investigative resources are small and declining and often diverted to other "higher priority" tasks.

c) Within police 'Economic Crime' departments, which is where many fraud squads are located, the allocation of resources is being prioritised towards Financial Intelligence and Money Laundering and away from fraud.

d) By comparison, investigations into frauds committed against some areas of the public sector (NHS, DWP, HMRC) are well resourced.

e) Other public sector bodies investigate some frauds against business and the personal sector (e.g. FSA, DTI, Trading Standards Officers) but have limited scope and powers.

f) Most large financial institutions have internal investigative capacity which is largely directed at disciplining staff who commit fraud and seeking civil redress where this is worthwhile. They seldom involve the police when they discover fraud.

g) SFO investigates serious and complex fraud but its caseload is limited to 60-70 cases at any one time.

h) SOCA will have the capacity to investigate serious and organised crimes, including those involving fraud.

i) A lot of fraud, especially mid and lower level against the private sector is not investigated.

7.2 To address these problems two projects were established in the second phase of the Review to examine ways of improving police and civilian capacity to investigate fraud, including through public/private partnerships. One possibility considered was that boosting civilian capacity might, to some extent, replace police investigative capacity so that fraud investigations were increasingly carried out by civilians and even that police fraud squads would in future predominately consist of civilian investigators. As the rest of the chapter explains, this did not survive scrutiny and the recommendations made for increasing civilian capacity are in addition to, not instead of, improving police capacity.

Police Fraud Squads

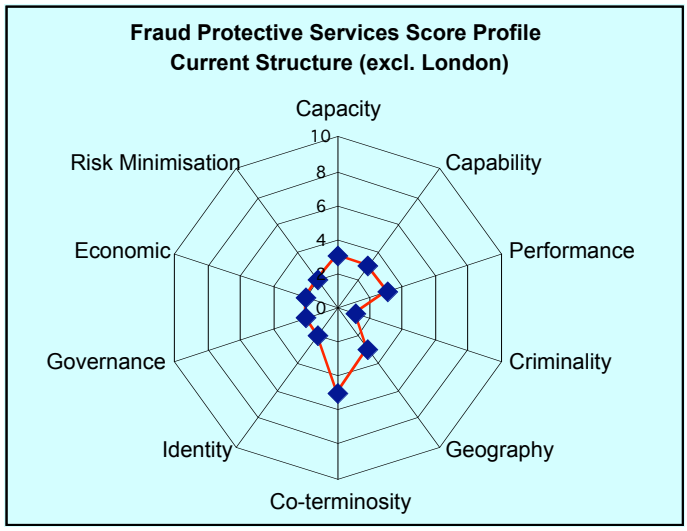
The Problem

7.3 The Fraud Review Team approached its consideration of the police response to fraud by using the methodology recommended by HMIC for assessing the strengths and weaknesses of police forces as part of the police restructuring exercise. This involves scoring the quality of protective services (fraud is a protective service) against ten criteria on a scale of 1-10 and showing the outcome in a spider diagram. The scoring was done initially by an Expert Panel, consisting of police officers currently working in Fraud Squads and carrying out fraud investigations, and then reviewed by an Executive Panel of representatives from public and private sector organizations who were vulnerable to fraud and could be regarded as the "customers".

7.4 Scoring was done separately for the City of London Police (which has the largest Fraud Squad in England and Wales) and the remaining 42 police forces in England and Wales, some of which have no dedicated Fraud Squad at all. In these forces frauds are either investigated by the Criminal Investigations at Borough Command Unit level or, often, not investigated at all. The results of the scoring are set out below.

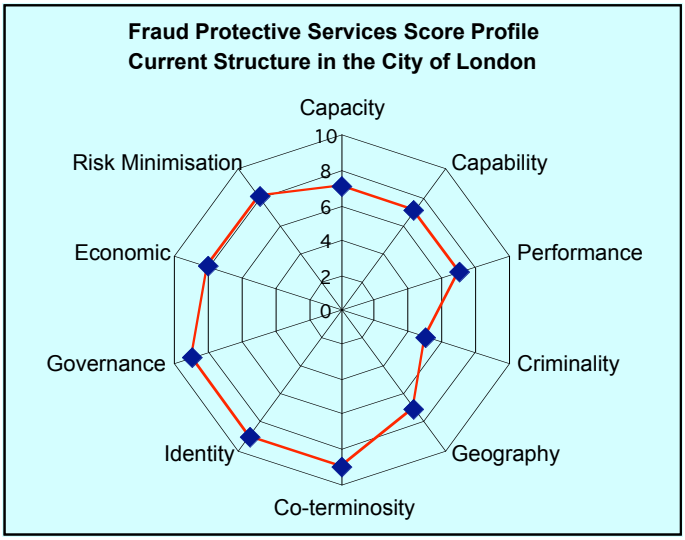
Police Forces (excluding City of London)

- Capacity - 3
- Capability - 3
- Performance - 3
- Criminality - 1
- Geography - 3
- Co-terminosity - 5
- Identity - 2
- Governance - 2
- Economic - 2
- Risk - 2



City of London Police

- Capacity - 7
- Capability - 7
- Performance - 7
- Criminality - 5
- Geography - 7
- Co-terminosity - 9
- Identity - 9
- Governance - 9
- Economic – 8
- Risk - 8



7.5 The main features can be summarised as follows:

- The difference in performance between the City Police and the rest of the country reflected the different priority assigned to fraud. In the City, fraud is a priority because its police authority, the City of London Corporation and its major stakeholders in the City Financial insist upon this. As a consequence the Fraud Squad has ring fenced resources and priority access to specialist support, such as surveillance teams and technical services. Elsewhere, reflecting the absence of any mention of fraud in National Police Priorities, fraud is largely a "Cinderella" function.

- Problems faced by these fraud squads are not just small and declining resources but the frequent diversion of these resources from ongoing fraud investigations into other work. They are also generally the lowest priority call on specialist support, e.g. deployment of a surveillance team, with the force.

- This leads to recruitment and retention problems, and a perception that working on fraud is a negative career move.

- As well as the absence of positive signals from government about prioritising fraud investigations, there are some disincentives to undertaking fraud investigations.

    - First, the Home Office Counting Rules (HOCR) on clear up rates count detecting a complex fraud, which will be costly and time consuming, as one crime in the same way as one minor shoplifting theft. Changes already proposed to the HOCR will improve this situation.

    - Second, fraud investigations yielding proceeds returned to victims as compensation are less attractive investigative targets than money laundering investigations where (because there are no identifiable victims) the assets seized are usually confiscated and retained by the police.

- A problem affecting all fraud squads was the lack of adequate data about fraud because of the inaccurate and distorted picture produced by the current Counting Rules and the well known problems experienced by victims in making fraud reports.

- Apart from the poor service to victims (in some cases, no service at all) this deprived the police of vital intelligence about fraud and made it harder to mount effective investigations.

- Particular concern was expressed that the linkages of some types of fraud with organized crime and terrorist funding were being missed and that there was no national or regional tasking of fraud investigations.

Strategy

7.6 Within a national fraud strategy, the need to improve police structures for investigating fraud is a "generic action" within the process model and concerns the contribution that the police service makes towards the deterrence, prevention, detection and investigation of fraud.

7.7 As a vital part of a strategic approach, any move to improve police structures for investigating fraud must be seen in the context of the statutory charging initiative (see chapter 9) whereby the police, where the CPS is the prosecutor, are now required to obtain a CPS lawyer's advice during the investigation stage and cannot charge until authorisation is obtained from that lawyer.

Options

7.8 The panels considered three structural options:

- National Fraud Squad;
- National Lead Force;
- Regional Fraud Squads.

7.9 A National Fraud Squad would be responsible for the investigation of Level 2 and Level 3 frauds in England and Wales. (Level 1 frauds would continue to be investigated by Borough Command Units). The model we considered was a force with its headquarters in London and a regional office in each of the eight other ACPO regions in England and Wales. Initially it would just deal with fraud but there would be options later to expand its remit into other economic crime issues. The nucleus of the headquarters would be the existing City of London Police Fraud Squad and initially the regional offices would be staffed by police officers with fraud experience in current forces. The National Fraud Squad would either be a separate force with its own chief officer or, more likely, a national function of the City of London Police.

7.10 A National Lead Force would be a formal recognition that the City of London Fraud Squad has a leadership role in the investigation of fraud throughout England and Wales. The Commissioner is already the Chair of the Association of Chief Police Officers, Economic Crime Portfolio (ACPO-ECP) and the City leads the National Fraud Working Group. It was given Regional Lead Force status for South East and London in 2003 and investigates a number of complex frauds arising throughout the region which have not been accepted by the

Serious Fraud Office. The Fraud Squad was expanded to deal with this role and the £2 million cost shared between central government and the City of London Corporation.

7.11 A Regional Fraud Squad option would retain responsibility for all fraud investigations within local forces but, recognising that some forces were too small to maintain viable fraud squads, would create a smaller number of fraud squads of sufficient scale to investigate fraud throughout the regions. There would be a number of possibilities for such reorganization but the obvious one was to reflect the pattern of new strategic regional forces being created in the police force restructuring exercise. The recent decision by Home Office Ministers not to proceed with enforced mergers of police authorities has removed this potential synergy.

Conclusions

7.12 A National Fraud Squad would have advantages of focus and professionalism and would generate ring fenced resourcing of fraud investigation. However, there would be disruption in establishing it and difficult issues of funding and governance. A National Fraud Squad is not therefore favoured, although most members of the expert and executive panels believed it would have to be reconsidered if alternative arrangements did not improve the police response to fraud.

7.13 The panels considered that a basic weakness in the current arrangements was the absence of any proper fraud reporting mechanism which, in turn, meant that there was no proper intelligence or analytical picture of fraud, and therefore no sensible basis for prioritising fraud investigations. This was another reason why major structural change, such as the establishment of a National Fraud Squad, was therefore considered to be premature. Instead attention should focus on the immediate problems that had been identified; lack of quality intelligence about fraud and the low priority given to fraud.

7.14 The panel believed this required two responses. First, building some central capacity to analyse fraud properly. Second, improving the ability of police forces to respond to fraud by providing better support services. These requirements could be achieved by a combination of a National Lead Force to deliver some central functions and improving support available to forces on a regional basis. There will be different options for how the latter might be done and we believe these should be considered as part of the further work on police reform.

7.15 The panels considered the response of the police to an HMIC thematic inspection of Special Branch (SB) which discovered that many of the problems afflicting SB (e.g. diversion of SB officers to other tasks, lack of specialist resources) were also experienced by some fraud squads. While the HMIC inspection praised the considerable expertise and dedication of Special Branch officers it found that the existing arrangements were not fit for purpose and recommended a number of changes that led to the structure outlined below.

- Local police forces required to maintain a Special Branch with necessary resources to be effective;

- A network of Regional Intelligence Centres comprised of specialist resources (e.g. surveillance teams, analytical support) available to support Special Branch investigations;

- Each Regional Intelligence Centre to have a Head of Profession (Detective Superintendent level) to coordinate Special Branch work throughout the region;

- Creation of a National Coordinator for Special Branch (NCSB) at Deputy Chief Constable level who coordinates national tasking and whose office houses a National Special Branch Technology Unit;

- Some National functions are provided by the Metropolitan Police Service as a National Lead Force.

7.16 Similar arrangements might well be appropriate for dealing with fraud; although a post of National Coordinator of Fraud Investigations would not be necessary: this role could be assumed by the Chair of ACPO (ECP) and the support could be provided by existing ACPO staff based in London.

7.17 There are three "national" functions proposed for a National Lead Force that could have resource implications:

- National Fraud Reporting Centre and associated intelligence and analytical capacity. The costs are considered in Chapter 13;

- The Centre of Excellence function. This would likely be cost neutral or very small amounts, using current expertise and resources;

- National investigations. If the Lead Force were to assist with or direct certain complex fraud investigations outside its force area, there would be a need for additional detectives. The City of London Corporation (the police authority for the City of London Police) is aware of the Review's recommendations and is supportive of them. Following the City Police becoming Regional Lead Force for the South East and London in 2004, increased funding of £2 million a year was provided by the Corporation and the Home Office for the investigation of cases by the City Police in conjunction with the Serious Fraud Office. The Corporation has indicated informally that it would be prepared to discuss constructively financial arrangements in respect of the current Review.

<u>Recommendations</u>

7.18 The Home Secretary should consider making fraud a policing priority within the National Community Safety (Policing) Plan and law enforcement agencies should be encouraged to develop plans which include local performance targets for fraud.

7.19 As part of the developing work on police reform consideration should be given to the best way of enabling police forces to investigate Level 2 and Level 3 frauds that arise within their jurisdiction.

7.20 Chief Crown Prosecutors should ensure that each police fraud squad has access to specialist area fraud prosecutors from whom early pre-charge advice can be sought in those cases not being dealt with by the Fraud Prosecution Service.

7.21 As a minimum the existing capacity of fraud squads should be maintained and these resources should be ring fenced so far as possible.

7.22 Additional to fraud squad resources there should be appropriate capacity and capability to deal with Level 1 frauds that meet the agreed acceptance criteria and occurring at a local Borough Command Unit level.

7.23 A mechanism should be agreed to ensure that intelligence emanating from crime reports, recorded by the NFRC but not allocated to a strategic police force for investigation, should be readily available to forces.

7.24 Fraud squads should have available to them a forensic computer capacity sufficient to handle the amount of digital material commonly seized during serious fraud investigations. This capacity should be a uniform system across the regions.

7.25 One option for improving support to forces in tackling fraud would be to create a number of RSCs comprising specialist resources like surveillance and technical services. At present fraud squads are often regarded as a low priority call on these resources. This approach would need to be assessed for fit against the wider picture of police reform.

7.26 Such RSCs should be answerable to the relevant Chief Constables' Management Committees.

7.27 Each Regional Support Centre should have a Head of Profession who would task deployment of these resources and coordinate fraud investigations and anti-fraud police activity throughout the ACPO region.

7.28 Further study would be needed to determine the appropriate number of locations of such Regional Support Centres. One possibility would be to establish an RSC in each ACPO region in England and Wales outside London. This would imply eight centres.

7.29 Further study would also be necessary to determine the appropriate size of an RSC. The costs of a 37 person unit, comprising a Regional Coordinator and staff plus 20 detective constables and 12 civilians providing analytical and technical services, would be £2 million per year.

7.30 A National Lead Force for fraud should be established with the following functions:

a) To create, develop and manage the National Fraud Reporting Centre and its analytical unit;

b) To disseminate intelligence and analysis to the network of police fraud squads and, subject to appropriate protocols, other organizations investigating fraud (e.g. Serious Organized Crime Agency (SOCA)) to help them target fraud investigations and anti-fraud work generally;

c) To act as a Centre of Excellence for fraud investigations, including organized training, disseminating best practice, general fraud prevention advice, advising on complex enquiries in other regions, and assisting with or even directing the most complex of such investigations.

7.31 The National Lead Force should be based around the existing City Of London Police Fraud Squad. (This is without prejudice to the issue of whether that squad

would remain part of a separate City force, as now or within a revised London police structure.)

7.32 These arrangements are to be the subject of a "thematic" inspection by Her Majesty's Inspectorate of Justice, Community Safety and Custody within two years of their establishment. The Chief Inspector of Constabulary has indicated support for this recommendation.

Cost of Recommendations

7.33 The base case is:

- No increase in fraud squad investigators, except for National Lead Force;

- Some increase in capacity in the National Lead Force to assist with or carry out some enquiries outside its force area at a cost of £2 million per year.

7.34 In addition, and if the idea of RSCs was deemed the best way forward: the creation of eight Regional Support Centres with 37 staff to support fraud squads would cost around £16million a year ie £2million per visit. This sum could be reduced by a smaller number of Regional Support Centres, greater use of non-police investigators, or by eliminating the National Investigative function.

7.35 A variant would be to double the number of officers in police fraud squads outside London, which would mean an extra 290 detectives and 16 additional senior officers. The cost would be £15.5 million per year and would be an immediate response to the problem of inadequate investigatory capacity in the regions.

Civilianization of Investigations and Public/Private Partnerships

The Problem

7.36 Increasing police capacity is not the only way to improve the investigation of fraud. Most fraud investigations are carried out by civilian staff outside police forces. The Interim Report found that while police fraud squad numbers were just over 400, there were over 11,000 fraud investigators in public sector organizations and several thousand more in private businesses. Could the problem of declining police resources be, at least partially, addressed by replacing them with more civilian investigators?

Options

7.37 Five options were identified:

a) Police fraud squad investigators, as well as support staff, to be civilians;

b) Fraud to be investigated by other public and private sector organizations instead of police;

c) Police fraud squads to be directly financed by business;

d) Creation of joint police/private/public sector investigative units with joint funding and staffing;

e) Closer police/private/public collaboration.

7.38 The project team discussed these options with a number of police forces, other public sector bodies which investigate fraud, companies, and organizations providing specialist skills such as forensic accountants.

Conclusions

A. Police Fraud Squad Investigators as well as Support Staff to be Civilians.

7.39 Police fraud squads already employ civilians, some of them in 'investigative' roles such as financial investigation, intelligence/analytical roles, forensic accountancy and computer forensics. Additionally civilians carry out administrative duties within fraud investigation departments such as file preparation, witness liaison and property store duties.

7.40 Investigating fraud is not something that only police officers can do. The only functions reserved to the police are search, arrest and detention. In these circumstances there is an argument for civilianising most fraud investigations if police forces are no longer able to spare police officers for such investigations. There would be two main benefits. First, lower costs as civilians are generally cheaper to employ than warranted police officers. The table below shows that civilians could be 10-15 percent cheaper. Second, effective ring fencing as civilians could only be employed in these roles as they would not have general police powers.

Salary (plus allowance) Comparisons

TITLE	ORGANIZATION	RANGE (£)	MIDPOINT
Detective Constable	City of London Police	30,423 – 39,359	34,891
Civilian Investigator	City of London Police	27,150 – 32,410	29,780
Financial Investigator	Serious Fraud Office	23,500 – 32,300	27,900

7.41 Civilians could be recruited either by hiring police or Customs' officers as they retired, or through agencies that specialise in placing retired police officers, or by open recruitment of civilians without previous experience of fraud investigative work. Employing retired police officers would retain police skills and lessen training needs, but it will not solve the long term problem of declining skills. A lot of retired police fraud squad officers already work in fraud investigations for other public sector agencies or private sector companies and care would be needed to avoid excessive competitive bidding to drive up their cost. Direct recruitment of

civilians with no previous investigative experience would mean greater training needs but would avoid the problem of competitive bidding.

7.42 The City of London Police is in the process of hiring four civilian investigators who would work within the fraud squad. The salaries payable will be less than those paid to a fully trained detective constable. The City Police recognizes that these civilians may need extensive training in investigative techniques but believe that, once trained they would be a useful additional resource.

7.43 Civilian investigators have been successfully deployed in several forces and the Fraud Review Team was mindful of a pioneering initiative being piloted by Surrey Police. The Surrey Police 'Mixed Economy of Policing' two-year pilot is supported by £3m Home Office funding and aims to develop, pilot and evaluate a strategic integration model to deliver a mixed economy workforce.

7.44 This innovative approach has completely re-engineered both the staff mix and the supporting processes in the pilot area and evaluation suggests the new configuration is producing an enhanced level of policing capability and unit capacity linked with a significant reduction in costs.

7.45 The Mixed Economy of Policing pilot is in keeping with the National Volume Crime Investigation Project, driven by the National Centre for Policing Excellence (NCPE), which seeks to introduce greater business efficiency and effectiveness into the investigation of volume crime.

7.46 The project has received positive feedback and provides a model for a mixed workforce. Whilst not fully evaluated, the model gives an indication of some of the benefits that can be accrued from such an approach and it may be reasonable to assume that this approach or parts of it could be applied to police structures for investigating fraud.

Surrey Police Case Study
"The Mixed Economy of Policing"

Workforce Modernisation Project

Surrey Police's 'Mixed Economy of Policing', pilot went live on one of the Force's four basic command units, West Surrey Division on 1st November 2004. The pilot implemented a re-configuration of the staff, management procedures and working practices in two frontline services, one of which is the investigation of volume crime on Waverly Division.

Central to this project has been the focus on building new 'optimal' capabilities by:

- Examining traditional working practices and processes.
- Separating out tasks to the most appropriate resource and,
- Examining existing and new technologies to support crime investigation.

The Divisional CID at Waverley was reconfigured from a structure that had 27 staff (all police officers and costing £1.8m per annum) to a structure with 28 staff (13 police officers, 11 non-police investigating officers and 5 team coordinators costing £1.2m). This provided an efficiency saving of over £600,000 (33%).

The savings were achieved in the main by reduced staffing costs. To arrive at a reliable figure for staff, Surrey Police compared the total costs of constables and civilian staff, including the investments made in each. This revealed the total average daily cost of a constable is in the region of £305 compared to a non-police investigator rate of £156.

The project is subject to an independent evaluation by the Institute for Employment Studies (IES). The December 2005 Quarterly Report from IES produced some impressive findings:

- Crimes are resolved at least 27% faster than a neighbouring borough.
- For the period July – Oct 05, the CID in the pilot area showed the highest increase in detection rates in the country (27.8% compared to an average 7.7%).
- The CID teams in the pilot area investigated and detected more volume crimes per team and with less staff.

In short, evidence is emerging that police performance in volume crime investigation can be improved and costs reduced through use of the 'Mixed Economy of Policing' approach.

B. Fraud Investigators to be undertaken by other public and private sector organizations instead of police

7.47 In principle, the police were prepared to see public and private sector organizations investigate fraud and bring the results back to the police for follow up if necessary e.g. when an arrest needed to be made. This would allow the police to focus on frauds where victims could not themselves investigate and would allow the relevant body to have more control over its own cases. They were also prepared to see, indeed would welcome, other public sector bodies to take on fraud investigations that the police were not resourced to investigate.

7.48 As described in the Fraud Review Interim Report, this already happens to some extent. Public sector organizations largely investigate fraud against their own revenues themselves. And some of them have responsibilities for dealing with particular types of fraud against the public. Examples of this are the 1600 Local Authority benefit fraud investigators and the work of Trading Standards officers. Sometimes they work with police but, more often, they investigate themselves and use their own powers to deal with the culprits.

7.49 However, there was no appetite from other public sector bodies consulted to take on any of the investigative process against frauds currently the responsibility of the police. Several said that they currently investigated a lot of fraud cases that fell within their statutory remit and found that when an investigation had become serious or complex enough to warrant police attention, the police frequently declined involvement for resource reasons. The same response came from private industry. Several already carried out the initial stages of an investigation and handed over to police for follow up and complained of a poor response.

Increasingly the private sector investigated these cases with a view to dismissing dishonest employees and/or civil recovery but saw little point in involving police.

C. Direct financing of Police by Private Enterprise

7.50 The Interim Report drew attention to a number of initiatives in which police investigative units were directly financed by the organizations which benefited from them. For example, the Vehicle Leasing Squad financed by the FLA (Finance and Leasing Association) which is a unit of five police officers based in the Metropolitan Police which investigates fraud involving vehicle financing. Another example concerns the London Borough of Greenwich who pays for a Metropolitan Police officer to be seconded to the authority and works to counter fraud directed against the local authority. There are plans to extend this to other London boroughs. There is also a unit in the Metropolitan Police being set up to combat copyright theft which will be financed by FACT.

7.51 In all these cases, the sponsor finances the unit or officer and so has a guarantee that crimes where it is the victim will be investigated by a dedicated resource that cannot be diverted to other duties. There is no question of the sponsor specifying or directing the course of individual enquiries.

7.52 The team explored the scope for extending these arrangements with a number of private sector organizations who were victims of fraud. The response from private industry was not favourable. Secondments and partnerships (see below) were the preferred method of providing support to police. There was concern that such arrangements might be seen as "private policing" and arguments that business was being asked to pay twice for policing through taxation and sponsorship.

7.53 There was even less support for the idea of direct business support for individual investigations. A recent case where police had solicited financial contributions towards the expense of an investigation from three insurance companies had attracted serious criticism.[54] It may compromise the essential independence and objectivity of the police when carrying out a criminal investigation. It might lead to

victims persuading a police investigating team to act partially. It might also lead to investigating officers carrying out a more thorough preparation of the evidence in a case of a "paying" victim; or a less careful preparation of the evidence in the case of a non-contributing victim.

D. Creation of joint police/public/private sector investigative units with joint funding and staffing.

7.54 The Interim Report described the arrangements under which the Dedicated Cheque and Plastic Card Unit (DCPCU) operates. It was established in 2002 to provide a dedicated resource to investigate cheque and credit card fraud. It comprises officers from the City of London and Metropolitan Police working side by side with representatives of APACS. There are currently 23 police officers and eight civilian staff and the running costs are £2 million a year. It is 100% financed by the private sector and the resources are ring fenced. Since it was established in 2002 it is estimated to have achieved savings of over £100 million for an investment of less than £10 million.

7.55 A further example is the current joint working between the City Police and SFO regarding computer forensic services. Two police officers permanently attached to the SFO Computer Forensics Team and use these facilities to work on City of London Police non-SFO enquiries. They have trained with the SFO officers and have access to their resources and expertise. In exchange for this the City of London Police will jointly fund with the SFO a mobile computer forensics facility.

7.56 These arrangements go well beyond business sponsorship of the police and involve joint working. Potential benefits highlighted by the police are being able to freely access skills and information not normally available to the police, and the increase in resources leads to more investigations taking place. Just as important are the benefits of working together with both the private and public sector, including raised awareness to business concerns and a different approach to investigations based on recovery priorities, losses and not just emphasis on convictions. The ability to focus on prevention by identifying and sharing information on trends and patterns are also a key benefit.

7.57 There are some issues concerning the operation and management of joint units, such as adequate security vetting for non-police officers in sensitive investigations and sometimes tensions arising from differing priorities of the agencies that made up the joint unit. But such problems have been successfully handled and the DCPCU and the City/SFO collaboration were seen to be great successes.

7.58 While it was not part of the Fraud Review's remit to create new joint units during the lifetime of the Review it did seek to ascertain the general attitude of the police, other public sector bodies and the private sector towards the creation of further units. Amongst the public sector, joint investigative units had not been widely considered but were viewed as having some potential. Most of the bodies consulted were able to quote examples of particular investigations where they had worked with one or more other agencies. For some agencies joint investigative work is sufficiently frequent that it is governed by MOUs. For example, the NHS and DWP have such agreements.

7.59 Private industry was also to a degree, supportive of the concept of joint investigative units and current initiatives such as the DCPCU were praised for developing the skills of investigators from all sectors and enhancing cross sector working relationships. Such joint working could also promote better preventative as well as investigative activities through enhanced data sharing.

7.60 All parties agreed that there were benefits to joint units for the investigation of types of crimes that required a coordinated approach. No specific proposals were made, other than existing joint units were successful and should continue in operation. When there are further opportunities to create such units the governance and financing model developed for DPCU would be a useful template but this is not to say that it would need to be exactly replicated. These details would depend on the nature of the collaboration with the DCPCU model if 100 percent private sector funding could be raised.

E. <u>Closer Police/Private/Public Collaboration</u>

7.61 A final option would be for the police, public sector and private sector bodies with expertise in countering fraud to work more closely together. A variety of approaches are possible. Individuals with such expertise could volunteer it to the police. This already happens to some degree. One example is that a number of forensic accountants have been appointed as special constables by the Metropolitan Police. However, they do not carry out the full range of special constable duties but concentrate on providing financial advice on investigations involving complex fraud issues. Special constables are unpaid and this is a good example of obtaining specialist services without having to pay full market price. Forensic accountants are expensive to employ.

7.62 The scheme is a success but has certain limitations. The hours that special constables are available are restricted and are often outside normal office hours when they usually have to do their "day job". This means their work is spread over a considerable time scale and can delay investigations. There are also sometimes problems when police officers working full time on the enquiry need to liaise with the special constables and if they have to give evidence in court.

7.63 It is of course always open to the police or other investigators to engage forensic accountants and other specialists on commercial terms to help with particular investigations. This is done from time to time, notably by the Serious Fraud Office. These resources can be very expensive to employ. There are also options for obtaining these resources on non-commercial terms through secondments and partnerships. Possibilities include a long term arrangement in which the police could provide training and experience in such activities as interviews and searches to staff in a forensic accounting firm in return for accounting services. Another would be reciprocated secondments which would benefit both parties, with each side continuing to pay existing salary and allowances to their outward secondee, while getting the services of the inward secondee for nothing.

7.64 Collaboration on specific investigations could also be envisaged. The police have frequently undertaken joint operations with other public sector bodies such

as NHS, DWP and the Immigration Service. There have also been effectively joint police/private sector investigations. For example, a victim bank had used its in house investigators to obtain witness statements from overseas for use in a criminal prosecution. This had been viewed as very successful and the local force was looking at other ways that the bank's investigators could work closer with their police counterparts in the future. The private sector has a wealth of investigative resources being able to harness that resource in a police investigation, would be beneficial. While there are issues around security and vetting these can be handled.

7.65 If joint investigations are to take place on a more systematic basis, they will require a minimum standard of training and probably some form of accreditation. This has been tried in the past but not successfully. A joint City, MPS and CBI initiative called "Partners Against Crime" was developed to an advanced stage in 2004. It envisaged that organizations which were victims of fraud would be able to use accredited investigators to investigate the fraud in collaboration with the police, who could delegate certain investigative tasks to them. The scheme was never implemented but the reasons for its abandonment are obscure.

7.66 The private sector organizations consulted were ready to try again. There was support for standardisation of investigative training particularly if this would lead to a closer working relationship with the police. Sharing of information and intelligence was also highlighted as a major priority for the private sector with closer and more coordinated working enhancing data sharing and improved fraud prevention. A system for accrediting investigators, which is going to be essential if any of these proposals are to be taken forward, was supported.

7.67 A considerable amount of training is already available:

- The National Fraud Working Group on Fraud co-ordinate police training and agree syllabus, exams and accreditation.

- Three centres currently provide police fraud training:

- GMP. Accreditation supplied by Tayside University (Alan Doig);
- West Midlands Police. Accreditation supplied by Tayside University (Alan Doig);
- CoLP. Accreditation will be supplied by CASS Business School.

- The CoLP are also currently developing modular courses for other sectors, both public and private, covering fraud investigation, which is due to be launched in November 2006.

- The Directorate of Counter Fraud Services (NHS) and the University of Portsmouth have co-operated to link a skills based training into a course of academic learning, which can lead to academic qualifications. At least 8,000 people from various organizations have gone through this course and accreditation system.

- The Assets Recovery Agency also train various organisations, however this course is designed for financial investigators and deals with proceeds of crime and confiscation rather than general counter fraud investigation.

- The SFO are on a training programme provided by Bond Solan, who provide various investigation courses, covering such topics as interviewing, court room skills etc.

7.68 There is a variety of training currently available from a number of sources each serving a particular sector of the market. Each course has its own syllabus and often accreditation, but there is not yet a national standard of accreditation. Establishing such a standard would facilitate the designation of accredited investigators.

7.69 There is a basis on which to build. The Counter Fraud Professional Accreditation Board (CFPAB) was created in 2001 from the merger of the National Counter Fraud Accreditation Board and the NHS National Professional Accreditation Board. It has representatives from both the public and private sectors, including:

- Department for Work and Pensions.
- NHS Counter Fraud and Security Management Service.
- NHS Trusts.
- UK Passport Service.
- Charity Commission.
- Local authorities.
- Child Support Agency.
- HM Revenue and Customs.
- Abbey Bank.
- University of Portsmouth.

7.70 The CFPAB seeks to undertake the following role across the United Kingdom:

- To establish and maintain professional standards in the delivery of a portfolio of professional training courses in the field of counter fraud work, encompassing a 'Foundation Level' syllabus and qualification.

- To formally recognise the successful completion of a portfolio of professional training courses in the field of counter fraud work encompassing a 'Foundation Level' syllabus and qualification.

- To oversee the delivery of the training courses taking into account the quality and effectiveness of the courses.

- To ensure that individual courses, and the portfolio of courses as a whole, are conducted so that Higher Education credits can be awarded, and that in particular a recommended credit rating is communicated to the higher education institution(s).

- To establish and maintain professional standards in the delivery of an 'Advanced Level' counter fraud qualification based on an agreed common syllabus, to be delivered by higher education institutions and resulting in an Award at Certificate of Higher Education level.

- To recognise formally the successful completion of the 'Advanced Level' counter fraud qualification with the award of Certified Counter Fraud Specialist (CCFS) status.

- To promote actively professional training for counter fraud specialists, to work with organisations with a common interest in the development of professional training and access to relevant programmes of Higher Education.

7.71 The CFPAB has made several thousand awards since its establishment awarding the categories below:

- Accredited Counter Fraud Officers;
- Accredited Counter Fraud Specialists;
- Accredited Counter Fraud Trainer;
- Accredited Counter Fraud Managers;
- Certified Counter Fraud Specialists;

and could be the basis of a national standard of fraud accreditation.

Recommendations

7.72 There are a number of options for increasing the non-police role in fraud investigations and for increasing public/private partnerships. Their benefits are not just providing extra resources for fraud investigations but improving their quality, through sharing of expertise and experience between the various investigatory agencies. This can only be beneficial and the recommendations made for joint training and partnership working should develop a community of fraud investigators with increasingly interchangeable skills who can work in a number of investigative agencies. More secondments and exchanges have been welcomed by everyone consulted.

7.73 The most radical idea of entirely civilianising fraud investigations is undesirable. There are a few functions that only the police can perform, such as arrest, which are sometimes necessary when dealing with fraud. In addition, some fraudsters

are connected to organized crime and are the sort of people who should be tackled by investigators will the full range of powers and experience. The recommendations below are designed to generate a modest increase in the civilian component of fraud investigations and increase partnership working. They are an addition to, not a substitute for, the recommendations to improve the police response.

7.74 The following specific recommendations are made:

a) The current exercise by the City of London Police to recruit and train civilian investigators should be monitored to see if it could be applied in other forces.

b) A similar approach should be piloted in another force to see if it would be suitable in a smaller fraud squad where the civilians would be a greater component of the anti-fraud effort of the force.

c) The current project by Surrey Police to deliver a mixed economy workforce to tackle volume crime investigations should be monitored to see if it could be applied to support police fraud investigations.

d) The NFSA when drawing up the first National Strategic plan should consider the scope for extending private / public partnership arrangements.

e) Further cooperation and collaboration over investigations between police, other public sector investigative bodies, and the private sector should be pursued as follows:

- The police and public sector bodies, who regularly purchase external advice such as forensic accounting and computer analysis, should coordinate their procurement activity to obtain best value for money;

- The National Fraud Strategic Authority should organize a more structured programme of secondments and exchanges between public and private sector investigative bodies;

- Police forces should consider the scope for obtaining specialist support for fraud investigators by recruiting individuals with such expertise as special constables;

- The National Fraud Strategic Authority should design a system for the nationwide accreditation of fraud investigators based on the certification of current training courses, identifying any gaps.

Costs

7.75 None of the recommendations have immediate cost implications. The proposed national accreditation of fraud investigators and the certification of training courses will have resources implications but it is envisaged that they would be included as part of the ongoing work of the NFSA.

CHAPTER 8 PENALISING FRAUD

8 SUMMARY

"If there was no punishment there would be no justice"[55]

- The punitive and deterrent elements of a criminal sentence rank high in public expectations of the criminal justice system. However, the statutory purposes of sentencing[56] are more varied than this and the victim survey [57] undertaken by the Fraud Review indicates a strong preference for both restorative and preventive elements in a criminal sentence as well. The Interim Report highlighted the very narrow range of sentencing options available to the Crown Court following a fraud conviction.

- This Chapter explores two suggestions made by Lord Justice Auld[58] and echoed (in part) by the Society for Advanced Legal Studies[59]:

  - In cases of fraud and other financial offences courts should, wherever possible and appropriate, exercise their existing powers of a regulatory nature as part of their sentencing disposal;

  - Consideration should be given, in appropriate offences, to enlarging or extending the courts' conventional sentencing powers in this respect…

  - …Consideration, for appropriate case of parallel proceedings, of combining the criminal justice and regulatory processes, with a judge as the common president and with lay members or expert assessors for the second and regulatory part.

- Most of those consulted during the Fraud Review would welcome a wider range of sentence options for fraud offences. Variety is the key both to ensuring proportionality of punishment (a punishment to fit the crime) and to addressing the other purposes of sentencing. Professor McCrory[60] in his current consultation paper is recommending a similar broad approach to

regulatory penalties. Punishment is not the only response to non violent acquisitive crime, but there needs to be a deterrent. Victim reparation, preventive measures and elements designed to protect the public also have an important part to play.

- The Fraud Review has considered the options for extending the sentencing powers and the jurisdiction of the Crown Court, and, more radically, for rationalising the way the civil and criminal courts interact in fraud related cases. Option (a) is the basis of the recommended approach. Option (b) is the more radical recommendation to link the jurisdictions of the Crown and High Court in a "virtual" Financial Court, able to deal with fraud trials and all ancillary cases arising out of them.

  (a) <u>The Sentence Option</u>

  Extending the range of non custodial sentences available to the Crown Court following conviction for a fraud offence, by adding:

  - Power to wind up companies used in the fraud;
  - Power to award compensation to all victims of a fraud offences (whether their loss is the subject of a specific charge or not);
  - Power to appoint a receiver to recover property and distribute compensation awards;
  - Power to prohibit or restrict an offender engaging in professional or commercial activities;
  - Power to make orders dealing with consequential insolvency.

  (b) <u>The Financial Court jurisdiction</u>

A more radical option, going beyond Lord Auld's recommendations, would involve establishing what could be described as a financial court jurisdiction in the Queen's Bench Division, linking the Crown Court and the High Court to handle and co-ordinate civil and criminal fraud work. This would enable more frequent allocation of High Court or long trial specialist judges to complex Crown Court fraud trials and the allocation of ancillary High Court matters arising from a fraud offence to the Crown Court, where it would be just and appropriate to do so. This joinder of jurisdiction would eliminate much of the current wasteful duplication of court and judicial resources by enabling related ancillary civil matters to be based on a single basic facts hearing, and to be heard by the same (trial) judge.

(c) In addition, it is proposed that greater use could be made of the administrative and civil court options available to regulators, as an alternative to criminal proceedings for appropriate fraud offences.

Option (a) is likely to require primary or secondary legislation. Option (b) will require further detailed analysis as to the extent to which it could be achieved under existing rules of court under the framework of the Supreme [Senior Courts] Act 1981. Direct cost savings may be modest, though efficiency gains may be considerable. The principal impact will be on public confidence in the criminal justice system.

The First Problem, Penalties and Remedies for Fraud

8.1 In the Interim Report it was noted that the term "fraud offence" covers a wide range of criminal activity[61] and that there are numerous government departments and agencies involved in prosecuting or otherwise dealing with it, These authorities have recourse to a variety of remedies or penalties for fraud offences; obtainable from different courts or imposed by administrative action.

8.2 Historically the Government has always maintained a variety of specialist statutory prosecuting authorities, in addition to the national Crown Prosecution Service created in 1986. The departments that have powers of prosecution are either public regulators that enforce standards of conduct imposed on the public and the business community, or departments that have needed to police their own financial relationship with the public and to protect the public revenue.

8.3 The Crown Prosecution Service (CPS), Serious Fraud Office (SFO), Department of Trade and Industry (DTI), Financial Services Authority (FSA), Pensions Regulator (formerly OPRA), and the Office of Fair Trading (OFT), which coordinates prosecutions under the Enterprise Act brought by Trading Standards Offices (TSOs) and the local authorities; are the principal government bodies concerned with prosecuting frauds on businesses and the general public.

8.4 The Department for the Environment, Food and Rural Affairs (DEFRA), Department for Work and Pensions (DWP), Department of Health (DOH, through the NHS Counter Fraud Service) and the Revenue and Customs Prosecuting Organisation (RCPO) are the principal actors concerned with prosecuting fraud on the public revenue. Any government department or agency can of course become the victim of fraud. In addition, the Asset Recovery Agency (ARA) which does not prosecute has power under the Proceeds of Crime Act 2003 (POCA) to recover proceeds of all criminal offences by civil action or taxation and to assist prosecutors with criminal confiscation investigations and enforcement.

8.5 There is inevitably overlap between regulators and the traditional criminal investigators and prosecutors. Business and Financial Regulators play a primary fraud preventive role by gate-keeping access to regulated businesses, encouraging and enforcing high standards of business efficiency and propriety and educating consumers about the risks. Professor McCrory's Penalties Review[62] proposes key principles for regulatory penalties that echo the statutory purposes of sentencing in the criminal courts[63].

- Sanctions should change the behaviour of the offender;
- Sanctions should ensure that there is no financial benefit from non compliance;
- Sanctions should be responsive (appropriate to the offenders and the regulatory issue);
- Sanctions should be proportionate to the nature of the offence and the harm caused;
- Sanctions should aim to restore the harm caused;
- Sanctions should aim to deter future non compliance.

8.6 It should be noted that the Law Society and the Institute of Chartered Accountants for England and Wales (ICAEW) have a preventative and deterrent role in respect of their professions, both of which have proved highly vulnerable to abuse by fraud. Both sets of professional regulators can mount disciplinary proceedings but neither have prosecution powers. The current Legal Services Bill will provide for statutory regulation of the legal profession, following the Clementi recommendations; but Accountants are not subject to statutory regulation and remain subject only to the discipline of their various professional Institutes and Associations.

8.7 The current distribution of powers between regulators and prosecutors is illustrated below. The colours reflect whether they are criminal (green) or civil (yellow) court based (or both – blue); or purely administrative (purple).

Table 1: Fraud Penalties, Criminal, Civil, Administrative[64]

Tool/ Org.	Crim. Pros.	Comp./ Crim.	Conf. & restraint	Disqual /Ban	Civil Debt etc.	Injunction	Insolvency	Settle/ Undertaking	Enf./ stop orders	Caution	Admin.Fine
CPS	•	•	•	•						• *	
SFO	•	•	•	•						• *	
DTI/CIB/IS	•	•	•	•	•		•	•	•	• *	
FSA	•	•	•	•	•	•	•	•	•	•	•
OFT/TSO	•	•	•	•		•		•	•		•
Pensions	•	•	•		•		•	•			
Police			Cash							•	
DoH/NHS	•	•	•	•	•	•	•	•			•
DEFRA	•	•	•	•	•		•	•	•	•	
RCPO	•		•	•						• *	
HMRC	•		Cash	•	•		•	•			•
DWP	•	•	•	•	•	•				•	•
ARA			•					•			tax

(* conditional cautions not yet in force)

The Second Problem, Parallel Proceedings

8.8 The range of criminal, civil and administrative remedies and penalties illustrated in Table 1 inevitably gives rise to parallel proceedings in different courts or tribunals before, alongside or after prosecutions. In addition, victims[65] may take their own proceedings. These can sometimes even thwart prosecution (e.g. Prudential case 2005 and the SFO Balfron case 2004).

A Case Study

A current SFO case concerns an alleged conspiracy to defraud the Department of Health by the manufacturers of certain generic drugs. It is alleged that the principal beneficiaries are the companies themselves rather than the individual, managers and directors who allegedly planned and implemented the price fixing arrangements. The loser is principally the DOH.

The SFO has charged nine individuals and five companies with conspiracy to defraud. The trial has not yet been fixed.

The DOH has brought civil claims in the High Court for damages arising from some of the price fixing arrangements. Three of the companies have settled the proceedings for a total of £30 million. Two of the companies charged in the criminal proceedings have not yet settled the civil claims.

The SFO has been judicially reviewed three times, challenging the Director's decision to assist the DOH in its civil claim by the provision of documents seized under warrant in the course of the criminal investigation. Although these applications have been unsuccessful, the pursuit of them through the courts up to the ECHR have been costly, time consuming and have diverted SFO resources from the criminal investigation.

The Court of Appeal has ruled that the exercise of the Director's discretion (to pass evidence to another department via the statutory gateway) should normally be subject to notification to the affected parties of the intention to do so and the provision to them of an opportunity for them to make representations and/or to seek legal restraint. This ruling has led to a suspension of further potentially important disclosure in this case and has significant wider implications.

As long as the two sets civil and criminal proceedings run in parallel, there is a risk that something said or done in the civil proceedings may damage the criminal proceedings. (See the BALFRON case, in which a finding by a Chancery Judge in the trial of a claim to recover funds stolen from a pension fund led to a successful application to stay a criminal indictment against a solicitor charged by the SFO for his part in assisting the fraud.)

The criminal proceedings are likely to lead to an application by the defendants to stay the civil proceedings pending the completion of the criminal proceedings.

8.9 Often regulatory enquiries start first and provoke a later criminal investigation. There is little consistency or predictability about priority between civil, criminal regulatory hearings. Some urgent action by regulators may need to be taken in advance of the prosecution, not least because criminal fraud investigation, dependent as it is on international co-operation and technical analysis, is often painfully slow.

8.10 The collapse of BCCI and the Maxwell empire both provide stark examples of the years taken to deal with all the serial proceedings arising out of a fraud. In the former, prosecutions preceded by many years the last of the civil cases. In the latter the reverse was true, with publication of the original DTI report (containing some important lessons and warnings for industry and the public) delayed until after the last of the criminal trials. In most cases there are several different factual hearings, with witnesses being recalled on more than one occasion and different counsel and judges spending long hours "reading in" to the written evidence.

The Third Problem, the "Justice Gap" for Fraud Victims

8.11 The Interim Report considered how the courts' restorative and preventive sentencing powers could be enhanced. The most obvious justice gap was in relation to compensation orders[66]. Compensation orders are obtainable, following conviction, for specific individual losses and are restricted to victims of offences actually charged and convicted, or formally taken into consideration (t.i.c.) on sentence. The Criminal Injuries Compensation Board does not cover fraud offences, so the criminal courts' willingness (and capacity) to compensate fraud victims is the only restorative element in criminal sentences.

8.12 The court has power to appoint a receiver to recover and distribute assets subject to confiscation orders[67]; but none in respect of complicated compensation orders[68]. The authorities suggest that "the Court of Appeal has discouraged criminal courts from embarking on complicated investigations" in this area. Where multiple victims are involved, very few will survive the

focussing and trial management decisions made prior to the trial. Their only recourse is to the civil courts in separate, possibly individual action. The cost of these is increased by the inability of prosecutors or the police to supply evidence to civil litigants without a court order.[69]

8.13 Our victim survey[70] indicated the sense of injustice caused to many by this:

> "Considering it was my life savings and I was not compensated in any way… I feel that [the offender] should work off the outstanding money he owes".
>
> "I am not entirely happy with the conviction as I did not receive any compensation, as the police could not find any assets..."
>
> "The law needs to address the victim's needs fairly… the money recovered in my case was paid out to the Crown, accountant, solicitors and two victims on preferential grounds. The rest of us got nothing..."

As the comments above bear out, compensation orders will also depend on the availability of assets and the competing claims of confiscation and costs awards as well as legal restrictions.

The Place of the Courts in a Fraud Strategy

8.14 In a National Fraud Strategy, criminal prosecution is the ultimate enforcement activity. The sentencing powers of criminal courts in this process are pivotal. Tests of the strategy will include its success in:

- Preventing more frauds, by encouraging awareness and caution (see chapter 6);

- Reducing the number of full trials, by effective and appropriate negotiation of guilty pleas (See chapter 9);

- Keeping more cases out of the criminal courts, by effective use of civil or regulatory remedies which meet the justice of the case (and by other alternatives to trial - see chapter 11);

- Reserving criminal prosecution (and potential imposition of sentences of imprisonment) for the most serious cases.

8.15 The administrative structure of the criminal courts has recently undergone radical change, largely as recommended by Lord Justice Auld[71]. The Crown Court, however, remains a superior court of record and its jurisdiction is exercisable by:

a) Any judge of the High Court;
b) Any Circuit Judge, Recorder or District Judge (Magistrates Court) [72]

8.16 The purposes of sentencing have now been given statutory expression[73]. They are:

- The punishment of offenders;
- The reduction of crime (including reduction by deterrence);
- The reform and rehabilitation of offenders;
- The protection of the public;
- The making of reparation by offenders to persons affected by their offences.

These are considered in more detail in chapter 10.

8.17 The current range of sentencing options available to the Crown Court in fraud cases includes:

- Imprisonment (immediate, suspended or community sentences);
- Fine;
- Compensation Orders (limited to victims on final charges or TIC sheet);
- Confiscation Orders (can include appointment of a receiver);
- Company Director's Disqualification Order (rarely imposed).

8.18 In terms of a strategy; four out of five of these options could be classified as punitive and deterrent. New community orders under CJA 2003 are also preventive. Imprisonment is recordable and attracts publicity, social and employment consequences. Confiscation of an offender's assets or orders for compensation will be deterrent only if the sums concerned are proportionate to the actual or potential gain; though promotion (since 2002) of asset recovery as a major plank in the Government's crime deterrent policy is likely to make a considerable impact over time.

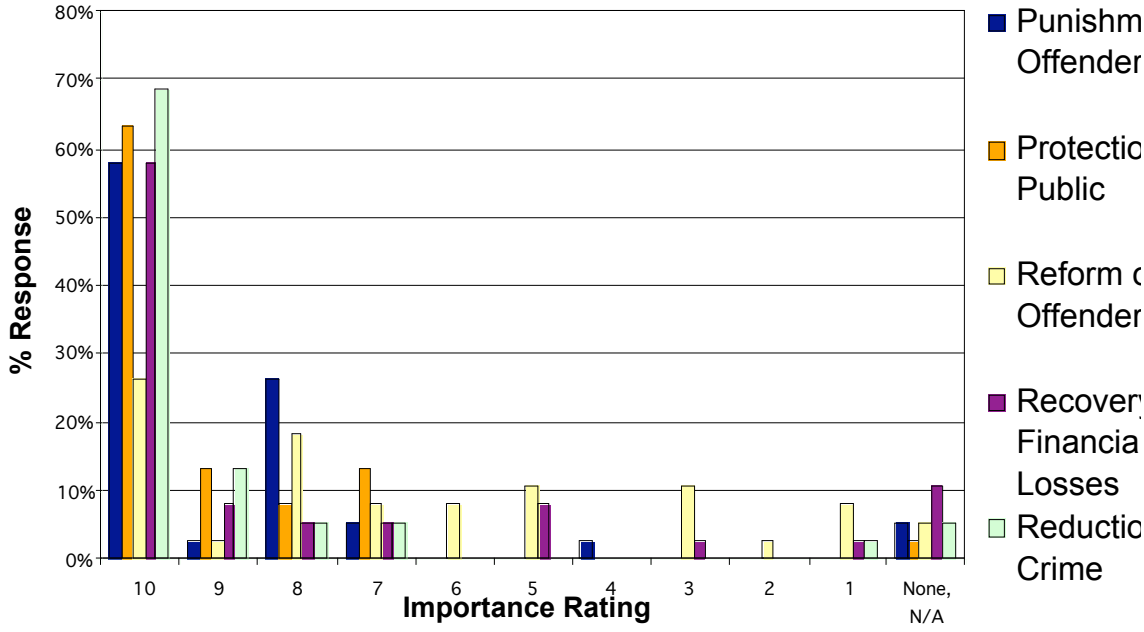
8.19 Unfortunately, in many frauds the cash "proceeds" are spent on maintaining the necessary façade of luxury yachts and cars, or on "pump priming" with phoney interest payments. There are seldom sufficient assets to compensate all victims. In corporate frauds, the offence may be the invention of assets or income streams, there are simply no proceeds as such; merely an illusion.

8.20 The Fraud Review victim survey[74] revealed a strong preference (63%) for prevention; illustrating an expectation that the criminal trial process will deliver an element of public protection from future offences. Close behind (58%) was punishment of the offender. Few expected the offender to reform, though one summed up the general opinion:

"sentences should be severe enough to make the offender want to reform and rehabilitate"

Figure 1 reflects the ratings given in the victim survey to the various statutory purposes of sentencing:

Figure 1. Victims desired outcomes



Lower Level Fraud and Consumer Abuse

8.21 Fraud offences are extremely variable in scale. They can range from the thousands of small Trading Standards offences involving double glazing and fly by night roofers, to the deliberate inflation of sales by a major PLC and "prime bank guarantee" or PONZI schemes attracting millions of pounds in a few months.

8.22 The Interim Report noted that there are already a variety of ways of dealing with the vast majority of “lesser” fraud cases; depending on the powers of the authority charged with investigating them. DTI, OFT and FSA have (see above Table 1) an extensive “toolkit” of regulatory (administrative), civil and criminal remedies to enable them to protect the public from consumer fraud offences without necessarily going to court at all.

8.23 The FSA case study below illustrates the gradual approach possible using FSMA powers, informal warnings backed by civil court action and finally criminal prosecution.

Case Study, Alan Evitts

Alan Evitts, an unqualified accountant, got into financial difficulties. He abused the trust of his clients by encouraging them to lend him money for fictitious investment opportunities. He took over £204,000 from 14 clients. At first, in 2002, the FSA initially accepted his undertakings not to accept further deposits but he breached this; so the FSA obtained a civil injunction that also froze his assets. The FSA also obtained a Bankruptcy Order and finally prosecuted him for offences under FSMA 2000 and the prior Banking Act 1987. In June 2005 Evitts was sentenced to 18 months imprisonment.

8.24 The vast majority of even criminal cases (over 81%) in England & Wales are dealt with by lay magistrates. With the recent doubling of their maximum sentencing powers[75] (6 to 12 months), this will increase. Lower courts are more cost effective[76] and can deliver swifter justice for all concerned, including victims. CJA 2003 community sentences have most impact at this level.

8.25 There is a bewildering array of consumer fraud legislation at this level[77]; but the breadth of the current Fraud Bill offences[78] should ensure that it eventually subsumes most of what could properly be categorised as criminal fraud. Naturally enough, the Fraud Bill itself contains no specific provision for "settling" lower level cases outside court, but Professor McCrory has detailed proposals for this and further Fraud Review recommendations are considered in chapter 11.

8.26 The OFT is now harnessing the efforts of Trading Standards Officers and will co-ordinate all prosecutions under the Enterprise Act 2002. The OFT's Annual Plan 2006-7 contains a robust strategy for dealing with (amongst other issues) consumer fraud that is entirely complementary to the proposed fraud strategy. The OFT focuses on:

- Providing guidance and warning campaigns to empower consumers to make informed choices when they risk their money;

- Using complaints to gather intelligence and evaluate enforcement effectiveness;

- Encouraging out of court redress wherever appropriate;

- Using administrative action, disqualifications, publicity and financial penalties as well as court proceedings to enforce commercial standards.

Medium and Upper Level Fraud

8.27 At the upper (VHCC, etc) end of the fraud scale, much work is already being done by courts and prosecutors as considered in chapter 9. This is where the greatest savings in court time and costs will be concentrated if other elements of the fraud strategy pay off. It is also where the largest frauds on government revenue occur.

8.28 The Exchequer is losing billions on MTIC fraud alone.[79] HMRC has been targeting investigation and prosecution efforts in this area for some time and SOCA's fraud priority will ensure further disruption to the criminal networks involved. At this level of serious, organised crime, increased maximum sentencing powers may have the most deterrent impact, particularly when coupled with confiscation (both civil and criminal). In such cases, which invariably involve complex and lengthy overseas investigation, a greater number of guilty pleas will obviously impact costs (see chapter 11)

Option (a) The Case for an Extended Criminal Court "Toolkit"

8.29 There remains a gap at Level 2/3 (crown court fraud cases below VHCC), where the choice of remedies is severely restricted. This is also the areas where criminal investigation resources are most stretched (see Chapter 7) and where most fraud goes unreported; the two are obviously connected.

Nevertheless, criminal prosecution will remain the principal method of dealing with mid to upper level frauds as well as orchestrated low value, high volume offences.

8.30 There is no doubt that where other remedies and penalties for fraud are available to a state "victim" (e.g. HMRC, DOH, DWP, DEFRA), or large corporate loser, these may be considered sufficient to meet the public interest without the need for a criminal prosecution. Civil debt recovery and settlements of civil action are routinely used for Revenue and other government losses. The power to compound offences on payment of an administrative fine is available to HMRC.

8.31 For individual losers and small business victims of frauds that fall outside the reach of consumer and financial regulation, criminal prosecution is all that the state offers. The CPS and SFO have no direct access to the variety of options available to regulatory bodies, nor to the preventive and deterrent remedies of the civil courts[80] Compensation orders, for example, are strictly limited to victims of charged offences, which may only be representative[81] or bargained away.

8.32 Lord Justice Auld recommended[82] that " in cases of fraud or other financial offences, courts should wherever possible and appropriate, exercise their existing powers of a regulatory nature as part of their sentencing disposal" and that "consideration should be given, in appropriate offences, to enlarging or extending the courts' conventional sentencing powers in this respect."

8.33 The Society for Advanced Legal Studies had also recommended in its Report on Parallel Proceedings[83] that criminal courts should be equipped with powers to close down fraudulently run businesses, compensate all victims, freeze assets and impose restrictions on authorisation[84] under Financial Services and Markets Act 2000; in addition to the current Company Directors Disqualification Act powers.

8.34 The consensus of Fraud Review consultations across a wide range of court practitioners was to the effect that the Crown Court could contribute more to prevention and deterrence, as well as to victim restitution, if it had an extended range of non custodial sentencing powers such as those suggested below. Some important issues arose if the new powers were to be made available after acquittal as well as following conviction. Obviously, like confiscation, the lower standard of proof would apply when dealing with the civil and regulatory elements of a case.

8.35 Professor McCrory has come to largely the same conclusion in relation to regulatory prosecutions.[85] Whilst proposing that, "the use of criminal prosecution should be maintained to sanction serious regulatory non compliance..." he also suggests that, "magistrates and crown court judges may also benefit from having an extending toolkit, which could include options beyond financial penalties or imprisonment. This could include options such as conditional cautions or publicity orders".

8.36 Criminal proceedings thus inevitably leave a residue of unresolved matters, such as those below. Possible extensions to sentencing options are underlined:

a) Victims who cannot be compensated because they did not feature on charges tried on the indictment;

<u>Wider compensation or restitution orders?</u>

b) Corporate vehicles used to commit the fraud (which may have no other purpose);

<u>Public interest company winding up?</u>

c) Insolvency issues arising before or after the court considers asset recovery for confiscation;

<u>Bankruptcy or winding up?</u>

d) Professional qualifications or regulatory authorisation abused by the offender;

<u>Restrictions or withdrawal of qualification/authorisation?</u>

e) Preventive elements.

Injunctions cease & desist prohibitory orders?

8.37 The Fraud Review discussed these suggestions with different small groups of court practitioners. There was considerable enthusiasm amongst some of them for extending the range of crown court sentencing options, subject to safeguards outlined below. It should be emphasised that these discussions were informal and that full formal consultation will be necessary prior to adoption of any legislative measures.

8.38 The value of increased sentencing powers becomes more obvious when prosecution is viewed as part of an overall national strategy for fraud. Disqualification and company winding up can be powerful fraud preventive tools, as professionals and companies feature heavily in many fraud offences. Removing as many of the opportunities for fraud offending as possible can rank with confiscation (civil or criminal) as an effective deterrent.

Suggested Additional Sentencing Options for the Crown Court

8.39 These options fall into two categories: those that merely extend existing sentencing powers and those that bring existing High Court civil powers within the jurisdiction of the criminal court. To this extent Option (a) overlaps Option (b). It will be important to ensure that some of these powers are exercisable before trial on a preventative basis (as they are now) in the same way as restraint orders can precede confiscation where there is a risk that assets will be dissipated.

a) Extending existing crown court powers to order compensation to all victims of a fraud offence (not only those on the indictment or t.i.c.); coupled with the power to appoint a receiver to administer assets and payment, would significantly reduce the number of parallel civil proceedings currently necessary.

It will be important to publicise this extension with a clear message that the court will (as it does now) have an absolute discretion to award compensation strictly according to the justice and merits of the individual case, reflecting the claimant's conduct or contributory negligence in the amount awarded.

Criminal assets may be limited and, although compensation takes statutory priority, other claims such as prosecution costs and confiscation already require the court's consideration too. The nature and duration of the fraud may be such as to have generated no proceeds; although compensation is not dependent (as confiscation is) on their actually being any.

Powers to appoint receivers, which could be adapted from or aligned with those available under POCA 2002, would avoid the court staff or prosecution being left to gather in assets and administer complicated claims. As under POCA, the receiver's fees and costs would be met from the criminal property.

Where assets are likely to be dissipated the court should have a linked power to order early restraint of assets.

b) Giving the Crown Court power to wind up companies and dissolve partnerships that have been used in the fraud. These remedies are currently only available from the High Court on application by DTI or the Insolvency Service. This could be achieved by an extension of the Insolvency Act 1986 sec 122 (1) (g) provisions for winding up in the public interest (on the grounds that it is just and equitable to do so); which already applies to overseas companies carrying on business in the UK.

   It will be important to ensure that the Crown Court has power to make provisional orders in cases where the risks of the fraudulent company or partnership continuing to trade pending trial represent a significant threat to the public.

c) Giving the Crown Court power to make Personal bankruptcy orders for offenders who cannot meet fines, compensation or confiscation orders. This

is already available to FSA under FSMA 2000 and to the DTI and Insolvency Services under Insolvency Act 1986 (as amended), but only in the civil courts.

Criminal Bankruptcy Orders were available to crown courts under Powers of Criminal Courts Act 1973 sec 39(1) but this was repealed by 1988 Criminal Justice Act. The procedure for imposing CBOs was cumbersome and involved the DTI Official Petitioner making a separate application under the Insolvency Act once the criminal proceedings had concluded.

A new power could be based on the Company Directors Disqualification Act, which gives jurisdiction to the Crown Court itself to impose disqualification, without the intervention of a petition process in a civil court.

d) Giving the Crown Court prohibitory (injunctive) powers in respect of business or commercial activity.

At present the FSA may obtain injunctions from the High Court restraining illegal investment or deposit taking (and some other consumer regulatory law breaches. Where the breach appears to have stopped the FSA has accepted undertakings in some cases. This can be seen as an alternative, where appropriate, to taking civil proceedings. Such proceedings are in fact often settled on undertakings or agreed terms; see the Evitt case study in an earlier paragraph, as an alternative to taking civil proceedings. Civil plaintiffs can also obtain injunctions to restrain illegal activity or breaches of contract.

The Criminal Justice Act 2003 introduced the concept of preventive orders into criminal law as part of the community sentence. The latter can contain a prohibited activity requirement[86] , the offender must refrain from participating in activities specified in the order (b) for a period so specified. Orders are made only in consultation with the Probation Service, whose job it is to monitor compliance. Football banning orders are another example, enabling the courts to restrict travel as well.

The Serious Organised Crime and Police Act 2005 secs 76-81 also contain provision for financial restriction orders for some fraud offence convictions[87]. These involve the offender reporting on his own financial situation and earnings at set intervals for up to 15 years.

The power could alternatively be adapted from the current High Court power to grant injunctions; i.e. as orders preventing a convicted offender from engaging in specified (but otherwise lawful) business activities that present him with a particular temptation or opportunity for fraud. Such a sentence could be confined to repeat offenders. Such orders could include:

- Not to take employment or voluntary work involving the handling of money for others; [or the selling of shares; or in the promotion of companies, etc.];

- Not to be involved in the promotion of travel or holiday clubs or timeshare property;

- Not to operate a premium telephone line.

The banning orders would complement the disqualifications from professional activity described below, and could be used to prevent authorisation being given for a regulated activity for a specified future period. For example a trainee solicitor convicted of fraud offences could be banned for a period from completing his training or applying for admission to the roll. The FSA has taken regulatory action to prohibit individuals from conducting regulated activities and hence from applying for authorisation, where they have already conducted unauthorised business. However, this is only useful where the individual wishes to become authorised.

It will be important to ensure that these injunctive powers can be exercised pre trial (as they can now) for preventative purposes; particularly in cases of persistent unauthorised regulated activity.

e) Extending the Crown Court power to impose disqualification of company directors to other professional disqualifications or restrictions on practice.

At present some activities require positive authorisation, in the absence of which the activity is criminalised. Statutory regulators such as FSA (FSMA requires authorisation for a wide range of financial services), OFT (for Estate Agents & Consumer Credit Licence-holders) and the Law Society are left to take disciplinary action against authorised persons or members who are convicted of criminal offences. As noted above, financial services professionals and solicitors and accountants feature regularly in fraud offences; either as offenders or as willing or foolish dupes whose professional standing assists the commission of the offence.

The legal profession is about to be made subject to a single statutory regulator under the Legal Services Bill[88] but accountants are not subject to statutory regulation at all. The Financial Advisory Panel has pointed out the dangers of this lacuna on a number of occasions; though it is fair to say that most major professional bodies (ICAEW, ACCA, ICMA) regard a conviction for fraud as prima facie ground for expulsion, at least for a period.

Professional restriction or disqualification is thus decided in a different forum from the Crown Court which heard the evidence. Considerable delay can result and the process of disclosing prosecution evidence to disciplinary bodies can be tortuous.

It is suggested that the statutory format employed in the Company Directors' (Disqualification) Act could be adapted for amendments to FSMA 2000, Enterprise Act 2002 and in due course the Legal Services Bill, to enable the Crown Court to disqualify offenders from conducting regulated business.

Unfortunately, the position for accountants is radically different. In law there is nothing to prevent even a struck off accountant from continuing to practice as such. Until the accountancy profession is regulated by law, the most a crown court would be able to do is make a recommendation for disqualification or

restriction to the professional body concerned. Wide publicity, and the maintenance of a publicly accessible Register of disqualifications (as DTI currently maintain for CDDA disqualifications) would go some way to ensuring effectiveness.

Advantages of Extended Sentencing Powers

8.40 The "new" powers described above are based entirely on those already exercised; albeit in different proceedings in different courts. The Fraud Review does not propose any changes to the essential nature of the proceedings or the remedies, merely to rationalise their uses and the fora in which they are deployed. In short, we are proposing to augment the criminal court's (principally the Crown Court's) sentencing powers with remedies borrowed from the civil courts. Fraud is unique as an offence that invariably spawns regulatory action and satellite proceedings in the civil courts. In these circumstances a certain amount of one stop shopping is bound to bring benefits to offenders, victims, witnesses and the justice system. The principal benefits are suggested below.

Effect on Plea Bargaining

8.41 With a wider range of penalties available to the criminal court, there could be more incentive for a fraud offender to plead guilty. A range of remedial, deterrent and preventive penalties may secure just outcomes more readily in the fraud context, by placing more emphasis on compensating victims and removing the means and opportunity for repeat offending. Wider court sentencing powers would give prosecutors more to bargain with, before or after charge. The judicial attitude to potential discussions between prosecution and defence on possible sentence to be imposed has changed since the Goodyear case. Our consultations indicated that, given the recent developments in early plea procedures and SOCAP 2005 arrangements for

Queen's Evidence, it would be possible for proper exploration of the appropriate sentence “package” by prosecution and defence to be conducted as part of the preliminaries to a plea. (See Chapter 11.)

Impact on Custodial Sentences

8.42 Increased public satisfaction with a wider range of sentences could mitigate the impact of any further decline in immediate custodial sentences. Fraud offenders are inevitably low risk and well behaved; open prisons are not popularly seen as either a punishment or a deterrent. Financial penalties and even offering repayment to victims have in the past been viewed as “buying out” a custodial sentence. Less used but even more valuable, the Director’s Disqualification is seen by courts and offenders as a particularly condign punishment (therefore rare); yet it effectively removes opportunities for repeat offending using corporate vehicles and, being closely linked to abuse of trust, is more likely to satisfy victims who cannot be compensated.

Reduction in Serial/Parallel Proceedings

8.43 Giving the Crown Court more preventive/regulatory and compensatory sentencing powers, would obviate the need for the State to bring serial proceedings for regulatory remedies, in different courts and should reduce the need for at least some parallel civil proceedings by victims[89]. Such additional proceedings currently involve separate, full facts hearings; recall of witnesses and extra strain on the defendant and his family. The early restraint provisions of POCA 2000 now enable the Crown Court to freeze assets at an early stage; so the risk of dissipation should be eliminated.

8.44 It will, however, be important to ensure that the High Court retains its existing pre-emptive preventive powers to grant emergency injunctions before a criminal investigation has even started. Until formal charges are brought and bail is granted the public may be at risk from a determined criminal. The FSA case study mentioned previously provides an example. Evitts breached his undertaking and accepted more deposits, only a High Court injunction and the

threat of imprisonment for contempt prevented further offences as the FSA investigation had only just begun.

Issues Arising

8.45 Many of the issues discussed below apply equally to the proposals for a Financial Court. At present, serial proceedings involve different counsel and court costs which are unlikely to be eligible for legal aid. Issues such as quantum, insurance and third party liability (or property ownership) may be complex. Safeguards, both for the trial judge and for the defendant will need to be built into the system if either extended sentencing powers or the Financial Court arrangements for a single facts hearing are adopted.

8.46 Some valuable suggestions emerged from our consultations with various court practitioners:

a) Make more use of High Court judges (Commercial[90] and/or Chancery) in complex fraud trials;

b) Provide a mechanism for co-ordinating parallel civil and criminal proceedings; for example by appointing a co-ordinating judge for fraud cases, who could deal with directions and the development of judicial expertise and skills;

c) Trial judge to have power to refer case for separate civil proceedings;

d) Trial judge to have power to hear additional evidence on "civil" aspects following the criminal trial.

Legal Aid

8.47 Care will need to be taken to ensure that no unnecessary burden is imposed on legal aid simply by bringing more civil/regulatory remedies within the Crown Court's sentencing powers. The proposed non custodial sentencing options are likely to increase both defence legal aid and prosecution costs

and to extend post trial hearings. At present, confiscation is dealt with as part of the trial process and legal aid is available for POCA hearings, which may include both pre-trial restraint orders and postponed confiscation hearings[91] following conviction. The additional sentencing options proposed are currently classified as civil remedies, available only in the civil courts, notwithstanding that the defendant may be a convicted offender. Fraud review consultees have urged strongly that a reversion to the civil arena altogether must be possible when the satellite issues are so complex that they require additional evidence, additional parties and separate consideration. The additional sentencing powers must be a convenience, not a burden to both the civil and criminal courts.

8.48 For example, wider compensation powers may require extended hearings (as confiscation currently does; though the appointment of a receiver should relieve the court of dealing with most of the detail. Compensation and company winding up may involve the judge in consideration of third party rights. Again, these already feature in confiscation hearings and though the third parties are not eligible for assistance, hearings may be prolonged by their intervention. Wider powers to disqualify or restrict offenders from commercial or professional practice may involve professional bodies[92] or require the assistance of regulators. It will be vital to explore all costs implications in a full business case and this has not been possible in the restricted review period.

8.49 In a few cases the involvement of one or more complicating factors, or the need to call additional evidence on the particular issues involved would delay the final criminal sentence beyond reasonable limits[93]. For these reasons it will be essential to have a co-ordinating mechanism in cases where it is in the interests of justice to have these matters dealt with separately, albeit ideally by the same judge. This should not be allowed to delay the commencement of any custodial sentence.

8.50 Under the Access to Justice Act 1999 it is likely that all ancillary sentences will attract legal aid. If the trial judge were to consider that an ancillary matter

required separate High (or District) Court proceedings, the link with the criminal sentence would need to be severed and the costs would be borne by the parties, subject to final order. Directions would need to be given. Nevertheless, it is suggested that the additional burden of publicly funding those ancillary hearings that were dealt with as part of the sentence (in the Crown Court) would be outweighed by the benefits of:

- Fewer High Court ancillary actions; and
- More guilty pleas and conditional cautions;
- Fewer custodial sentences.

Compensation/Confiscation and Restricted Assets

8.51 Increasing the availability of compensation orders in the criminal court as recommended may in some cases reduce the assets available for confiscation. POCA 2002 provides extensive investigation powers for tracing criminal proceeds and an offender's assets. A confiscation investigation can be lengthy and expensive; if the net result is a series of compensation orders with nothing left to reimburse the prosecution; then issues of fairness arise. Prosecution costs orders are seldom made now for other than specific items such as medical or other scientific reports. However, there is nothing to prevent such judicial considerations featuring in sentencing guidelines. In addition, prevention campaigns and warnings must emphasise the discretionary nature of the compensation order; so that there is no expectation of entitlement to compensation amongst fraud victims. The judge in the criminal court would take into account the same factors as he would in trying a civil claim by the same victims.

8.52 Welcome augmentation of the pot of assets from which compensation is payable in civil proceedings can be achieved when third parties are found to be "knowingly concerned" in the offence. This is a concept imported many years ago into criminal offences under Customs and Excise and Financial Services legislation. It survives in FSMA and it is hoped will survive in merged Revenue legislation. It is also under consideration by the Law Commission in

its consultation on secondary offenders. The recent October 2005 FSA case against John Martin and his law firm Adrian Sam & Co illustrates this neatly.

Case Study

Investors were sold worthless shares in a "boiler-room" operation run abroad. They sent their money to and received share certificates from a firm of solicitors in London. The FSA brought a civil action in the High Court alleging that the solicitor and his firm had been knowingly concerned in the illegal share offering. The firm was ordered to pay £360,000, even though they had passed on most of the money to the overseas fraudsters. It is likely that payment may involve the firm's professional negligence insurance.

Evidence

8.53 Use of overseas evidence other than for the purposes of the criminal trial requires the express permission of the requested state. Most international treaties and Mutual Legal Assistance (MLA) Conventions impose such restrictions on use, as does the Crime (International Co-operation) Act 2003 itself. Consent for other use (e.g. for regulatory proceedings) can normally be secured by an exchange of letters; but delays can be considerable and some countries do not respond.

8.54 Confiscation is widely accepted as part of the criminal trial process and it is reasonable to suppose that any ancillary proceedings that are categorised as a criminal sentence will be included in the permitted uses of evidence obtained by MLA. However, when directions are given for separate trial of ancillary sentence elements; it is likely to be necessary to obtain the Requested State's permission to use any overseas evidence needed for determination of the ancillary matters.

Standard of Proof and Admissibility

8.55 POCA and its predecessor provisions specifically apply the civil standard to hearings relating to confiscation orders; so it should be possible to apply the same wording to the proposed new powers. There is now very little difference in the rules of admissibility[94] between civil and criminal courts; though there may be a need for additional evidence to be called in relation to some sentencing hearings where specific issues did not arise in the trial proper. The interests of justice might well require additional evidence to be called on particular aspects of sentence which had not been relevant in the trial; for instance when a judge had been robust in excluding evidence at the trial for management purposes.

8.56 It was suggested during consultations that some of the proposed preventive sentences should be available to the court even following an acquittal. This may seem a contradiction in terms; but as the purposes of compensation, disqualification, company measures and insolvency action are not punitive but preventive and regulatory, it is perhaps not so radical as may first appear. ARA may act after an acquittal, of course, but its proceedings are in rem, brought against the property or goods themselves rather than against an individual personally. Likewise, company winding up technically involves the company itself as defendant, not the individual(s) whose offences triggered the court's power. Regulators such as FSA, DTI and the Law Society can currently take action or bring proceedings after an acquittal. This is more likely when a clear case of professional negligence or breaches of specific regulatory rules, rather than criminality or dishonestly, emerges from the evidence presented at trial.

Option (b) A Financial Court Jurisdiction

8.57 The elements of deterrence, reparation and prevention are not well reflected in current criminal sentencing powers; simply because they have always been available elsewhere in the justice system. English law has no notion of the "partie civile"; thus victim compensation and other forms of restitution have traditionally been provided outside the criminal courts. Rather than extending the jurisdiction of the criminal courts to encompass some of the remaining

(post acquittal) civil proceedings arising out of a fraud offence, option (b) rationalises the separate proceedings into a single, tiered Financial Court exercising both jurisdictions.

Past Suggestions for Reform

8.58 Lord Justice Auld[95] considered that a form of unification of civil and criminal proceedings naturally arising out of fraud cases, based on the criminal courts, might be worthy of consideration. The then Lord Chancellor proposed a similar two stage procedure in his 1998 KPMG lecture[96]. Lord Auld described it thus:

> "The court would deal with issues of guilt and sentence as it does now. Present, but not participating in those proceedings, would be two expert assessors. At the end of the criminal proceedings the judge would discharge the jury and he and the two assessors would then deal with the regulatory issues."

8.59 The Society for Advanced Legal Studies' Financial Regulation working group[97] did not favour the proposal. It considered such serial proceedings would lead to delay; that acquittals would cause difficulties and that:

> "Combining the proceedings in this way would compromise the independence and effectiveness of regulatory processes".

Models for a Financial Court

8.60 In fact, the two stage hearing has now been adopted both for confiscation hearings and (though not yet in force) for multiple offending[98]. The latter reflect recommendations of the Law Commission and do not involve lay assessors. In POCA 2002, the notion of civil proceedings (in rem) following even an acquitted defendant's assets underpins the procedure in Part 5.

8.61 The Fraud Review examined two possible models for a Financial Court. The Technology and Construction Court (TCC) utilises both Crown Court and High Court Judges hearing cases on RCJ and Regional lists. The Judge in Charge of the TCC liaises with presiding judges on workflow, makes suggestions for authorisation and provides a leadership role which enables the extended "virtual" court's cross tier jurisdiction to function more efficiently than the original arrangements for these highly specialised cases.

8.62 A similar "virtual court" framework is illustrated by the Commercial Court in the Queen's Bench Division of the High Court. It has regional Mercantile judges with a jurisdiction over slightly more valuable monetary claims that that of the District (County) Courts. There is no Judge in Charge, as the Presiding Judge of the Commercial Court allocates all the work. However, following the Woolf reforms in civil work, a number of senior civil judges were appointed as designated civil judges in civil trial centres, to provide leadership and to promote effective and consistent approaches to case management. They liaise with the Senior Presiding Judge on casework and are involved in judicial training on case management. For the same reasons it is recommended that a similar approach be adopted for the Financial Court jurisdiction of the High Court to enable the permanent link between the criminal and civil jurisdictions of the court to function efficiently.

8.63 Both the TCC and Commercial/Mercantile court framework enables cases to be dealt with flexibly at the different court tiers, relieving the High Court of some of its business. The greater numbers (and higher proportion of Crown Court, rather than High Court cases) of fraud trials and circuits involved might overburden Presiding Judges. It will be necessary to consider a detailed pilot, to estimate whether they would be assisted by a similar arrangement to that already operating nationally in respect of ticketed judges for sex offences.

8.64 A separate financial court jurisdiction linking the High Court and the Crown Court more closely would enable Crown Court judges with complex case authorisation to be deployed on longer criminal cases and on appropriate "bolted on" civil cases. It is accepted that a fixed diet of financial fraud cases

could limit both judicial development and deployment; though it should be possible to make maximum use of individual skills and experience where these have most valuable effect; i.e. on the length of the most expensive trials. However, there is clearly no necessity for a "fixed location, fixed resource" pattern in modern courts. Both Mercantile and regional TCC judges hear other civil cases and do not exclusively operate in one area. Lord Woolf envisaged the concentration of larger civil cases at regional trial centres that would have all the necessary resources including specialist judges. In fact the current locations of District Registries with Mercantile lists and specialist civil judges largely mirror those of Crown Court first tier centres.

Suggestions for Jurisdiction

8.65 Financial Court jurisdiction could as now be roughly determined by monetary levels. Some remedies would be within the current jurisdiction of the High Court and would need to be allocated to suitable judges in tiers below, as happens now with Mercantile and regional TCC judges. The current distribution of work amongst the different Divisions and courts of the High Court is wide; cases involving fraud we understand could be commenced in any one of three. For example, FSA cases currently go to Chancery judges, whereas ARA's go to the Administrative Court (QBD).

A Financial Court jurisdiction could include:

a) Crown court fraud cases (VHCC and as designated)(non jury trials);

b) Criminal assets (freezing and confiscation, including ARA's in rem proceedings);

c) Victim compensation (with insolvency orders as necessary);

d) Civil Regulatory injunctions (CDDA, FSMA, Enterprise Act);

e) Corporate vehicles (winding up, appointment of receivers or administrators).

f) Restrictions on commercial activity (injunctions or cease & desist orders).

Potential Caseload

8.66 It has proved difficult to obtain accurate figures for the number, length and outcome of non VHCC fraud trials. As a rough guide to the number of cases a Financial Court might try, the current Crown Court fraud workload is estimated as 222 cases[99] (involving some £942m), an increase on the 172 cases recorded in 2004. However, of these:

- The SFO bring 15-20 cases per year;
- The CPS Fraud Prosecution Service is estimating 205 cases per year RCPO HMC&E prosecuted 1,689 individuals[100] in the Crown Court in 2004;
- Inland Revenue prosecuted an average of 60 individuals p.a. prior to merger of the Revenue departments;
- DTI brought 352 Companies Act prosecutions and sought 155 disqualifications[101];
- Dept of Health brought 56 and DEFRA 6 prosecutions[102];
- FSA brought 3 criminal prosecutions and 13 civil actions in the Chancery Division between 2002-2005;
- ARA applied for 24 freezing and 52 Receiving Orders and was granted 28 recovery orders in its first two years (2004 & 2005).

8.67 It appears that the Woolf reforms and increasing use of ADR have resulted in a recent decrease in civil court actions[103]. It is not known how many claims involve allegations of fraud, whether at High Court, or District (County) court

level. Likewise there are no statistics for appeals from POCA 2000[104] forfeiture orders made by magistrates that are heard by the Crown Court.

Benefits of a Financial Court Jurisdiction

8.68 Some of these benefits could, of course, be achieved by extension of the Crown Court's sentencing powers. However, there would be no question of the civil satellite cases attracting criminal legal aid. Each satellite would benefit from the single facts hearing and continuity of judge, but would be civil or regulatory as designated by the statute concerned.

- All matters would be resolved on the basis of a single unified "set" of evidence; i.e. one facts hearing with a variety of outcomes.

- Reduction of inefficiencies and delays of parallel and serial hearings in different courts.

- Addressing the justice gap for victims, who are unable to obtain full redress from the criminal court and are then unable to obtain the evidence to commence civil action.

- Elimination of inconsistent findings by different Tribunals hearing different evidence in relation to the same facts.

- Elimination of differences in the current civil and criminal disclosure regimes.

- Removal of costly and time consuming difficulties associated with the current use of statutory gateways following the Court of Appeals ruling in the Kent Pharmaceutical case.

- Unification of confiscation, compensation, and civil recovery regimes.

- Orders could be made against third parties "concerned" in the offending[105].

- Variety of work at all levels for judiciary, and opportunities to increase experience and professional development.

- Some reduction of work in the High court.

- No need for lay assessors.

Issues Arising

8.69 As with Option (a) (as mentioned previously) there would be some issues to be ironed out in the areas of:

- Use of overseas evidence;
- Civil procedure rules (to enable the related civil or regulatory hearings to proceed on facts established at the criminal trial).

In addition, the following difficulties could arise:

- Some plaintiffs might be reluctant to have their cases dealt with by the criminal trial judge, for example insurance cases such as the Balfron case mentioned above.
- Complex 3rd part proceedings relating to e.g. ownership of assets might arise out of a relatively simple fraud.
- A series of complicated cases might require the authority and experience of a senior full time judge.

The solution would be to ensure that the High Court remained in charge of allocation of Financial Court civil work to trial judges. If for any reason a matter is not considered appropriate for hearing in the lower court, Rules of Court could provide for the evidence to be transmitted to the allocated judge.

Costs

8.70 Increasing sentencing options will not impact the Crown Court's estates or resources and should considerably reduce the number of High Court cases required for the same fraud offence.

8.71 The Fraud Review has not obtained sufficient evidence in the time available to calculate precise costs implications of establishing a Financial Court jurisdcition. It is proposed that a pilot scheme could be run linking a group of Crown Courts with a division of the High Court; superintended by a nominated High Court judge. Crown Court sitting days cost £4,601 and High Court days £2,844. Speeding up the first with more experienced judges and reducing trial time in the second with a basic single facts hearing and the same judge would have a positive effect that could be measured from a pilot. It is appreciated that any project aimed at delivering a pilot of such fundamental change to the criminal justice system will itself be a large undertaking. More detailed modelling work with the HM Courts Service will be needed when considering the establishment of the pilot.

8.72 The costs associated with the enhanced judicial training needed to ensure appropriate allocations between court tiers are likely to be the same for any of the options and are suggested as necessary anyway for the success of existing efficiency initiatives such as the Case Management Protocol. There will however, be financial implications for the JSB that will need to be assessed in a full business case.

8.73 There will be cost benefits and some savings in court time inherent in a single hearing even of the basic facts and contextual evidence by the same judge who later deals with the civil and regulatory issues as part of a planned and co-ordinated series of proceedings. To estimate these fully, a pilot scheme will be essential.

8.74 Some elements may involve more initial cost in order to achieve overall savings. The organisations that make savings will not necessarily be the ones which bear the costs; so there may need to be some balancing of resources. For example, CPS Prosecutors are not trained to conduct civil proceedings[106].

DTI, FSA, OFT, ARA lawyers may still need to be involved in secondary hearings and different counsel may be required, even though the judge remains the same. Existing serial cases already necessitate reading in by all those involved.

Legislation

8.75 Augmenting the Crown Court's powers of sentence under Option (a) will require primary legislation along the lines of Powers of the Criminal Courts (Sentencing) Act 2000. It is possible that primary legislation would be needed for the establishment of a Financial Court jurisdiction in the Supreme (Senior) Court;[107] though the TCC required none. In terms of deployment, High Court judges already have jurisdiction to sit in the Crown Court and the Supreme Court Rules permit allocation of high court work to lower courts.

8.76 Amendments to Prosecution of Offenders Act 1985 and Criminal Justice Act 1987 may be needed to enable CPS and SFO lawyers to act in relation to civil proceedings.

Regulatory and Administrative Alternatives to Criminal Trials

8.77 Finally, the Fraud Review considered other, related proposals to make more use of regulatory and administrative penalties as alternatives to criminal trials for fraud offences. Judges have expressed concern from time to time (particularly in SFO cases) that the more arcane corporate fraud offences (e.g. insider dealing, contract manipulation, sec 19 Theft Act) cause real difficulties in the criminal courts.

8.78 The Fraud Review has found no public or Government appetite for wholesale decriminalisation of fraud; public confidence may well be enhanced by more severe penalties for more harmful offences, particularly conspiracy to defraud. However, implicit in Lord Auld's recommendations was the possibility that more use could be made of existing regulatory and administrative sanctions for fraud offences, without engaging the criminal law in appropriate cases. As

noted previously, a great many of the lesser fraud offences are dealt with outside court; although always with criminal charges in terrorem, to encourage and enforce settlement and undertakings.

8.79 For example, the "perimeter" fraud offences under FSMA 2000 are currently very little used and there could be more scope, within a national fraud strategy, for harnessing the civil injunctive and restitutional powers of the FSA to protect the public from first time and medium level fraudsters without the need for prosecution in most cases. A considerable number of fraud offences involve investment schemes which the police are ill-equipped to deal with.

8.80 The present FSMA regime for insider dealing and market manipulation balances the need to mark the worst and most deliberately criminal cases with criminal prosecution and the convenience and efficiency of providing regulatory sanctions for "sharp practice" amongst professionals, sanctions which are in fact condign in their financial scale. As suggested below, and extension of these financial powers to unauthorised individuals and businesses, along the lines recommended by Professor McCrory for other regulators, would enable FSA to deal with more mid level fraud outside the criminal courts.

8.81 Lord Roskill's allusions to the public distaste for "trials of suits by suits" remain true. Neither public confidence nor Government policy (as exemplified by the recent criminalisation of individual cartel offences[108] as well as the Fraud Bill) would be served by wholesale handing over of "city" fraud offences to the regulator. The trick will be to separate the regulatory sheep from the criminal goats, in an open and transparent way that commands confidence in the strategy behind the choice.

Making More Use of Regulatory Powers

8.82 Regulatory remedies in e.g. FSMA are modern and sophisticated. As Professor McCrory remarked in his Review.[109]

"Many of the more recently created economic and financial regulators have very modern sanctioning toolkits which include flexible and proportionate responses to regulatory non compliance, including monetary administrative penalties."

8.83 The OFT and DTI already work closely together in the field of consumer protection generally and the FSA is a natural partner in a regulatory attack on lower level fraud outside the criminal justice system. The FSA also has consumer protection responsibilities through its statutory aims and its additional responsibilities under the Enterprise Act and related Regulations.[110]

8.84 Like the OFT, the FSA is an innovative and energetic regulator, quick to use press publicity to warn both consumers and its regulated community. The prevalent boiler room share pushing scams and the recent Cheshire Building Society mortgage fraud have both been the subject of proactive FSA press releases and website warnings during May 2006. The Chancery Division, to which the FSA's (admittedly rare) civil proceedings are brought, has shown itself willing to use FSMA to its fullest potential[111]. The combination of Declaration and Injunction is a particularly effective preventive measure that can be widely publicised, even though monitoring injunctions is a continuing burden for the Regulator. It is thus disappointing that the FSA has mounted so few civil actions or criminal prosecutions against unauthorised investment or deposit takers in the last few years[112]; concentrating its enforcement efforts predominantly on the regulated sector.

8.85 The FSA receives over 1000 queries annually reporting possible unauthorised business. It deals with these in a variety of ways ranging from explanatory and warning letters to investigation or referral to other law enforcement agencies here or abroad. The FSA's approach is determined on a risk basis. A National Fraud Reporting Centre could well refer more complaints to FSA and would provide more robust statistics for assessing risks to the public, leaving the FSA free to determine appropriate action as it does now.

Administrative Penalties

8.86 At present the administrative (fining) powers of the FSA can only be used in respect of regulatory breaches by regulated persons and firms, and are not available in respect of unauthorised businesses, including fraud. The OFT has powers to impose some monetary penalties under some, but not all consumer legislation and the current McCrory review consultation examines these in some depth; making proposals for streamlining and improvement.[113]

8.87 Extending the new conditional cautions and allowing prosecutors to make use of compounded penalties in Revenue fraud cases[114] could also reduce use of the criminal courts. This is explored more fully in Chapter 11. There are a great many overseas precedents for such a framework, for example the German system of administrative fines, imposed by prosecutors, which are increasingly being used for fraud cases[115]. A number of international comparisons are considered in Chapter 12 and Professor McCrory gives several more in his consultation paper.

8.88 All comparisons point to the cost benefits to be obtained from applying a national strategy to combine the efforts of regulators and law enforcement agencies. A National Fraud Strategy would require a closer and more detailed co-ordination of casework between all those involved in dealing with fraud. MOUs and liaison meetings exist, but they are perhaps not exploited as fully as they might be. Mention must be made here of the Financial Fraud Information Network (FFIN) which was established some years ago to provide a meeting point for regulators, police and prosecutors to co-ordinate action and exchange information. Together with the (former) Attorney General's Prosecutors' Convention, which provides for co-ordination of criminal prosecutions, FFIN offers a ready made framework for "vetting" fraud cases with the potential to be dealt with by more than one government body.

Conclusions

8.89 The Fraud Review has explored each of Lord Justice Auld's four linked proposals for addressing the number of current costly and inefficient parallel and serial proceedings uniquely associated with fraud offences. Like

Professor McCrory in a related area, the Review has concluded that there is indeed scope for rationalising both sentencing powers and procedures.

8.90 It is certainly possible that more use could be made of regulatory penalties for small and medium level fraud offences within a national fraud strategy; but as Professor McCrory suggests:

"the use of criminal proceedings should be maintained to sanction serious regulatory non-compliance where there is evidence of intentional or reckless behaviour or where the actual or potential consequences are so serious that public interest demands a criminal prosecution"

Recommendations

8.91 The recommendations are as follows:

1) The range of non custodial sentences available to the Crown Court following conviction for a fraud offence, should be extended by adding:

   - Power to wind up companies and dissolve partnerships used in the fraud;
   - Power to award compensation to all victims of a fraud offences (whether their loss is the subject of a specific charge, offence tic or not);
   - Power to appoint a Receiver to recover property and distribute compensation awards;
   - Power to disqualify, prohibit or restrict an offender engaging in particular professional, or commercial activities;
   - Power to make orders dealing with consequential insolvency.

2) A Financial Court jurisdiction should be established in the High Court; to link the Crown Court with a division of the High Court. Such a jurisdiction would

encompass fraud trials and related High Court matters throughout England and Wales. Any matter civil or criminal that arises out of an offence involving fraud should be dealt with and co-ordinated within the Financial Court jurisdiction and heard by the same judge; unless the interests of justice require otherwise.

3) Consideration should be given to running a pilot scheme to assess the precise costs/ benefits of a Financial Court jurisdiction.

4) Greater use should be made of the administrative and civil court options available to regulators, as an alternative to criminal proceedings for appropriate fraud offences.

CHAPTER 9 FRAUD TRIALS

9 SUMMARY

- The Fraud Review has consulted as widely as possible with some of those responsible for prosecuting, defending and trying fraud trials in England and Wales.

- During the last 2 years there has been a lot of work carried out to improve the preparation of cases and trial management. Nevertheless, our consultations suggest that additional measures could be introduced to ensure that the most complex and costly fraud trials are only tried by judges who have the experience and skills to do so, that the provisions governing disclosure of unused material are properly observed and that best use is made of electronic means of presenting evidence.

Introduction

9.1 A lot of valuable work has been done recently to improve the management of cases in the criminal courts. Under the auspices of the Law Officers and the Department for Constitutional Affairs, the Criminal Case Management Programme is being delivered. This comprises 3 strands namely statutory charging (ensuring prosecutors decide on whether and when a suspect is charged), the No Witness No Justice (NWNJ) initiative and the Effective Trial Management Programme (ETMP).The benefits of this work should emerge over time and, although relevant to all contested criminal cases, should improve the way that fraud cases at all levels are tried.

9.2 The importance of the decisions now being made by investigators and prosecutors pre- charge cannot be overstated as the quality of this work greatly affects the chances of successfully managing a case once it has come to court. The statutory charging scheme is designed to ensure that, in cases being investigated by police, officers have the advice and guidance of a prosecutor at an early stage with the aim of ensuring that the best and strongest of cases are

built and that, where practicable, there are no loose ends at the point of charge. We have been encouraged by the emphasis being placed on proper observance of this principle by the CPS.

9.3 Closely allied to these initiatives are 2 important documents. The Criminal Procedure Rules (CPR) took effect in April 2005 and they provide a modern procedural code for cases in the criminal courts. The Rules and the Criminal Casework Management Framework (CCMF)[116] provide guidance to everybody involved in a criminal case as to their functions and duties. The Rules specifically make it a duty of the court to manage cases actively and to give any direction appropriate to the case as early as possible.

9.4 In addition, judges, prosecutors and defence practitioners are assisted in managing the more complex cases at the crown court by The Lord Chief Justice's Protocol on the Control and Management of Heavy Fraud and Other Complex Criminal Cases (2005) and the 3 practice directions handed down on the same day[117]. The LCJ Protocol has been issued to supplement the CPR and CCMF and to summarise good practice in relation to the more complex cases.

9.5 All of these initiatives are designed to achieve more streamlined court processes and better quality in the delivery of justice. This should mean, among other things:

- Minimising delays in bringing cases to trial;

- Fewer ineffective trials by improved case preparation and progression from charge through to trial thus enabling the trial to start on time;

- Fewer cracked trials; i.e. those case where defendants plead guilty on the day of trial, or where the prosecution accepts a plea to lesser offences or offers no evidence;

- A better service to victims, witnesses and defendants;

- More cost effective trials.

9.6 An integral part of preparation for trial and its management is how material retained by the prosecution but not used as part of its evidence is dealt with. The current law on disclosure of unused material is contained within the following:

- The Criminal Procedure and Investigations Act 1996 (CPIA).
- The Code of Practice issued under section 23 of the CPIA (the Code).
- Parts 25-28 of the Criminal Procedure Rules 2005 (the Rules).
- The Criminal Procedure and Investigations Act 1996 (Defence Disclosure Time Limits) Regulations 1997 issued under Section 12 of the CPIA (the Regulations).

9.7 Very simply, the law requires the following approach to unused material to be adopted by the prosecution team in criminal cases:

- In conducting an investigation, the investigators should pursue all reasonable lines of inquiry.
- Any material, including information, which may be relevant to an investigation must be retained and unrecorded material recorded in some form.
- Relevant material which the disclosure officer believes will not form part of the prosecution case must be listed on a schedule which is given to the prosecutor (a separate schedule is required for any material the disclosure officer considers to be sensitive)
- The disclosure officer must draw to the attention of the prosecutor any material on the schedules that may assist the defence or may undermine the prosecution

case.

- The prosecutor is under a duty to disclose to the defence any material that may undermine the prosecution case or assist the defence (the disclosure test), unless that material is considered to be subject to public interest immunity (PII) in which case an application must be made to the court to withhold the material.

- The disclosure officer and prosecutor must keep the process under review throughout the life of the case, especially following the receipt of the defence case statement following initial disclosure, and further disclose any material not previously disclosed which meets the disclosure test (unless it is considered to be subject to PII).

9.8 The Attorney General has issued guidelines on disclosure (the Guidelines) which build on the existing law[118]. These Guidelines emphasise that 'the disclosure regime set out in the Act must be scrupulously followed'. This means that, for example, the practice that has grown up of the prosecution giving 'blanket' disclosure to the defence without applying the disclosure test, or the judge ordering such disclosure, should cease. In addition, the Guidelines also make it clear that where the defence seek further disclosure they should serve detailed case statements and make proper applications to the court explaining why they contend that the further material may undermine the prosecution case or assist theirs.

9.9 Very recently the President of the Queen's Bench Division, the Right Hon. Sir Igor Judge, has issued a Protocol for the Control and Management of Unused Material in the Crown Court (the Disclosure Protocol)[119]. Like the Guidelines the Disclosure Protocol stresses the importance of proper compliance with the Act and the need for proper defence disclosure.

9.10 In May 2005, a protocol covering, among other things, the disclosure of unused material in magistrates' courts was also issued. Although it is being introduced in 4 pilot sites, it is expected that all magistrates' courts and their practitioners will

be guided by the document. This protocol concludes that, *'The public rightly expects that the delays and failures that have been present in the past where there has been scant adherence to sound disclosure principles will be eradicated….It is now the duty of judges and magistrates to actively manage disclosure issues in every case. The court must seize the initiative and drive the case along towards an efficient, effective and timely resolution…In this way the interests of justice will be better served and public confidence in the criminal justice system will be increased.'*[120]

9.11 Recently joint CPS/ACPO operational instructions have been issued in the form of a comprehensive disclosure manual. This is to be regarded as the authoritative guidance on practice and procedure for all police investigators and CPS prosecutors.

9.12 HMRC and RCPO, the SFO and the DTI have their own internal guidance to investigators and prosecutors which is similar in spirit to the document referred to in paragraph 12.

9.13 As can be seen there is a real drive to ensure that disclosure is now handled properly in our criminal courts. We commend this approach.

Problem

9.14 Fraud trials can range from very straightforward 1 or 2 day cases involving a couple of forged cheques to cases involving highly complex business or financial issues, or sophisticated organised criminal gangs, often with an international dimension. The majority of fraud cases are straightforward and tried routinely in our courts by magistrates or judges with no particular expertise in fraud. We have not identified any real concern in the way that these cases are handled.

9.15 In order to understand the particular challenges that managing complex fraud trials pose to prosecutors, defence practitioners and judges the Fraud Review Team held meetings and seminars with investigators, prosecutors, criminal

solicitors, members of the judiciary and those responsible for delivering training to judges.

9.16 We found that there was a general consensus among those consulted that complex cases, including serious fraud, present particular problems for trial management and the handling of disclosure issues, notwithstanding the initiatives referred to above which are welcomed by everybody we spoke to. The failure to handle these problems properly can be extremely costly both in terms of money and the interests of justice.

9.17 The most expensive 1% of cases in England and Wales consume roughly 50% of the Crown Court legal aid budget. Fraud cases in that band are disproportionately expensive so that in 2003/4 they represented only 0.2% of Crown Court cases but 16% of the legal aid budget in the Crown Court (around £95 million). Of course these figures do not take into account investigation, prosecution and court costs. When one considers the length of some fraud investigations and eventual trial, these costs can be very high and doubtless run into hundreds of millions of pounds. Therefore failures in the pre trial and trial management process can have significant financial repercussions for limited public resources.

9.18 Such failures, which lead to trials being longer than necessary, can also lead to unfairness to the jury and to the parties in the case. For example, in the 'Jubilee Line' case[121], the jury was actually hearing evidence for less than 20% of the 21 month period the case lasted. This can hardly be a satisfactory state of affairs. That case collapsed before all of the evidence had been heard and without a verdict being returned. The official report into the handling of that case was published by HMCPSI on 27th June 2006.[122]

9.19 The Fraud Review therefore welcomes the setting up last year of a new body, the High Cost Cases Review Board (HCCRB), which has started to examine in detail the reasons for exceptional case length and cost in all cases estimated to last more than 6 weeks and to provide a general oversight of such cases. The Board's aim, as stated in its terms of reference, is 'to improve the financial control

and overall management of the highest cost cases, achieving more timely and effective disposal and restricting practice that leads to unnecessary expenditure'. The Board comprises key players from across the criminal justice system and looks at the whole issues raised by high cost cases.

9.20 As the CPS is responsible for prosecuting about 65% of high cost fraud cases, as well as the vast majority of fraud cases generally, we welcome the setting up of the CPS Fraud Prosecution Service in November 2005. This unit has responsibility for the handling, advice and prosecution of all serious fraud cases investigated in London by the City of London Fraud and Economic Crime Department and the Metropolitan Police. It also undertakes the prosecution of serious and complex fraud cases nationally. The FPS is a source of knowledge and expertise for the whole of the CPS. It has developed close and effective working relationships with other agencies such as the SFO, RCPO and is in dialogue with the Court Service over the effective listing, case progression and management of complex cases in line with the Lord Chief Justice's Protocol.

9.21 However, notwithstanding these positive steps, our consultations have led us to consider that there remain major concerns in the following areas: trial management; disclosure; electronic presentation of evidence.

Trial Management

9.22 The Review recognises that a great deal of responsibility lies with the prosecution and defence in such cases to ensure that cases are properly prepared clearly focused and that court orders are met. We have concluded that poorly thought out and executed prosecutions, or the unwillingness of the defence to provide properly detailed defence case statements or focus on narrowing the issues, can and do contribute to delay and waste of resources in some cases. Timely and comprehensive Defence case statements in particular can affect the progress and length of the trial in a variety of ways. The best can form the foundation for a true trial management partnership between prosecution and defence: producing agreed lists of admissions and live witnesses, reducing time spent on disclosed material and giving the judge proper information on which to base admissibility

rulings. The worst can prolong pre trial hearings, provoke late disclosure arguments and delay the trial. For example, in the GWT case examined recently by the Very High Costs Case Review Board (VHCCRB), late service (some 18 months after prosecution primary disclosure) of defence case statements delayed access to 3rd party unused material, raised new disclosure issues for the Judge and delayed the start of the trial.

9.23 As mentioned above, there is work being done within prosecuting authorities to improve the standard of case preparation and decision making in high cost cases. For example, as well as an intensive training initiative to ensure that prosecutors are being more proactive at the pre charge stage, the Crown Prosecution Service has established Case Management Panels which ensure a thorough scrutiny by senior prosecutors of cases likely to last 8 weeks or more. The CPS is also currently working on developing a complex case management framework aimed at addressing the legal, financial and strategic risks associated with large, serious and complex cases. The SFO and RCPO have also taken steps to tighten case management arrangements.

9.24 However we also recognise that the judicial role in case management is vital. A robust judge can ensure that the parties fall into line and co-operate with the spirit of the LCJ Protocol. This requires that once a case has reached the crown court, a trial judge of the requisite skills and experience should be identified at a very early stage and that judge should ensure that there is tight and robust judicial control of all aspects of the proceedings.

9.25 In his protocol the then Lord Chief Justice advised: *'The best handling technique for a long case is continuous management by an experienced judge nominated for the purpose'.*[123] Many elements of the scheme have been adapted from the civil courts. Lord Woolf has commented: *'If one is looking at a trial which threatens to run for months, pre –trial case management on an intensive scale is essential'*. It is inevitable that judges need adequate time, resources and training to achieve this.

9.26 At present it is the responsibility of the presiding judge on the relevant circuit to identify which judge should be responsible to hear a complex case. That judge

does so in consultation with the resident judge for the crown court where the case is to be tried, and with the Senior Presiding Judge of England and Wales who we know is acutely aware of the need to ensure that the right judges handle the most complex cases in our courts. We have seen the guidance issued by Lord Justice Thomas to all resident judges in May 2005 emphasising the need to refer to presiding judges all serious fraud cases even where the trial is estimated to last less than 4 weeks. The presiding judges are assisted in their task by regional listing coordinators whose function is to support them in managing the listing arrangements for the region and planning, developing, implementing and taking forward listing policy for the region.

9.27 In the past there has been a ticketing system for judges to hear 'serious fraud' cases. However, owing to the increasing difficulties of establishing a boundary for when a fraud trial became a 'serious fraud' trial (and merited a ticketed judge), and the general increase in trials involving a fraudulent element, the Senior Presiding Judge decided to cease issuing any further 'serious fraud' tickets. Nevertheless we believe that all Presiding and Resident judges continue to have regard to the appropriate skills and qualities required for trials in long and complex cases.

9.28 The Judicial Studies Board had in turn run specific course in the past for those with a serious fraud ticket with some useful input from the Serious Fraud Office. However, having trained all those ticketed, and with no new tickets being issued, two years ago the JSB was given approval by senior judiciary to expand the course to a wider audience by developing it into a seminar that dealt with the management of long and complex trials. This was also very much in line with helping to introduce the protocol issues by the Lord Chief Justice.

9.29 We have been told that whilst there is an appraisal system in place for Deputy District judges (and lay Magistrates), no such system exists for circuit judges or high court judges entrusted with the management of very high cost cases. In an age when performance appraisal is seen as a crucial management tool we were somewhat surprised at this, although we know that there would be practical difficulties to be overcome if such a system was introduced. We understand that

a useful pilot for the appraisal of recorders was conducted in the North West but that this has not been taken any further owing to the lack of available funding. We strongly suggest this is developed further as resources allow.

9.30 We note that the VCCRB has begun to analyse some high cost cases with a view to informing debate on the wider picture. However, without an appropriate study into the judicial handling of such cases, or any judicial appraisal system, the Fraud Review has been faced with the difficulty of not being able to identify the scale of the problem or training needs. The problems associated with dealing with disclosure of unused material in serious fraud cases are referred to below. These offences are likely to have been committed in a commercial or financially complex way with complex disclosure issues to be handled. Robust judicial intervention to ensure adherence to CPIA and requirements for proper defence case statements can be crucial.

9.31 The general principle that runs through the initiatives and protocols in place is that when a case actually comes to trial the issues in dispute should be clear, the expert evidence should have been narrowed down to focus on those issues, disclosure of unused material should have been dealt with and only those prosecution witnesses whose evidence is to be challenged should have to attend court. This can only be achieved if the Defence is obliged to play its full part in both the trial management and disclosure processes. There should be no place for ambush defences in complex fraud trials.

9.32 The criminal law has moved steadily over the past decades towards closer alignment with the civil courts in a variety of ways. Rules of evidence, use of skeleton arguments and preliminary hearings were all unknown in the Crown Court 30 years ago. All “importations” up to and including the latest complex trial protocol have been designed to improve the quality and efficiency of justice and the speed at which fair trials can be delivered. The time may now be right to move towards a full “civil” degree of mutual disclosure between prosecution and defence in fraud and other complex criminal trials. The prosecution are now bound to provide pleadings in the form of a case outline, lists of admissions and

issues and they must select relevant unused material to disclose. For the court, the picture can only be complete when the defence is also obliged to provide more than an "outline" of its case.

9.33 As a result of the wide ranging discussions we have had with Court practitioners we have concluded that whilst many fraud trials are managed well both before and during trial, some are not. We need not labour the point that even if only one of these trials is poorly handled this can have serious consequences for the interests of justice and the public purse. We have also come across instances of judicial difficulty in tackling repetitive cross examination and excessively long submissions during the trial. This may well also exist in the civil courts, though the recent BCCI case is not – as popularly thought – an example[124].

9.34 However we note that judges are not helped by the lack of effective sanctions available to them to address problems such as long-winded counsel, time wasting tactics and inefficient pre-trial preparation. As already mentioned, the consequences of inadequate judicial management of serious fraud trials can be serious in terms of expense to the public purse and the interests of justice. There is now a recent Court of Appeal authority which should give judges more confidence in robustly managing cases. As Sir Igor Judge says in this case: *' We should therefore emphasise that when dealing with matters preliminary to the trial…[the judge's] new case management powers permitted him to deal with these issues exclusively by reference to written submissions and…submissions limited to a length specified by him. He is not bound to allow oral submissions, and he is certainly entitled to put a time limit on them."*[125]

9.35 It is our conclusion that, as the LCJ Protocol recommends, the appointment at an early stage of a trial judge with robust case management skills and specialist knowledge where required is essential in all serious fraud cases scheduled to last more than 6 weeks. Our findings suggest that this does not always happen. For example, we were told of a complex fraud case at a crown court which deals with a lot of such cases where a 4th case management hearing was held in front of its 3rd judge. Even if each of those judges is experienced in dealing with such cases

this lack of continuity can lead to some trials lasting longer than necessary and some even spiralling out of control.

Electronic Preparation and Presentation of Evidence (EPPE)

9.36 The Review has also had consultations with practitioners about the value of electronic preparation and presentation of evidence (EPPE) in serious fraud trials. EPPE provides for the presentation of evidence to all parties by way of monitors installed in the court room so that everyone can look at the same document at the same time. We learned that there is current work being carried out by criminal justice agencies, surrounding proposing a common system for managing case documents during the investigative, pre-trial and trial stages. We believe that it is inevitable that such a system will have to be introduced at some point.

9.37 The general view we encountered was that long fraud trials benefit from electronic presentation of evidence, although some have expressed scepticism about this and pointed out that there is an absence of any empirical or statistical evidence of cost savings because of the use of EPPE.

9.38 Nevertheless the Review has concluded that there is a growing body of credible anecdotal evidence to suggest that EPPE can save between 10 and 25% of court time. The general consensus is that prosecution openings tend to be clearer and shorter. For example, use can be made of graphics to explain how an alleged fraud was committed and to show money trails, and the relationships between parties, companies etc. We were shown a good example of this used by the Serious Fraud Office in an environmental fraud case involving landfill tax credits which they prosecuted in 2004[126].

9.39 We have been told that time is also saved during the trial because of the ability quickly to bring up documents or schedules on to screens when required rather then having to direct the witness, jurors, judge, counsel and defendants to particular pages in their paper bundles. This causes inevitable delays while everyone finds the right page.

9.40 From the discussions it appears that although use of technology in such trials is growing, it remains subject to counsel's ability or willingness to adopt the practice and also to the availability of the equipment in the court room. Only a few court rooms throughout the country are permanently equipped with the required IT.

9.41 In 2001 the Courts Service began a pilot exercise as part of its Courts and Tribunals Modernisation Programme (CTMP) to install an EPPE court room into 10 court rooms at 9 crown court centres. The evaluation of the project was largely positive but concluded that a more detailed analysis needed to be done to evaluate the potential workload attracting the need for EPPE.

9.42 The pilot officially ended in 2003 and has not been further implemented since. Although the original sites are still used, we understand that there are practical problems which sometimes hinder the effective use of EPPE in those courts. When other courts are used the prosecution has to engage external suppliers on a case by case basis which proves extremely costly.

9.43 Currently there is a further EPPE pilot being carried out at Liverpool Crown Court. This is the HMCS Courtroom Audio Visual Solution (CAVS) project which envisages all crown courts being equipped with cabling and monitors to allow for electronic presentation of evidence, among other things. Currently we understand that there is no funding for this project to be rolled out further so again prosecution costs are often being incurred on an ad hoc basis to engage external suppliers. The Fraud Review acknowledges that there is further work being carried out to try to release funding for CAVS, and also to look at the use of compatible systems during the investigation stage, but has been struck by the lack of a rigorous cost benefit analysis into the savings that EPPE is likely to achieve in the long term. This would appear to be a significant factor in the lack of progress made during the last few years.

Disclosure

9.44 This issue has particular relevance to the Fraud Review as it has become clear that it is a major cost driver in complex fraud cases.

9.45 To take one example, it has been estimated that in the environmental fraud case prosecuted by the Serious Fraud Office (referred to at page 10), which culminated in a 94 day trial at Wood Green Crown Court in 2005, 6,000 prosecution man hours (250 complete days) were spent on dealing with disclosure issues. The defence spent 2643 hours just reading the material disclosed to them.

9.46 From our consultations with the SFO and other prosecuting authorities it is clear that this figure is likely to be dwarfed by the time spent on disclosure in other cases being investigated and then prosecuted in our courts. For example, in our consultations we learnt that there have been occasions where entire investigation branches at HMRC have been closed down for a period of time so that Investigators can give their full attention to disclosure on a given case. It has been suggested to the Fraud Review Team that up to 80% of investigators' and prosecutors' time can be spent on dealing with unused material in serious fraud cases.

9.47 The increase in the amount of material stored in a digital form will exacerbate this problem and pose a significant challenge to the effective investigation and effective management of complex fraud trials. We have found that concerns about the disclosure burden in serious fraud investigations are acting as a disincentive to police forces to accept cases. Even the SFO, which is specifically geared up to investigate and prosecute the most complex fraud cases, is being stretched by the increase in the amount of unused material, especially in digital form, which it is now encountering. One major concern of the Fraud Review is whether many police fraud squads in their current form have the resources to take on investigations of those complex cases which, not being dealt with by the SFO, would naturally fall to them. The Fraud Review has found evidence that strongly suggests that some serious fraud cases involving organised criminal networks are not being investigated owing to lack of police capacity.

9.48 We have learnt that increasingly in serious fraud investigations there is a massive amount of material, often in digital form, which is seized or copied by investigators. They are anxious to ensure that they have pursued all reasonable lines of inquiry and that they have retained all material that may have some relevance to the investigation. It is hardly surprising that many investigators in complex cases will err on the side of caution and retain all or most of this material rather than risk not retaining something that may later be regarded as potentially relevant and the lack of which may form the basis of an abuse of process argument. We have heard the argument that, when the obligations under the CPIA were being drawn up, the current difficulties caused by the sheer volume of material now commonly found during fraud investigations could not have been envisaged.

9.49 This problem is set to become even more acute. Our consultations strongly suggest that the time and resources required to deal properly with material stored in digital form in an average fraud case are increasing. This material is not just found on desk top computers but also on mobile phones, laptops, Blackberries and personal digital assistants which are frequently being issued by businesses to staff. This has tremendous implications. To give an example, the Computer Forensic Unit at the Serious Fraud Office has recently calculated that the average case it deals with now has between 5.3 and 6.7 Terabytes of digital material to be analysed. To put this into perspective, 5 Terabytes is very roughly the equivalent of a pile of paper 62 miles high (or 12 Mount Everests). A couple of years before, the average case it dealt with generated less than half of that amount. It is important that the sheer amount of material that has to be handled in most fraud cases of any complexity is appreciated by all those adjudicating in our courts on disclosure issues.

9.50 A great deal of this material will often not be used in evidence by the prosecution and will therefore be unused material. It is therefore vital that all parties in such a criminal prosecution have the resources and technology to deal with such material in an efficient and focused manner.

9.51 The recently published Disclosure Protocol (see para. 9.4) advises that if the CPIA is followed correctly further disclosure requested by the defence (after the prosecution has made its initial disclosure) should only be ordered by judges following service of proper defence case statements and where proper applications have been made in court. Section 8 CPIA relates to where the defence has given a defence case statement and the prosecution has provided disclosure of material that it has assessed may undermine its case or assist the defence. In that situation, where the defence has reasonable cause to believe that there is still undisclosed material that may assist it, the accused may apply to the court for an order requiring disclosure.

9.52 From the consultations we have had it appears that this procedure is not always followed leading to unnecessary costs and delays being incurred. We have been told of one serious fraud case where, some 2 years after the defendants had been charged, a defence submission that there had been an abuse of process because of failures in the disclosure process was upheld by the trial judge. The fact that not one section 8 CPIA hearing had been held during the case management stages, in a case where the amount of unused material was huge, strongly suggests that the disclosure provisions were being honoured more in the breach than the observance.

9.53 The Criminal Court practitioners that we have spoken to have broadly welcomed the initiatives to ensure that disclosure is dealt with strictly in accordance with the CPIA. This should ensure that, if followed correctly, there are fewer delays in bringing cases to trial and during the trial itself. In addition, dealing with unused material should become less of a cost driver in serious and complex fraud cases. However, there are still some practitioners who prefer the pre CPIA position of blanket disclosure. This nervousness can be caused by lack of confidence on the part of prosecutors about their understanding of the defence case. Proper and timely defence participation in the disclosure process is vital both to enable the court to make rulings (including rulings on PII) and to enable the prosecutor to identify "supporting" material. In this respect, fraud cases can be "special". As the LCJ Protocol on 22 March 2005 points out: *"…defendants are likely to be*

intelligent people, who know their own business affairs and who (for the most part) will know what documents…they are looking for."

9.54 We particularly commend the following passage from the disclosure section in the LCJ Protocol; ' *At the outset the judge should set a timetable for dealing with disclosure issues. In particular, the judge should fix a date by which all defence applications for specific disclosure should be made. In this regard, it is relevant that the defendants are likely to be intelligent people who know their own business affairs and who…will know what documents or categories of documents they are looking for…the judge should insist upon a list which is specific, manageable and realistic. The judge may also require justification of any request'.*[127]

9.55 The Attorney General's Guidelines state that, although generally unused material must be examined in detail by the disclosure officer, 'exceptionally the extent and manner of inspecting, viewing or listening will depend on the nature of material and its form. For example it might be reasonable to examine digital material by using software search tools, or to establish the contents of large volumes of material by dip sampling…the extent and manner of its examination must also be described together with justification for such action'.[128]

9.56 It is clear that in many fraud cases it can only be reasonable to examine digital material using such methods. The Review is concerned however that the increase in the amount of material stored in a digital form is making it more and more difficult and time consuming for investigators and prosecutors to comply with their disclosure duties under the CPIA, especially in cases where there is insufficient indication of what is in issue and what areas are particularly relevant to the defence. An experienced member of the judiciary to whom we spoke described it to us as an extraordinary and onerous obligation on the prosecution in some cases.

9.57 A special project group set up by the Fraud Advisory Panel in a recent report states that it 'does not believe that the problems regarding the ability to focus an investigation and the consequent disclosure of large volumes of unused material

will be solved until there is change in the provisions of the CPIA Code of Practice….the SPG believes the obligation upon the investigating authority to pursue all reasonable lines of inquiry to be wholly unrealistic in the circumstances of a serious fraud case.'[129] The Fraud Review has some sympathy with this conclusion bearing in mind the finite resources available to those investigating and prosecuting such cases. However, as a balance to this, it has been pointed out to us that the disclosure Code has always made it clear that reasonableness depends on the particular circumstances of the case and that the revised Code states that: '..*where material is held on computer, it is a matter for the investigator to decide which material on the computer it is reasonable to inquire into, and in what manner.'*

Strategy

9.58 The Fraud Review aims to develop a national anti-fraud strategy, which will provide a comprehensive understanding of the scale and nature of the fraud problem and a long term co-ordinated approach to tackling fraud. The effective management of cases that come before the criminal courts is one of a number of generic actions identified in the strategic model. A strategic approach is necessary to ensure that there is consistency in the quality of trial management and that, where there are weaknesses, they can be identified and rectified.

9.59 A co-ordinated approach to strengthen the national response to tackling fraud will include the need for an effective trial management regime which can identify where there are weaknesses and address them effectively.

Options

9.60 Having considered the evidence and the results of our consultations, we identified and considered a number of options aimed at improving trial management in complex fraud cases and to provide an assurance of quality to the public who foot the bill for criminal trials, whilst retaining their confidence in the fairness of the proceedings.

A National/Regional mechanism for the co-ordination of fraud cases

9.61 A mechanism for co-ordinating fraud cases will be necessary to provide for the oversight of complex fraud trials in England and Wales, either on a regional or national basis. Appropriate co-ordination would control the 'ticketing' arrangements (see paragraph 45), ensure liasion with the Senior Presiding Judge, presiding judges and regional listing co-ordinators over the allocation of cases, promote a consistent and co-ordinated approach to the training of judges authorised to hear serious fraud cases, oversee any appraisal in relation to the 'fraud' judges and provide a valuable link with the Very High Cost Case Review Board.

Specialised Judges

9.62 The creation of a cadre or panel of specialist fraud judges from which presiding or resident judges must draw when allocating the judge for fraud cases estimated to last more than six weeks has been recommended by the VHCCRB. It is suggested that there should be a mix of High Court and Crown Court judges with fraud 'tickets' but each would have familiarity with financial and commercial matters and robust trial management skills. We have rejected the idea that such judges would only try serious fraud cases as it has been persuasively argued that the best judges tend to be good trial managers across the board. However, bearing in mind the costs of these trials, such a panel would provide some safeguard that scarce public resources are being used in the most efficient way possible.

Ad hoc appointment

9.63 Given the Government's intention to introduce a Bill reflecting Lord Justice Auld's recommendation that some complex fraud trials should be tried without juries, it may be possible to consider using either experienced barristers or City solicitors

who specialise in fraud or commercial work as recorders on an ad hoc basis to try specific complex fraud trials. Such appointments might well be worthy of consideration in the context of non jury trials.

Specialist Fraud Training

9.64 Judges attend training courses once a year organised by their own circuit. This training involves a range of topics including sentencing and anything identified as particularly relevant at the time. They also attend a 3-4 day continuation course every 3 years, which has modules covering various topics in which trial management features as an element. These courses are regarded highly by the judiciary. However, there is no specific training course offered to judges on managing serious fraud trials, although there is a 1 day course that they can attend on long and complex trial management. This option envisages a compulsory training course for the specialised judges referred to above covering financial matters and dealing with disclosure in high volume cases, as well as case management skills.

Specialist Training in Complex Case Management Skills

9.65 An alternative option reflects the view among most judges that specialist case management skills are more important than specialised financial knowledge and are essentially the same whether handling complex drug trafficking cases or complex fraud cases. This option takes into account the current training available to judges from the JSB but suggests that the course should be longer than 1 day to take into account the requirement to cover issues such as disclosure, use of IT, assertiveness training etc in more detail.

Amendment to CPIA

9.66 This option is based on the premise that when the CPIA was drafted the amount of digital material now come across by investigators in serious fraud cases could not have been envisaged. The rationale is that there has to be some way found of allowing those responsible for disclosure in such cases to do so with a clear

focus on what the issues are at an earlier stage than hitherto. In this way they can intelligently search the unused material for items that are relevant and need to be scheduled; and then intelligently identify those items on the schedule that may undermine the prosecution case or assist the defence.

9.67 The CPIA could be amended so that in high volume cases such as serious fraud, there is a requirement on the defence to provide a defence case statement, or a pleading document, once the prosecution case has been served and that only when that has been done would the prosecution be under a duty to consider initial disclosure of unused material. Such an approach would ensure that the defence case statement would be based on the response to the prosecution case rather than what happens to emerge from the unused material in the case.

9.68 Alternatively, a system could be introduced similar to that in the USA and which has found favour with the Fraud Advisory Panel's recent report. That proposal envisages that the prosecuting authority could go before a judge with a particular class or classes of material that have not yet been analysed where there is nothing at that point to suggest relevance to the case. The authority could seek a ruling to support that assessment and, if successful, the burden then shifts to the defence to show a sound basis for any request for disclosure of that material. It is argued that in complex fraud cases the accused is often in a better position than the investigators to know whether certain material is relevant.

9.69 Although this is controversial, it has been argued that at some point a choice will have to be made between amending the CPIA, together with the Code of Practice, and a lot of complex fraud cases simply being beyond the resources of investigating and prosecuting authorities.

Access to a Judge During Investigation Stage

9.70 This option also envisages an amendment to the CPIA by removing the obligation on the prosecution to pursue all reasonable lines of inquiry, but introducing safeguards in the form of judicial oversight and the ability for the defence to make representations to the judge. The prosecuting authority could be

given access to one of the specialist fraud judges to apply for authority to confine its investigation in a certain area. This could be at a pre charge or post charge phase. Where such approval is sought the suspect, or defendant if already charged, could make representations to the judge that the investigator should pursue a particular line of inquiry or to obtain and/or disclose unused material where the court was satisfied that this was necessary to allow the suspect/defendant to advance his defence.

Introducing a Specific Protocol for Disclosure in Complex Fraud Cases

9.71 As mentioned, the Senior Presiding judge has issued a specific protocol giving guidance on disclosure in crown court cases and there is a specific protocol issued by Lord Woolf, the former Lord Chief Justice, on the management and control of complex cases. The latter includes a section on how disclosure should be handled in these cases. This option envisages no change to legislation but instead a specific protocol being issued on the handling of disclosure in complex fraud and other high volume cases. Such a protocol would reflect the unique problems faced by those handling disclosure in this area, including the need for the Defence to play a more active part in the disclosure process.

Cost Benefit Analysis for EPPE

9.72 At present the evidence given to us about the savings EPPE would deliver has been largely anecdotal. Because financial resources will be needed in order to introduce a standardised IT system into our court rooms to facilitate EPPE, any business case would be much stronger if it was based on a rigorous cost benefit analysis rather than practitioners' own experience and impressions.

Conclusions

9.73 Complex fraud trials consume large amounts of public money and require judges highly skilled in case management. They also often require specialised financial or business familiarity; both amongst counsel and the judiciary who must

currently advise the (fact finding) jury. . As a matter of principle, the public which foots the bill for these trials is entitled to expect that such cases are dealt with in the most efficient way possible.

9.74 Our overall conclusion is that, whilst many complex fraud trials are dealt with in a focused and efficient way, some are not. We welcome the initiatives now in place to improve case preparation and trial management. These provide judges with some of the tools to manage effectively. We accept that it is perhaps early days to evaluate the impact these are having but feel that because of the pivotal role of the trial judge in ensuring efficiency there needs to be a more rigorous system in place to ensure that the selected judge uses these tools properly. This requires robustness, support and a high level of case management skills as well as performance monitoring, not least in dealing with disclosure issues.

9.75 Judges can only manage effectively if they have the support and assistance of both Prosecution and Defence. We consider that in Fraud and perhaps other complex cases it would now be reasonable to expect the Defence to produce clear and comprehensive statements of case (in a form more akin to civil court pleadings), addressing in detail the individual issues and facts in dispute. This would provide the fullest assistance to the Judge whose pre trial responsibilities are constantly increasing.

9.76 We have concluded however that judges have few effective sanctions available to them to tackle non compliance with the spirit of the new effective trial management culture and that this is an area that could usefully be looked at further. We also consider that professional bodies have a responsibility to provide a lead by robustly dealing with those who fail to abide by the spirit of the various initiatives now in existence.

9.77 In addition, we are convinced that there is an unprecedented challenge facing the criminal justice system as a whole in relation to the handling of material stored on computers and other digital media. This poses particular problems in the area of disclosure of unused material. We have heard a great deal of evidence to suggest that investigators and prosecutors in complex fraud cases are finding it

increasingly difficult to deal with the sheer volume of material uncovered in such cases, and that too often judges are acceding to speculative defence requests for further disclosure rather than strictly applying the CPIA test.

9.78 However, we believe that any recommendation to amend the CPIA or the Code at this stage would be premature because our research has suggested that they have not been applied consistently and properly by some practitioners and some of the judiciary. In our view it is likely that proper observance of the CPIA and the Code will remove some of the difficulties faced by disclosure officers and prosecutors in discharging their duties in this area. The current drive to ensure that the Act is properly and rigorously observed in our courts must be given a chance to work, but we also would like to ensure that the position in relation to serious fraud cases is reviewed again in two years time.

Recommendations

9.79 The recommendations are as follows:

- That a national judicial serious fraud co-ordinating mechanism be set up to cover responsibility for controlling the 'ticketing' arrangements, liaising between the Senior Presiding Judge, presiding judges and regional listing co-ordinators over the allocation of cases, promoting a consistent and co-ordinated approach to the training of judges authorised to hear serious fraud cases and exercising a leadership role over fraud issues within the judiciary. This mechanism should also provide for an appraisal function in relation to the 'fraud' judges and provide a link with the Very High Cost Case Review Board.

- That a panel of judges be created from judges who have been identified as having the relevant expertise to handle complex cases and familiarity with the financial or commercial elements involved. Initial appointment to be based on evaluation by the presiding judges of the circuits but thereafter being dependent on having undergone appropriate specific training. This recommendation does not envisage that these judges would be confined only to fraud work.

- Specialist training should be provided in skills identified by the judiciary as required to satisfy public confidence and the development needs of the judges. This must include dealing with disclosure issues and trial management according to the Lord Chief Justice's Protocol.

- We also recommend that there should be a study carried out on the effectiveness of the sanctions currently available to judges when faced with inefficiency or obstruction (including failures to provide adequate defence case statements), with a view to consideration being given to increasing the powers available.

- We recommend that in appropriate cases the prosecuting authorities ought to have a facility for early access to the appointed judge any time post charge to argue in the presence of the defence that they be excused from actually examining a category of material where to do so would be unduly onerous. This would only be where there is no suggestion at that stage, in the absence of any detailed defence case statement, that the material is relevant.

- At this stage we make no recommendation concerning changing the disclosure regime or amending the CPIA in high volume cases as a great deal of work has been done in this area in the past couple of years and the impact of this work, and the more general work on trial management, cannot yet be assessed. However, we do recommend that this specific area is looked at again in 2008 by a special working group, consisting of practitioners and members of the judiciary experienced in complex fraud, as well as representatives of relevant government departments, specifically to review the success of current improvements to the disclosure and trial management regimes and to consider whether amendments to the Protocols and/or CPIA ought to be considered or recommended.

- A cost benefit analysis should be commissioned into Electronic Presentation of Evidence to provide rigorous evidence of any savings in time and resources.

CHAPTER 10 SENTENCING FRAUD

10 SUMMARY

- The Interim report of the Fraud Review noted that: 'there is a perception that those convicted of fraud receive relatively light sentences compared with those convicted of other acquisitive crimes.'

- The Review found that the average custodial sentence in a case brought by the Serious Fraud Office, where by definition the fraud involves at least £1 million, is three years.

- The average custodial sentence in the magistrates court for fraud was three months. The average custodial sentence in the Crown Court (for Fraud and Forgery) was 15.4 months. The average length of a custodial sentence for conspiracy to defraud was 25.6 months.

- Fraud is punished as severely as theft and handling but less severely than burglary or robbery, even though the amounts of money involved are usually much greater.

- Sentences in breach of trust cases appear to be lower than (Court of Appeal) guidelines suggest. The Sentencing Guidelines Council has not published specific guidelines for fraud offences.

- The Review has considered ways of improving fraud sentencing and recommends that with the introduction of the Fraud Bill, the Sentencing Guidelines Council should issue specific sentencing guidelines for all fraud offences and should commission further work into an advisory matrix system.

- The Review also recommends that for the most serious offences the maximum sentence for fraud should be increased from 10 to 14 years.

Introduction

10.1 This chapter highlights the current approaches to fraud sentencing; it provides some statistical information about the relative sentences for fraud offences compared with other acquisitive crime; identifies areas of weakness in the present arrangements and makes recommendations for change.

10.2 This chapter draws on consultations with the Home Office, Sentencing Guidelines Secretariat and others with an interest in the sentencing process. The results of specially commissioned research into this area by Professor Levi have also been drawn on in preparing this chapter. (A full copy of Professor Levi's research will be published separately.)

Sentencing Data - Key Findings

10.3 In 2004, across all courts in England and Wales, custodial sentences were imposed on 20 out of 42 defendants sentenced for 'fraud by company director'; 176 out of 709 defendants were given custodial sentences for 'false accounting' and a total of 2,371 out of 11,662 defendants were given custodial sentences for 'other fraud' (which includes credit card frauds) whilst 31 out of 173 defendants were sentenced for bankruptcy offences.[130]

10.4 The statistics for the period 1994-2004 show that custody rates and average custodial sentences for fraud and forgery are similar to custody rates and sentences for theft and handling, however those for burglary and robbery remain significantly higher.

10.5 The Court of Appeal guidelines for breach of trust (which were issued in respect of theft) highlight the public significance of the breach of responsibility in such cases and recommend custodial sentences in most circumstances. However Crown Court data for 2004 showed that just over two thirds of offenders in conspiracy to defraud cases (not all of which involve an element of breach of trust) were given custodial sentences.

10.6 Over a period of five years, the average custodial sentence for persons convicted in SFO cases was 31.7 months; half of those convicted received sentences of 3 years or less. Out of the 53 cases in which convictions were obtained, the average sentence of the most severely sentenced person per case was 37.7 months imprisonment.[131]

10.7 The following sections examine the sentencing framework and the role of the Sentencing Guidelines Council.

Sentencing: Basic Framework

10.8 Parliament creates the framework in which sentencing takes place by setting the maximum sentence for different offences and by creating different sentencing categories. The three main statutes which have had an impact on recent sentencing practice are: The Criminal Justice Act 1991; The Powers of Criminal Courts (Sentencing) Act 2000 and The Criminal Justice Act 2003.

10.9 The sentences available under the Criminal Justice Act 2003 for adult offenders include: compensation orders; fine; community sentence and imprisonment. There is also a list of ancillary orders and/ or preventative orders which the courts may use in appropriate cases, such as ASBOs, deportation and confiscation orders.

10.10 Section 142 of the Criminal Justice Act 2003 sets out the purpose of sentencing (see table below), but it does not clarify how sentencers should balance the differing priorities. This may lead to inconsistency and inequity in fraud sentencing since there is evidence to suggest that 'white collar crime'[132] and for example, benefit fraud are treated very differently.

Purpose of Sentencing: Section 142 of the Criminal Justice Act 2003

- The punishment of offenders
- The reduction of crime (including its reduction by deterrence),
- The reform and rehabilitation of offenders
- The protection of the public
- The making of reparation by offenders to persons affected by their offences

10.11 A sentencing judge will need to begin by considering the nature of the offence, keeping in mind any relevant guidelines. Section 143 of the CJA 2003 also requires the court to consider 'the culpability of the defendant and any harm which the offence caused, was intended to cause or might foreseeably have caused'. The judge will also need to consider the aggravating and mitigating features of the offence and any sentences imposed on other defendants connected with the case. Having taken these matters into account the judge will decide on the starting point for the offence and will then consider the defendant's plea, personal mitigation and any pre-sentence report.[133]

10.12 In passing sentence, the court should also consider whether compensation is appropriate, whether costs should be awarded against the defendant and whether there is any other ancillary order which should be added to the sentence. In appropriate cases a confiscation order will also be made, but the effect of such an order does not impact on the length of custodial sentence.

Role of Sentencing Guidelines Council

10.13 The Sentencing Guidelines Council and the Sentencing Advisory Panel are independent non-departmental bodies that work together to research, consult on and publish sentencing guidelines. The Sentencing Guidelines Council was created in 2004 in order to frame guidelines to assist courts as they deal with criminal cases.

10.14 The Sentencing Guidelines Council, guideline: 'Overarching Principles: Seriousness' assists the courts with the assessment of offence seriousness in accordance with Section 143 of the Criminal Justice Act 2003. This guideline discusses the key concepts of culpability and harm referred to in Section 143, and identifies common aggravating and mitigating factors which may bear upon the levels of culpability and harm present in a particular case. Under the Criminal Justice Act 2003, the courts' assessment of offence seriousness is central to determining whether the thresholds for imposing community or custodial sentences have been passed.

10.15 The Sentencing Guidelines Council's general approach in its guidelines for specific offences is to identify common forms of the offence and to indicate starting points and sentencing ranges for each form. The guidelines also identify aggravating and mitigating factors likely to be of particular relevance to the offence, which may take the sentence up or down from the indicated starting point. A list of general aggravating and mitigating factors, to which sentencers should also have regard, (see Annex E) is set out in the guideline 'Overarching Principles : Seriousness'.

Fraud Guidelines

10.16 Until the Fraud Bill is introduced, there remains no set definition for fraud offences. In addition, the Sentencing Guidelines Council has not published guidelines on fraud offences. However the Sentencing Advisory Panel is currently undertaking work on guidelines around theft and dishonesty offences. These include: theft from a shop, theft in breach of trust, and theft from the person. There are also plans to consider offences involving deception, fraud and forgery in a future consultation paper.

10.17 Prior to the establishment of the Council, the Court of Appeal gave judgements which, in addition to dealing with the case in hand, provided guidance on sentencing future similar cases. A collection of these Court of Appeal guideline judgments has been published by the Sentencing Guidelines Council. The compendium includes Theft Act offences/fraud and involves a range of cases

including benefit and mortgage fraud, obtaining money transfer by deception and Excise/Revenue fraud.[134]

Sentencing Rationales

10.18 A comprehension of the rationales of sentencing is important in informing our understanding of the current sentencing practices. The main rationales focus on deterrence, incapacitation, rehabilitation, desert, and reparation.

10.19 Judges are required to give attention to the variety of different and often conflicting purposes contained in Section 142 of the CJA, however issues arise over the discretion they may have in selecting which type of sentencing rationale to adopt in each case. In the words of an academic commentator: this may be 'more of a licence for judges to pursue their own penal philosophies than an encouragement to respond sensitively to the facts of each case.'[135]

10.20 The rationale of general deterrence has been viewed by many proponents as a key aim of sentencing, the assumption being that individuals will adjust their behaviour according to sentencing laws. The deterrence rationale has featured in offences such as robbery and drug trafficking, where sentence penalties are severe in order to achieve a high level of prevention of such crimes. However opinions about the success of deterrence as a rationale remain divided. Research indicates that the probability of detection has a bigger impact on reducing offending than an increase in the length of sentence (unless sentences are substantially increased.) This may be particularly true for fraud offences which are perceived as a low risk activity.

10.21 The high prevalence of fraud much of which is not reported or prosecuted suggests that current fraud sentences in the UK are not viewed a deterrent and in particular, 'white collar' fraudsters may be treated more leniently by the Courts. In a recent survey carried out by BDO Stoy Hayward, three quarters of people interviewed thought that the average custodial sentence was insufficient to deter a fraudster.[136]

10.22 Professor Levi notes that most of the criminological evidence against the deterrent effects of imprisonment for property crimes has been collected in areas of opportunist, low-value crime. He argues that for high value crime, the deterrent effect must take into account not only the prospect of being caught and sanctioned by the courts but also the impact of confiscation, since fraudsters may be willing to go to prison for short periods if the rewards are great enough on their release. [137] In addition there may be variations in the deterrent effect depending on personality and how embedded those contemplating fraud are in respectable social networks and on their beliefs about levels of disapproval from those they care about.

10.23 Incapacitation of offenders or 'public protection' is another widely cited rationale. This is usually applied to groups of dangerous, organised or persistent offenders. Such offenders may receive very long custodial sentences in order to prevent them from committing a further serious offence, and causing harm to future victims. In the context of fraud, however, protecting the public from future frauds is an important aspect of sentencing which has hitherto received insufficient attention. Crown Court sentencing powers could therefore involve a wider range of public protection remedies than is presently utilised. (See chapter 8 for further details.)

10.24 The rehabilitative rationale is concerned with the rehabilitation of the offender as a means of achieving the prevention of crime and unlike the deterrence theory regards offenders as being in need of help and support. Critics of this approach view treatment programmes as largely ineffectual and point to high re-offending rates for those released from prison. In a recent speech which focussed on those serving short sentences for the less serious offences, Lord Phillips noted that whilst rehabilitation can start in prison for serious offenders, for others it can more effectively be achieved as part of a community sentence.[138]

10.25 Desert theory or 'just deserts' is a modern form of retributive philosophy, which highlights that proportionate sentences are needed to punish offenders and also deter others. It has however been argued that it is difficult to provide guidance on proportionality and it is also important to distinguish between 'ordinal

proportionality which concerns the relative seriousness of offences and cardinal proportionality, which relates the ordinal ranking to a scale of punishments, and requires the penalty to be in proportion to the gravity of the crime involved'.[139] Issues remain about what makes offences more or less serious, however Professor Levi notes that retributivism contains two dimensions of sentencing - harm and culpability, around which various aggravating and mitigating factors are clustered.[140]

10.26 The rationale of restoration and reparation has gained increasing significance in the light of government initiatives to place victims at the centre of the criminal justice system. This rationale focuses on the need for the offender, victim and wider community to take a role in deciding the appropriate measures for an offence. Emphasis is placed on compensating victims and ensuring that the offence is not repeated. In the context of sentencing fraudsters, the need for punishment must be balanced with restitution, since a key element for victims involves a greater focus on compensation and the recovery of assets. In order to facilitate this, the criminal court has at its disposal, ancillary orders which include confiscation, restitution and forfeiture orders.

10.27 It is evident that different prosecuting departments such as the CPS, FSA and NHS, employ different strategies for dealing with fraud offences and some departments such as HMRC and DWP focus primarily on protecting the public revenue from fraud. Professor Levi acknowledges that there has historically been a major difference between utilitarian and retributivist approaches to criminal justice and to sentencing and these approaches are reflected in the way that fraud is detected, investigated, prosecuted and punished across different departments. Such differences may be driven by resource issues, departmental traditions or investigative and prosecutorial difficulties rather than evidence about harm.[141]

10.28 The Review does not seek to address the differences in approaches to sentencing; however the introduction of a national anti-fraud strategy and other proposals will provide a more coherent framework for those involved in targeting

the prosecution and punishment of fraud and will ensure that objectives and resources are targeted in the best way possible.

10.29 The following sections will examine the statistical evidence around sentences in more detail, but it is noteworthy that the lack of fraud sentencing information compiled by government departments may indicate that the sentencing of serious fraud has never been seen as anyone's core or even subsidiary business.[142] Whilst the Home Office is responsible for providing sentencing statistics, it does not collect any information about the value involved in offences of theft or fraud. This can make it difficult to analyse information about sentence lengths for high value frauds.

Problem:

Relatively Low Sentence Levels for Fraud:
Magistrates & Crown Court

10.30 It must be noted that the comparability issue for fraud and other acquisitive crime is problematic, since offences such as robbery and burglary, which contain elements of threatened or perceived violence are accorded a greater harm priority by the general public and the media. In addition, especially in frauds committed within organisations by high status people, serious fraud offenders may typically have fewer previous convictions than other offenders.

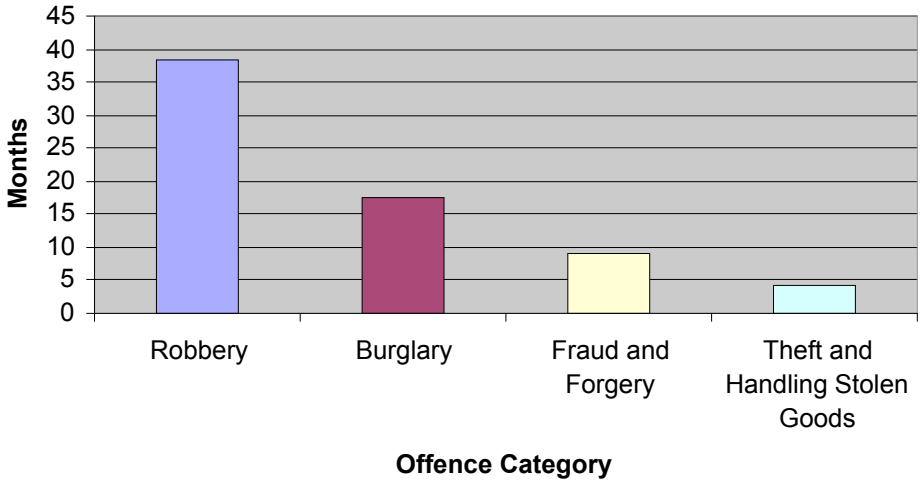
10.31 Nevertheless the statistics for fraud and forgery show a level of similarity with those for theft and handling offences. Between 1994 and 2004, community sentences were the most common sentence for fraud offences. This was also the case for burglary and theft and handling. However it is to be remembered that Home Office figures for fraud and forgery cover a wide range of seriousness from very low level dishonesty to very serious frauds which can significantly affect the lives of victims.

10.32 Between 1994 and 2004 there was a general increase in custody rates but a slight decrease in the average custodial sentence length for fraud and forgery

offences. In 2004, the average custodial sentence length for fraud and forgery was 9.2 months in comparison to 4.3 months for Theft and Handling, 17.5 months for burglary and 38.4 months for robbery (see fig 1).

10.33 In 2004, the average custodial sentence length in the Magistrates Court for fraud was 3 months in comparison to 4 months for commercial burglary and 3 months for theft and handling stolen goods.

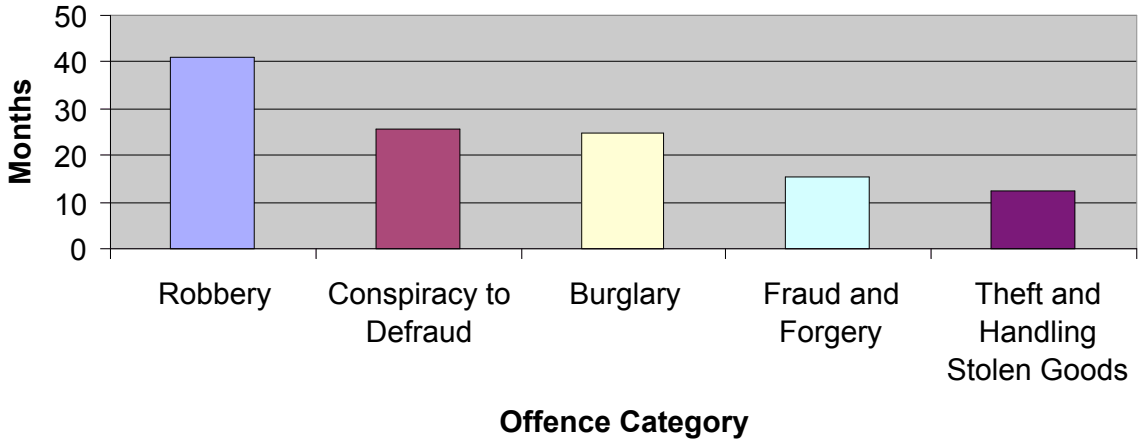
Fig.1. Combined Average Statistics from Crown and Magistrates Court - 2004



Crown Court

10.34 Conspiracies to defraud offences (which carry a maximum sentence of 10 years) are typically heard in the Crown Court. In 2004, 68.65% of conspiracy to defraud cases were given custodial sentences and the average custodial sentence length for conspiracy to defraud was 25.6 months. The average custodial sentence length for fraud and forgery was 15.4 months, theft and handling was 12.3 months, burglary was 24.6 months and robbery was 41.1 months (see fig 2).

Fig. 2. Crown Court Only - 2004



10.35 Comparative figures for fraud and other acquisitive crimes between 1994 and 2004 are illustrated in figures 3 and 4 below.

Figure 3. Crown Court Custody Rate 1994-2004

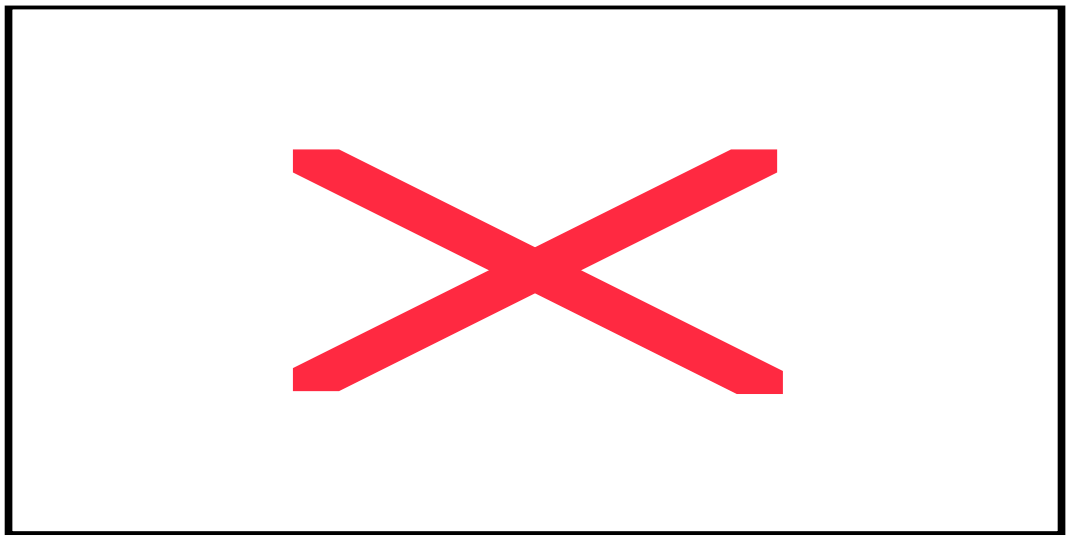
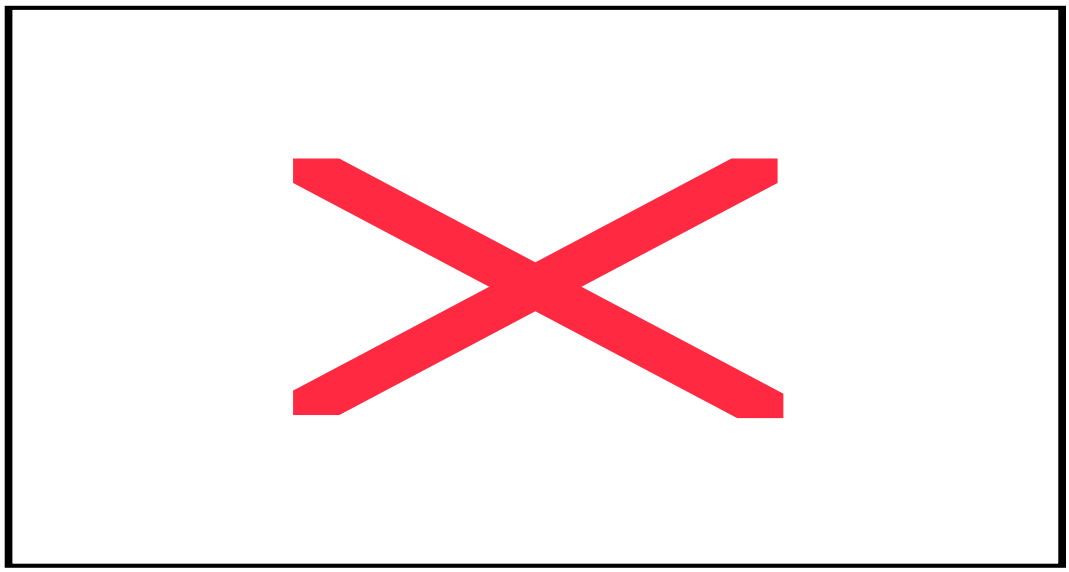


Figure 4. Crown Court Average Custodial Sentence Length (months) 1994-2004



10.36 Custodial sentences for fraud appear relatively low. Just over half of those convicted for fraud and forgery in the Crown Court in 2004 received custodial sentences. However it is important to view these sentences in the light of government policy which advocates that prison should be reserved for dangerous, serious and seriously persistent offenders. 'Fraudsters do not generally fall into that category, and sentencers are aware that the prisons are full and expensive so where they find offences that do not attract so much opprobrium in the media…it may be tempting to reflect this in lighter sentencing.' [143]

10.37 Statistical data for the Serious Fraud Office which typically handles the most complex fraud cases for amounts in excess of £1 million, shows that between 2000- 2005, 109 convictions were achieved and the average sentence length was 31.7 months. Half of those convicted received 3 years or less, the average sentence imposed on the most severely sentenced person per case was 37.7 months. Eight defendants received sentences longer than five years, 19 defendants received 4-5 year sentences; and 22 defendants (mostly co-defendants in cases where others were imprisoned) received non-custodial sentences.

10.38 Despite the fact that defendants who assist the authorities and plead guilty are likely to receive substantial discounts on the starting point for sentences, the SFO data is still surprising. The research of accountancy firm BDO Stoy Hayward which noted that for those frauds over £5m, (some but not all of which would have been SFO cases), the average sentence had reduced from 4.2 years in 2003 to 3 years in 2005 lends support to the perception that those convicted of fraud receive relatively light sentences.

Inadequate Sentencing Guidelines for Fraud Offences:

10.39 The lack of a systematic sentencing system has raised issues around consistency and transparency. In his foreword to the 'Guideline Judgments Case Compendium' published by the Sentencing Guidelines Council, Lord Justice Rose, the then Deputy Chairman of the Council noted that: 'sentencing is a complex and difficult exercise. It can never be a rigid, mechanistic or scientific process'[144]. Nevertheless it has been argued that mitigating and aggravating factors which the UK judiciary must consider can lead to a wide disparity in sentencing even where guidelines for that offence exist.

10.40 It is pertinent in our discussion of sentencing serious fraudsters to examine the guidelines for conspiracy to defraud/ breach of trust cases, since these cases often raise issues of appropriate sentencing for the more serious crimes and may present sentencers with difficult issues in terms of aggravating and mitigating factors

10.41 Cases may involve defendants who are first time offenders and who have acted 'out of character'. Such offenders are often regarded as low risk and well behaved. The very nature of the offence and internal disciplinary sanctions taken against such offenders may also prevent them from future employment. These are issues which are unlikely to confront a judge sentencing other types of crime where perpetrators have different characteristics. On the other hand, breach of trust cases should be treated as particularly serious since abuse has been perpetrated by those in positions of responsibility. Such offenders may occupy positions of high seniority, but this will not always apply as even those in lower

positions can abuse the trust associated with their official responsibilities. Such offences may also have continued over a substantial period of time and involved a degree of planning.

10.42 A study by Martin Gill, which was based on interviews with 16 convicted fraudsters, found that offenders abused the position of trust because 'it was that that gave them the autonomy and the lack of visibility to commit offences and caused them to feel they would not be detected'.[145] In addition, the research showed that offences had been committed over many months and often over a number of years.

10.43 The Court of Appeal under Lord Lane CJ made some important findings by issuing guideline judgements for breach of trust cases. In the Court of Appeal guideline case of R v Barrick (1985), the defendant was convicted of stealing £9,000 from a small company to which he had acted as an accountant for some years. He was 41 years old and was of previous good character. He was sentenced to two years imprisonment on conviction following a plea of not guilty. The case of Barrick also set out nine factors relevant to seriousness which the sentencing courts would need to take into account. These included the rank of the offender and the degree of trust in which he or she was held; the period over which the fraud had been committed and the use to which the money had been put. The guidelines in Barrick were subsequently revised by R v Clark (1998) which adopted the tariff at [figure 5.]

10.44 Interestingly in his guideline judgment, Lord Lane CJ concluded that professional men should expect to be punished as severely as the others and in some cases more severely. In general, a term of immediate imprisonment would be inevitable, save in very exceptional circumstances or where the amount of money obtained was very small.

10.45 To what extent have these guidelines been adopted by the courts? A Home Office research study conducted in the mid 1990's noted that just over half of the cases involving breach of trust did not receive a custodial sentence. [146] Despite

the Barrick guidelines, it would appear that 'white collar' offenders may still be treated more leniently than others.

Figure 5. Tariff: Breach of Trust Cases

Amount Stolen	Guideline Sentence
Amount stolen is not small but is less than £17,500	Custodial terms from the very short to 21 months
£17,500 - £100,000	2 - 3 years custodial sentence
£100,000- £250,000	3 - 4 years custodial sentence
£250,00- £1million	5-9 years custodial sentence
Over £1million	Custodial sentence of 10 years or more

Low Levels of Victim Satisfaction with the Prosecution and Punishment of Fraud

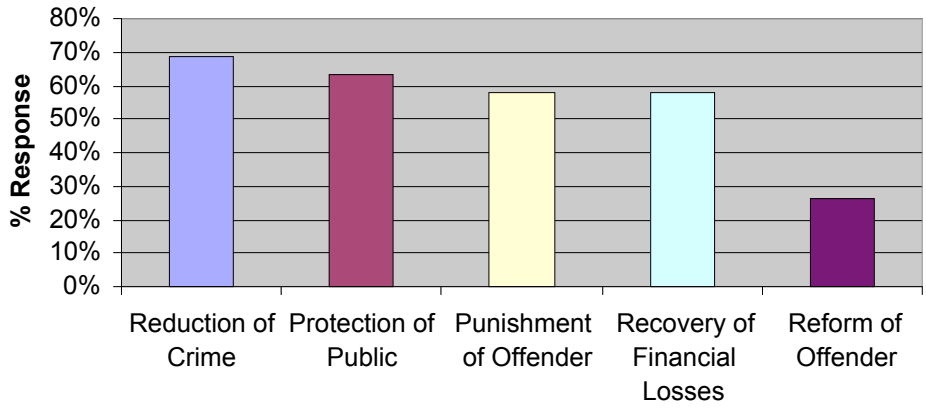
10.46 Unlike other acquisitive crime, fraud involves exploiting a victim's weakness and trust, since compliance is generally the key to a successful fraud. Victims often suffer greatly from fraud and that suffering can span a number of years. The long term impact of the fraud remains, causing financial, emotional and health problems whilst offenders are perceived as being dealt with lightly.

10.47 The impact of fraud is often underestimated, but the effects can be particularly devastating for vulnerable victims 'such as the elderly, the socially isolated and the disabled… for some the betrayal of trust can be the same or worse than the actual loss itself.[147] More effective sentencing and use of ancillary orders to deal with the restorative and preventive elements of sanctions is clearly needed.

10.48 The Fraud Review has conducted a small scale survey of victims of fraud. (Annex D) Over half the victims ranked the punishment of the offender as being

very important in the outcome of their case, however a higher number wanted the public to be protected against future frauds. (See Fig 6).

Fig. 6 Results of Victims Survey



10.49 The results of the survey showed that only 18% of victims expressed a high level of confidence in the criminal justice system. A number of victims expressed frustration at the lengthy process of bringing offenders to court as well as the inconsistency in sentencing outcomes (see extracts below).

- "Regrettably the offender will probably only serve half of his sentence but his investors got nothing back."

- "Heavy penalties would help so the cost to the criminal is greater than his gain. Prison is only a part of it."

- "It has ruined my life- both working (I can never retire) and my personal life. The thought of what happened haunts me 24 hours a day!"

- "Conviction did not match crime/stress involved as funds were never recovered."

- "The penalty was OK but the offender will still be a multi-millionaire when he gets out. But his millions belong to the victims who invested with him- they get nothing."

Extracts from Fraud Review Victims Survey (2006)

10.50 Victim satisfaction now plays a much more central role in the criminal justice system and the making of reparation by offenders to victims is cited as a purpose of sentencing under Section 142 of the Criminal Justice Act. This is part of a more general move to recognise the rights and needs of victims. Recent initiatives include the introduction of the use of victim impact statements in court, and the Code of Practice for Victims of Crime, which places an obligation on various organisations to inform victims about the progress and outcome of their case.

10.51 Compensation orders clearly play a significant element in the assistance of fraud victims, who wish to avoid the expense of civil proceedings. It has also been established that an offender's ability to pay compensation should not be allowed to deflect the court from imposing a custodial or community sentence, if that is what the offence justifies.[148]

10.52 Home Office figures show that in 2004, 57% of those convicted of fraud and forgery paid compensation, compared with 37% for theft and handling and much lower proportions for burglary and for robbery. The average compensation order for fraud and forgery was £8,488, which was more than twice that for theft or burglary. However, the court is restricted by the need to consider the means of the offender to pay. In addition victims who are not featured on charges tried on the indictment are often frustrated at the lack of redress in this area, and the courts' preference for sample charges to reduce trial length and complexity makes this a significant issue.

10.53 Confiscation of the proceeds of crime has become an important issue in the context of the Proceeds of Crime Act 2002. During 2004-05 there were eight confiscation orders in relation to five cases, for orders amounting to a total of

£2,882,110. Compensation orders were made in three of these cases for amounts ranging from ranging from £1,287,241 to £426,353.[149]

10.54 Having considered the statistics and existing guidelines for fraud, the sentencing problems can be summarised as follows:

- No set definition of fraud, no specific guidelines for fraud offences published by the Sentencing Guidelines Council.

- Mitigating and aggravating factors can result in a wide disparity in fraud sentencing even where Court of Appeal guidelines exist.

- Sentences in breach of trust cases appear to be lower than guidelines suggest.

- Relatively low sentence levels for high value fraud - average sentence for SFO case is 3 years.

- Lack of preventive and restorative sanctions.

Strategy

10.55 The Fraud Review aims to develop a national anti-fraud strategy, which will provide a comprehensive understanding of the scale and nature of the fraud problem and a long term co-ordinated approach to tackling fraud. Sanctions and redress are two of a number of generic actions identified in the strategic model. A strategic approach is necessary to address not only the lack of government information about the size and nature of fraud but also the poorly organised sentencing data. Further research into the impact and appropriate length of fraud sentences and a wide scale survey of fraud victims is also necessary.

10.56 A co-ordinated approach to strengthen the national response to tackling fraud will include the need for a robust, transparent sentencing framework which can be utilised by all of the sectors involved in tackling fraud. It will address wider issues

such as inconsistency in the treatment of types of offences and the impact of longer sentences on prison resources. Such an approach would not advocate consistency of prosecution and sentences across sectors since each prosecuting department has its own remit; but it would better inform those involved in this arena and promote a more targeted approach.

10.57 Having considered the evidence and the results of consultation, the Review has identified a number of options to improve fraud sentencing, which are explored in the sections below.

Options

A. New Sentencing Guidelines for Fraud Offences

10.58 The current fraud guidelines raise issues of inconsistency and there is clearly a need for greater clarity for the courts, prosecutors and defendants on the range and level of sentences available. The Fraud Bill which is due to come into force in the latter part of 2006 will have a bearing on the need for new guidelines and the level of appropriate sentences. It will for the first time provide a definition of the offence of fraud in a single piece of legislation. This will assist departments such as the SFO, CPS and DTI in the prosecution of both the serious and more routine cases of fraud.

10.59 The Fraud Review has encountered wide support from public and private sector representatives and some members of the judiciary, for the introduction of specific sentencing guidelines for fraud offences as soon as practicable. The Guidelines would need to cover all of the offences under the Fraud Bill and those listed at Annex F. This area is the responsibility of the Sentencing Guidelines Council.

10.60 The Sentencing Guidelines Council aims to give authoritative guidance on sentencing, particularly where new legislation which affects the courts comes into force. It is regrettable that the introduction of new guidelines for fraud could not have been more closely aligned to the introduction of the Fraud Bill.

Nevertheless, the Secretariat to the Sentencing Advisory Panel have indicated that the development of guidelines for fraud offences, including those created in the Fraud Bill, is on the Sentencing Guidelines Council's forward work programme. It is not anticipated, however, that the consultation process will commence before 2007.

B. Increase in Length for Maximum Sentences

10.61 During our consultation exercise, different sectors expressed concern about the relatively light sentence levels for fraud. The statistical research tends to support this. There was some concern about the reduction in 1991 in the maximum sentence for theft from 10 to 7 years. It was felt that this reduction and the impact of sentence reductions for guilty pleas and personal mitigation often resulted in low starting levels for serious offences. There was concern that this could lead to disproportionate sentencing and could distort sentences for the less serious fraud offences.

10.62 The common law offence of 'conspiracy to defraud' has been retained under the Fraud Bill and the proposed maximum sentence for fraud contained in the Fraud Bill is 10 years. However the maximum sentence for money laundering which features similar characteristics to fraud is 14 years. This is commensurate with other countries such as Canada where the maximum sentence for some fraud offences is 14 years. The Fraud Bill's sentencing provisions reflect a Law Commission recommendation made after a process of consultation by the Commission, and a Home Office consultation exercise in 2004. We understand that there was no concern expressed at that stage at the maximum sentence being put at 10 years and neither has concern been raised in Parliament, although there was some concern expressed about actual sentence levels being imposed in fraud cases.

10.63 During our consultations however there was general support for the maximum length of sentence for serious frauds to be increased beyond the provision of 10 years. An increase in the maximum sentence for fraud would not necessarily mean a substantial rise in long sentences. Rather, it would allow the courts to

adequately reflect mitigating and aggravating factors in order to achieve a more appropriate sentence than is presently the case. This would in turn, allow lower level offences to be adequately accommodated within the new sentencing band. Any increase in the maximum sentence length will of course require new legislation or current legislation to be amended.

Cost Impact of Longer Sentences

10.64 Any recommendations to increase the maximum sentence length for serious fraud must be considered in the light of government policy and other relative offences. A recent Home Office Report which addresses the high re-offending rates amongst prisoners emphasises that prison is the place for serious violent and dangerous offenders from whom the public should be protected but not for others.[150] Prison resources must also be considered as the prison population has increased by over 50% in the last ten years and reached an all time peak of 75,544 (in 2004). It now costs an average of £31,140 per local prison place and £18,874 per open prison place.[151] These statistics have implications for overstretched resources and the adequate assessment of prisoners.

10.65 In view of the above data, it is important to consider sanctions as part of an overall strategic approach to tackle fraud. An appropriate range of penalties will better ensure that the punishment fits the crime, thus alleviating the need for lengthy custodial sentences in certain circumstances. More use could also be made of open prisons and weekend confinement. A wider range of penalties which go beyond sentencing should better meet the expectations of victims and provide for speedier and more effective justice.

C. Advisory Matrix System

USA Comparisons

10.66 It is useful to consider the US model to inform our discussions on sentencing and to see if there are lessons to be learned.

10.67 In the US, fraud sentences are calculated using a complex formula, the federal guidelines assign some two or three points to several factors; the court starts with a 'base level' of points for the category of offence, and then adds and subtracts in order to reflect the presence and strength of various aggravating and mitigating factors. The total number of points is then converted into a range of guideline sentences'[152]

10.68 In comparison to the US matrix system which uses a more automatic approach, the UK system gives more weight to judicial discretion in each case. UK Sentencing guidelines may provide a starting point, but aggravating and mitigating factors can take the sentence up or down from that point. Additionally there is a recognised system of reduction in sentence of up to 30% for early guilty pleas.

10.69 US sentencing policies are generally punitive and the Sarbanes Oxley Act has further increased the penalties for fraud. Available sentences for white collar crime offences are higher than for similar offences in England. Offenders can expect to receive 25 years (see Box below).[153] Custodial sentences are often served in full and offenders are not sent to open prisons but normally serve their sentence in regular or maximum security prisons.

Examples of US White Collar Crime Sentences

Bernard J. Ebbers WorldCom Chief executive
CASE: Masterminding an $11 billion accounting fraud
SENTENCE, IN YEARS: 25

Jamie Olis Dynegy Mid-level executive
CONVICTED: Falsifying the company's books to hide a $300 million loan
SENTENCE, IN YEARS: 24 (under review because of harm estimation)

Timothy J. Rigas Adelphia Chief financial officer
CONVICTED: Looting the company and lying to investors and regulators
SENTENCE, IN YEARS: 20

Martin R. Frankel Financier
PLEADED GUILTY: Looting insurance companies and racketeering.
SENTENCE, IN YEARS: 16.7

Reed Slatkin Money manager
PLEADED GUILTY: Stealing hundreds of millions from investors
SENTENCE , IN YEARS: 14

10.70 In the US there is also considerably more publicity surrounding fraud investigations and prosecutions which not only keeps the public informed but also keeps the pressure on the defendant and investigators. Investigations are generally completed more quickly than in the UK and the defendant is encouraged to participate in plea bargaining. Whilst sentence length is important, the process of being prosecuted, appearing in court and receiving adverse publicity may have a more powerful impact than the sentence, particularly on 'white collar' fraudsters.

10.71 Whilst there is currently no formal plea bargaining system in England and Wales, the Review has found wide support from many sectors for the introduction of a

properly sanctioned plea negotiation system. (This issue is discussed in more detail in chapter 11). One factor which will clearly affect the success of the introduction of a UK plea bargain system is the certainty and predictability of sentences as well as a wider range of sanctions including longer prison sentences for the most serious offences.

10.72 It is clear that the general level of sentences in the US Federal and other Sentencing Guidelines have a powerful effect on plea bargaining. Professor Levi notes that it is unlikely that senior staff and companies such as 'Enron and WorldCom would be keen to assist the prosecutors or to settle tax/SEC/ New York cases if it were not for the prospect of lengthy prison sentences plus no sentencing discount unless they both confess first and implicate others.'[154]

10.73 It is perhaps unrealistic to expect that the UK sentences for fraud will ever match those found in the US or that a US style matrix system will be welcome by the judiciary, however one option would be to have an advisory matrix (which preserved judicial discretion in certain instances) and clearer sentencing and prosecution guidelines. These measures may offer more predictability for fraud sentencing in a similar way to the systematic sentencing approach found in the US.

10.74 It is noteworthy that following the US Supreme Court decision in the case of Booker, (January 2005) the Court ruled that the federal guidelines were wholly advisory and whilst federal judges were still required to consider them they were also obliged to weigh other mitigating factors generally precluded from consideration previously.[155]

Conclusions

10.75 The ease with which many fraudsters commit their crimes, the delays and expense associated with criminal proceedings and the relatively low sentence levels received upon conviction lead many in the anti fraud effort to conclude that greater sanctions are necessary to deter and punish fraudsters.

10.76 Whilst it is debatable whether increasing sentence lengths alone, will deter fraudsters, a strategic approach to sanctions which advocates a wider range of penalties, a strategy to address underlying systemic weaknesses, more coherent sentencing data and information about the impact of fraud on victims would go some way to improving the problem.

New Sentencing Guidelines

10.77 There are clearly benefits to be gained from introducing specific guidelines for fraud, to promote clear, effective and consistent sentencing. In view of the new Fraud Bill, the production of new guidelines would be consistent with the policy of the Sentencing Guidelines Council to take into account the impact of new legislation on the courts. Whilst new guidelines would inevitably create some pressure on an already full programme for the SGC, such guidelines would help to reduce the wide disparity in fraud sentencing and should provide a greater degree of certainty for prosecutors and defendants.

Advisory Matrix System

10.78 There was no support for a “compulsory” matrix system from those members of the judiciary we consulted. However, an advisory matrix for fraud cases, which the courts are advised to follow unless there are specific mitigating or aggravating circumstances, together with specific sentencing and prosecutorial guidelines may constitute a more transparent system which would assist with plea bargaining. This would be little more than our current system of Court of Appeal guideline judgements, though these do not so far include Fraud.

Increase in Maximum Sentences

10.79 Whilst government policy on custodial sentences must be observed, the Review found general support for an increase in the maximum sentence for very serious fraud offences. Whilst it is unrealistic to expect that UK sentences for serious fraud will ever match those of the US, it was felt that sentences should be

increased for serious offences to better reflect the harm caused. The Review recommends that the maximum sentence for fraud offences, including those under Theft Act 1968 and Companies Act 1986, should be reviewed and that the Home Office should consider increasing the maximum sentence for all serious or repeated fraud offences to 14 years in line with the maximum sentence for money laundering. This would require legislative change.

Recommendations

10.80 The recommendations are listed below.

- The Sentencing Guidelines Council should be invited urgently to consider publishing specific guidelines for fraud offences covered under the Fraud Bill and associated legislation (See Annex F)

- The Sentencing Guidelines Council should be invited to commission further research into an advisory matrix system in order to assist with a plea bargaining system.

- The maximum sentence for the most serious (and/or repeated) fraud offences should be increased to 14 years.

CHAPTER 11 PLEA BARGAINING

11 SUMMARY

- Because of the enormous cost involved, and the strain on defendants, victims, witnesses and juries, it is important to ensure that there are appropriate alternatives which the parties can explore prior to embarking on a contested serious fraud trial. Any alternatives must preserve the principles of fairness to those accused of crime and to the victims of criminal conduct, as well as not conflicting with the wider public interest. The principle of judicial independence must also be preserved.

- We have consulted widely with criminal justice court practitioners. We fully accept that the individual views expressed to us during these consultations cannot be taken as representing the official views of the Criminal Bar, the Law Society or the Judiciary. However, from our discussions we have concluded that it is time for a change in approach so that a formal system of plea bargaining be introduced at a pre charge stage, enabling discussions to take place between the prosecuting authorities and the defence to see whether acceptable pleas can be agreed at that stage and, if so, to allow access to the courts before charge so that judicial approval can be sought. We also recommend that the parties be allowed to recommend to the judge a sentence package which the judge would be free to agree to or reject.

- We see this as more an evolutionary change than a revolutionary one, building on recent authority that allows the defence to seek an indication of sentence before a plea is entered, and also building on the existing discussions that regularly take place between the prosecution and defence in respect of acceptable pleas once the original charge or charges have been laid.

- There are clear advantages of offering the parties in serious fraud cases the opportunity to consider reaching a court sanctioned agreement at a much earlier stage than hitherto. These relate to the large financial savings to the public purse that can be made by early disposal of even a few of these cases

and easing the strain caused by delay on defendants, victims and witnesses. In some cases it would also give the investigators and prosecuting authorities more information at an early stage to allow a more focused and efficient investigation into the role of others involved in the criminality and with whom no such agreement is reached.

Introduction

11.1 The Fraud Review interim report noted that prosecution opportunities to engage formally in discussions with the defence over possible pleas are more limited in England and Wales than in some other jurisdictions. As there can be no plea tendered until charges have been preferred, it follows that plea bargaining here cannot save significant investigative costs or time. The case must always be prepared to a criminal standard before charges can be brought or pleas accepted.

11.2 Very large amounts of public money are expended on serious fraud cases in investigative, prosecution, defence and court costs. In addition, investigations into such cases are becoming more time consuming and therefore more expensive owing to the increase year on year in the amount of business and financial material that is being stored in an electronic form.

11.3 The Fraud Review has concluded that, whilst it is important that these trials are run as efficiently as possible, it is also important that there are systems in place to allow the early resolution of cases where appropriate so that unnecessary costs and delay can be avoided. We stress that these alternatives to full criminal trials must preserve the principles of fairness to defendants and victims as well as be consistent with the general public interest.

11.4 There is at present no formal system of plea bargaining in our courts. Traditionally the criminal justice system in England and Wales has shied away from sanctioning any sort of formal plea bargaining system. There have been concerns to ensure that judges retain their independence from either party, and that no undue pressure is brought on a defendant to plead guilty. We completely

accept that no judge should be expected simply to rubber stamp agreements on plea made between the parties. Judges act in the public interest to ensure that disposal of matters in the courts satisfy the interests of justice.

11.5 In reviewing cases the CPS, RCPO, DTI, SFO and other prosecuting agencies apply two tests, the evidential and the public interest tests. If a case satisfies both tests, a prosecution will follow. The Code for Crown Prosecutors specifically prohibits prosecutors from charging more offences than are necessary just to encourage a defendant to plead guilty to a few. In the same way, they are prohibited from putting a more serious charge just to encourage a defendant to plead guilty to a less serious one.

11.6 Chapter 10 of the Code considers the circumstances where defendants may want to plead guilty to some, but not all, of the charges. Alternatively, defendants may wish to plead guilty to a different, possibly less serious, charge because they are only admitting part of the crime. Prosecutors should only accept the defendant's plea if that allows the court to pass a sentence that adequately reflects the seriousness of the offending, particularly where there are aggravating features. They should ensure that the interests of the victim, and where possible, any views expressed by the victim or their family are taken into account. However, the decision rests with the prosecutor.

11.7 The Attorney General has issued binding Guidelines[156] to prosecuting advocates and authorities on the approach that should be adopted when considering the acceptance of pleas to a reduced number or less serious charges. The basis of plea, agreed by the parties and reduced to writing, is central to the sentencing process. Where the basis of plea cannot be agreed and the discrepancy between the two accounts is such as to have a potentially significant effect on the level of sentence the prosecuting advocate has an overriding duty to inform the court. The Guidelines refer to the risk of the prosecution being unable to refer an unduly lenient sentence to the Attorney General because of an illogical or unsupported basis of plea.

11.8 It should be noted that a prosecutor has no role in suggesting or recommending any particular sentence but nevertheless has certain duties to perform at the sentencing stage. These include drawing the judge's attention to any victim personal statement, any statutory provisions relevant to the offender or the offences and any aggravating or mitigating factors. The prosecutor may also offer assistance to the court by making submissions, in the light of all these factors, as to the appropriate sentencing range.

11.9 Until the recent case of R v Goodyear (Karl)[157] there was no formal process by which a defendant could seek an indication of sentence, though a judge could, if he saw fit, exercise the power recognised in R v Turner[158] to indicate whether the sentence, or type of sentence, would be the same whether the case proceeded as a guilty plea or resulted in conviction after trial.

11.10 The Deputy Lord Chief Justice sitting in the Court of Appeal (Criminal) Division in considering the appeal against sentence in R v Goodyear issued guidelines that amount to the introduction of a formalised procedure of advance sentence indication. An indication of sentence may be sought by the defence once a basis of plea has been agreed. The Attorney General's Guidance on the topic states that in difficult or complex cases, no less than 7 days notice in writing of an intention to seek an indication should normally be given to the prosecution and the court. The Guidance also states that prosecutors should not agree a basis of plea unless and until the necessary consultation has taken place first with the victim and/or with the victim's family.

11.11 Before the judge gives the indication, the prosecution advocate should draw the judge's attention to any minimum or mandatory statutory sentencing requirements. Where the prosecution advocate would be expected to offer the judge assistance with relevant guideline cases or the views of the Sentencing Guidelines Council, he or she should invite the judge to allow them to do so. Prosecuting advocates should ensure that the judge is in possession of or has access to all the evidence relied on by the prosecution, including any victim personal statement, as well as any information about relevant previous convictions recorded against the defendant (in line with the Farquharson

Guidelines)[159]. The prosecution advocate should not say anything which may create the impression that the sentence indication has the support or approval of the Crown.

11.12 It should be noted that the Deputy Lord Chief Justice was emphatic that a judge should not be invited to give an indication in what would be, or what would appear to be a "plea bargain".[160] "He should not be asked or become involved in discussions linking the acceptability to the prosecution of a plea or basis of plea, and the sentence which may be imposed. He is not conducting or involving himself in any plea bargaining"

11.13 The judge gives an indication of the maximum sentence he or she would pass if D pleaded guilty at that stage. He retains an unfettered discretion to refuse to give any indication. This can protect a defendant who is under inappropriate pressure to plead guilty from a co accused for instance. Defence counsel bears a personal responsibility to ensure that the client fully appreciates their position. A judge may also defer giving an indication until he feels in a proper position to do so until reports are available for example. Once an indication is given it is binding and remains binding on the judge who gives it as well as any other judge who subsequently hears the case. Following an indication a defendant is allowed a "reasonable opportunity" to consider his or her position; if after that the defendant does not plead guilty, the indication will cease to have effect. Its existence is not admissible in any subsequent trial.

11.14 The potential benefits of the practice is clear; the defendant has some certainty as to the benefits of pleading guilty, It is not yet clear whether there has been an increase in timely guilty pleas as a result. If there are, there will be significant savings in terms of court time and public funds as well as benefits for victims and witnesses. The safeguards should ensure that the defendant does not come under undue or inappropriate pressure to plead guilty.

11.15 The Sentencing Guidelines Council published guidance on the reduction in sentence available on a guilty plea in December 2004.[161] It aims to promote consistency in sentencing. The reduction in sentence available varies between

1/3 and 1/10 depending on when in the proceedings the plea has been entered. A sliding scale is applied. There are specific directions to be applied in the case of dangerous offenders, multiple offending and murder. There is always a precedent or guideline available to a sentencer but none will enable a defendant to predict his sentence with as much certainty as is possible within the U.S. system (see below).

11.16 Prosecutors have always had the power to accept pleas to a lesser offence or offences charged if they feel that it is in the public interest to do so. However they have no power to come to even a provisional arrangement with the defendant regarding confiscation, compensation, disqualification or any other aspect of sentence. There are now provisions in the Serious Organised Crime and Police Act 2005[162] regarding offenders who agree to assist investigations and prosecutions. These provide for 'contractual' immunities from prosecutions, undertakings as to use of evidence and reductions in sentence for offenders who have assisted the prosecution.

11.17 The responsibility for deciding on plea is entirely that of the defendant alone, although of course he will be assisted by his legal representative in making the decision. If the defendant offers to plead guilty to some of the offences charged, or to a lesser offence or offences, then the prosecutor has to decide whether it is in the public interest to accept those pleas. Although the responsibility for that decision lies with the prosecutor, he should bear in mind the guidance contained in the Code for Crown Prosecutors, the Attorney General's Guidelines on the acceptance of pleas (reissued in 2005) and the views of any victim or victims. Key considerations are whether the acceptance of the plea will allow the court to sentence on a proper basis and allow the interests of the victim to be taken into account. In addition, at the crown court any plea accepted is subject to the approval of the judge.

11.18 In contrast to the positions in countries where formal plea bargaining systems are in place, there is little scope for a plea package to be agreed between the prosecution and defence encompassing for example an agreement regarding reparation, preventive or punitive measures that might (subject to judicial

discretion) meet the justice of the case. One reason why this has not been practicable is because of the lack of certainty about the punishment that a defendant will face once the judge has been given the facts of the case and the antecedents of the offender.

11.19 The role of the prosecution thus remains very limited, whereas in true plea bargaining systems the prosecution has an extremely active role in negotiating with the defence and other interested parties, such as victims or regulators, when seeking to settle a case in an appropriate way.

The US Plea Bargaining Model

11.20 We have looked at the position in the United States which has fully developed plea bargaining systems in place. It is illuminating to go into this model in some detail as in our view it demonstrates that a plea bargaining system can incorporate the non negotiable principles of fairness to defendants, judicial independence and safeguarding the public interest by means of checks and balances.

11.21 The Americans appear to have few jurisprudential qualms in offering this as an option for the prosecution and defence to explore even before anyone has been charged. The Federal government and many states have written rules that explicitly set out how plea bargains are to be conducted. The Americans are assisted by having a high degree of certainty about the sentence that will be imposed by a court in respect of any particular agreement because of the relatively rigid guidelines laid down by their sentencing guidelines bodies.

11.22 As with other federal crimes, fraud sentences are calculated using a complex formula laid down by the United States Sentencing Commission in the Federal Sentencing Guidelines Manual[163]. It should be noted that the Supreme Court in 2005[164] ruled that the U.S.Guidelines breached the sixth amendment and therefore they could only be regarded as advisory. As Professor Levi points out elsewhere[165], factors that can increase a sentence must be found by a jury or

admitted by a defendant before a judge can have regard to them when sentencing.

11.23 The Manual calls for adjusting sentences based on the severity of the fraud, with severity determined largely by the magnitude of financial losses and the number of victims. The success of plea bargaining in the USA (over 95% of cases plead) depends on the prosecutor's ability to predict the judge's powers and thus to assure the defendant of a lower sentence than he would face after trial. The US Sentencing Guidelines took effect in 1987. It was Congress's aim to ensure that offenders with similar histories who committed similar acts would be treated alike.

11.24 The concern that prosecutors might constrain the judge's sentencing powers by manipulating the charges was addressed by requiring the judge to have regard to the "relevant conduct" of the defendant. Federal probation officers are assigned to act as the court's independent investigator and are required to disclose all "reliable" information to the court. This process effectively limits the degree to which the choice of charges dictates the guideline sentence. In addition, the Guidelines call upon judges to reject plea bargains proposed by the parties when those bargains threaten to undermine the sentencing guidelines (i.e. too lenient a sentence).

11.25 Prosecutors have a right of appeal against downward departures from the guideline range. When they do appeal, they are usually successful (losing only 29% of cases between 1996 and 2001).[166]

11.26 The Commission is required by the Sentencing Reform Act 1984 to prescribe an appropriate sentence range for each class of convicted persons. A sentencing court must select a sentence from within the guideline range but can depart if a case presents atypical features. If a court sentences within the range an appellate court may review the sentence to determine whether the guidelines were correctly applied. If the court departs from the guideline range, an appellate court may review the reasonableness of the departure.

11.27 The Guidelines are reviewed regularly and were last reviewed in November 2005. There are individual offence guidelines that specify the range and give detailed instructions on increases and decreases in level (1-43) for each of specific mitigating and aggravating features. The Commission established a sentencing table that contains 43 levels. Each level in the table prescribes levels that overlap. By doing so, the table is intended to discourage unnecessary litigation. Both prosecutor and defence will realise that the difference between one level and another will not necessarily make a difference in the sentence that the court imposes. At the same time, levels work to increase sentences proportionately. A change of 6 levels roughly doubles the sentence irrespective of the level at which one starts.

11.28 The U.S. Congress's basic objective in enacting the Sentence Reform Act 1984 was to enhance the ability of the criminal justice system to combat crime through an effective, fair, sentencing system. They sought honesty, reasonable uniformity and proportionality in sentencing. Parole was abolished. The sentence handed down is the sentence served less approximately 15% for good behaviour.

11.29 One of the most important questions for the Commission to decide was whether to base sentences upon the defendant's actual conduct regardless of the charges for which he was indicted or convicted ("real offence" sentencing) or upon the conduct that constitutes the elements of the offence with which he was charged and convicted ("charge offence" sentencing). The outcome is a combined system, charges are the starting point but the guidelines take account of a number of important, commonly occurring real offence elements such as role in the offence or the amount of money actually taken. One of the most important drawbacks of a charge offence system is the potential it affords the prosecution to increase sentences by increasing or decreasing the number of counts on an indictment. Thus for multi-count convictions the Commission has written rules with an eye to eliminating unfair treatment that might flow from count manipulation.

11.30 Departures from a guideline specified sentence are permitted only where the court finds aggravating or mitigating circumstances of a kind, or to a degree, not

adequately taken into consideration by the Council when formulating the guidelines.

11.31 There are 2 types of “Departure”, the first specified and given a level within the specific offence guidelines, the second, for example “substantial assistance to the authorities” or “voluntary disclosure of an offence” is unguided i.e. there is no prescribed increase or decrease in level. The second category is not closed; the Commission recognises that there may be other grounds for departure that are not mentioned.

11.32 Plea Agreements merit a chapter to themselves within the guidelines. The Commission issued general policy statements concerning the acceptance of agreements. The Commission stated their expectation that the guidelines would have a positive, rationalising impact on plea agreements for 2 reasons (page 12). First, the guidelines create a clear, definite expectation in respect to the sentence that a court will impose if a trial takes place. In the event that a prosecutor and defence lawyer explore the possibility of a negotiated plea, they will no longer work in the dark. Secondly, the guidelines create a norm to which courts can refer when they decide whether to accept or reject a plea agreement.

11.33 It is significant that the Commission deliberately changed the way in which certain offences were viewed. For example, it published guidelines classifying as serious many financial offences for which non custodial penalties were previously given and to provide for at least a short period of imprisonment in such cases. They concluded that the definite prospect of prison, even for a short term would serve as a significant deterrent, no doubt a by product was also an increased willingness on the part of defendants to reach a plea agreement in order to achieve the most lenient sentence.

11.34 Since the creation of the Sentencing Guidelines in 1987, the proportion of adjudicated federal cases that ended in guilty pleas has risen from 85% in that year to 94% in 2001 and 95.7% in 2003. The highest rate was in Arizona, 99% and the lowest in Middle Alabama 88.5%.

11.35 The plea rate can be broken down by offence category. In 2003 the rates were: fraud, 95.2%; embezzlement, 98.4%; forgery/counterfeiting 98.3%; bribery, 96.4%; tax, 91.8%; money laundering, 88.4%; racketeering/extortion 89%.

11.36 A memorandum was issued to all U.S. prosecutors and attorneys on 7th April 1997 which stated: “The Principles of Federal Prosecution[167]…. (the "Principles"), and an October 12, 1993, bluesheet issued by Attorney General Reno (the "Bluesheet"), provide guidance to prosecutors regarding charging and plea agreement decisions. One of the primary purposes of the Principles is to assure that charging and plea bargaining decisions do not undermine the Sentencing Reform Act goal of reducing unwarranted sentencing disparity. The basic policy is that prosecutors must charge "the most serious offence that is consistent with the nature of the defendant's conduct, and that is likely to result in a sustainable conviction."[168] Prosecutors similarly should seek a plea to the "the most serious readily provable offence charged."[169])…. As indicated above, the Principles seek to prevent circumvention of the sentencing guidelines through improper charging decisions and "charge agreements." In addition, the Principles seek to prevent "sentence agreements" that may undermine the sentencing guidelines[170]….Thus, prosecutors are not free to recommend, or to agree to, a sentence that is outside the applicable guideline range but not based on an appropriate departure from the guidelines that is identified to the court.”

11.37 Chapter 6B of the Sentencing Commission Guidelines sets out the Commission’s policy once agreements have been reached. Sentencing is a judicial function and the appropriate sentence in a guilty plea case is to be determined by the judge. The basis for any judicial decision to depart from the Guidelines must be explained on the court record.

11.38 The parties must disclose the plea agreement in open court. If pleas to a reduced number of charges are accepted the court may accept the agreement if it determines, for reasons stated on the record, that the remaining charges adequately reflect the seriousness of the actual offence behaviour and that accepting the agreement will not undermine the statutory purposes of sentencing

or the Guidelines[171]. However, this requirement does not authorise the judge to intrude upon the charging discretion of the prosecutor[172].

11.39 The court should only accept a recommended sentence or a plea agreement requiring the imposition of a specific sentence if the court is satisfied either that such a sentence is appropriate within the applicable guideline range or, if not, that the sentence departs from the applicable guideline range for justifiable reasons. The court can reject a plea agreement.

11.40 Chapter 6A sets out the sentencing procedure. “Reliable fact finding is essential to procedural due process and to the accuracy and uniformity of sentencing”. In addition to the case put before the court by the parties, a probation officer must conduct a pre-sentence investigation and submit a report to the court other than in if statute requires otherwise or if the court finds that it has sufficient information and explains that finding on the record. The defendant may not waive preparation of a pre-sentence report.[173]

11.41 A plea agreement must be accompanied by a written stipulation of facts relevant to sentencing including the actual offence conduct, offender characteristics, it must not contain misleading facts and it must set out “with meaningful specificity” the reasons why the sentencing range resulting from the proposed agreement is appropriate.[174] The parties are not obliged to reach agreement on all issues. The stipulation should identify all areas of agreement, disagreement and uncertainty that may be relevant to the determination of sentence. In determining the factual basis for the sentence, the court will consider the stipulation, together with the results of the pre-sentence investigation and any other relevant information.

11.42 The sentencing task is approached by the judge in the following way:

- Determine the offence guideline applicable to the offence of conviction.

- Determine the base offence level and apply any specific offence characteristics, cross references (guidelines from other relevant offences

which are specified within the applicable offence guideline), and special instructions contained in the particular guideline.

- Apply the adjustments as appropriate related to victim, role, obstruction of justice, impeding the administration of justice or multiple counts, a single, combined offence level is established. Adjust the offence level accordingly.

- Adjust as appropriate for the defendant's acceptance of responsibility including an additional single level reduction for pre-warning the authorities of an intention to plead guilty if the conditions are met.

- Adjust for the defendant's criminal history and any other applicable adjustments.

- Determine the guideline range.

- Determine the sentencing requirements and options related to probation, imprisonment, supervision conditions, fines, restitution. Note the zones on the table. For example, probation is available if the applicable Guideline range is within Zone A, or Zone B if a court adds a condition or conditions requiring intermittent confinement, community confinement or home detention. A fine can be the sole sanction if the Guidelines do not require a term of imprisonment.

- Refer to the sections of the Guidelines that refer to Specific Offender Characteristics and Departures and to any other policy statements or commentary in the guidelines that might warrant consideration in imposing sentence. It is in this section that discretion can be exercised, there are no prescriptive level adjustments. Specific Offender Characteristics specifically exclude such factors as the offender's age, education, mental and emotional conditions.

11.43 The most significant Departure is "substantial assistance to the authorities", its significance in plea agreements will be obvious.

11.44 The advent of the Guidelines allowed defendants and their representatives to predict quite accurately the costs of risking trial and losing. A range of bargaining takes place, charge bargaining (pre and post charge), fact bargaining and range bargaining, in which lawyers agree to recommend to the judge a sentence at the lower end of the guideline range. It is now the dominant force in U.S. courtroom procedure.

The Situation in Australia

11.45 Plea bargaining in Australia generally refers to discussions between the parties about the possible reduction or alteration of charges or a reduction in sentence if a guilty plea is entered. It also refers to sentence indication which occurs when the presiding judge provides an indication of the likely sentence a defendant will receive if he pleads guilty. Sentence indication is not approved of in Victoria but it does operate in New South Wales.

11.46 Various prosecution guidelines in Australia now recognise the existence and operation of some sort of bargaining between the parties and view it as an acceptable practice, although not one that should be initiated by the prosecution. For example, the Prosecution Policy of the Commonwealth 1990 outlines the concept of what it describes as charge bargaining and its operation in reference to Commonwealth prosecutions as opposed to those initiated in State courts under State legislation.[175] The guidelines make it clear that anything which suggests an arrangement between a judge and counsel in relation to the plea to be made or the sentence to be imposed must be studiously avoided. It is objectionable as it does not take place in public and serves to weaken public confidence in the administration of justice.

11.47 The guidelines go on to advise prosecutors that they may accept a defence request not to oppose their submission that the penalty fall within a nominated range provided that the penalty or range of sentence nominated is considered to be within acceptable limits to a proper exercise of the sentencing discretion.

11.48 In New South Wales, the Government has approved reforms to introduce a procedure of compulsory conferencing for indictable offences prior to committal to the district courts. The reforms would oblige the prosecution to serve a full brief of evidence on the defence, together with any relevant unused material, so that the defence can make a realistic assessment of the evidence. Then, unless the defence indicate a plea, the parties are required to hold a compulsory conference where the 2 sides have the opportunity for formal discussion to decide whether a plea can be made prior to committal.[176]

A General Comparison

11.49 There is little doubt that the existence of some form of bargaining is seen as a key factor in dealing with fraud effectively in the USA and Australia, although clearly the American model is far more regulated.

11.50 However, there are 2 major factors that apply to the USA but not to the same extent in the courts here. First, in many serious fraud cases the potential custodial penalties available to judges following a trial are so punitive that this undoubtedly makes plea bargaining an attractive option to many defendants. Secondly, because of the United States sentencing guidelines there is a degree of certainty as to the sentence to be expected on plea of guilty or after a contested trial (although, as mentioned, recent authority has confirmed that these guidelines are advisory only).

11.51 For example, in the 'Enron' case 2 of the star prosecution witnesses were the ex-chief financial officer and ex-chief accounting officer both of whom entered into plea bargain arrangements whereby they will serve 10 and 5-7 years respectively rather than the 25 plus years they would have faced had they been found guilty after contesting the matter.

Cautioning Offenders

11.52 Cautioning offenders has long been an option in the UK as a response to certain offending. The rationale behind this option is that it is not always necessary to prosecute an offender through the courts, for example where a caution would have a good chance of deterring the person from reoffending. Cautioning by the police is guided by government. The most recent guidelines were published by the Home Office in 2005. The criteria to be met are that there must be sufficient evidence for a realistic prospect of conviction, there must be a full admission of guilt and the offender understands the significance of a caution and gives informed consent to being cautioned. In respect of children and young persons, a formal cautioning scheme was introduced by sections 65 and 66 Crime and Disorder Act 1998. This replaces cautions by a system of reprimands and warnings.

11.53 It is not only the police who have the power to caution. For example, some regulatory enforcement agencies, including those policing factory safety and pollution, have this option available to them. A feature of police cautioning is that it is not possible to link it to conditions. So, when making a decision, an officer can take into account an offender's willingness to address his offending behaviour, for example by attending a course aimed at anger management. However, the caution cannot be made conditional on this happening.

11.54 The idea of conditional cautions was raised in the Auld review.[177] The report recommended that such a scheme be introduced for minor offending, provided the victim consents, the court approves and the offender consents to comply with specified conditions. The proposal differed from existing cautions as the offender could be prosecuted and punished for the original offence if the conditions were not complied with.

11.55 Sections 22-27 of the Criminal Justice Act 2003 cover the introduction of the scheme. So far it has been implemented in 6 CPS/police areas in the country. The CPS aim is that conditional cautioning will be rolled out across the whole of England and Wales by April 2008. In brief, when fully implemented the scheme will allow all constables, other investigators employed by a police force, the National Crime Squad or the National Criminal Intelligence Service and

prosecutors to administer conditional cautions. The power is given in the Act to a specified list of prosecuting authorities, including the SFO, CPS and Revenue and Customs. The actual decision to dispose of a matter in this way has to be taken by a prosecutor. Such a caution may only be administered to those over 18 and is subject to 5 conditions being met:

- There is evidence that the offender has committed an offence;

- A relevant prosecutor has decided that there is sufficient evidence to charge, and that a conditional caution should be given;

- The offender has admitted the offence;

- The effect of the conditional caution has been explained to the offender and a warning given as to the consequences for not complying with the conditions;

- The offender signs a document containing details of the offence, his admission, his consent to the conditional caution and the actual conditions.

11.56 Section 24 of the Act provides that criminal proceedings may be instituted against the offender if he fails without reasonable excuse to comply with any of the conditions. Of course it is also open to an offender to reject the offer and opt to be prosecuted. A code of practice has been published by the Home Office.[178] It is made clear that the conditions must be for the purpose of facilitating the rehabilitation of the offender and/or ensuring that he makes reparation for the offence. The conditions should be proportionate, achievable and appropriate. The Code also makes it clear that the prosecutor should take into account the views of the victim and the impact the crime had on them. In the areas where the scheme has been implemented, one of the most frequently used conditions (in over half of the cases) has been the payment of compensation to the victim.

11.57 Traditionally cautions have been used to tackle minor, mostly first time, offenders. The Home Office code of practice on conditional cautions gives guidance to prosecutors on deciding when these should be considered. It says

that prosecutors should consider the seriousness of the offence and the ACPO 'gravity factors'. It also goes on to suggest that such a disposal could be considered where the offender is willing and able to undertake an act which might be conducive to reparation or rehabilitation. If this would be a preferable alternative to prosecution then a conditional caution may be appropriate.

11.58 However, it is notable that section 27 of the Act includes the SFO and Revenue and Customs as relevant prosecutors, suggesting that in appropriate circumstances conditional cautions may be used for dealing with some fraudsters. The point was made to us that conditional cautions might appropriate where the only defendant was a company and the criminal conduct was admitted. A company cannot be imprisoned and therefore, rather than take the case to court, a conditional caution could be used to ensure financial recompense of victims.

Problem

11.59 Although there have always been complex fraud cases, the complexities of international banking and financing systems, the increase in the volume of digital material available and the rise in the number of organised gangs involved in fraud mean that an increasing strain is being put on the capacity of investigators and the criminal justice system to cope.

11.60 We have concluded that, whilst it is important that trials are run as efficiently as possible, it is time to seriously consider building on the principles in Goodyear and putting systems in place to allow for the early resolution of more cases, where appropriate, so that unnecessary costs and delay can be avoided.

11.61 We stress that these alternatives to full criminal trials must preserve the principles of fairness to defendants and victims as well as the general public interest. Transparency and public confidence must be retained and any recommendation must safeguard the principle that a plea must be entered voluntarily.

Strategy

11.62 The Fraud Review aims to develop a national anti-fraud strategy, which will provide a comprehensive understanding of the scale and nature of the fraud problem and a long term co-ordinated approach to tackling fraud. Considering alternatives to full criminal trials in serious fraud cases is one of a number of generic actions identified in the strategic model. A strategic approach is necessary to ensure that there is consistency in the way that such alternatives are applied. A co-ordinated approach to strengthen the national response to tackling fraud will include the need for an effective means of diverting some high cost fraud cases from the courts' system prior to the full trial.

Options

Plea Bargaining Framework

11.63 The introduction of a plea bargaining framework into the crown courts in England and Wales either generally or in relation to complex fraud cases only.

Pre or Post Charge Sentence Canvassing

11.64 Sentence canvassing at an early stage, either pre charge or post charge. The Serious Fraud Office has long supported a slightly different approach to plea bargaining, namely sentence canvassing at an early stage. Goodyear has made it possible for an advance indication to be sought now. However, the approach supported by the Serious Fraud Office envisages that such an indication could be sought in serious fraud cases where a defendant was prepared to admit guilt at an early stage of the investigation, rather than when the full investigation had been completed. It would only be appropriate where there was certainty at that early stage as to the extent of alleged criminality. Defence co-operation and involvement would therefore be essential. The advantages of this system for the prosecution in serious fraud cases are that there would be a shorter investigation that would free resources for other work and the avoidance of a full trial with the consequent cost savings. From the defence perspective there would be early

resolution, thus reducing stress and costs, and an early knowledge of the sentencing package on offer.

Non-court options

11.65 The use of 'conditional cautions' provided for in the Criminal Justice Act 2003 allowing prosecutors and police to combine 'suspended prosecution' with restorative corrections such as 'modest financial compensation'. Although intended as a cost-effective response to low level crime it may be possible to consider a modified option for some fraud cases.

Conclusions

11.66 We acknowledge that there needs to be a fundamental debate concerning the place of plea bargaining in the criminal justice system as a whole. Such a debate is beyond the scope of this review. However, as a result of our consultations with a wide range of practitioners we consider that the time is ripe for a rethink of our traditional opposition to a formal plea bargaining system specifically in relation to serious fraud cases. Given the startling success in reducing trials the system has enjoyed in the USA and the recent changes to the frameworks for Queen's Evidence and indications of sentence in this country ; we are confident that such a system could be introduced that maintains the principles of transparency, fairness and judicial independence and commands public confidence.

11.67 In chapter 10 there is a recommendation that the Sentencing Guidelines Council be invited to consider issuing guidelines on sentencing in fraud cases. Once this has been done we would argue that a plea bargaining system in this area becomes more feasible and the position here as far as predictability of sentence is concerned becomes more like the position in the USA, although we accept that sentences of imprisonment in serious fraud cases here are unlikely to reach the levels sometimes imposed by the Americans.

11.68 In our consultations we also encountered little opposition to proper exploration of the appropriate sentence by the prosecution and defence as part of any plea

bargain package brought before a judge (see chapter 9, Penalising Fraud), provided there was no suggestion that this had any status beyond merely being a recommendation to the court.

11.69 Our conclusion is based on the need to rise to the challenge posed by increasingly complex and resource intensive fraud cases. Any solution should provide an opportunity for the prosecution and defence to enter into negotiations at an earlier stage than currently possible, preferably pre charge, at the point where the prosecuting authority is in a position to show the essential core of a case against an individual or individuals.

11.70 We note that such a system could link in with the new powers available to prosecutors under recent legislation[179] that allows prosecutors to enter into written agreements with potential defendants who offer to give 'Queen's Evidence' or other assistance to the prosecution, in return for either:

- Immunity from prosecution;
- Undertakings not to use certain evidence in criminal proceedings; or
- Expectation of a reduction in sentence.

11.71 A plea bargaining system, in some instances with the new powers available under SOCPA, should also have the effect of providing investigators and prosecutors with more information at an earlier stage which will allow them to be more focused when obtaining further evidence in multi handed cases and when deciding on the relevance of unused material. This should contribute to better charging decisions and speedier and more efficient trials which would benefit all parties.

11.72 We have also concluded that in certain serious fraud cases, notably where the only proposed defendants are a company or companies, conditional cautions may be an appropriate disposal of the matter provided conditions proposed meet the requirement to compensate victims and prevent further fraud. We fully accept however that there would have to be highly exceptional circumstances for a serious fraudster, white-collar or otherwise, to be dealt with in such a fashion.

11.73 Clearly legal aid would have to be extended to enable suspects and their representatives to do this work at an earlier stage than hitherto, but we are confident that this cost would be heavily outweighed by the savings made if even a handful of serious fraud cases are resolved prior to trial as a result of the new system. We have also concluded that, even where no agreement is reached, any work done by the defence pre-charge should mean a reduction of the work that was needed post-charge.

11.74 As the existing plea framework in England and Wales is a mixture of case law, guidelines and protocols, it appears to us that there would be no legislative implications from the introduction of a plea bargaining system unless, of course, a statutory framework was considered necessary. There would be legislative implications, however, if legal aid was extended to defence representatives at the pre-charge stage.

Recommendations

11.75 That a study be carried out into whether the introduction of the 'Goodyear' guidelines has had any effect on the rate of guilty pleas and their timeliness at the crown court.

11.76 We recommend that there be a formal plea bargaining system agreed in principle specifically for cases dealt with by the Serious Fraud Office, the Fraud Prosecution Service in the CPS and serious and complex fraud cases brought by other prosecuting authorities. The detail of the system, including the justifications for confining it (at least initially) to fraud cases should be set out in a legal framework to be devised by a working group comprising appropriately senior figures from the judiciary, prosecuting authorities, the criminal bar and criminal solicitors' association. The framework should cover the following:

- Provision for a suspect to be legally aided during pre charge negotiations;

- The prosecuting authority's option to provide a case statement to a suspect and his representative as to the nature of the case and his role in it at the pre-charge stage;

- The suspect's option to respond to that statement with a 'without prejudice' statement setting out the extent of his accepted criminality and then for both sides to engage in 'without prejudice' negotiation to see whether an early agreement as to criminality can be reached; this negotiation to include a recommended realistic sentence package, to include consideration of the extended sentencing options considered in chapter 8;

- Access to a specialised fraud judge at a pre charge stage to seek judicial approval of an agreed plea and sentence package or simply for the defence to seek an early sentence indication from the judge prior to further consideration (i.e. early sentence canvassing).

11.77 We also recommend that new guidelines on the conduct and acceptance of plea bargains by prosecutors be issued by the Attorney General once a plea bargaining framework is in force, to offer specific guidance in this area.

CHAPTER 12 INTERNATIONAL COMPARISONS

12 Introduction

12.1 The Fraud Review undertook a brief study of the experience of other countries when dealing with the fraud problem in order to highlight points of interest, show examples of best practice, and to identify any commonalities. To this end, in February 2006 the Research Unit (RU) of the NHS Counter Fraud Service was asked to undertake research into six countries, Australia, Canada, France, Germany, Ireland, and United States of America.

12.2 In the limited time available the RU has sought information in the following areas to allow comparisons with the UK to be drawn:

- The nature and scale of the problem of fraud;
- Anti-fraud strategies;
- Legislation specific to fraud and corruption;
- Organisations (both public and private sector) with a counter fraud remit, including investigative bodies.

12.3 The purpose of this chapter is to highlight common problems and examples of best practice to inform the conclusions of the Fraud Review. The information is divided into the following areas to fall in line with the work of the team: defining and measuring fraud; national fraud strategy; reporting fraud; data sharing; investigating fraud; and prosecuting and penalising fraud.

The Nature and Scale of the Problem

12.4 The Fraud Review team has identified problems that exist in relation to measuring the cost of fraud. The Government Departments that collect figures on fraud use a variety of methods. Additionally, private sector bodies that publish fraud statistics do not have a standardised method of collation. Therefore, wherever fraud figures exist, they cannot accurately be compared as they have not been gathered using a common methodology.

12.5 Attempts have been made in each country researched to estimate the cost of fraud to the economy as a whole. However, there does not appear to be any robust calculation of the cost of fraud in any of the countries examined. As such, these estimates should be treated with caution as the methodologies used vary in nature and validity. The table below provides a summary of the estimated cost of fraud in each country:

Table 1: Estimated Cost of Fraud in Each Country

Country	**Estimated cost of fraud**[180]	**Cost of fraud as a % of GDP**
United States	**£378 billion** ($660 billion)[181]	6%[182]
Germany	**£137.1 billion** (€200 billion)[183]	9%[184]
United Kingdom	**£14 billion**[185]	2%[186]
Canada	**£10 billion**[187] (CAD $20 billion)	2.1%[188]
Ireland	**£4.35 billion**[189]	4%[190]
Australia	**£2.3 billion** (AUS$5.8 billion)[191]	1.3%[192]
France	It has not been possible to find a satisfactory estimate.[193]	-

12.6 Overall, the research found that the private sector appears to be more advanced than the public sector in attempting to measure the cost of fraud; the majority of estimates referring to fraud came from the private sector. The following table presents the information that was found in the course of our research:

Table 2: Types of Fraud Measured in Each Country Divided by Sector

Country	Types of fraud for which estimations were available	
	Private Sector Fraud	**Public Sector Fraud**
Australia	Insurance fraud	(Not available)
Canada	Insurance fraud, Financial Services fraud, Telemarketing fraud	Health Care fraud
France	Bank Card fraud	Customs fraud
Germany	(Not available)	(Not available)
Ireland	Private Sector fraud as a whole	(Not available)
UK	Insurance fraud, Plastic Card fraud, Non-Plastic Card fraud, particularly Cheque fraud, Telecommunications fraud	Customs and Excise fraud, Benefit fraud, Health Care fraud, Defence fraud
USA	Insurance fraud, Telemarketing fraud	Health Care fraud

12.7 During our research into the estimates of the cost of fraud in each country, it has become evident that there is a distinct lack of robust methodologies for recording or even estimating the cost of fraud; for example, in the UK, only the National Health Service has a strategy that measures fraud before and after each new anti-fraud initiative has been introduced. Therefore, it is hard to arrive at any accurate conclusions regarding the level of resources required to counter fraud. In summary, not only is there insufficient information available in each country to accurately calculate the level of resources required, but there is also a distinct lack of information available to measure the effect of counter fraud initiatives imposed in order to make a successful evaluation.

A National Fraud Strategy and a National Fraud Authority

12.8 At present, the UK does not have a national strategy for fighting fraud. Many public and private sector organisations and institutions have developed their own

strategies for countering fraud within their own areas. Our research has indicated that this is also the case for many other countries.

Australia

12.9 The Australian Consumer Fraud Taskforce, established in March 2005, launches a number of campaigns to raise fraud awareness of various types of fraud that fall under the umbrella of Consumer Fraud Prevention Month as part of its strategy to counter consumer fraud; for example, in March 2006, four week awareness campaign was launched focussing on Internet scams, and another focuses on overseas lottery scams. The Taskforce comprises 18 government regulatory agencies and departments each with a remit to counter fraud and scams in consumer protection. It is a cross-border initiative of the state, territory and the Australian and New Zealand governments. The Taskforce's overall aim is to create an annual awareness campaign that coincides with the Global Consumer Fraud Prevention Month co-ordinated by the International Consumer Protection and Enforcement Network (ICPEN), a network comprising law enforcement agencies from over 30 countries including Australia.

Canada

12.10 The closest we have come to in finding a national fraud strategy that we have been able to find is the federal strategy for private sector fraud in Canada. This strategy is aimed at countering 'serious capital market fraud' also known as 'corporate fraud'. The Canadian federal government's coordinated strategy is based on the following proposals:

- Expanding resources dedicated to investigating serious cases of capital market fraud. Integrated Market Enforcement Teams (IMETs) are to be established in key Canadian financial centres;

- Provision of additional resources to support prosecutions of capital market fraud offences under the Canadian Criminal Code;

- Proposing legislative amendments to the Canadian Criminal Code that will create new offences and evidence-gathering tools, toughen sentencing, and establish concurrent jurisdiction with the provinces in the prosecution of serious cases of this fraud.

12.11 Phone Busters is the Canadian is a national anti-fraud call centre jointly operated by the Ontario Provincial Police and the Royal Canadian Mounted Police. Its national strategy is aimed at informing consumers of how to detect a telemarketing scam. Phone Busters It is the central agency in Canada that collects information on telemarketing fraud, advanced fee fraud letters and identity fraud complaints and disseminates this to the public in a bid to prevent this type of fraud.

12.12 The proposed UK national anti-fraud strategy will set the basis for developing an anti-fraud culture. Similarly, the Fraud Prevention Forum (FPF) of Canada, aiming to prevent Canadians from becoming victims of fraud, declared the month of March was officially declared 'Fraud Prevention Month' in Ottawa in 2006. During this month, the Fraud Prevention Forum members attempt to raise the awareness of the Canadian public in a bid to prevent the occurrence of fraud through the distribution of fraud prevention material as well as airing public service documents. The FPF comprises private sector bodies, government agencies, law enforcement agencies, and consumer and volunteer groups. Its members include, but are not restricted to, the following bodies: Competition Bureau Canada (Chair); Canada Post; Canadian Bankers' Association; Toronto Police Service; Royal Canadian Mounted Police; and Western Union. A Fraud Awareness Month was also launched in February 2005 by the FPF in conjunction with private sector organisations. It has not been possible to find statistics on the audience reached during the Fraud Prevention Month or Fraud Awareness Month, so we cannot evaluate its effectiveness in this communications objective. However, this does provide a good example of a national approach to educate the public about fraud prevention and to raise fraud awareness amongst the public in general.

United States of America

12.13 Leading on from this, the US has conducted a national joint effort to develop an anti-fraud culture and raise fraud awareness amongst consumers. 'Project kNOw' is a large consumer protection effort, whose partners consist of key federal government consumer protection agencies and private sector organisations. Its partners include, but are not limited to: Council of Better Business Bureaus Foundation; Department of Justice; Federal Bureau of Intelligence; Federal Trade Commission; National Association of Attorney Generals; Securities and Exchange Commission; and the US Postal Inspection Service. To date, the project has conducted a mail-shot to 120 million households in the U.S. to raise fraud awareness of telemarketing fraud amongst consumers.

Reporting Fraud

12.14 The Fraud Review is making recommendations that aim to improve the UK arrangements for reporting and recording fraud. One of the methods proposed to achieve this is to create a central reporting centre. Our research has found that national reporting centres currently exist in other countries.

Canada

12.15 Reporting Economic Crime Online (RECOL) is a fraud reporting initiative in Canada which incorporates an integrated partnership between federal and provincial law enforcement agencies and private sector organisations with a vested investigative interest in receiving copies of complaints of economic crime including: investment fraud, property fraud, fraudulent bankruptcy, counterfeit fraud, corruption, identity fraud, advance fee fraud, online auction fraud and health fraud. It is a public sector body administered by the National White Collar Crime Centre of Canada (NW4C) and is supported by the Royal Canadian Mounted Police. Members of the NW4C have access to the information monitored and filed by RECOL. More than 1,000 fraud complaints were filed with the RECOL website in its first six months of operation in 2005. Consumers valued the crimes they reported at more than £191 million (CAD $400 million) in the first six months alone.

12.16 The examples provided above indicate that it is possible for such a centre to be created, for example in Canada, which comprises 13 provinces, each of which can create offences over which they have jurisdiction. Of the two countries described here, Canada bears the closest resemblance to the UK in that it is divided into a number of provinces. Similarly the UK and British Islands contain different jurisdictions.

United States of America

12.17 Consumer Sentinel, based in the USA, describes itself as 'a one-stop, secure investigative cyber tool and complaint database, on a separate restricted-access secure web site, that provides hundreds of law enforcement agencies immediate access to Internet cons, telemarketing scams and other consumer fraud-related complaints. It gives consumers a way to voice their complaints about fraud to law enforcement officials worldwide'.[194] The Consumer Sentinel website is maintained by the Federal Trade Commission (a government body that polices anticompetitive practices), which contained over one million fraud complaints as at 2005. These complaints were then filed with federal, state, and local law enforcement agencies, as well as private sector organisations.

12.18 The Internet Crime Complaint Centre (IC3) is a partnership between the Federal Bureau of Investigations and the National White Collar Crime Centre. The IC3 receives Internet crime complaints, researches them and then refers them on to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation. There appears to be some overlap between the IC3 and Consumer Sentinel, however, the Federal Trade Commission which maintains the Consumer Sentinel website is a member of the IC3's public and private sector alliances.

12.19 Both Consumer Sentinel and IC3 perform the dual function of both a reporting and referral centre. However, Consumer Sentinel focuses specifically on consumer fraud, whereas IC3 has a remit that expands to all types of Internet crime defined as 'any illegal activity involving one or more components of the

Internet, such as websites, chat rooms, and/or email. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes.'[195]

Data Sharing

12.20 The Fraud Review explored the area of intelligence, and data-sharing particularly, improving the way fraud intelligence is collated and shared. A number of countries have established systems in which data is shared amongst agencies.

Australia

12.21 Two data matching programmes have been established in Australia. The first is a Data Matching Programme Protocol entitled Pay as You Go (PAYG) which was created as a result of the government's efforts to focus on the detection of customers failing to declare or falsifying details of their income. PAYG matches Centrelink customers (a government agency delivering a range of services to Australian citizens) with customers identified by the Australian Taxation Office that have a PAYG Payment Summary. (The Australian Taxation Office is responsible for the PAYG taxation system). Where anomalies are identified, the cases are then reviewed. The purpose of the PAYG Programme is to deter potential fraudsters and identify monies that have been lost to fraud in order to seek its recovery, as well as identifying cases for further action to be sought such as prosecution. The first pilot schemes of this programme were divided into two phases, the first delivered in 2000-01, and the second in December 2002 to June 2003. This pilot saved Centrelink a total of £6.5 million (AUS $15,944,769) from 2001 to 2003. Additionally, 'the project realized $12,789,000[196] for the 2002-2003 financial year, which exceeds the $12,672,000[197] estimated in the Budget papers'.[198] The total running costs for 2001-02 amounted to £488,592 (AUS $1,210,141)[199] which decreased to £375,964 (AUS $930,594)[200] in 2002-03.

12.22 The second programme comprises matching data from the Australian Securities and Investment Commission (ASIC), Australian Taxation Office and Centrelink – although this time the focus is on Centrelink customers. This data includes information in respect of people who have failed to declare shareholdings in small proprietary companies and non-listed public companies while in receipt of Centrelink payments. The main purpose of this programme is to deter potential fraudsters from claiming payments that they are not entitled to. The total savings from the pilot programme run that began in April 2000 amounted to £197,395 (AUS $485,873). After the first full year of the programme's operation, a total saving to pensions, benefits and allowances (excluding Youth Allowance) amounted to £2.2 million (AUS $5.4 million) equating to a cost benefit ratio of 1: 4.41. [201]

United States of America

12.23 Consumer Sentinel in the US (as mentioned in paragraph 1.18) allows law enforcement agencies across the US to access information through an encrypted website which can be used to source further information about a reported scheme, as well as spot fraud trends discovered as a result of Consumer Sentinel data analysis. The Sentinel also shares information on fraud alerts about companies under investigation. More than 90 federal law enforcement organisations contribute data to Consumer Sentinel. The data can also be accessed by various Canadian and Australian law enforcement organisations.

12.24 Leading on from this, the National White Collar Crime Centre (NW3C), founded in 1992, is funded by the US Department of Justice and provides national support for the prevention, investigation and prosecution of white collar and economic crimes, including: investment fraud, telemarketing fraud, securities fraud and advance-fee loan schemes. The Centre shares information with federal, state, local and international law enforcement, regulatory and prosecution agencies, as well as constituted permanent task forces. The Investigative Support Section of NW3C provides support services such as analytical support, public database searches, and case funding, for member agencies who are involved in the investigation or prosecution of a white collar crime. The NW3C does not allocate

cases and does not have any investigative authority. Therefore the NW3C acts as centre of excellence sharing information; including intelligence, research, and technologically advanced investigative expertise, with member agencies, and also provides support services including acting as a source of funding for member agencies, that are faced with budgetary shortfalls.

12.25 Running costs for the NW3C are estimated at approximately £6.4 million ($12 million) per year. As the Centre provides support services, training and research, it has not been possible to find hard statistics on its success in countering fraud.

12.26 IC3 also work closely with RECOL in Canada (described in paragraph 1.15) in regards to data-sharing, and provides another example of cross-border cooperation.

Investigating Fraud

12.27 In the UK, the current arrangements for the investigation of fraud are varied. Regional police forces have limited capacity to investigate fraud and as a result, the Fraud Review has considered a more effective structure for police forces to investigate fraud, such as increasing the use of specialist civilian investigators, improving the partnerships between the police and private sector organisations, and harnessing the resources of current fraud squads into regional forces.

12.28 In order to provide a like comparison, we directed further research into the Garda Bureau of Fraud Investigation (GBFI) of Ireland, established in 1995 which provides a like comparison. The GBFI is the Garda Síochána's dedicated fraud unit, and its remit involves the investigation of fraud on a national basis as well as collating information and fraud intelligence, and playing a proactive role in the prevention and detection of fraud. The GBFI comprises five separate sections: Assessment Unit (examines and analyses all fraud complaints at an early stage); Commercial Fraud Unit (deals with complex fraud cases); Money Laundering Unit (investigates breaches of the Criminal Justice Act); Cheque/Credit Card Fraud Unit (investigates serious cases of these types of fraud); and the Computer

Crime Unit (a national reference centre for the Garda which examines computer hardware and storage devices used in fraud cases).

12.29 The Garda also works closely with the Police Service of Northern Ireland, along with the Fraud Unit and the Organised Crime Task Force. Cooperative measures between the two police forces include the formation of the first joint Cross Border Organised Crime Assessment in September 2004. A report was compiled to provide an overview of cross border crime common to Northern Ireland and the Republic of Ireland with a special focus on serious and organised crime conducted on both sides of the border. Six out of the eight areas of organised criminal activity highlighted were fraud-specific[202]:

a) Money laundering and fraud.
b) Intellectual property crime (including counterfeiting).
c) Drugs trafficking.
d) Oils fraud.
e) Tobacco fraud.
f) Alcohol fraud.

12.30 The production of the Cross Border Organised Crime Assessment marks a significant milestone in the fight against organised crime on both sides of the border. This example also indicates that cooperation between law enforcement agencies is essential in countering organised crime.

Prosecuting and Penalising Fraud

12.31 In 2001, Lord Justice Auld published a major review of criminal courts in England and Wales. His review recommended that the establishment of specialised financial courts should be considered. These courts would examine the criminal, regulatory and civil aspects of the case to see if they could be dealt with in combination. Of the countries examined, a small number had financial courts in existence. German financial courts deal with taxation and related matters. France has also established a number of Economic and Financial Crime Centres. These Centres contain civil servants with specialist knowledge or experience in

economic and financial issues employed in the post of specialised assistants under Section 91-I of Act no. 98-546 of July 2nd 1998. These assistants help to lessen the workload of Investigating Magistrates, although they are not authorised to participate in questioning, searching or seizing evidence. The first courts to benefit from this initiative were based in Paris, Marseille, Lyon and Bastia (Corsica). The Paris Centre was the largest centre in 1998-99, comprising 32 judges, 37 civil servants, 11 judicial assistants and four specialised assistants in the Public Prosecutor's Office; and 60 judges, 65 civil servants, 12 judicial assistants and four specialised assistants.

12.32 France has two types of court in its legal system, Judicial and Administrative. The national audit function is subsumed in its court system. (The UK National Audit Office which performs the same function is not part of the UK court system). High ranking officials appointed by Presidential decree (préfets) have the power, in certain circumstances, to refer the budgets of local authorities to the Regional Courts of Accounts (Chambres des Comptes). These Regional Courts were created in 1982 and play a key role in guaranteeing the public accountability of local government and other public bodies and their use of public funds. It is a statutory requirement that all public accounts and supporting documents are submitted to the Regional Courts. However, the Court of Accounts still retains its function as a court of appeal against judgements made by the regional courts. The Court of Accounts also audits government accounts.

12.33 A further piece of legislation which, amongst other things, is designed to counter fraud in the USA, is the Sarbanes-Oxley Act (2002). This Act was designed as a response to the Enron and WorldCom fraud and corruption scandals of 2001. The purpose of the Act is to review legislative audit requirements to improve the accuracy of corporate financial reporting in public companies. The Act includes a provision, under Section 802, which prohibits fraudulent activity in relation to federal investigations.

12.34 The principal relevant provisions of SOX with regards to public companies are as follows:

- Audit firms are prohibited from undertaking a variety of non-audit work for their clients;

- Companies must establish independent audit committees;

- Company executives can no longer take out company loans;

- Top executives must certify company accounts;

- Whistleblowers are better protected, no company may discharge, demote, suspend, threaten, harass, or discriminate against an employee because of any information on a suspected fraud that they have lawfully provided.;

- Managers are responsible for maintaining an adequate internal control structure and procedures for financial reporting;

- Company auditors must affirm the management's assessment of these internal controls.

12.35 However, SOX is not without its critics. A number of businesses have spoken out against the SOX Act, particularly Section 404 which is the most difficult and expensive part of the legislation to comply with; on the grounds that compliance with the internal control rules do not do much to enhance the company's systems or to protect shareholders.

12.36 In 2005, a survey of Section 404 compliance costs was conducted by Financial Executives International, a group of 15,000 chief financial officers and other senior financial executives. The findings showed that public companies were spending on average £2.32 million ($4.36 million) in the first year of compliance with Section 404. However, the estimated cost of compliance was set at £1.67 million ($3.14 million), equating to a 39% increase on estimated expenditure. The majority of this increase resulted from external costs for consulting and software, and an increase in the fees charged by external auditors. It is not clear how many of these were 'one-off' or recurring costs.

Canada

12.37 Phone Busters, as described in paragraph 1.11, also has a remit to prosecute fraudsters conducting in telemarketing fraud in Ontario and Quebec. This remit has been extended to include the facilitation of cross-border prosecutions with US agencies through extradition.

Legal Definitions of Fraud

12.38 Three out of the six countries examined have a legal definition of criminal fraud. The remaining countries had provisions for fraud-related offences although not for the offence of fraud per se. The table below summarises the sentences imposed for both fraud and fraud-related offences in each of the six countries.

Table 3. Sentences Imposed for Fraud and Fraud Related Offences

Country	Offence	Sentence Imposed		
		Imprisonment (maximum)	**Fine**	**Both penalties can be imposed**
Australia	Obtaining property by deception	10 years		
	Obtaining financial advantage by deception	10 years		
	Conspiracy to defraud	10 years		
Canada	Defraud the public or any person of any property, money, valuable security or any service	14 years (if the subject matter of the offence is greater than £2,500) 2 years (if subject matter of offence is less than £2,500)		
	Fraudulent manipulation of stock exchange transactions	10 years		

	Fraudulently impersonating any person to gain a financial advantage	10 years		
France	Fraudulent obtaining	5 years	£263,000[203] (€375,000)	✓
	Fraudulent obtaining (when committed by a person in public office, public authority, or making a public appeal)	7 years	£526,000 (€750,000)[204]	✓
	Fraudulent obtaining (when committed by natural persons [e.g. – corporations])	5 years		
Germany	Fraudulent obtaining	5 years	(Amount not stated)	(Both are not applicable)
	Fraudulent obtaining (serious cases involving gangs, huge losses, places another person in financial need, involves a public official, or feigns an insurance claim)	10 years		
	Computer fraud	5 years	(Amount not stated)	(Both are not applicable)
	Computer fraud (serious cases)	10 years		
	Subsidy fraud	5 years		
	Subsidy fraud (serious cases)	10 years	-	
	Obtaining benefits by devious means	1 year	(Amount not stated)	
	Capital investment fraud	3 years	(Amount not stated)	(Both are not applicable)
	Credit fraud	3 years	(Amount not stated)	(Both are not applicable)
Ireland	Making a gain or causing loss by deception	5 years	(Amount not stated)	✓
	Obtaining services by deception	5 years	(Amount not stated)	✓
	Forgery	10 years	(Amount not stated)	✓
	Using a false instrument	10 years	(Amount not stated)	✓

	Copying a false instrument	10 years	(Amount not stated)	✓
	Using a copy of a false instrument	10 years	(Amount not stated)	✓
UK	Obtaining services by deception	5 years	-	-
	Obtaining property by deception	10 years	-	-
	Obtaining a money transfer	10 years	-	-
	Obtaining a wrongful credit	10 years	-	-
	Obtaining a pecuniary advantage by deception	5 years	-	-
	False accounting	7 years	-	-
	Making, copying or using a false instrument	10 years	-	-
USA	Fraudulent activity in relation to federal investigations	20 years	(Amount not stated)	✓
	Deceit and misrepresentation in relation to the sale of securities	5 years	£5,742 ($10,000)	✓

12.39 The proposed maximum sentence for fraud contained in the Fraud Bill is 14 years' imprisonment. This length of sentence will fall into line with Canada, while 10 years would be comparable with Australia and Germany. The highest sentence imposed for a fraud-related offence is that of the USA for conducting in fraudulent activity in relation to federal investigations. This offence carries a maximum penalty of 20 years' imprisonment.

12.40 The topic of prisons and the cost of imprisonment is a serious issue in the UK due to overcrowding. One of the considerations of the Fraud Review was to look at alternatives to custodial sentences for prosecuted fraudsters. In Canada, there are a few examples where non-custodial sentences, such as community service - have been imposed for convicted fraudsters. The following case provided by the Church Council on Justice and Correction[205] presents an example of such non-custodial alternative sentencing:

"The offender is a 38-year-old divorced mother of two children who was in receipt of social assistance. She was accused in a $14,000 social assistance fraud case. It was agreed between the victim and the offender that restitution would be

an acceptable resolution. As is the procedure with our program, the charge was laid (sworn) by police but not placed on the court docket. The police made the referral directly to our staff, contact was established with the victim to determine their wishes/concerns and the offender was interviewed to determine her interest in participating in the diversion option. Following an assessment interview with the diversion (probation) officer regarding the offence and the proposed resolution of it, a written agreement was signed by the client outlining her obligation to make monthly payments of $100.00 each directly to the social assistance office."[206]

Conclusions

12.41 In conclusion, the research undertaken has found that consumer and corporate frauds are the two main areas where national strategies and initiatives have been launched by other countries. There is also substantial evidence of cross-border working and data sharing between different national and international agencies. Overall, the examples portrayed from each of the countries provides an indicator to the Fraud Review of England and Wales that its aims are achievable despite the obstacles that are currently faced in the two countries.

12.42 In summary, three out of the six countries examined have a legal definition of criminal fraud. The longest maximum sentence of imprisonment imposed for a fraud offence is that of 14 years in Canada, if the subject matter of the offence is greater than £2,500. Of the figures found, the greatest cost of fraud was £378 billion ($660 billion) in the USA. However, the greatest cost of fraud as a percentage of the countries gross domestic product belonged to Germany totalling 9% of their GDP. With regards to the creation of a national strategy, although other countries such as a Canada have devised a national strategy for corporate fraud; none of the countries have created a national policy that covers all types of fraud. The majority of strategies in all the countries researched are designed to counter consumer fraud.

12.43 With regards to central fraud reporting agencies, a number of centres have been set up for this specific purpose that have either an exclusive focus on fraud

reporting, or include fraud within their remit amongst other types of crime. Consumer Sentinel in the USA provides law enforcement agencies access to consumer fraud-related complaints. The Internet Crime Compliance Centre (IC3) is a central reporting mechanism for cyber crime complaints including, but not limited to, various types of fraud that occur under the umbrella of consumer fraud in the USA. RECOL is a reporting initiative in Canada, incorporating federal law enforcement agencies and private sector bodies. A national fraud prevention month was declared in March 2006 in Canada, which was constructed by the Fraud Prevention Forum comprising a number of public and private sector Canadian bodies. This multi-agency approach provides a useful platform for countering fraud across both sectors.

12.44 Examples of multi-agency working within sectors have also been displayed. In Australia, Centrelink (a government agency delivering a range of services to Australian citizens) join forces with the Australian Tax Office to implement their data matching programme protocol focussing on fraud detection. Similarly, these two bodies have also joined forces with the Australian Securities and Investment Commission to detect fraud cases in which Centrelink customers have claimed payments that they are not entitled to. This approach saved Centrelink a total of £6.5 million (AUS $15,944,769) from 2001 to 2003. Therefore a multi-agency approach can be effective in intercepting specific types of fraud that may only occur in one sector.

12.45 There is evidence of cross-border counter fraud work, particularly between the USA and Canada, in the form of IC3 which as formed alliances with RECOL. Another example is the Office of Consumer Litigation of the Civil Division of the Department of Justice (USA), which conducts both civil and criminal cross border litigation in consumer-related cases, and has the authority to seek civil remedies and freeze assets in foreign jurisdictions such as Canada. Additionally, the Garda Síochána (Ireland's national police service) contains a dedicated fraud unit that works closely with the Fraud Squad of the Police Service of Northern Ireland and the Organized Crime Task Force of the UK (a multi-agency approach to counter organized crime in Northern Ireland comprising UK government

departments and the PSNI). Countries in the EU are bound by EU requirements to counter fraud and corruption and also work in a cross-border capacity.

12.46 The examples of counter fraud work presented in this report strongly indicate that a multi-agency approach encompassing both public and private sector organisations is required to establish an effective approach to counter fraud. This would also provide a strong deterrent message to potential fraudsters that fraud is being taken seriously and that a united stand is being taken to combat its existence.

CHAPTER 13 COSTINGS AND LEGISLATION

13 SUMMARY

- This chapter summarizes the cost and savings estimates for the recommendations in the report. These estimates are confined to the direct cost or savings to government of the proposed measures. They make no estimate of savings from reducing fraud losses, either to government or business or consumers, which are the main benefits flowing from the recommendations.

- Overall the recommendations should save public money.

- The costs amount to between £13 million and £27 million a year, depending on the number of Regional Support Centres established to provide specialist support to police fraud squads. (Doubling the size of police fraud squads, the best option for making an immediate improvement in the police response to fraud, would cost a further £14.5 million a year.)

- Private sector contributions may provide £5 million towards these costs.

- Savings of legal aid, prosecution and court costs are estimated at £49 million, leaving net savings of between £23 and £37 million a year.

- Many of the recommendations make provision for services which will enable fraud to be better understood and prevented. Where fraud can be prevented there are direct savings to both the public and the private sector. Where figures exist they reveal an excellent rate of return on investment in anti-fraud measures. For example the NHS Counter Fraud Service reports a ratio of benefits to cost ratio of 13:1 from activities and the National Fraud Initiative run by the Audit Commission reports a benefit to cost ratio of over 100:1.

- Most of the recommendations do not require legislation, but where legislation is necessary, this is noted.

Introduction

13.1 Some of the recommendations do not have direct costs or savings for government, although all the recommendations will contribute towards a more effective response to fraud and reduced fraud losses in the economy as a whole. This chapter deals with the costs and/or savings to government of these measures which do have such direct effects. In some cases these estimates are orders of magnitude and have not been subject to full business cases. For these recommendations, the Review further recommends that those cases be developed.

13.2 The table below summarises the estimates.

Table 1. Summary of Recommendations with Associated Costs/Savings

Recommendation	Cost (£m)	Legislation
1. National Fraud Strategic Authority.	3.0*	No
2. National Fraud Reporting Centre.	5.2*	No
3. Establish National Lead Force to assist with or carry out some major fraud investigation enquiries outside its force area.	2.0*	No
4. Creation of 1-8 Regional Support Centres to support fraud squads.	2.0-16.0	No
5. Pilot to assess benefits of a Financial Court jurisdiction.	0.3	No
6. Extend Crown Court non custodial sentencing options.	none	Yes
7. Increased training for panel of judges hearing serious fraud trials.	0.06	No
8. Cost/benefit study into Electronic Presentation of Evidence.	0.015	No
9. Introduction of formal plea bargaining system.	(49.3)	Possibly
10. Increase in maximum sentence for serious fraud offences.	None	Yes

(*Gross cost. Net cost to government should be reduced by private sector contributions.)

Summary	£m
Costs	12.575 to 26.575
Savings	(49.3)
Net Position	(36.725 to 22.775)

Memo

It is plausible to assume that half the cost of the asterisked items will be contributed from the private sector, with a total contribution of £5 million a year.

National Fraud Strategic Authority

13.3 A National Fraud Strategic Authority will have the following benefits:

- Increase efficiency of government anti-fraud activity.
- Identify harm from fraud to the UK economy.
- Increase market transparency on fraud and increase confidence in UK markets capacity to tackle fraud.
- Measure and monitor the impact of fraud on the consumer.
- Increase fraud prevention and detection through best practice.
- Provide an efficient mechanism for business to direct fraud enquiries and information to government.

13.4 It is not possible to calculate the amount by which fraud will be reduced as a consequence of establishing the NFSA. However, it is a vital piece of infrastructure which will enable economic benefits and efficiency gains to be made across the private and the public sectors.

13.5 The NFSA will probably comprise five main units, as set out in the table below.

Table 2. National Fraud Strategic Authority and Fraud Measurement Team

FUNCTION	STAFF	COST
NFSA Head and Support	3	£0.2m
Develop and Measure Methodology Develop Performance Indicators Direct Fraud Measurement Team Work Programme	6	£0.3m
Fraud Measurement Team	13	£0.45m
Fraud Strategy Stakeholders Committee Conflicts/Troubleshoot	8	£0.4m
Structure/Resources Developments Government-wide Policy, Legislation	6	£0.3
Anti-fraud Awareness Best Practice Expertise Provision Compliance	14	£0.6
TOTAL	**50**	**£2.25m**

13.6 The above costs comprise the salary and associated personnel costs of 50 staff but not other running costs such as accommodation. Although this has not been subject to a detailed costing a prudent allowance for the additional costs would be £0.75 million per year, taking the overall cost to £3 million per year. The NFSA would be a public/private partnership and it is reasonable to expect that 50 per cent of the costs would be provided by private sector contributions.

National Fraud Reporting Centre (Chapter 4)

13.7 The National Fraud Reporting Centre would offer the following functions:

- Victims reporting, online or through a call centre.
- Allocation of cases to police forces.
- Business reporting, capacity to report suspected frauds.
- Government reporting, capacity to report suspected frauds.

- Analysis, trends, warnings and alerts.

13.8 There are two major areas of savings for fraud which will be facilitated by the NFRC:

- Identification and efficient investigation of existing frauds, and
- Prevention of losses through risk management.

13.9 The savings generated by identification and efficient investigation of existing frauds will be produced by:

- Efficiency gains in the investigative response;
- Being able to target those groups where the largest harm occurs (e.g. fraud ring associated with other types of organised crime); and
- Asset recovery and victims compensation.

13.10 Of these, the public sector will benefit most from efficiency gains. Victims will benefit from an improved response to fraud.

13.11 The table below shows existing activities across these areas. The first two rows are those exercises which comprise investigation and response. The next three rows are data sharing exercises.

13.12 The DCPCU is a police unit which identifies trends and investigates card and plastic fraud. The rate of return of investment in DCPCU is 10 to 1.

13.13 The NHS undertakes a range of activities from prevention and awareness, measurement as well as investigation, prosecution and asset recovery. The savings calculated by the NHS are on the basis of measurement, action, and repeated measurement. They are proven reductions in fraudulent activity through active engagement in spending areas. The average rate of return for the NHS Counter Fraud and Security Management Service since it was established in 1998 has been 13 to 1.

Table 3. Savings from Anti-fraud Activity

	Investment in Fighting Fraud 2004-5	Fraud Savings[207] 2004-5
DCPCU	£3,700,000	£10million
NHS	£17,812,000	£189,116,000
NFI	£1,000,000	£111,000,000
IFB	circa £1,000,000	Estimated ranges £50,000,000 - £200,000,000
CIFAS	£2,500,000	£ 682,000,000

13.14 The savings generated by the prevention of losses in the first place are potentially very large, but it must be recognised that calculation of savings from preventing fraud will always be, statistically, less rigorous than savings which are proven over time. In order to 'realise' savings from preventative mechanisms an efficient, real time system of risk management must be in place. This is part of the investment envisaged when establishing the NFRC.

13.15 Other systems such as CIFAS demonstrate how this can be a useful mechanism. The Insurance Fraud Bureau also estimates that it could prevent up to £200 million worth of fraud to the industry when it is fully established. The National Fraud Initiative also demonstrates how sharing information can identify frauds, but more must be done to make the system capable of preventing frauds as well as identifying frauds which have occurred.

13.16 It must be recognised that the associated costs of responding to identified frauds are not included in the examples of the NFI, IFB and CIFAS.

13.17 A full business case outlining in more detail the role of the NFRC, its performance measures and estimated savings should be made by the National Strategic Fraud Authority. The table below shows an initial estimate of the costs of establishing the NFRC. There are three potential outcomes, which are affected

by the number of calls received by the telephone call centre. The more calls, the higher the costs of the call centre. These are represented below.

13.18 The Fraud Review believes that when combined with online reporting the lower volume of 500,000 calls would be expected in Year 1.

Table 4. National Fraud Reporting Centre

NFRC Costs			
Calls per annum	500,000 calls p.a.	1.25 million calls p.a.	2 million calls p.a.
Call centre	£2,370,000	£7,250,000	£9,500,000
Online Reporting capacity	£1,250,000	£1,250,000	£1,250,000
Analytical Support Unit*	£1,125,000	£1,125,000	£1,125,000
Premises & Infrastructure	£250,000	£250,000	£250,000
Sub-Total	£995,000	£875,000	£12,125,000
Contingency (5%)	£231,600	£475,600	£588,100
TOTAL	**£5,226,600**	**£10,350,600**	**£12,713,100**

(* The Analytical Support Unit is assumed to comprise a 20 person unit.)

Increase in Police Capacity to Investigate Fraud (Chapter 7)

Base Case

13.19 The base case comprises two elements:

a) Creation of a National Lead Force to act as a centre of excellence for England and Wales police forces and assist those forces with or, on occasions, carry out complex fraud investigations arising outside London and South East;

b) Creation of eight Regional Support Centres to provide specialist resources to support fraud squad investigations outside London.

13.20 When the City of London Police was given lead force status for London and the South East in 2003, it was expected to carry out a number of investigations where the fraud fell below the SFO threshold for investigation, which arose in the London and South East ACPO region. To finance this additional work the City of London Police received additional funding of £2 million per year, of which half was provided by the Home Office and half by the City of London Corporation. The new proposal is to extend this role to similar serious fraud cases arising in other ACPO regions in England and Wales. It is difficult to estimate the appropriate level of new resources necessary to undertake this work without a full feasibility study but an opening allocation of another £2 million per year would enable a start to be made. No detailed discussions have been held on funding but the City of London Corporation have indicated that they would be prepared to consider making a contribution provided the City of London Police remained a separate force.

Regional Support Centres

13.21 A Regional Support Centre (RSC) would comprise a range of specialist and technical services dedicated to fraud investigations such as surveillance, analysis, research and hi-tech interventions. Similar units are being established to support Special Branch operations and typically consist of 37 police and support staff. A breakdown is in the box below. While the precise mix of expertise and ranks require further work the numbers and costings are of the right order of magnitude.

13.22 To provide one RSC per ACPO region (outside London and the South East) would therefore cost £16 million per year. It would be possible, although at the cost of some loss of service, to reduce these costs in two ways:

- Either fewer RSCs; or
- Replacing some of the police officers with non-police personnel (which might reduce the cost of each RSC to £1.5 million).

Table 5. Regional Fraud Intelligence & Co-ordination Centre

Regional Fraud Intelligence & Co-ordination Centre		
POSITION	**GRADE**	**POSTS**
Regional Coordinator	Det. Supt	1
Deputy Coordinator	DCI	1
Operational Managers	Det. Insp.	1
Supervisors	Det. Sgt.	2
Operational Officers (fraud desk, technical, high tech unit, surveillance & source handlers)	Det.Con.	20
Support	AO	3
Analytical	AO	4
Research	AO	4
TOTAL		**37**
Ongoing yearly cost per Region, outside London		**£2,050.196**

Variant

13.23 If it were decided to make an immediate increase in the police investigative response to fraud the best option would be to start to rebuild the capacity and capability of police forces outside of London and the South East to deal with fraud investigations. Doubling resources from present levels would mean an extra 290 detectives and 16 additional senior officers. The cost would be around £14.5 million a year. The details are set out in the box below.

Table 6. Fraud Squads

Fraud Squads (Police Officers Only)		
Current Position	Staff	Cost
London	126	7.24
Elsewhere	290	13.45
TOTAL	**416**	**20.69**
Double Regional Squads		
London	126	7.24
Elsewhere	580	26.90
Additional senior officers	16	1.08
TOTAL	**722**	**35.22**
DIFFERENCE	**316**	**14.53**

Increasing Civilian Investigative Capacity

13.24 Increasing civilian capacity within police forces is aimed at maximising use of skills available. There would be no cost implications above current spend, as the chapter proposes the use of secondments, training schemes and co-operation to increase the efficiency and responsiveness of law enforcement investigations.

13.25 The expansion of training to provide comprehensive fraud training would be facilitated by the NFSA (costs already incorporated) and courses would be run as professional concerns. Service providers would be accredited, and current training budgets would accommodate the cost of training.

13.26 There are also no cost implications for public private partnerships specifically; these have been detailed in other parts of the report through costing recommendations which could potentially be supported by both the public and private sectors, for example the NFRC.

Pilot to assess the benefits/drawbacks of a Court

13.27 The expected benefits of a financial court jurisdiction would be as follows:

- Reductions in High Court hearings of civil cases arising out of fraud offences.
- Reduction in judicial 'reading in' time for complex cases.
- Reduction in High Court costs element of civil legal aid when hearings take place in the crown court.
- Improved public confidence consequent upon a reduction in delays and injustices caused by parallel proceedings in different courts.
- Improved efficiency and increased consistency in the CJS as a result of co-ordinated hearings based on a single set of basic facts established by evidence presented in the first hearing only.
- Reductions in expense and inconvenience to witnesses.
- Improved efficiency and reductions in the length of criminal fraud trials by utilising and developing judicial expertise.
- Improved efficiency and reduced inconsistencies by unification of confiscation, compensation and civil recovery regimes.
- More transparent and efficient framework for allocation of High Court work to the crown court.
- More opportunities for professional development of circuit judges and more efficient use of the skills and experience of High Court judges.

Costs

13.28 A rigorous business case for a Financial Court jurisdiction can only be determined by use of a pilot scheme. Such a scheme should run for at least a year in view of the length of the average medium to long fraud trial and the delay ordinarily met between conviction and the beginning of associated regulatory or civil proceedings.

13.29 Any pilot should be conducted in close consultation with the Senior Presiding Judge and the presiding judge(s) for the region/regions selected; and with representatives of local criminal justice performance units, court users' committees, the JSB, Bar Council and Law Society. We estimate a pilot could cost in the region of £300k.

Extend Crown Court Non Custodial Sentencing Options

13.30 Extended non custodial sentencing powers would have the following benefits:

- Reduction of the number of separate High Court proceedings by victims and regulators.
- Promotion of effective plea bargaining.
- Reduction of the number of custodial sentences for fraud offences.
- An increase in confidence in the criminal justice system.

13.31 It is not thought likely that this option will increase the costs of operating the justice system. There could be some upward cost pressures. For example, the extended range of sentences proposed could increase legal aid. All ancillary hearings would be eligible under the Access to Justice Act 1999 leading to an increase in prosecution and defence costs and crown court ancillary hearings.

13.32 On the other hand, there should be savings in other parts of the system. For example, savings in DTI (Insolvency Service) and FSA resources will be made when crown courts impose the new sentences. Each sentence of disqualification or winding up, for example, will obviate the necessity, for the DTI to bring separate High Cost proceedings for the same remedy.

13.33 While it is not certain where the balance lies, there is no basis for believing this recommendation will cost money and no allowance is made in the table. However, this change would require legislation.

Increased Training for Panel of Judges Hearing Serious Fraud Trials

13.34 This recommendation is aimed at maximising the skills already available to the courts. There would be no cost implications other then the cost of running the training courses; and for “filling in” behind the judge being trained. The expected benefits are greater efficiency in the management of complex fraud trials leading to increased public confidence in the criminal justice system, more offences being brought to justice and better value for money.

13.35 The estimated cost of judicial training courses is £15,000 per day. Thus one annual 4 day training course for judges hearing serious fraud trials would cost approximately £60,000.

Commission Cost Benefit Analysis into Electronic Preparation and Presentation of Evidence

13.36 If the study demonstrates, as appears likely, that there would be significant long term financial savings by introducing a comprehensive and CJS wide system for electronic presentation of evidence, this would provide the basis for the essential pre requisite of a fully developed business case. Without such a study a proper business case cannot be prepared. The cost of such a study is put at approximately £15,000.

Defence "pleadings" to inform case management and disclosure

13.37 Further reductions in time spent on disclosure (both prior to and during trials) and the recommended move towards greater and more comprehensive defence "pleadings" should save direct Legal Aid costs as well as prosecution resources. The Carter Review recommendations for front loading of criminal advice fees should also ensure that Counsel enter preliminary hearings properly instructed and prepared to make full defence case statements. Thereafter, both prosecution disclosure choices and judicial case management will be informed by a more accurate understanding of the needs of the defence case. The VHCC Review Board's study of the GWT case showed (and CPS, RCPO and SFO experience bears this out) that up to one third of pre trial hours are spent on disclosure. This points to substantial savings being possible in this area provided that early and comprehensive defence case statements are served.

Introduction of Formal Plea Bargaining System

13.38 This recommendation is designed to achieve the following benefits:

- A reduction in the number of very high cost fraud cases going to trial, leading to a reduction in legal aid, investigative, prosecution and court costs.
- An increase in the number of offences brought to justice by increasing the capacity of investigators, prosecutors and courts.
- A speedier and more cost effective process for victims, witnesses and defendants.

13.39 There are a number of variables to be considered in assessing the likely cost savings if a plea bargaining system were to be introduced for serious fraud cases. Therefore there are some uncertainties estimating the extent of these savings. Clearly if a trial does not take place then the actual trial costs incurred by the prosecution, the defence and the court are avoided. However, in order for defence representatives to advise their clients properly before making a decision on a plea bargain in a particular case, significant legal aid work would have to be done which would undoubtedly mirror to some extent the work currently done pre trial. In addition, such work would occur at an earlier stage (i.e. pre charge) than hitherto.

13.40 The Fraud Review does not anticipate that extending legal aid to the pre charge sphere would mean that legal aid expenditure increased in those cases where a plea bargain is not agreed. The extensive work done by the defence pre trial should lead to a consequent reduction in the amount of work needed post charge.

13.41 Savings are assumed to arise from three sources:

a) A reduction in the number of trials because a proportion of defendants currently found guilty after contested trials will now plead guilty on the basis of a plea agreement;

b) A reduction in the number of trials ending in acquittal ordered by the judge as prosecutors become more rigorous in selecting cases brought to court;

c) A reduction in the number of trials which go the distance and end in acquittals as prosecutors become more rigorous in selecting cases brought to court;

d) A reduction in the length of trials, arising from better trial management by better trained judges including in relation to disclosure and trial procedures.

13.42 The estimates are based on statistics for 2003-2004, the latest year for which statistics are available. They are limited to fraud trials which passed the "Very High Cost Case" threshold established by the Department of Constitutional Affairs. They comprise the top one per cent of expensive trials and last for at least 41 days. The savings build-up as follows:

a) For cases where the defendant was found guilty after a contested trial, assume 75 percent would have reached a plea bargain. This would have avoided 46 trials involving 138 defendants. Savings per trial would have comprised:

- Legal Aid fees of £398,000;
- Prosecution fees of £133,000;
- Court costs of £189,000.

This is a saving per trial of around £720,000, which is £33.1 million for 46 trials.

b) 20 percent of acquittals for VHCC fraud cases are at the direction of the judge. Avoiding these, would avoid 10 trials with an overall saving of £7.2 million.

c) Assume that of the remaining acquittals a further 20 percent are avoidable; saving another 10 trials and £7.2 million.

d) Assume a 20 per cent reduction in the length of the remaining 28 trials, generating a savings of £1.8 million a year.

13.43 In total, the savings amount to £49.3 million a year. This does not take account of savings in respect of investigation costs, which are likely to be significant and which would increase capacity to undertake additional fraud investigations. It also does not take into account the savings on fraud cases that fall below the VHCC threshold but which could also be significant.

13.44 The calculations assume no reduction in legal aid paid to defence solicitors on the assumption that legal work by them would have to be undertaken prior to any plea bargain being considered. It also takes no account of time saved by prosecutors and investigators on disclosure issues. However, to the extent that plea bargaining arrangements encouraged earlier resolution of cases, further savings both in investigative time and time spent on disclosure are possible.

Increase in Maximum Sentence for Serious Fraud Offences

13.45 The Review has recommended that the maximum sentence length for serious offences should be increased from ten to 14 years. This recommendation forms part of an overall approach to penalise fraud. While it will lead to an increase in sentences for fraud and thus the average sentence served by those fraudsters jailed for fraud, it is not expected that the prison population will increase overall as a result of the Fraud Review. This is because the effect of widening the powers of the Crown Court to deal with fraud and the use of plea bargaining and conditional cautions is likely to reduce the number of frauds dealt with through full criminal trials rather than other outcomes.

13.46 The recommendation will provide courts with greater scope to accommodate aggravating factors for the very serious offences in order to achieve a more appropriate sentence than is currently possible. In addition to longer sentences for serious fraud offences the Review has proposed that the sentencing powers of the Crown Court should be extended to offer victims a wider range of remedies, and that a plea bargaining system should be introduced.

13.47 The need for lengthy custodial sentences in most fraud cases will diminish if there is an appropriate range of penalties which can better satisfy the needs of

victims. Earlier guilty pleas, wider use of conditional cautioning and other preventative measures recommended by the Review should also reduce the number of individuals jailed for fraud. So, while this recommendation will increase the average length of fraud sentences, other recommendations will reduce the numbers jailed for fraud and the costs and savings are assumed to balance out.

CHAPTER 14 LIST OF RECOMMENDATIONS

14 Introduction

14.1 The recommendations are included at the end of each chapter. This chapter lists the recommendations of the Fraud Review in full for ease of reference.

Chapter 2, Measuring Fraud (No legislation required)

1) A measurement unit should be established within the National Fraud Strategic Authority (NFSA) with a capacity to carry out four measurement exercises during its first year.

2) A programme should be established to measure the national extent of fraud based on a robust measurement methodologies.

Chapter 3, Fraud Strategy (No legislation required, but may be desirable)

3) A National Fraud Strategic Authority with the functions outlined in Chapter 3 should be established within central government.

4) The NFSA should report to a governing body consisting of the key stakeholders drawn from the private and public sectors.

5) A small committee drawn from potential stakeholders should be established to draw up a blue print for the NFSA.

6) A Multi-Agency Co-ordination Group (MACG) should be created as a subordinate group with the responsibility of co-ordinating operational work on priority areas as designated by the NFSA.

7) The MACG should be chaired by the Association of Chief Police Officers, Economic Crime Portfolio (ACPO-ECP) who would also be represented on the NFSA

Stakeholder Group. Its membership will be flexible and determined on the basis of identified priorities.

Chapter 4, Reporting Fraud (No legislation required)

8) A National Fraud Reporting Centre (NFRC) should be established for England and Wales, with capacity to link to domestic and international partners.

9) The NFRC should be housed within the National Lead (Police) Force (see Rec 39) and staffed by police officers and civilians. It should work closely with the NFSA.

10) The NFRC should have the capacity to accept crime reports from victims (including businesses and Government departments, Regulators, etc) according to the Home Office Counting Rules (HOCR) and the National Crime Reporting Statistics (NCRS).

11) The NFRC should work with police forces to agree criteria for screening and allocation of cases to forces. These criteria should be reviewed on a regular basis (e.g. annual or bi-annual).

12) The NFRC should be compatible with the IMPACT programme and searchable by police forces. The NFRC analytical unit should run reports on the system upon request from forces.

13) A pilot should be undertaken to match known frauds against other police data sets using IMPACT.

14) The NFRC should identify trusted partners in different sectors and establish working relationships with them to identify how information on known fraudsters can be shared efficiently to prevent and detect fraud.

15) The NFRC should analyse reports to provide strategic, tactical and other assessments to the police and partner organisations. Strategic assessment would

pass to the NFSA and inform the United Kingdom Threat Assessment (UKTA). Tactical assessments would inform an operational response.

Chapter 5, Data Sharing (Legislation already planned)

16) The Cabinet Committee Misc 31 should consider the recommendations of this Review with a view to increasing data sharing to prevent fraud.

17) Organisations which require consent to share or process data should explore adding crime prevention to any terms of consent they already offer, and the Government should support them in doing so.

18) The Department for Constitutional Affairs (DCA) should work with the proposed National Fraud Strategic Authority to co-ordinate the development of government wide guidance on data sharing to prevent fraud. The guidance should be developed in consultation with the Information Commissioner.

19) Public authorities should give the common law position on data sharing primacy and where legislative gateways exist, they should be widened if necessary to increase data sharing to prevent fraud.

20) Matching multiple data sets should be encouraged as part of a process of pursuing suspected frauds, and the proceeds of information matching be used to pursue crime.

21) The remit of the National Fraud Initiative (NFI) should be widened across more public sector authorities and the Audit Commission and National Audit Office should play an active role in developing anti-fraud measures in the public sector.

22) Data on deceased persons should be released as quickly and efficiently as possible to the public domain

Chapter 6, Preventing Fraud (No legislation required)

23) The NFSA and the NFRC and should have a direct role in relation to:

- Devising and implementing public anti fraud campaigns and warnings, drawing on generic and case specific information provided by NFRC;
- Liaising with the press for campaigns and case publicity;
- Devising and circulating best practice and advice on systemic fraud prevention within industry and government;
- Co-ordinating and informing the anti fraud awareness training provided to industry by other regional and sectoral groups.

24) Public authorities should reinvigorate fraud measurement and risk assessments in their financial processes in order to better assess the scale of fraud, risks face from fraud, and reduce losses to fraud

25) The National Audit Office and the Audit Commission should audit public bodies on the strength of their anti-fraud controls.

Chapter 7, Investigating Fraud (No legislation required)

26) The Home Secretary should consider making fraud a policing priority within the National Community Safety (Policing) Plan and law enforcement agencies should be encouraged to develop plans which include local performance targets for fraud.

27) As part of the developing work on police reform consideration should be given to the best way of enabling police forces to investigate Level 2 and Level 3 frauds that arise within their jurisdiction.

28) Chief Crown Prosecutors should ensure that each police fraud squad has access to specialist area fraud prosecutors from whom early pre-charge advice can be sought in those cases not being dealt with by the Fraud Prosecution Service.

29) As a minimum the existing capacity of fraud squads should be maintained and these resources should be ring fenced so far as possible.

30) Additional to fraud squad resources there should be appropriate capacity and capability to deal with Level 1 frauds that meet the agreed acceptance criteria and occurring at a local Borough Command Unit level.

31) A mechanism should be agreed to ensure that intelligence emanating from crime reports, recorded by the NFRC but not allocated to a strategic police force for investigation, should be readily available to forces.

32) Fraud squads should have available to them a forensic computer capacity sufficient to handle the amount of digital material commonly seized during serious fraud investigations. This capacity should be a uniform system across the regions.

33) One option for improving support to forces in tackling fraud would be to create a number of RSCs comprising specialist resources like surveillance and technical services. At present fraud squads are often regarded as a low priority call on these resources. This approach would need to be assessed for fit against the wider picture of police reform.

34) Such RSCs should be answerable to the relevant Chief Constables' Management Committees.

35) Each Regional Support Centre should have a Head of Profession who would task deployment of these resources and coordinate fraud investigations and anti-fraud police activity throughout the ACPO region.

36) Further study would be needed to determine the appropriate number of locations of such Regional Support Centres. One possibility would be to establish an RSC in each ACPO region in England and Wales outside London. This would imply eight centres.

37) Further study would also be necessary to determine the appropriate size of an RSC. The costs of a 37 person unit, comprising a Regional Coordinator and staff plus 20 detective constables and 12 civilians providing analytical and technical services, would be £2 million per year.

38) ACPO-ECP should commission further study to determine the appropriate size and number of locations of the Regional Support Centres.

39) A National Lead Force for fraud should be established with the following functions:

a) To create, develop and manage the National Fraud Reporting Centre and its analytical unit;

b) To disseminate intelligence and analysis to the network of Police Fraud Squads and, subject to appropriate protocols, other organizations investigating fraud (e.g. Serious Organized Crime Agency (SOCA)) to help them target fraud investigations and anti-fraud work generally;

c) To act as a Centre of Excellence for fraud investigations, including organized training, disseminating best practice, general fraud prevention advice, advising on complex enquiries in other regions, and assisting with or even directing the most complex of such investigations.

40) The National Lead Force should be based around the existing City Of London Police Fraud Squad. (This is without prejudice to the issue of whether that squad would remain part of a separate City force, as now or within a revised London police structure.)

41) These arrangements are to be the subject of a "thematic" inspection by Her Majesty's Inspectorate of Justice, Community Safety and Custody within two years of their establishment. The Chief Inspector of Constabulary has indicated support for this recommendation.

Civilianization of Investigations and Public/Private Partnerships (No legislation required)

(The following specific recommendations are an addition to, not a substitute for, the above recommendations for investigating fraud.)

42) The current exercise by the City of London Police to recruit and train civilian investigators should be monitored to see if it could be applied in other forces.

43) A similar approach should be piloted in another force to see if it would be suitable in a smaller fraud squad where the civilians would be a greater component of the anti-fraud effort of the force.

44) The current project by Surrey Police to deliver a mixed economy workforce to tackle volume crime investigations should be monitored to see if it could be applied to support police fraud investigations.

45) The NFSA when drawing up the first National Strategic plan should consider the scope for extending private / public partnership arrangements.

46) Further cooperation and collaboration over investigations between police, other public sector investigative bodies, and the private sector should be pursued as follows:

a) The police and public sector bodies, who regularly purchase external advice such as forensic accounting and computer analysis, should coordinate their procurement activity to obtain best value for money;

b) The NFSA should organize a more structured programme of secondments and exchanges between public and private sector investigative bodies;

c) Police forces should consider the scope for obtaining specialist support for fraud investigators by recruiting individuals with such expertise as special constables;

d) The NFSA should design a system for the nationwide accreditation of fraud investigators based on the certification of current training courses, identifying any gaps.

Chapter 8, Penalising Fraud (Some legislation required)

47) The range of non custodial sentences available to the Crown Court following conviction for a fraud offence, should be extended by adding:

a) Power to wind up companies and dissolve partnerships used in the fraud;

b) Power to award compensation to all victims of a fraud offences (whether their loss is the subject of a specific charge, offence tic or not);

c) Power to appoint a Receiver to recover property and distribute compensation awards;

d) Power to disqualify, prohibit or restrict an offender engaging in particular professional, or commercial activities;

e) Power to make orders dealing with consequential insolvency.

48) A Financial Court jurisdiction should be established in the High Court; to link the Crown Court with a division of the High Court. Such a jurisdiction would encompass fraud trials and related High Court matters throughout England and Wales. Any matter civil or criminal that arises out of an offence involving fraud should be dealt with and co-ordinated within the Financial Court jurisdiction and heard by the same judge; unless the interests of justice require otherwise.

49) Consideration should be given to running a pilot scheme to assess the precise costs/ benefits of a Financial Court jurisdiction.

50) Greater use should be made of the administrative and civil court options available to Regulators, as an alternative to criminal proceedings for appropriate fraud offences.

Chapter 9, Fraud Trials (No legislation required)

51) A national judicial co-ordinating mechanism for serious fraud cases should be set up to cover the following:

- The appointment of a panel of judges (see below Rec.52);
- Liaison between the Senior Presiding Judge, presiding judges and regional listing co-ordinators over the allocation of serious fraud cases;
- Promotion of a consistent and co-ordinated approach to the training of judges authorised to hear serious fraud cases;
- The exercising of a leadership role over fraud issues within the judiciary;
- Ensuring the appraisal and development of the skills of judges on the panel;
- Liaison with the Very High Cost Case Review Board;
- Oversight of the Financial Court pilot (Rec.49).

52) A panel of judges should be created from judges who have been identified by Presiding Judges and the above mechanism as having the relevant expertise to handle complex cases with a financial or commercial element. This recommendation does not envisage that panel judges would be confined only to fraud work; but they could form the cadre necessary for the establishment of a Financial Court (Recs.48 and 49).

53) Specialist training should be provided in skills identified as required to satisfy public confidence and the development needs of the judges. This must include dealing with disclosure issues and trial management according to the Lord Chief Justice's Protocol.

54) That there should be a study carried out on the effectiveness of the sanctions currently available to judges when faced with inefficiency or obstruction (including inadequate defence case statements both for trial management Protocol and CPIA disclosure purposes), with a view to consideration being given to increasing the powers available.

55) In appropriate cases the prosecuting authorities should have early access to the appointed trial judge any time post charge to argue in the presence of the defence that they be excused from actually examining a category of material where to do so would not constitute a reasonable line of inquiry in the absence of any indication of the issues in the case.

56) A working group consisting of practitioners, judges experienced in complex fraud and representatives of relevant government departments should be set up in 2008 to review the success of current improvements to the trial management and disclosure regimes and to consider whether necessary amendments to the Protocols or to the Criminal Procedure and Investigations Act (CPIA) ought to be considered or recommended.

57) A cost benefit analysis should be commissioned into Electronic Preparation and Presentation of Evidence to provide rigorous evidence of any savings in time and resources.

Chapter 10, Sentencing Fraud (Some legislation required)

58) The Sentencing Guidelines Council should urgently consider publishing specific guidelines for fraud offences covered under the Fraud Bill and associated legislation (see Annex F).

59) The Sentencing Guidelines Council should consider commissioning further research into an advisory matrix system in order to assist with a plea bargaining system. (See Rec.62)

60) The maximum sentence for fraud offences under the Theft Act 1968 and Companies Act 1986 (as amended) should be restored to 10 years. Consideration should be given to increasing to 14 years the maximum sentence for the most serious or repeated fraud offences. .

Chapter 11, Plea Bargaining, and other non-court option (some legislation required)

61) That a study be carried out into whether the introduction of the 'Goodyear' guidelines has had any effect on the rate of guilty pleas and their timeliness at the Crown Court.

We recommend that there be a formal plea bargaining system agreed in principle specifically for cases dealt with by the Serious Fraud Office, the Fraud Prosecution Service in the CPS and serious and complex fraud cases brought by other prosecuting authorities. The detail of the system, including the justifications for confining it (at least initially) to fraud cases should be set out in a legal framework to be devised by a working group comprising appropriately senior figures from the judiciary, prosecuting authorities, the criminal bar and criminal solicitors' association. The framework should cover the following:

- Provision for a suspect to be legally aided during pre charge negotiations;

- The prosecuting authority's option to provide a case statement to a suspect and his representative as to the nature of the case and his role in it at the pre-charge stage;

- The suspect's option to respond to that statement with a 'without prejudice' statement setting out the extent of his accepted criminality and then for both sides to engage in 'without prejudice' negotiation to see whether an early agreement as to criminality can be reached; this negotiation to include a recommended realistic sentence package, to include consideration of the extended sentencing options considered in chapter 8;

- Access to a specialised fraud judge at a pre charge stage to seek judicial approval of an agreed plea and sentence package or simply for the defence to seek an early sentence indication from the judge prior to further consideration (i.e. early sentence canvassing).

62) New guidelines on the conduct and acceptance of plea bargains by prosecutors should be issued by the Attorney General once a plea bargaining framework is in force, to offer specific guidance in this area.

How to respond

Do you have any comments or suggestions on specific Review recommendations, or groups of recommendations? If so, please supply these with reference to the recommendation numbers as in the report Chapter 14.

Please send your response by Friday 27th October 2006 to:

Jenny Rowe
Attorney General's Office
9 Buckingham Gate
London SW1E 6JP

Tel: 020 7271 2477
Fax: 020 7271 2433
Email: Fraudreview@attorneygeneral.gsi.gov.uk

Extra copies

Further paper copies of this consultation can be obtained from this address and it is also available on-line at www.attorney.general.gsi.gov.uk.

Publication of response

A paper summarising the responses to this consultation will be published in December 2006. The response paper will be available on-line at www.attorneygeneral.gsi.gov.uk.

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot given an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will, of itself, be regarded as binding.

We will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

The Consultation Criteria

The six consultation criteria are as follows:

1. Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.

2. Be clear about what your proposals are, who may be affected, what questions are being asked and the time scale for responses.

3. Ensure that your consultation is clear, concise and widely accessible.

4. Give feedback regarding the responses received and how the consultation process influenced the policy.

5. Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.

6. Ensure your consultation follows better regulation best practice, including carrying out a Regulatory Impact Assessment if appropriate.

These criteria must be reproduced within all consultation documents.

ANNEXES

ANNEX A Table 1. Research Methodologies used to Measure Fraud.		
ORGANISATION	**METHODOLOGIES USED TO CALCULATE FRAUD LOSSES**	**FIGURES**
APACS – The UK Payments Association	As at the last calendar day of the month, card issuers are required to provide details of transactions identified as fraudulent during the reporting month irrespective of when the transaction may have occurred. Each report is divided in to three main sections: 1) Product details (card type, scheme, turnover); 2) Value and volume of fraud transactions by circumstance of loss / compromise (how the fraudster was able to obtain card or card details); 3) Value and volume of fraud transactions by place of misuse (where the fraudster used the card or card details). Sections 2 & 3 are the same data aggregated different ways; both cuts of data should be reported on both a gross and net basis. These data form the basis of APACS monthly analysis and industry reporting. Twice yearly these data are made available publicly (mid-year and year-end) via media/press/APACS publications – all published data are gross, net losses are not made available. All fraud figures are confirmed losses and so real losses will be higher as some will go undetected[208].	Plastic card fraud[209] totalled £439.4m broken-down as: counterfeit (£96.8m); stolen or lost cards (£89m); card holder/card not present fraud (£183.2m); mail non-receipt fraud (£40m); card ID theft (£30.5m).
APACS – The UK Payments Association	The only released figures for non-plastic fraud are those for cheque fraud. APACS are still piloting methodologies for other areas of unsecured lending and other transfer payments i.e. CHAPS and SWIFT. They are also looking to complete some work on attempted fraud.	Non-plastic fraud: Cheque fraud losses fell from £46.2m in 2004 to £40.3m in 2005 (a 13% drop).
Association British Insurers (ABI)	"Quantifying the problem with any accuracy is difficult."[210] ABI estimates the total amount of fraud suffered by insurers on general personal lines business alone is over £1 billion per annum. By far the largest elements of this are personal lines motor and household. ABI estimate that around 10% of the total value of personal lines motor and 15% of the total value of household claims are fraudulent. By value, they estimate that there is slightly more opportunistic fraud than premeditated.	Last figures available are from 1999 annual report = £650m.

	Typically, there will be a large volume of small value opportunistic frauds and a relatively small volume of high value premeditated fraud. Included in this figure are proven frauds but also those evidenced by reductions in or withdrawals of claims once the insurer asked some searching questions. While such cases might not yield enough evidence to satisfy a court of law that a crime had been committed, where fraud specialists are confident that they do represent deliberately dishonest attempts against them, they are defined as fraud. It is this total measure of dishonesty that ABI attempts to capture in its fraud estimate.	
British Retail Consortium (BRC)	British Retail Consortium's 'Retail Crime Survey' sample is made up of 13,360 outlets in the UK. The respondents account for 42% in total UK retail sales. Screening methods are employed to ensure that there are no double returns. The figures from this are extrapolated out for the retail sector.	£68.1m Fraud: Cheque (£17m); Card (£14.1m); Application (£1.4m); Cardholder not present (£14m); Counterfeit cash (£8.2m) Other (£13.4m).[211]
The Commercial Insurance Fraud Syndicate[212] Group (MORI)	Commercial insurance fraud is an extremely serious issue for the insurance sector and the UK economy. However, it is an under-researched area and little is known about the extent or character of the problem. Until now, the insurance industry has focused on personal lines insurance fraud. To plug this gap, the syndicate asked MORI to carry out an investigation using both qualitative and quantitative research methods. The survey was combined with insurer's claims data to reveal a figure. Between March and May, MORI conducted research in two areas. First a business survey among individuals responsible for arranging and administering commercial insurance within their organisation (1,102 telephone interviews). Quotas on size of company and industry sector were used to ensure sub-samples could be examined with a reasonable degree of statistical certainty. Second an employee survey among company employees covered by their employer's commercial insurance policies	£550m[213] representing 5% of commercial insurance premiums (2005). The figure is made up of fraudulent claims by businesses against employers and claims against businesses by employees paid by

	(323 face to face interviews). Quotas were specified by company size and industry sector amongst three groups of employees: manual employees working in 'blue collar' jobs; office based workers in 'white collar' jobs and company vehicle drivers.	the employers insurance.
Telecommunications UK Fraud Forum (TUFF)	The figure of 2.4% of annual turnover has been arrived at through completion of a number of surveys. These surveys have established that losses to fraud within telecoms range from 3% to 15% with the upper limits more likely to be associated with new start ups. For example Azure[214] reported in November 2005 that global telecoms operators are losing an estimated 11.6 per cent of turnover ($170 billion) through fraud and other types of revenue leakage in 2005 compared to 10.7 per cent in 2004. This is one of the main findings of research Azure has conducted in conjunction with telecoms analysts. Therefore, this total is an informed estimate.	£866m this is 2.4% of annual turnover of total retail revenue for 2004.[215]
KPMG Fraud Barometer	Published every year since 1990, the KPMG Fraud Barometer considers major fraud cases being heard within the UK in excess of £100,000 in the Crown Court. They examine cases in relation to banking/financial, Government, commercial, investor and 'other sectors'. The methodology does not aim to give an overall picture of fraud in the UK economy but to act and as an indictor of fraud activity. 2005 saw the second highest recording since the Fraud Barometer began and concluded that the majority of fraud is committed in London and the South East.	£942m (2005). This figure is the total amount at stake in 222 cases heard in 2005. Of these cases £447 was for fraud against the Government who remain the main victim of fraud[216].
Mishcon de Reya[217]	Mishcon de Reya commissioned The Survey Shop to undertake a survey consisting of two phases. The objective of the first phase was to identify directors and managers with responsibility for managing internal and external investigations within the legal, finance and HR departments of FTSE 350 companies. This was achieved through telephone interviews. The second phase comprised a letter of invitation to	£72bn (2004/05)

	assist with the research followed by a telephone interview. Fifty-three interviews were conducted during the first quarter of 2005. Aside from the research which focused on the relationship between corporations and fraud investigators, Mishcon stated that the UK could be loosing £72bn to fraud every year. This figure was deduced from taking a figure released by the US Association of Certified Fraud Examiners (ACFE) which estimated that companies lose 6%, 'put in terms of the UK's GDP, that is equivalent to undetected and unreported fraud costing businesses over £72 billion every year'.	
Norwich Union	Norwich Union report entitled 'The Fraud Report - shedding light on hidden crime' completed a review of existing surveys and research on fraud to come up with an estimated figure for 2004. This methodology was very similar to that used for the NERA study (above).	£16bn (2004)
PUBLIC SECTOR		
British Broadcasting Corporation (BBC)	The BBC cross match the database they have of 28 million homes with the data on the count of number of households from ODPM[218], this is then crossed with data from BARB on the TV penetration rate (approx 98%)[219]. This system is considered by the NAO to be statistically valid and robust.[220]	5.7% of licence fee total is estimated to be evasion. This is equal to £159,486,000[221]. This figure was reduced to 5% in March 2005 as BARB's estimate of the number of households with TVs was reduced[222].
Department for Work and Pensions (DWP)	The DWP estimates fraud and error based on a mixture of in-depth rolling programmes that re-perform a large sample of benefits awards each year, and snapshots of fraud and error on other benefits which are up to six years old.	"Best estimate of fraud in the benefit system now stands

	Results are derived from the analysis of samples; therefore, the methodology is subject to statistical uncertainties. Because of uncertainties in measuring fraud and error, figures are rounded to the nearest £100 million. These uncertainties have been quantified and are presented in the results at 95%[223] confidence intervals.	at £0.9bn and at 0.8 per cent of benefit expenditure."[224] Internal Fraud is recorded in the Resource Accounts 2004/05 as being £11,789.
Driver and Vehicle Licensing Agency (DVLA)	Estimates of Vehicle Excise Duty (VED) evasion are derived from periodic roadside surveys. Contractors record the number plates of vehicles using public roads at 256 sites throughout the UK during a given period. DVLA database used to estimate number of unlicensed vehicles to each area. To ensure a statistically valid estimate of the national evasion rate, the data analyses is weighted for traffic volumes in different areas and adjusted to compensate, for example, for the likelihood of repeat sightings of individual vehicles.	An evasion level of 4.5% equates to a gross loss of VED revenue of £129m for 2004/05. [225]
Foreign and Commonwealth Office	One of the key problems faced by the FCO in identifying and tackling fraud is the wide geographical spread of the organisation. They therefore rely heavily on information received from others - primarily from management teams overseas. Many of the frauds they investigate are discovered by staff overseas either by the effective operation of standard control procedures or by questioning practices that appear unusual. For example, a large fraud uncovered in one of their Middle East posts was exposed as a result of the Deputy Head of Post questioning the amount and method of paying for airport clearance charges. Further checks confirmed that the receipts submitted for these costs were fraudulent. They have a publicised whistle blowing policy and receive a number of reports of fraud from whistleblowers. The unit carries out a number of pro-active visits to overseas posts every year. Their target is to carry out 15 pro-active visits this financial year. The most common type of fraud discovered by this means is	£646,000 in 2005/06 of which £625,500 was external. This represents 0.041% of outturn. 8% (£52,000) of this was recovered.

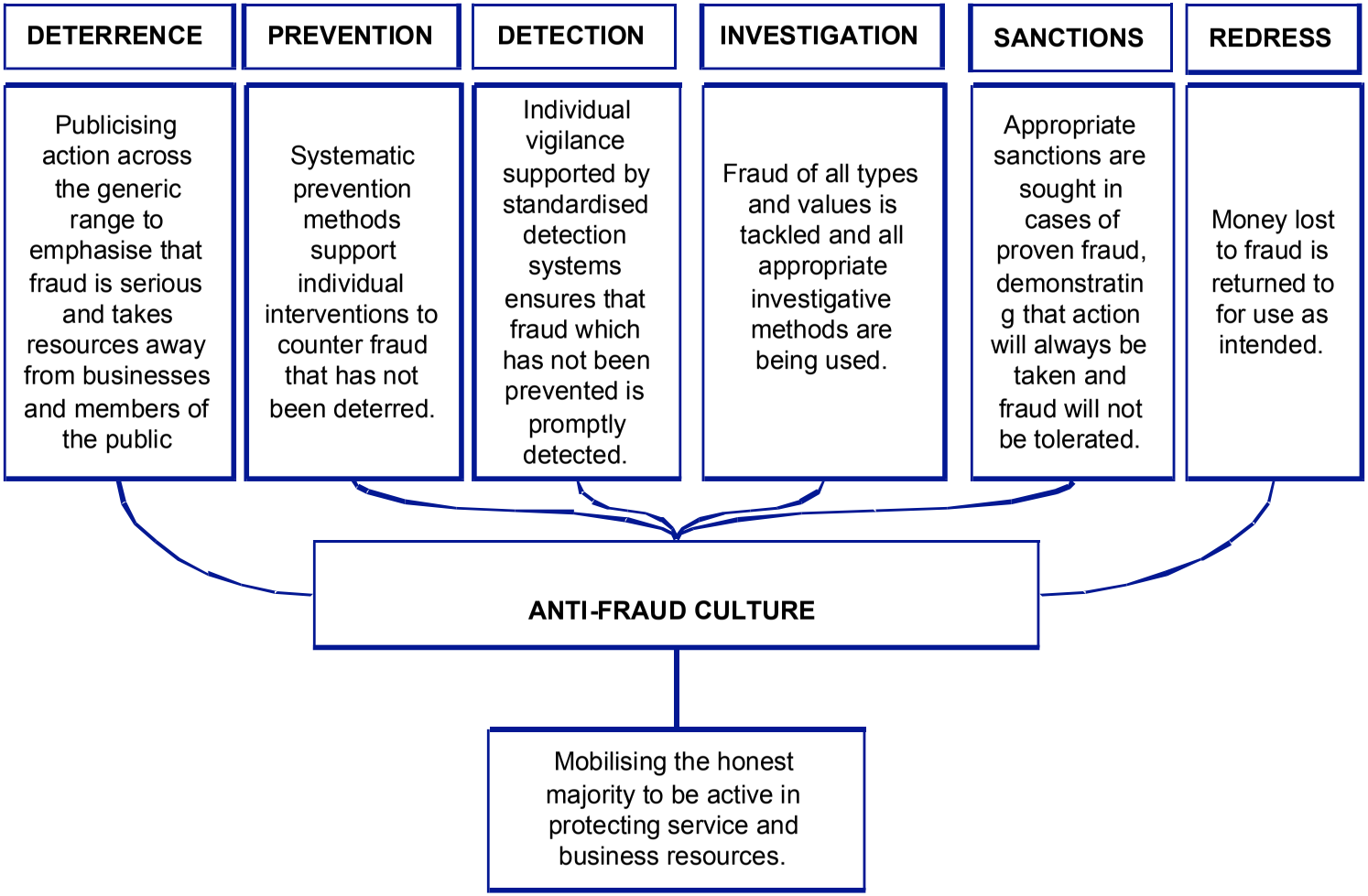
	procurement fraud where staff have submitted false and inflated receipts. The FCO Fraud Unit staff are Accredited Counter Fraud Specialists.	
Her Majesty's Revenue and Customs (HMRC)	There are no reliable estimates available of the total tax loss through non-compliance for the UK. There are fundamental differences between the way tax gaps can be estimated for direct and indirect taxes. For indirect taxes, such as VAT and Excise duties taxes, it is possible to carry out a top down gap analysis by comparing actual tax receipts against a theoretical expected tax yield calculated from externally available statistics on consumption. Such an approach is not possible with direct taxes because of the lack of reliable and independent data sources for income. This means that there is no one technique for producing a useable measure of the tax gap for direct taxes. It is important to note that the estimates of losses for excise duties have wide confidence intervals arising from the level of uncertainty in the survey data used to estimate consumption. For direct taxes HMRC have concentrated their efforts on improving their understanding of why and where tax non-compliance occurs through the use of programmes of enquiries on random samples of tax returns. A recent NAO study [226]reported the results of the Random Enquiry programme for returns sent to individuals for tax year 2000/01. This exercise produced an estimate of around £2.8bn tax at risk from inaccurate returns. However this figure underestimates the true extent of tax at risk in this population as not all enquiries will identify all non-disclosed income. The department is considering whether to update the figure to account for non-discovered non-compliance. It is important to note that the figure quoted in this NAO study does not represent an estimate of fraud for direct taxes. On the one hand it only covers one group of taxpayers. On the other hand the estimate includes all types of non-compliance – not just fraud.	Latest estimates of Indirect Tax Losses are described in detail in the document "Measuring Indirect Tax Losses – 2005" which is published on the HMRC website. This shows losses of VAT (£11.3bn for 2004/05); Excise duty on spirits (£250m for 2003/04); Excise duty on tobacco (£2.9bn for 2003/04); Excise duty on oils (£600m for 2004). It should be noted that the figure for VAT includes a variety of types of non-compliance other than fraud. The "top down" gap methodology used

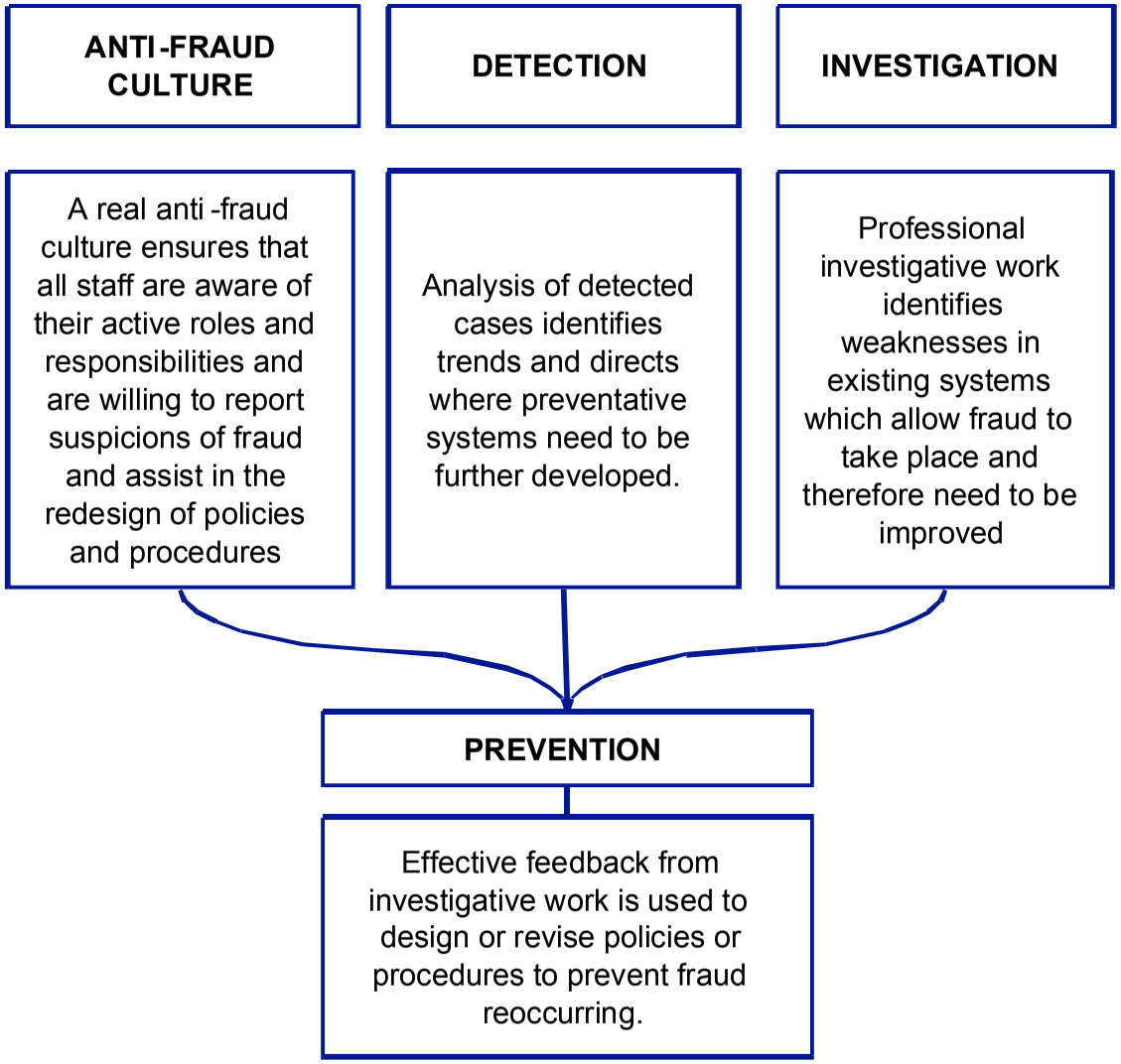
		does not allow for separate estimates by type of non-compliance. However a separate estimate of the extent of MTIC fraud (often referred to as carousel fraud) is shown of £1.1 to £1.9bn for 2004/05.
HM Treasury	HM Treasury collect data annually from central government departments and their executive agencies to produce the 'Annual Fraud Report'. The 2004/5 report contains an analysis of returns received from 38 Government Departments, 30 Agencies and 93 sponsored bodies (NDPB's mainly). The returns include data on theft, false accounting, bribery and corruption, deception and collusion. HMT website states this 'is an analysis of fraud perpetrated by staff within departments and their executive agencies'. The report does not aim to give an overall picture of fraud within government departments, it aims to inform departments of the scale and nature of certain categories of fraud which have been reported to the Treasury for the reporting year 2004-2005. This information is provided to help departments learn from the experiences of others when reviewing and developing their own control systems. The Report also aims to increase awareness of the risk of fraud and, in some areas, to suggest ways in which the risk can be managed and reduced.	£3,136,900 (2004/05 returns).
Ministry of Defence (MoD)	In 1999 the MoD set up the DFAU (Defence Fraud Analysis Unit). The DFAU takes a proactive response to the risk of fraud based on an awareness training programme. The theme of the programme is "something wrong tell us". This has encouraged whistleblowers to report suspicious activity. It used to be the case that over 90% of cases were reported by line management. Now approximately 55% of cases are reported by whistleblowers and 45% by line management or police.	Current figures not yet available.

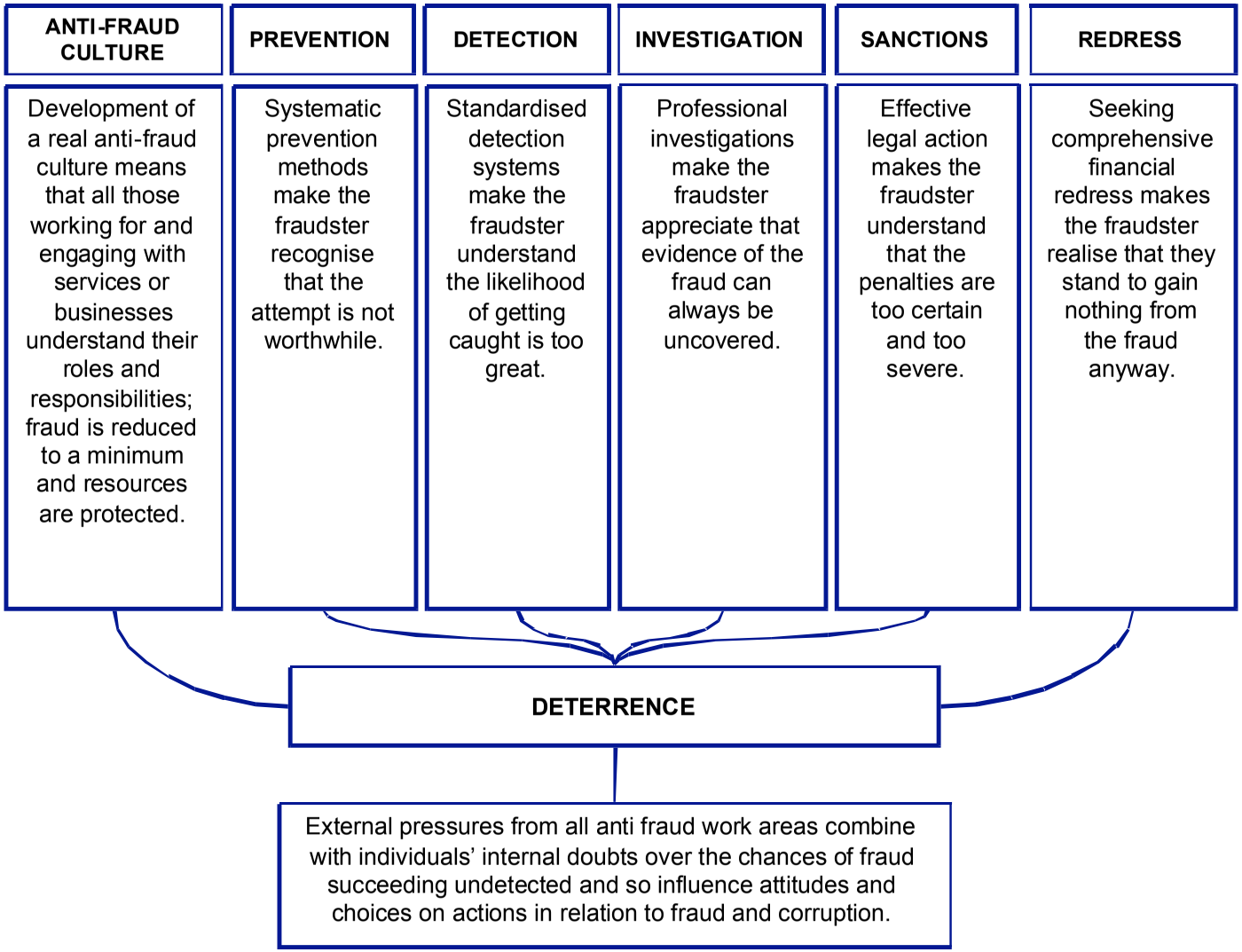
	However, the number reported by line management has been fairly consistent, thus actual reports have increased. The vast majority of the cases that make up this figure relate to theft and it is not clear whether this is made up of deception offences or misappropriation. The figure is includes fraudulent travel and subsistence claims, procurement, pay related issues, exploitation of assets, personnel management, and theft.	
National Health Service (NHS)	The NHS Counter Fraud Service (CFS) carries out Risk Measurement Exercises (RME) in line with its methodology:[227] The Risk Measurement Unit (RMU) chooses an area of spend with known losses. It then takes statistically valid samples of data (cleansed) from that area of spend. This is achieved by validating the data on a case by cases basis - decisions are made based on a civil definition[228]as to whether a fraud has occurred. This data is then analysed and extrapolated for the population as a whole and then statistically validated to a +/-1% figure. The NHS spends £22.2m[229] on countering fraud this is 0.028% of expenditure.[230] As each area of spend is measured separately there is no overall estimate of losses – this is because there is no point in estimating. By 2008 the NHS will have figures for overall losses contained in 75% of NHS spend. This will be the result of previous, current and planned exercises.	- Figures for all RME to date are: pharmaceutical patient fraud (£47m); dental patient fraud (£21.1m); optical patient fraud (£10.17m).[231] - Current exercises: 3rd optical patient fraud (end May 2006); health tourism pilot exercise (end April 2006); Payroll (end December 2006). - Planned: Health tourism exercise in secondary care (start April 2006); GMC Qualifications exercise (start June 2006); procurement of goods and services (start July

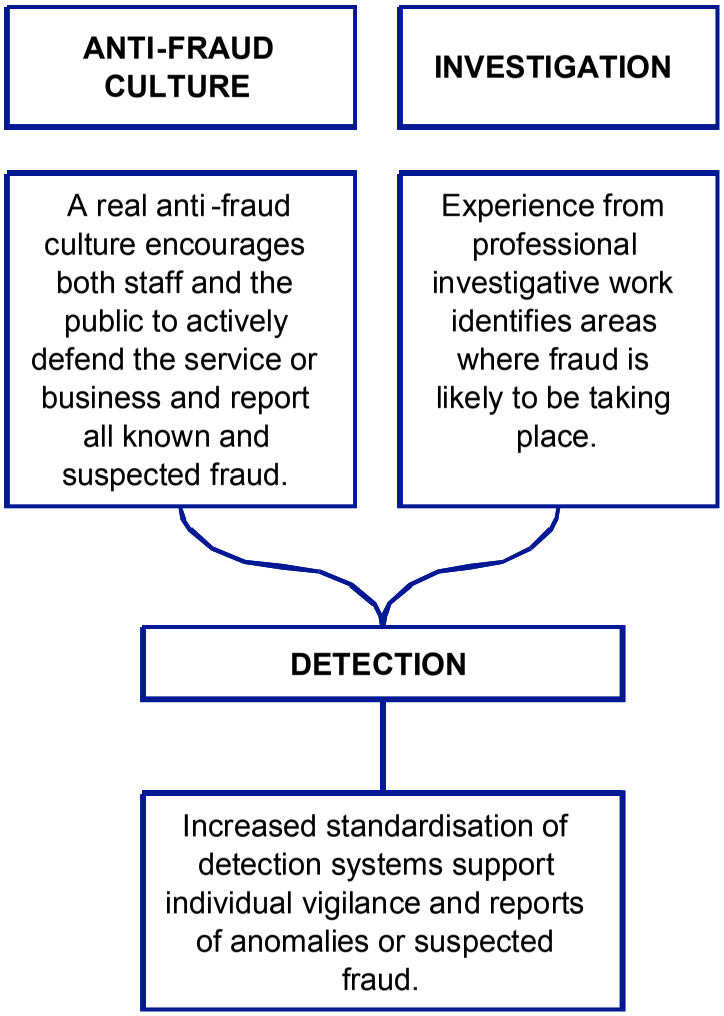
		2006); procurement of drugs (start 2007).
National Economic Research Associates (NERA) Report	The NERA report[232] produced in March 2000 is considered to be the most notable research in this area and the study provides the most widely quoted figure for the cost of fraud. NERA complied data from official, private institutional and reported survey work from private bodies as well as data on the criminal justice costs associated with fraud. The estimated costs were given as a range of lowest and highest figures. A range of definitions of fraud were used to compile the NERA report – they were based on the definitions of fraud used by those who prepared the original statistics reviewed by the NERA team.	£6.7bn - £13.8bn (low and high estimates) March 2000.

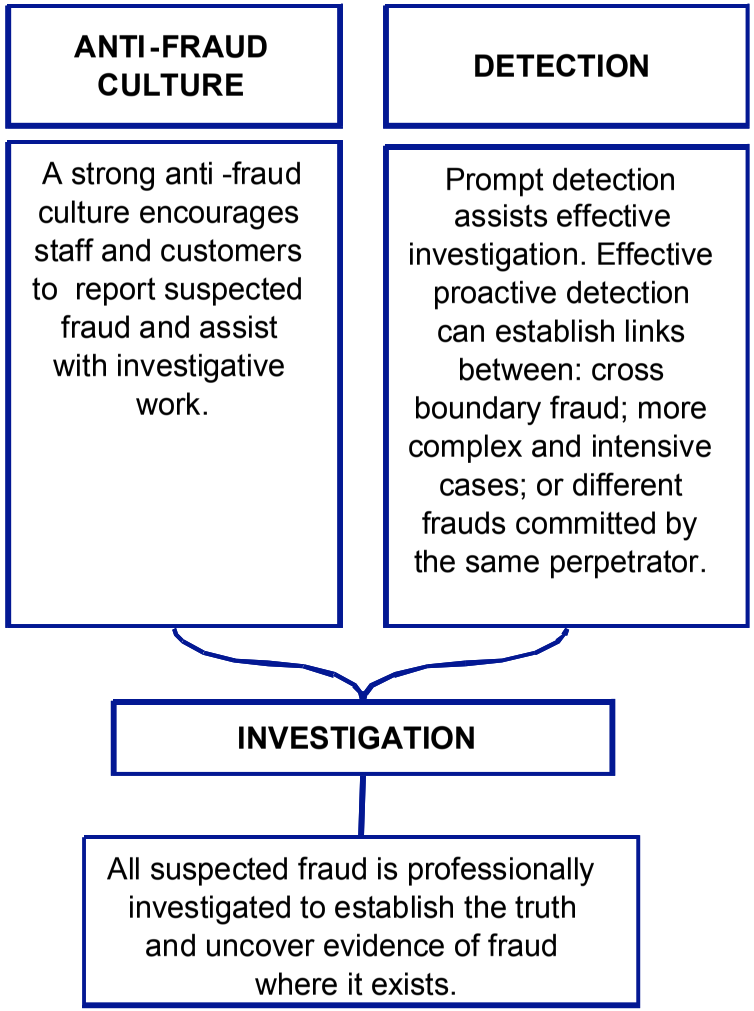
ANNEX B

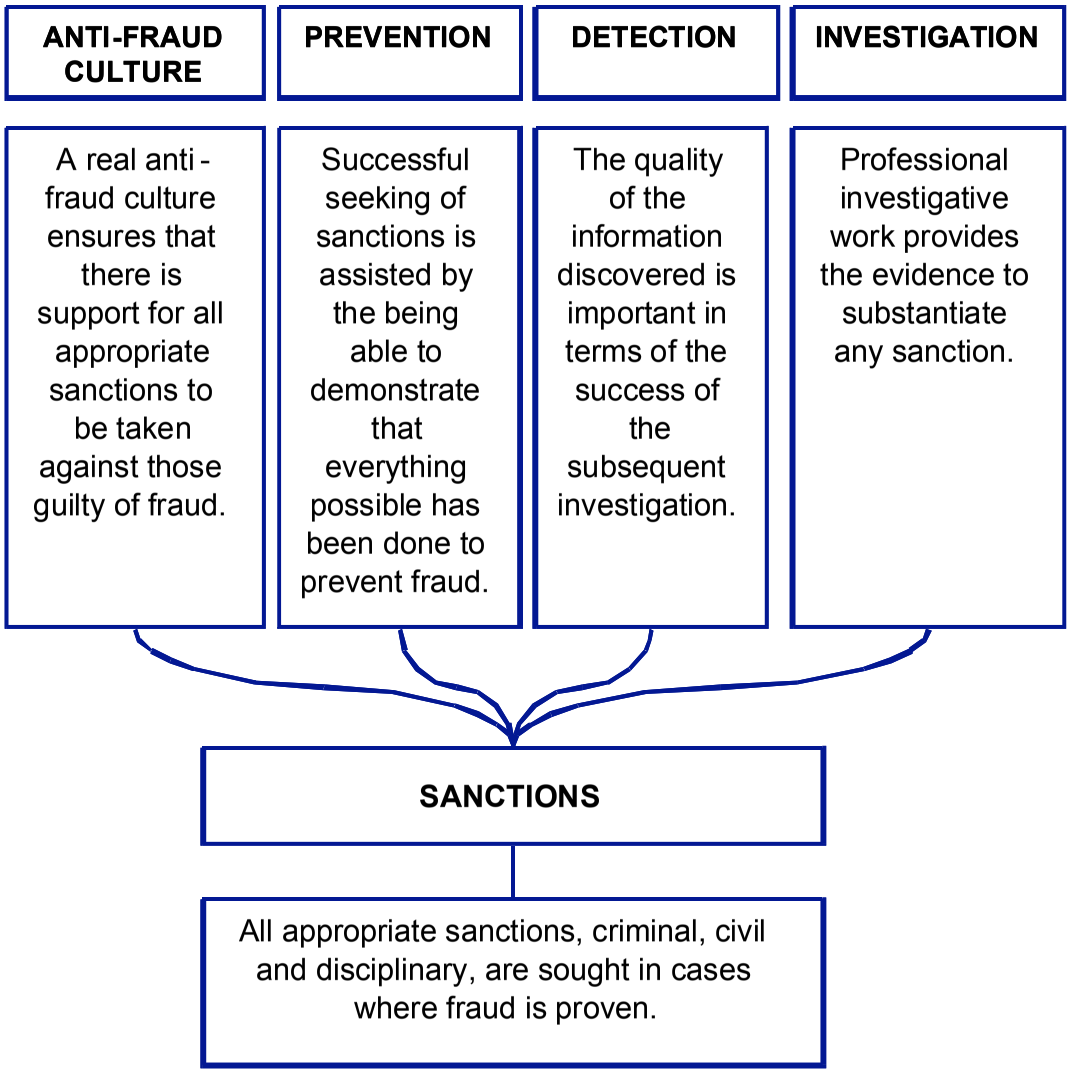

DETERRENCE
PREVENTION
DETECTION
INVESTIGATION
SANCTIONS
REDRESS
Publicising action across the generic range to emphasise that fraud is serious and takes resources away from businesses and members of the public
Systematic prevention methods support individual interventions to counter fraud that has not been deterred.
Individual vigilance supported by standardised detection systems ensures that fraud which has not been prevented is promptly detected.
Fraud of all types and values is tackled and all appropriate investigative methods are being used.
Appropriate sanctions are sought in cases of proven fraud, demonstrating that action will always be taken and fraud will not be tolerated.
Money lost to fraud is returned to for use as intended.
ANTI-FRAUD CULTURE
Mobilising the honest majority to be active in protecting service and business resources.

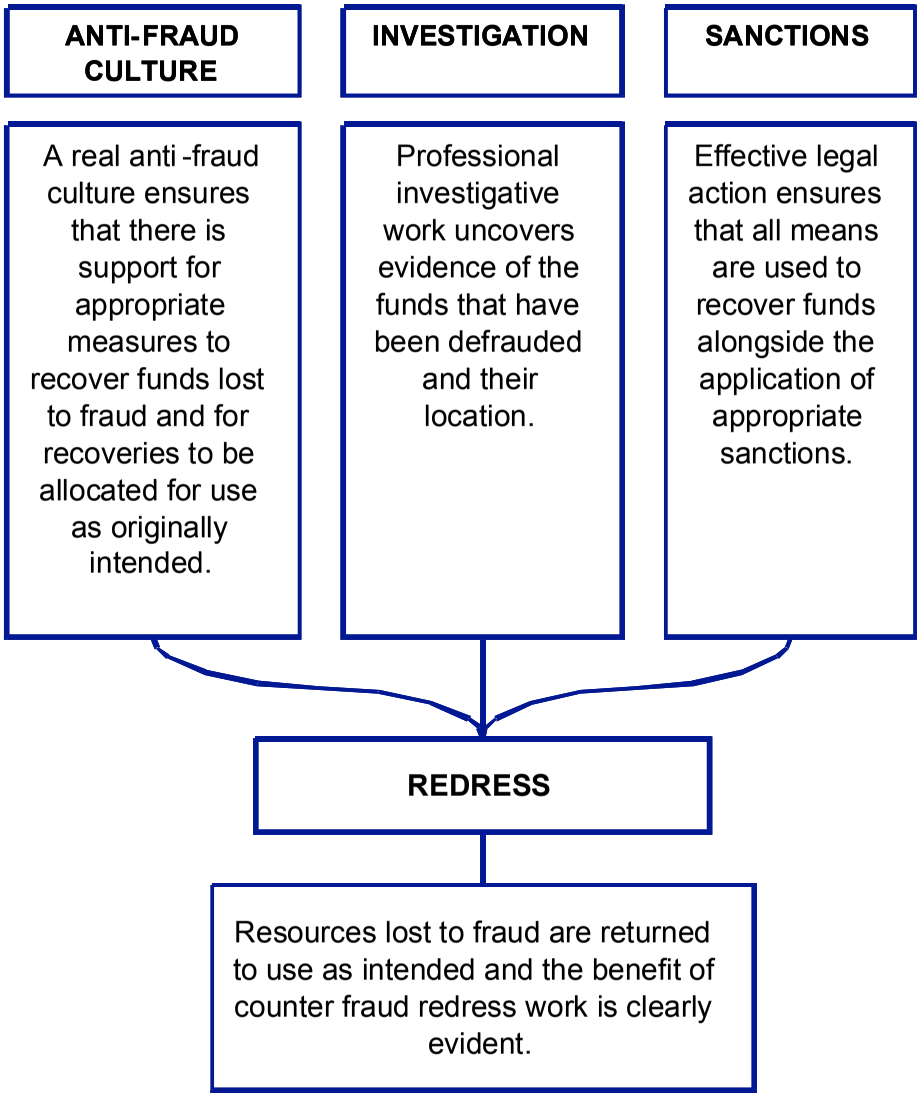

ANTI-FRAUD CULTURE
DETECTION
INVESTIGATION
A real anti-fraud culture ensures that all staff are aware of their active roles and responsibilities and are willing to report suspicions of fraud and assist in the redesign of policies and procedures
Analysis of detected cases identifies trends and directs where preventative systems need to be further developed.
Professional investigative work identifies weaknesses in existing systems which allow fraud to take place and therefore need to be improved
PREVENTION
Effective feedback from investigative work is used to design or revise policies or procedures to prevent fraud reoccurring.


ANTI-FRAUD CULTURE
Development of a real anti-fraud culture means that all those working for and engaging with services or businesses understand their roles and responsibilities; fraud is reduced to a minimum and resources are protected.
PREVENTION
Systematic prevention methods make the fraudster recognise that the attempt is not worthwhile.
DETECTION
Standardised detection systems make the fraudster understand the likelihood of getting caught is too great.
INVESTIGATION
Professional investigations make the fraudster appreciate that evidence of the fraud can always be uncovered.
SANCTIONS
Effective legal action makes the fraudster understand that the penalties are too certain and too severe.
REDRESS
Seeking comprehensive financial redress makes the fraudster realise that they stand to gain nothing from the fraud anyway.
DETERRENCE
External pressures from all anti fraud work areas combine with individuals' internal doubts over the chances of fraud succeeding undetected and so influence attitudes and choices on actions in relation to fraud and corruption.


ANTI-FRAUD CULTURE
INVESTIGATION
A real anti-fraud culture encourages both staff and the public to actively defend the service or business and report all known and suspected fraud.
Experience from professional investigative work identifies areas where fraud is likely to be taking place.
DETECTION
Increased standardisation of detection systems support individual vigilance and reports of anomalies or suspected fraud.


ANTI-FRAUD CULTURE
DETECTION
A strong anti -fraud culture encourages staff and customers to report suspected fraud and assist with investigative work.
Prompt detection assists effective investigation. Effective proactive detection can establish links between: cross boundary fraud; more complex and intensive cases; or different frauds committed by the same perpetrator.
INVESTIGATION
All suspected fraud is professionally investigated to establish the truth and uncover evidence of fraud where it exists.


ANTI-FRAUD CULTURE
PREVENTION
DETECTION
INVESTIGATION
A real anti-fraud culture ensures that there is support for all appropriate sanctions to be taken against those guilty of fraud.
Successful seeking of sanctions is assisted by the being able to demonstrate that everything possible has been done to prevent fraud.
The quality of the information discovered is important in terms of the success of the subsequent investigation.
Professional investigative work provides the evidence to substantiate any sanction.
SANCTIONS
All appropriate sanctions, criminal, civil and disciplinary, are sought in cases where fraud is proven.


ANTI-FRAUD CULTURE
INVESTIGATION
SANCTIONS
A real anti-fraud culture ensures that there is support for appropriate measures to recover funds lost to fraud and for recoveries to be allocated for use as originally intended.
Professional investigative work uncovers evidence of the funds that have been defrauded and their location.
Effective legal action ensures that all means are used to recover funds alongside the application of appropriate sanctions.
REDRESS
Resources lost to fraud are returned to use as intended and the benefit of counter fraud redress work is clearly evident.

ANNEX C

Fraud Review Questionnaire (Sent to Public Authorities)

Name of Organisation:	
Type of Organisation (please select from drop-down list)**:**	

Contact Details

Name:		**Telephone No:**	
e-Mail:			

1.	**Internal Fraud** Has your organisation assessed the threat of internal fraud (please select from drop-down list)?	
	Do you consider the risk of internal fraud to be High, Medium or Low please select from drop-down list)?	
	How vulnerable is your organisation to the risk of internal fraud (please record the amount at risk)?	
	How many cases of internal fraud were reported?	
	How many cases of internal fraud were investigated?	
	What was the estimated value of internal fraud?	
	How many cases resulted in prosecutions?	
	What targets, if any, were set by your organisation to reduce internal fraud?	
2.	**External Fraud** Has your organisation assessed the threat of external fraud (please select from drop-down menu)?	
	Do you consider the risk of external fraud to be High, Medium or Low (please select from drop-down menu)?	
	How vulnerable is your organisation to the risk of external fraud (please record the amount at risk)?	
	How many cases of external fraud were reported?	
	How many cases of external fraud were investigated?	
	What was the estimated value of external fraud?	
	How many cases resulted in prosecutions?	

	What targets, if any, were set by your organisation to reduce external fraud?	
3.	What was the total budget for your organisation in 2005-06?	
4.	What was the total budget for anti-fraud activities in 2005-06?	
5.	How much staff time was spent investigating fraud in 2005-06?	
6.	Please describe the methodologies used to evaluate losses to the department in individual cases.	
7.	Please describe any new or altered fraud risk management processes that were implemented or any new anti-fraud initiatives taken in the last 3 years??	

ANNEX D

FRAUD REVIEW TEAM
RESULTS OF VICTIMS SURVEY

April 2006

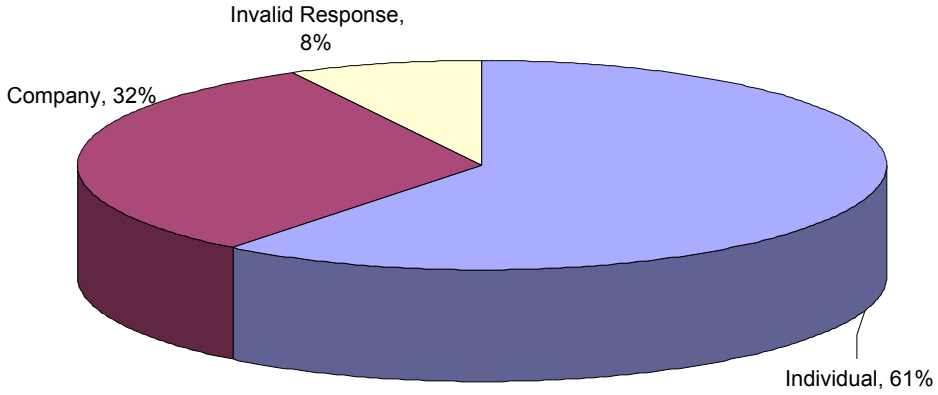
Summary

A survey of 150 randomly chosen corporate and individual victims of fraud reported to the City of London Police and Metropolitan Police was undertaken to identify the priorities among victims of the outcomes of fraud investigations, and the impact that the crimes have had upon the victims.

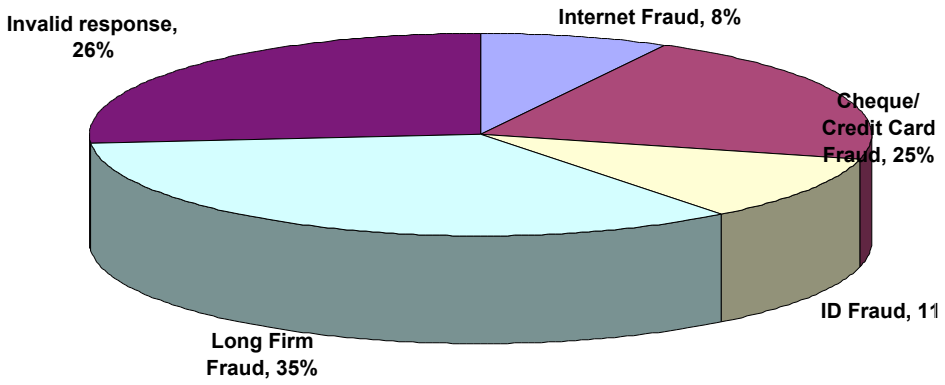
25% of survey participants responded.

---

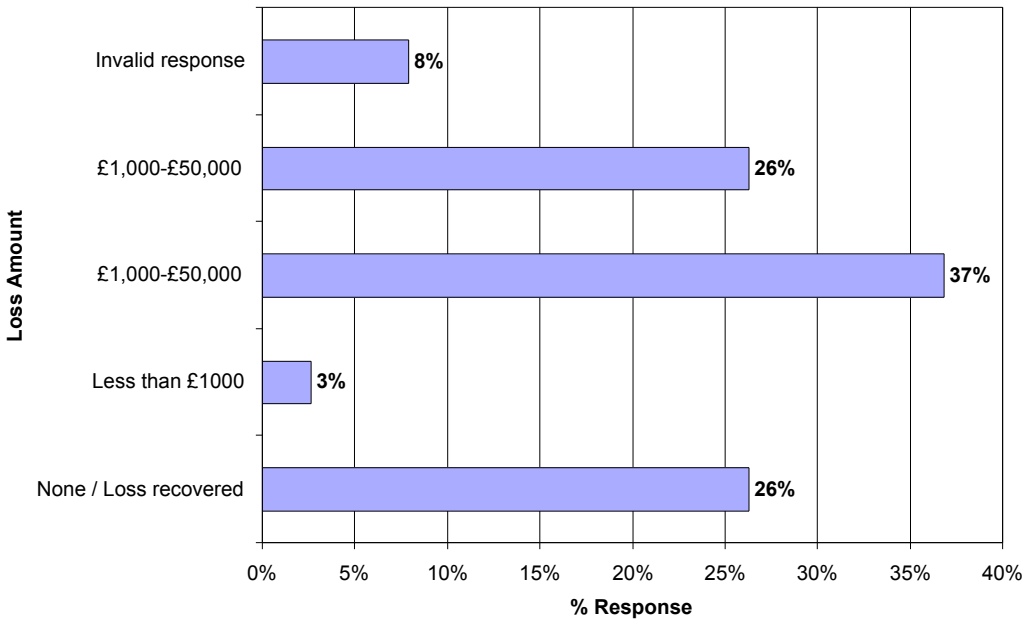
1. **Are you an individual victim of fraud or a member of a company that was the victim of fraud? (If the latter please give your position in the company)**



2. **What was the nature of the fraud carried out against you or your company?**



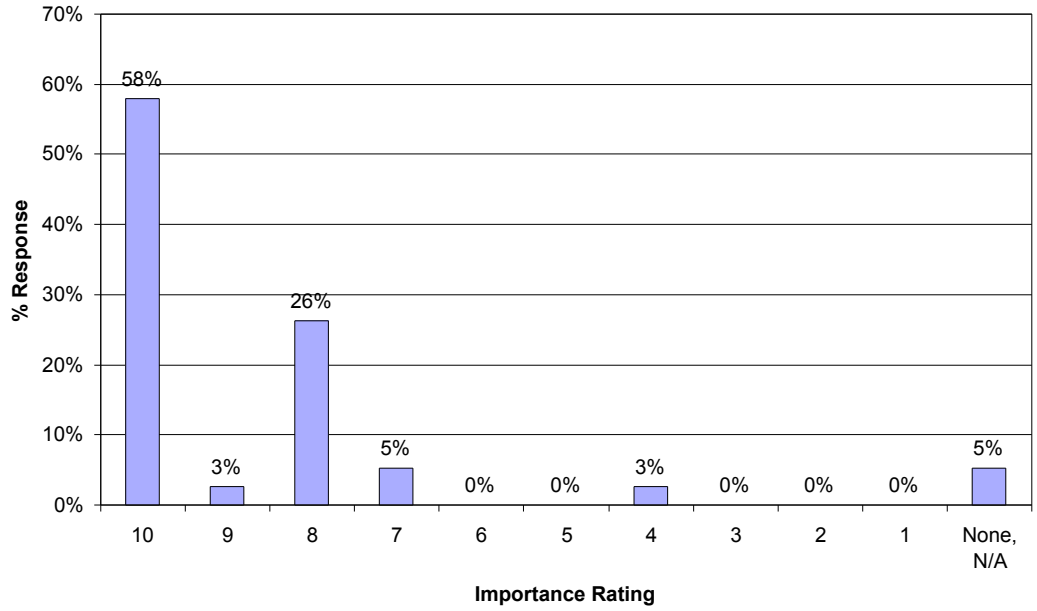
3. **Roughly what was the financial loss (if any) to you personally or your company?**



4. On a scale of 1 (not important) to 10 (very important), and adding any comments, how important to you were the following outcomes:

10 = Very Important **1 = Not Important**

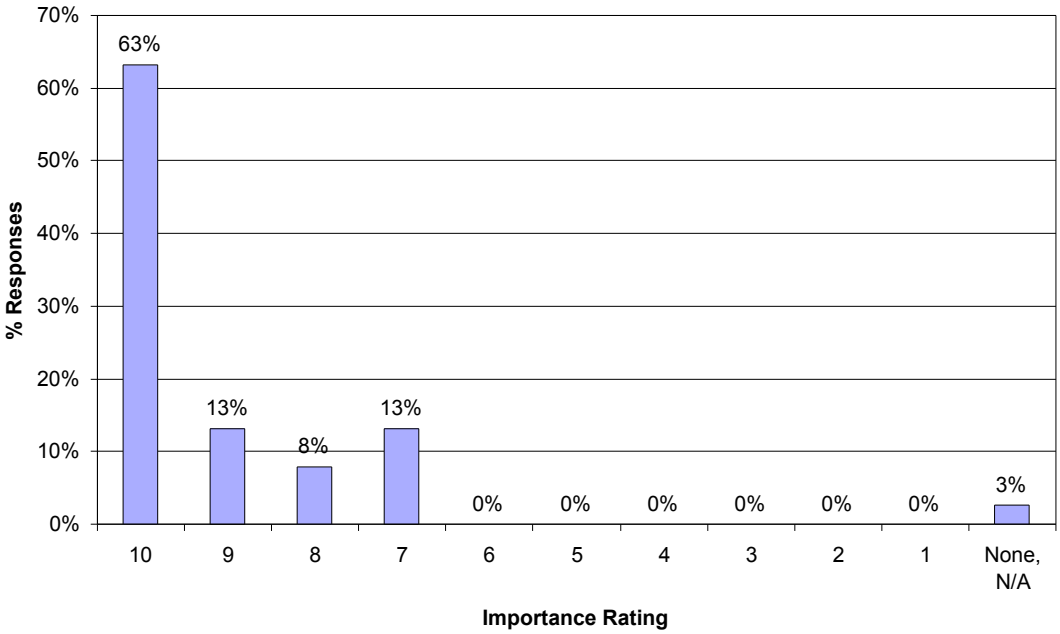
- **The punishment of the offender?**



Comments

- I wished the perpetrator to be punished as a way of showing him that he was not as clever as he thought.
- Most important aspects – offender must realise crime does not pay.
- If the attempt had been successful the subsequent loss could have been catastrophic.
- Regrettably the offender will probably only serve half of his sentence but his investors got nothing back.
- If there is no punishment there would be no justice.
- For someone to have taken my money in good faith and then seen to be enjoying trips to the US or driving a brand new Mercedes, in retrospect, I feel that the suffering incurred should have seen [the offender] incarcerated for a number of years and he should have some community service in the [form of] justice to pay off outstanding money owed.
- Punishment should also include financial penalties in excess of the cost to the victims.

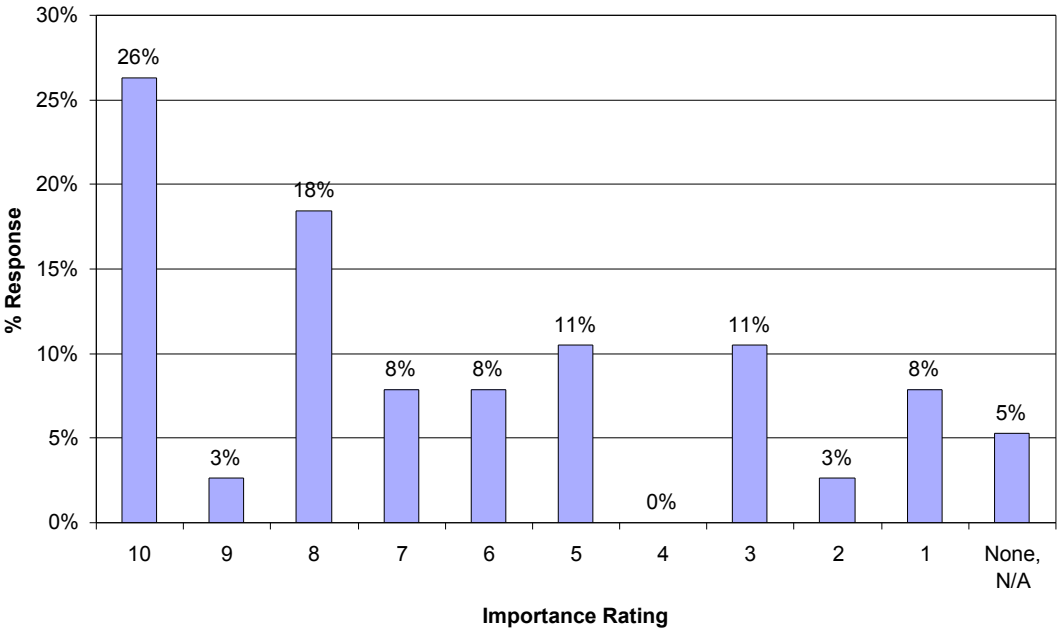
- **The protection of the public?**



Comments

- Many of the public should do more to protect themselves.
- The public should be made aware of these confidence tricksters (thieves) even if it is after the event.
- Becoming a victim of fraud is not a pleasant experience. Its stress affects people in different ways.
- ..Surely a monitoring systems should be employed to ensure that people who advertised in such a newspaper be qualified.
- I am glad he can't do the same to anyone else.
- Information should be readily available to the public. Whilst current information is available it is very difficult to understand and also the number of sources of this information.
- Fraud is often seen as a victimless crime when in reality we are all paying for it through increased charges/prices/interest etc.
- Tax payer's money is being wasted. It is important that public funds are protected (in regards to benefit fraud).

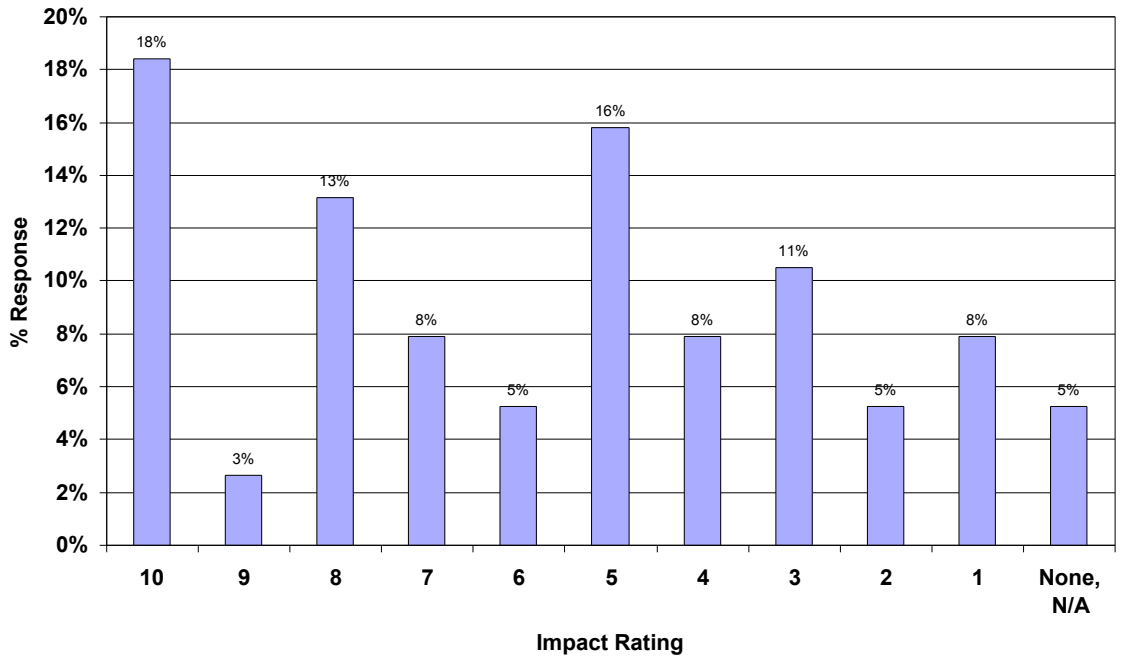
- **The reform and rehabilitation of the offender?**



Comments

- [The offender] has the money stashed away and when he has finished his prison sentence will be free to live without being made to repay.
- Sentences should be severe enough to make the offender want to reform and to rehabilitate.
- I do not think that the current systems of 'reform and rehabilitation' of such offenders is very effective at all. Monitoring systems such as tagging and Drug Treatment Orders are not rigorously followed because they must be seen to be successful for political ends. In reality they achieve little.
- This does not always guarantee a positive outcome.
- Criminal should refund financial loss as part of rehabilitation.
- I am positive that this should not occur again and that [the offender] should swear an oath to this effect and be checked on a regular basis as to his future work.
- Rehabilitation does not appear to be very successful - once a criminal always a criminal!
- As far as I am concerned – anyone who could commit such a crime cannot be reformed.
- The fraudster does not completely reform himself until he dies.

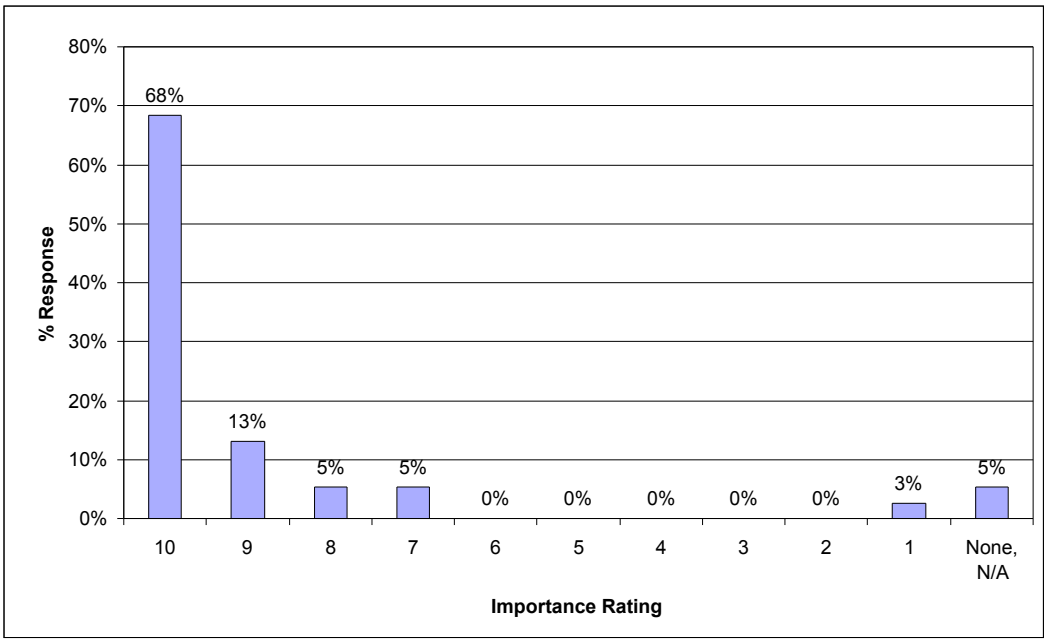
- **The recovery of your financial loss?**



Comments

- This is the most important aspect.
- Especially the losses of the investors. **All** the offender's assets should be seized even when the assets are abroad or in someone else's name.
- Although funds can be recovered through our insurance, the time and disruption caused does affect your morale.
- This was all my life savings and I suffered headaches…
- The loss has devastated me – I am 55 years of age; was conned into remortgaging my home – now in debt for over £90,000. Can't find help to compensate me – criminal went to gaol but only for a short time – let out before time! I have a life sentence!
- The law needs to address the victim's needs fairly and not give preference to any one victim or organisation. The money recovered in my case was paid out to the Crown, Accountant, Solicitors and two victims on preferential grounds. The rest of us got nothing.
- This is very important as lots of time has been wasted and so compensation and recovery of financial losses is essential.

- **The reduction of crime?**



Comments

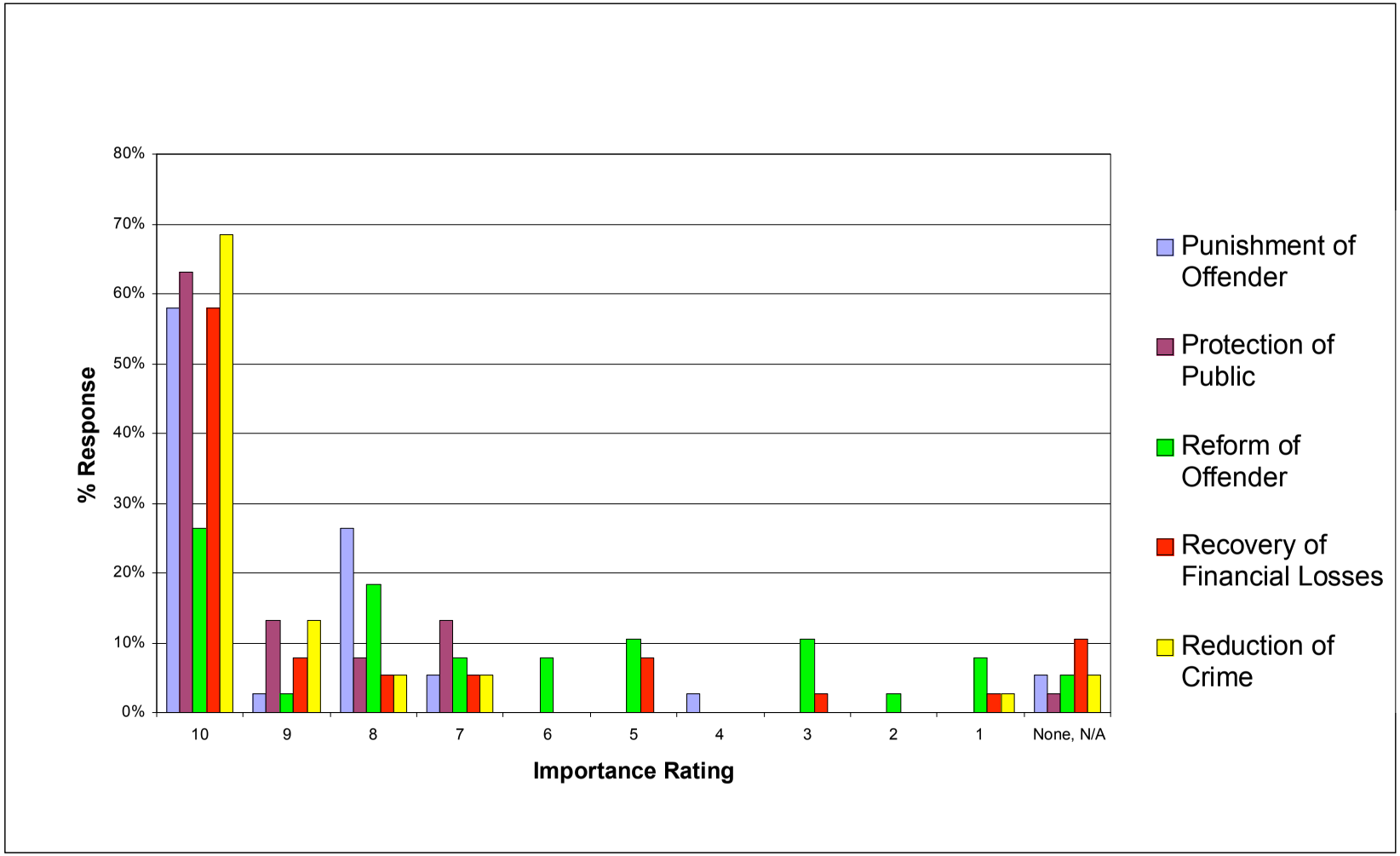
- You can only keep the lid on it – it will never be reduced.
- Very important but difficult to achieve.
- This will make it a safer place to live.
- Make the public more aware. Publish offenders' pictures.
- Analysis should be made as to why fraud is so prevalent.
- Of course everyone would welcome a reduction in crime, but the justice system in this country is too soft.
- I don't know how you can stop the public being as stupid as I was.
- Heavy penalties would help so the cost to the criminal is greater than his gain. Prison is only a part of it.
- Preventative measures should be as tight as possible to prevent these things happening to others again.
- The correct message needs to be given that fraud is a serious crime.

- **Stopping the offender carrying out fraud in future?**

Comments

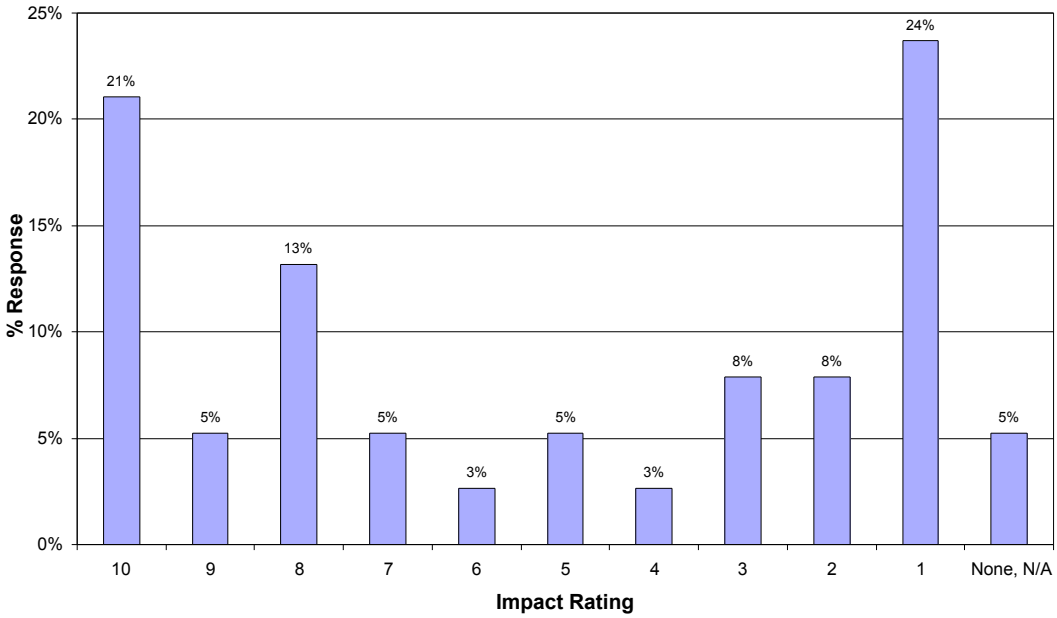
- It seems that this fraud was a way to fund other illegal activities (drug dealing), which was 'more' important to society as a whole – so it seems that the reduction would have wider implications.
- Important - restriction of access to business, credit and e-banking should occur but may be difficult to ensure.
- Very important – fraudsters tend to move from one financial institution to another.
- Name and shame and publish offenders' pictures.
- Learn more from fraudsters and apply new strategies to counter attach future events.
- No reduction of punishment.
- Hopefully the gaol term would be a sufficient deterrent but I feel that this sort of crime, which has ruined many people's lives financially as well as mentally, should see the perpetrator work off the money owed.
- IN my particular case offender got 1 year – but defrauded others as well – well over £1 million – he should have had all his assets taken away; longer jail term – better still send all offenders to an island of no return!
- I don't see how you can. Anyone who would do such a thing in the past is bound to think of fraud as a way of getting a living.
- Offenders should receive the maximum sentence to prevent other possible offenders, i.e. to make them think twice.
- Sentencing needs to reflect the crime.
- Organizations need to be more open with each other.

- **Comparison of Victim's Priorities**



5. On a scale of 1 (no effect) to 10 (great effect), and adding any comments, how did the fraud affect you in relation to:

- **Your health?**

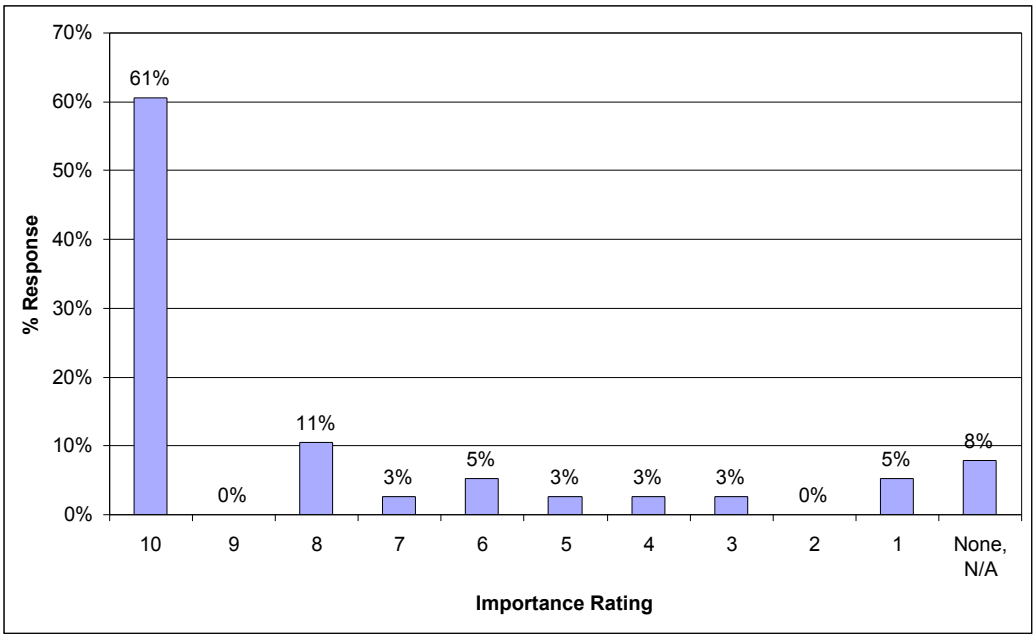


Comments

- I am pragmatic the money has gone. I was angry - now I am getting on with my life. I lost my business and my wife too.
- Cross examination unpleasant – concerns of any repercussions as a result of sentence. Family of offender could take action against witness.
- None, since the attempt was unsuccessful but it could have had a serious effect.
- Worry due to suffering of investors.
- It didn't affect my health; however time was applied to rectify the matter. You are comforted by the fact that the Bank's insurance will replace lost funds.
- I am a paranoiac schizophrenic and suffered immensely from the loss of my life savings.
- It has ruined my life – both working (I can never retire) and my personal life. The thought of what happened haunts me 24 hours a day!
- Gastric Ulcer – Hypertension.
- Having already had a stroke I found the pressure of attending court was very stressful and affected my health and well being for some months after.

- I became very depressed and am still having medication. This also caused a split in my family (my daughter and family) which I cannot foresee being healed.
- Caused unnecessary stress and worries which later developed into serous health problems.
- Lack of sleep due to stress and tiredness, still ongoing
- The worry of going to trial, defence trying to trivialise the offence, sitting with the offender's family outside court - all factors that are stressful.

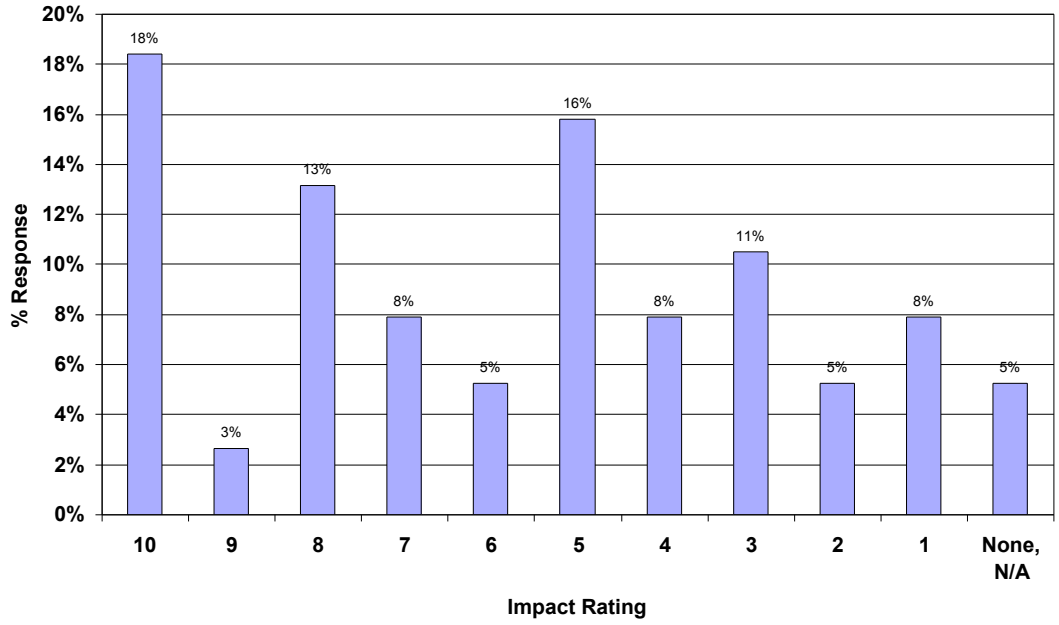
- **Your future approach to your financial affairs?**



Comments

- I am sceptical of electronic banking.
- Extreme care and awareness that not everything is what it seems.
- It has made me more aware and conscious when dealing with personal and financial dealings.
- [I will] restrict use of debit and credit cards to reliable banks and retailers.
- The Home Office brought in new regulations in April 2004, which help us to identify new clients. However the offender would probably have been able to provide fraudulent documentation.
- I have become more careful in my financial affairs.
- I will never trust again!
- Play safe always.
- With great caution.
- Vary careful in making investments due to loss of capital.
- From a company perspective, a greater emphasis placed upon fraud awareness within a claims department.

- **Your confidence in the justice system?**

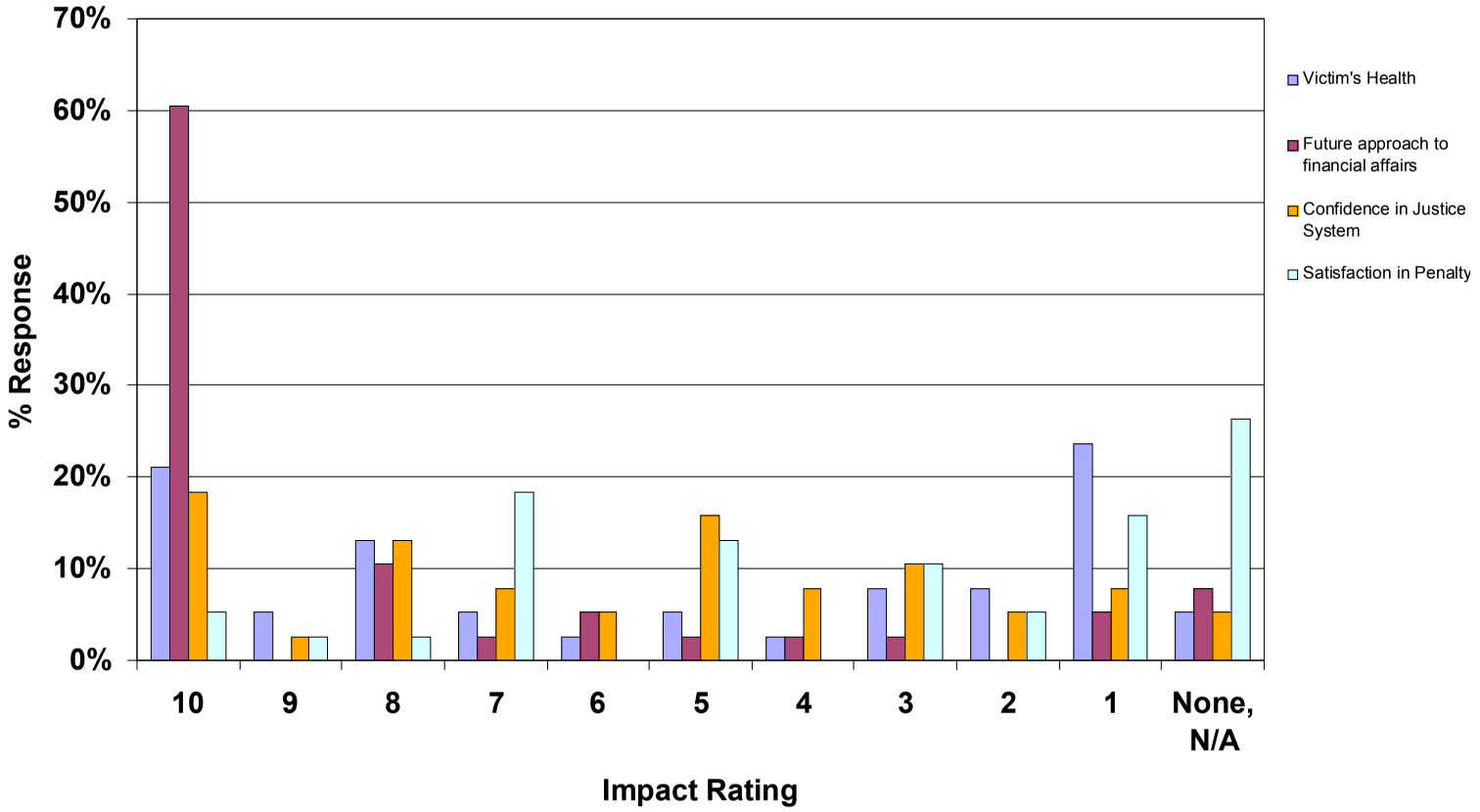


Comments

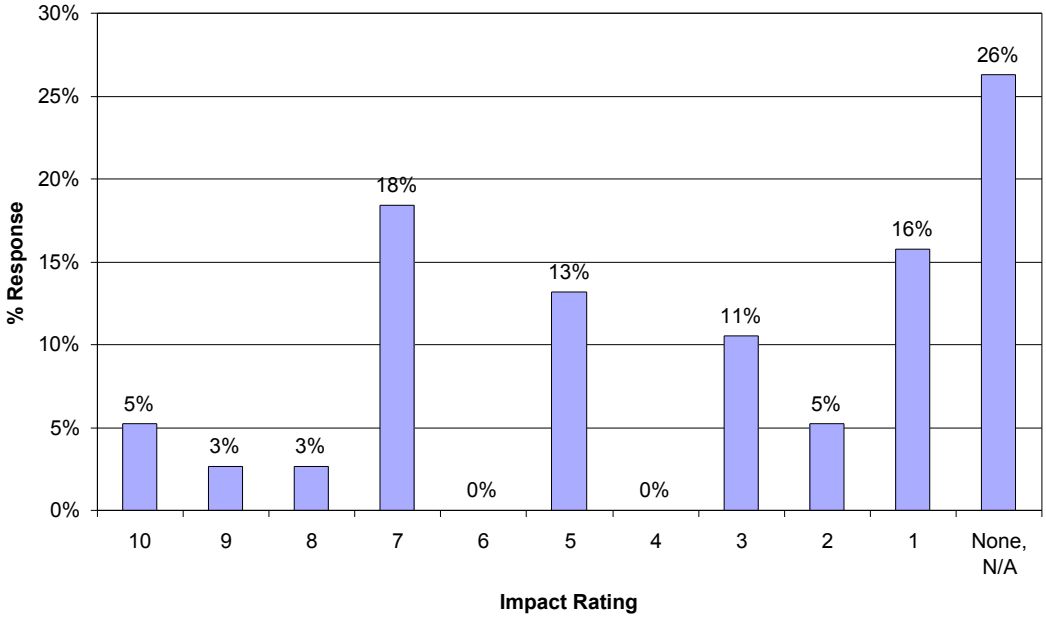
- I understand one of the defendants were found guilty of this crime but was conducting other illegal activities – a shame that it was not able to punish the whole gang.
- I've always had confidence.
- Confidence on this occasion but not always the case.
- The defendants were discharged due, I understand, to insufficient witnesses, but I have no further information.
- No prosecution was brought and no explanation given to me as to why not.
- Very high, but I wish the Government would reduce the benefit from good behaviour.
- Every time the justice system gets ahead of the chase, another loop is found and the chase keeps going.
- Sentences given should be the sentences served and not reduced.
- The City of London Police maintained contact with me and kept me up to date with the case.
- The justice system stinks! It works for the criminals!
- I feel the fraud squad did a great job and are to be congratulated as they were very helpful and reassuring throughout.
- The case was handled very well, I was kept informed at every stage of the case.

- We need a consistent approach to crimes of this nature – not just dependent on which postcode area the crime was committed in, or if a company, the "they can afford it view".
- Worry that jury will not understand fraud and will pass not guilty verdicts.
- Took five years to get to court and the offender failed to attend, never chased up on it, so not sentenced yet.

- **Comparison of Impact on Victims**



6. **If there was a conviction in your case, on a scale of 1 (not satisfied) to 10 (very satisfied) how satisfied were you about the penalty (including any compensation, confiscation or disqualification orders)? Please give reasons for your answer.**



Comments

- I was never informed of the outcome of the case.
- Problem is sentences always get reduced for good behaviour, which I do not agree with. Sentence to reflect crime at time of event, not be reduced based on future actions.
- The penalty was OK but the offender will still be a multi-millionaire when he gets out. But his millions belong to the victims who invested with him – they get nothing??
- I am satisfied with the sentence but we received no financial compensation.
- Considering it was my life savings and I was not compensated in any way I feel that [the offender] deserved his sentence though I feel that he should work off the outstanding money he owes.
- Conviction did not match crime/stress involved as funds were never recovered.
- Providing the offender serves a good long part of his sentence, I am satisfied.
- I am not entirely happy with the conviction as I did not receive any compensation, as the Police could not find any assets to pay the investors compensation.

7. **Bearing in mind your experience, is there anything that would help you, or others, avoid becoming a victim of fraud in the future?**

Comments

- Review of how banks distribute chequebooks or other ways/tools to access people's details and bank accounts. Effectively they admitted their failings by immediately reimbursing me.
- Greater care re: credit cards etc.. but little could be done to avoid the offence perpetrated on me.
- When being cross-examined [you are] was made to feel like you were the one that had committed a crime. Cross examination is a very unpleasant experience. Ensure you have full support when going to court, possibly talk to others who have experienced it first hand.
- Maintaining due vigilance and giving the authorities as much assistance as possible.
- A crime free postal service!
- All that glitters is not gold.
- Possible suggestion would be photo ID on cards.
- Don't take the financial advice of a friend.
- It is vital to identify all new clients/employees to ensure that they are who they claim to be.
- A system whereby all financial dealings within the newspaper media should be monitored and a qualifying regime for advertising more than average profitable investment licensed and regulated.
- The bank could keep details more secure, could vet employees more thoroughly and take more notice of fraud warnings. Our account was marked as a potential case for fraudulent activity even when the second activity (i.e. removal of money) took place.
- I think there should be a compensation fund set up to help victims like me.
- In our profession we as employees are highly scrutinised and this apparently was not done by the bank of this employee. Better scrutinising could be observed.
- You don't get something for nothing. Always be suspicious of high return investments. Better to be safe than sorry.
- We are all responsible for our actions and when it comes to money we are all looking for good return. Seek advice before you spend or invest.
- Before getting involved in any trade one should do a full due diligence regarding its authenticity and not work on trust.
- Take advice before committing any monies, certainly to very "plausible agents".

- Greater publicity of criminal investigations and court cases exampling types/ranges of frauds, the impact upon the public/private purse and effect on communities.

ANNEX E

General Aggravating and Mitigating Factors

Factors indicating higher culpability:

- Offence committed whilst on bail for other offences
- Failure to respond to previous sentences
- Offence was racially or religiously aggravated
- Offence motivated by, or demonstrating, hostility to the victim based on his or her sexual orientation (or presumed sexual orientation)
- Offence motivated by, or demonstrating, hostility based on the victim's disability (or presumed disability)
- Previous conviction(s), particularly where a pattern of repeat offending is disclosed
- Planning of an offence
- An intention to commit more serious harm than actually resulted from the offence
- Offenders operating in groups or gangs
- 'Professional' offending
- Commission of the offence for financial gain (where this is not inherent in the offence itself)
- High level of profit from the offence
- An attempt to conceal or dispose of evidence
- Failure to respond to warnings or concerns expressed by others about the offender's behaviour
- Offence committed whilst on licence
- Offence motivated by hostility towards a minority group, or a member/ members of it
- Deliberate targeting of vulnerable victim(s)
- Commission of an offence while under the influence of alcohol or drugs
- Use of a weapon and gratuitous violence or damage to property, over and above what is needed to carry out the offence
- Abuse of power
- Abuse of a position of trust

Factors indicating a more than usually serious degree of harm:

- Multiple victims
- An especially serious physical or psychological effect on the victim, even if unintended
- A sustained assault or repeated assaults on the same victim
- Victim is particularly vulnerable
- Location of the offence (for example, in an isolated place)
- Offence is committed against those working in the public sector or providing a service to the public
- Presence of others e.g. relatives, especially children or partner of the victim
- Additional degradation of the victim (e.g. taking photographs of a victim as part of a sexual offence)
- In property offences, high value (including sentimental value) of property to the victim, or substantial consequential loss (e.g. where the theft of equipment causes serious disruption to a victim's life or business)

Factors indicating significantly lower culpability:

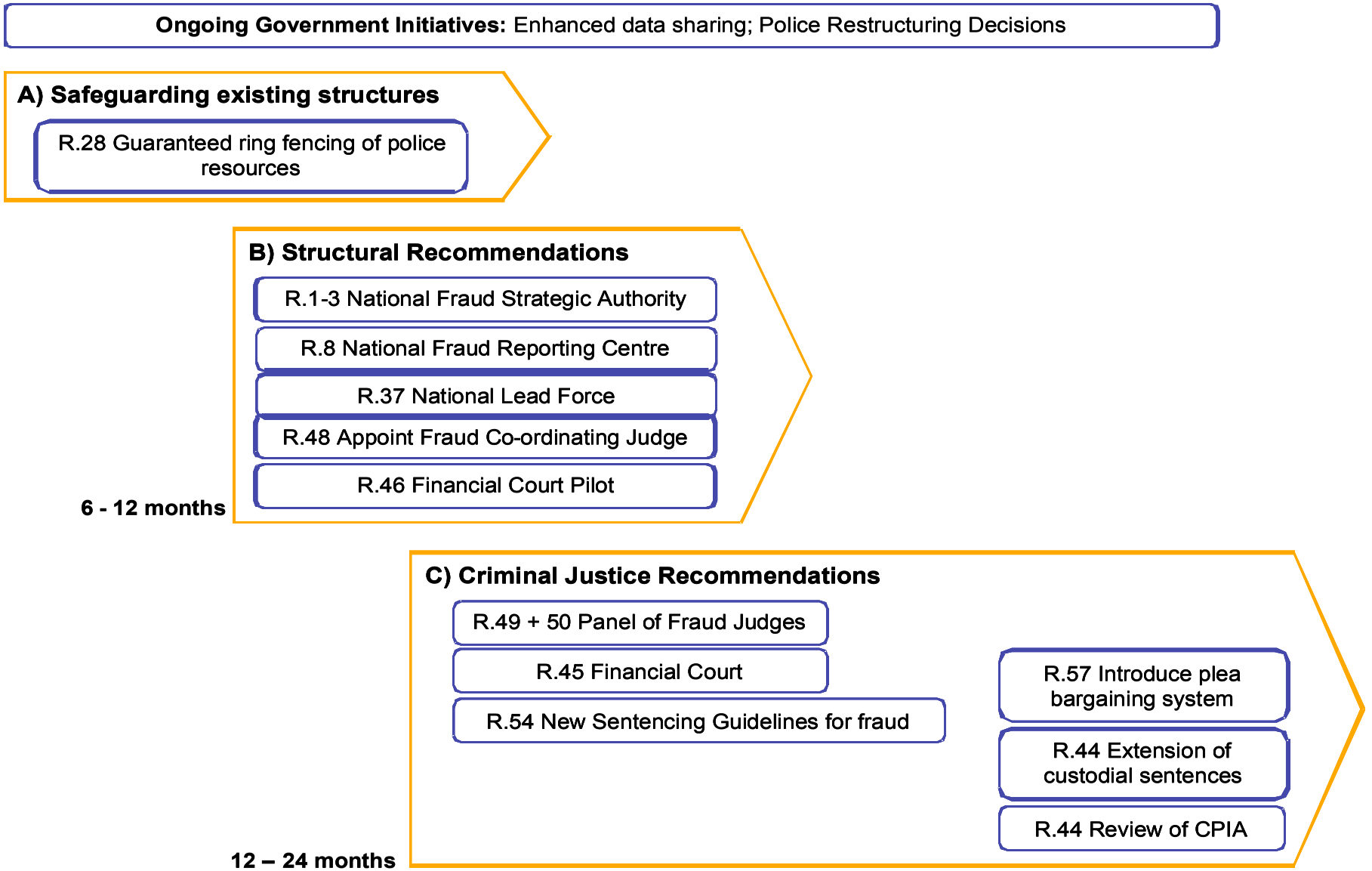
- A greater degree of provocation than normally expected
- Mental illness or disability
- Youth or age, where it affects the responsibility of the individual defendant
- The fact that the offender played only a minor role in the offence

ANNEX F

Offences not covered by the Fraud Bill for which sentencing guidelines are required.

- Conspiracy to defraud, contrary to common law
- Corruption contrary to section 1 of the Public Bodies Corrupt Practices Act 1889
- Corruption contrary to section 1 of the Prevention of Corruption Act 1906
- False accounting, contrary to section 17 of the Theft Act 1968
- Publishing a false statement with intent, contrary to section 19 of the Theft Act 1968
- Fraudulent Trading, contrary to section 458 of the Companies Act 1985
- Insider dealing, contrary to section 52 of the Criminal Justice Act 1993
- Offences contrary to sections 23, 24, 346 and 397 of the Financial Service and Markets Act 2000
- Money laundering, contrary to sections 327-329 Proceeds of Crime Act 2002
- Cartel offences, contrary to section 188 of the Enterprise Act 2002

ANNEX G Timeline for Implementation of Critical Recommendations



ANNEX H

REVIEW	LEAD ORGANISATION	LINKS TO FRAUD REVIEW
a. Nature, Extent, and Economic Impact of Fraud	ACPO / MHB Associates	Study will expose gaps in current measurement and make proposals for further measurement. Crossover with Chapter 2 and proposals for measurement unit envisage taking into account and building upon the study's conclusions.
b. Police Restructuring	Home Office	Police restructuring programme in the Home Office considers the future size and capabilities of police forces. Cross over with Chapter 7 on investigative arrangements, specifically the proposal to ensure each strategic force has a fraud squad of sufficient size to deal with large and complex cases.
c. Misc 31 Committee	Cabinet Office	MISC 31 mandated to establish data sharing strategy for Government. Cross over with Chapter 5, which discusses principles of data sharing on fraud.
d. Organised Crime Green Paper	Home Office	Green Paper proposes increased data sharing to combat crime, including fraud. Crossover with Chapters 4 and 5 which propose future framework and possible mechanisms for data sharing.
e. Carter Review of Legal Aid Procurement	Department for Constitutional Affairs	Review of legal aid procurement, especially criminal defence services. Implications for the legal aid costs of future fraud trials

f. Criminal Case Management	Office for Criminal Justice Reform	Programmes underway include: statutory charging; NWNJ; ETMP; CJIT/ CAVS project (Liverpool Crown Court). Recommendation in chapter 9 for cost benefit analysis of Electronic presentation of Evidence will impact on these cross cutting projects. Cross over with Chapters 9 and 11 which highlight disclosure issues; plea bargaining and other proposals to improve the length and conduct of future fraud trials.
g. Jubilee Line Case Review	HMCPSI	Implications for the way fraud is prosecuted by the CPS. Cross over with Chapter 9 recommendations on better trial management.
h. Regulatory Justice: Sanctioning in a Post Hampton world – Review and consultation document (Prof. McCrory)	Better Regulation Executive / Cabinet Office	Review of adequacy and efficiency of regulatory penalties and sanctions (including maximum criminal sentences in Magistrates and Crown Courts). Implications for civil and administrative alternatives to prosecution for low to medium level consumer fraud. Crossover with chapter 8, which considers extending the sentencing powers of the Crown Court to provide for a wider range of compensatory, preventive and deterrent orders

ANNEX I

Fraud Review Team Members:

David Clarke, Detective Chief Inspector (City of London Police)
Fiona Wong (Financial Services Authority)
James Jenkins (Crown Prosecution Service)
Joana Morison (Department of Constitutional Affairs)
Joseph Halligan (Treasury)
Laura Davies (Department of Health)
Mark Lugton, Detective Constable (City of London Police)
Paul Farley, Detective Sergeant (City of London Police)
Samantha Ankrah (Department of Health)
Steve Phillips (Department of Health)
Tricia Howse (Serious Fraud Office)
Wendy Hart (Department of Constitutional Affairs)

Steering Group Members:

Clive Maxwell (Treasury)
David Humphries (HMRC)
Hugh Giles (Department of Trade and Industry)
Jenny Rowe (Attorney General's Office)
Jim Gee (Department of Health)
Philip Geering (Crown Prosecution Service)
Philip Robinson (Financial Services Authority)
Robert Wardle (Serious Fraud Office)
Ros Wright (Fraud Advisory Panel)
Sarah Albon (Department of Constitutional Affairs)
Stephen Webb (Home Office)
Steve Wilmott, Detective Chief Superintendent (City of London Police)

Consultations in the course of the review included the following, and we thank them for their enthusiasm and engagement:

Ally Foat (Judicial Office)
Anne Sheedy (CIFAS)
Annewen Rowe (Crown Prosecution Service)
Alex Kelly (Scottish Business Crime Centre)
Alan Dobie (Scottish Business Crime Centre)
Barry Mayne (Law Society)
Bob Kennet, Detective Chief Inspector (PITO)
Brian Evans (Judicial Studies Board)
Carl Robinson (Home Office)
Chris Hannant (Association of British Insurers)
Chris Hill (Norwich Union)
Colin Woodcock (SOCA)
David Annets, Detective Inspector (NSCB)
David Levy (Crown Prosecution Service)
Debbie Wilson (Home Office)
Derek Elliot (Audit Commission)
Ed Whiting (Department of Constitutional Affairs)
Fatima Bodhee (HM Courts Service)
Giles Smith (Department of Trade and Industry)
Gillian Turner (Trading Standards Hertfordshire)

Graham Horne (The Insolvency Service)
Jacquie Morley (Lloyds TSB)
James Allen (Office of Fair Trading)
Jamie Bell (Association of British Insurers)
Jeremy Outen (KPMG)
Joanne Cheetham (RCPO)
John Nightingale (Department for Work and Pensions)
John Smith (Prudential)
Jon Simmonds (Home Office)
Judith Killock (Judicial Studies Board)
Katy Worobec (APACS)
Ken Farrow (Lloyds TSB)
Kevin McCormack (Sentencing Advisory Panel)
Lesley Dix (Sentencing Advisory Panel)
Louise Morland (Sentencing Advisory Panel)
Maria Mazur (HMRC)
Mark Abram (Home Office)
Michael Levi, Professor (Cardiff University)
Michael Schuck (Action Against Business Crime)
Mike Haley (Office of Fair Trading)
Nigel Mawer, Detective Chief Superintendent (Metropolitan Police)
Neil Trantum (Royal Bank of Scotland)
Oliver Shaw, Detective Chief Inspector (City of London Police)
Paul Aldred (HMRC)
Paul Cox (Criminal Justice Delivery Unit)
Paul Evans (SOCA)
Paul Martin (HSBC)
Paul Smith (British Retail Consortium)
Peter Marshall (Pensions Regulator)
Peter Yetzes (Audit Commission)
Phil Butler (North East Fraud Forum)
Richard Cook (British Bankers Association)
Richard Webb (Trading Standards Oxfordshire)
Robert Burns (Department of Trade and Industry)
Robert Street (Home Office)
Robin Nelson (DEFRA)
Roger Cook, Detective Chief Inspector (DCPCU)
Sean Byrne (Treasury)
Sonali Parekh (Department of Constitutional Affairs)
Stephen Low (Serious Fraud Office)
Steve Proffitt (Metropolitan Police)
Trevor Brooks (Department of Constitutional Affairs)
Vicki O'Keefe (Serious Fraud Office)

The respective heads of all the Police Economic Crime Departments for England and Wales.

The Financial Crime Team at the Financial Services Authority.

BIBLIOGRAPHY

ACPO & Association of British Insurers, Memorandum of Understanding: Guidelines on the exchange of information between the Police and Insurance Companies' Loss Adjusters. 2002

ACPO, Case Acceptance Criteria and Guidelines for Reporting Attempted and Suspected Fraud. 2000

ACPO, Code of Practice for Data Protection. 2002

ACPO, Guidance on the Management of Police Information. 2006

ACPO, Guidance on the National Intelligence Model. 2005

ACPO, Integrating the National Intelligence Model with a 'Problem Solving' Approach. 2004

ACPO/MHB Study on the Nature, Extent and Economic Impact of Fraud. Interim Report, May 2006.

APACS, Fraud: The Facts 2006. APACS 2006

Ashworth, Andrew. Sentencing and Criminal Justice. Cambridge University Press, 2005

Audit Commission, Code of Data Matching Practice 2006

Auld, LJ. Review of the Criminal Courts of England and Wales. DCA, 2001

BDO Stoy Hayward, Fraud explosion: white collar crime doubles a year. 2005

BDO Stoy Hayward, Fraud Track 3: Rising Fraud in the spotlight. 2006

BDO Stoy Hayward, Fraud Track Survey 2004-05

Beckett, Sophia. 'Criminal Case Processing: practice and procedure of indictable matters set for reform.' Law Society of NSW Journal, June 2005

Bichard, M. The Bichard Inquiry Report. TSO, 2004

Binder, R. and Gill, M. Identity Theft and Fraud: Learning from the U.S.A Perpetuity Research & Consultancy International Ltd, 2005

British Bankers Association, Data Protection: Practical Guidance for Banks. 2005

British Retail Consortium, British Retail Crime Survey 2004/5. 2005

Brown, Alex and Doig, Alan Fraud: Law, Practice and Procedure, Butterworths 2004

Cabinet Office McCrory Review of Regulatory Penalties, 2006.

Centrex, Code of Practice: National Intelligence Model. Home Office 2004

Clinton, W. J. Protecting Consumers for Fraud. Memorandum for the Attorney General. Consumer Sentinel, 1999

Cooper, Daniel P. 'Investigations: Understanding Data Privacy' Journal of Financial Crime, Vol. 12 No. 4 2005

Council for Science and Technology, Better Use of Personal Information: Opportunities and Risks. 2005

Department for Constitutional Affairs, Public Sector Data Sharing: Guidance on the Law. 2003

Department for Constitutional Affairs, Judicial Statistics Annual Report 2005

Department for Trade and Industry, Achieving Best Practice in Your Business. Information Security: BS 7799 and the Data Protection Act . 2004

Ernst & Young, Fraud: The Unmanaged Risk' , 2002

EURIM, Working Draft: Grid of Data Sharing Projects . 2006

Feldman, A, 'Surviving Sarbannes-Oxley'. Inc. Magazine 2005

Fisher, George, Plea Bargaining's Triumphs, A History of Plea Bargaining in America . Stanford University Press, 2003

Flood Page, Claire and Mackie, Alan. Sentencing Practice: An examination of decisions in magistrates courts and the Crown Court in the mid 1990's. Home Office, 1998

Flood, Brian. 'Strategic aspects of the UK National Intelligence Model' in Rafferty (ed.) Strategic Thinking in Criminal Intelligence . Sydney, Federation Press, 2004, p44.

Foundation for Information Policy Research, UK Information Commissioner Study Project: Privacy and Law Enforcement . FIPR 2004

Fraud Advisory Panel, Victims of Fraud, Occasional Paper: 01/ 06 2006

Gill. Martin, Learning From Fraudsters. Protiviti Ltd, 2005

Goldstein, Herbert. What is Problem Oriented Policing? 2001

Göpfert, A . 'The German Problem with Corruption' DW-World.de 2005

Halliday, John. Making Punishments Work: Report of a Review of the Sentencing Framework for England and Wales 2001

Her Majesty's Inspectorate of Constabulary, A Review of Crime Recording Procedures .1996

Her Majesty's Inspectorate of Constabulary, Policing with Intelligence: Criminal Intelligence – A Thematic Inspection on Good Practice . 1997

Her Majesty's Prison Service Annual Report and Accounts 2004-05 Home Office

Home Office, Statistical Bulletin 11/05-Crime in England and Wales 2004/2005

Home Office, Crime against retail and manufacturing premises: findings from the 2002 Commercial Victimisation Survey. 2002

Home Office, Crime In England and Wales 2001/2 ONS 2002

Home Office, Crime In England and Wales 2003/4 ONS 2004

Home Office, Crime in England and Wales 2004/5 ONS 2005

Home Office, Crime In England and Wales: Supplementary Volume 2001/2 ONS 2003

Home Office, Fraud and technology Crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey. Home Office 2005

Home Office, Prolific and other Priority Offenders: Information Sharing Protocol . 2004

Home Office, The application of the Home Office Counting Rules and the National Crime Recording Standards to Offences of Fraud . 2005

Home Office, The National Intelligence Model: key lessons from early research. 2004

Home Office. National Crime Recording Standard (NCRS): an analysis of the impact on recorded crime. Companion Volume to Crime in England and Wales 2002/2003. 2003

Home Office, A Five Year Strategy for Protecting the Public and Reducing Re-Offending 2006

Howard, Davia, Fraud 101: Techniques and Strategies for Detection. John Wiley and Sons Inc. 2000

Huber, Dr Barbara. Tribunal for Serious Fraud Max Planck Institute 2005

Information Commissioners Office, Data Protection Act 1998: Subject Access Rights and Third Party Information. 2000

Information Commissioners Office, Report on Information Commissioners Annual Track 2005. 2005

Information Commissioners Office, What Price Privacy? The unlawful trade in confidential personal information. 2006

International Auditing and Assurance Standards Board, The Auditor's Responsibility to consider Fraud in an Audit of Financial Statements. ISA 240 (Revised). International Federation of Accountants, 2004

John, T and Maguire, M. The National Intelligence Model: Early Implementation Experience in Three Police Force Areas. Cardiff University, 2004

Jones, S., Lewis, D. and Maggs, P. National Economic Research Associates: The Economic Cost of Fraud. Home Office, 2000 www.nera.com

KPMG Fraud Survey 2005

Lander, Stephen. Review of the Suspicious Activity Reports Regime. SOCA, 2006

Levi, Michael. Sentencing Frauds: A Review, 2006

Levi, Michael and Morgan, James. Reducing Business Crime, The responsibilities of directors of plcs to consider the possible impact of crime on business, and if necessary, initiate action. DTI Foresight Programme. 2002.

Mantix, Improving Information Sharing. Mantix Limited, 2006

The Metropolitan Police Service, Sterling: An Economic Crime Strategy for London. 2005

MORI, Privacy and Data-Sharing Survey of Public Awareness and Perceptions. 2003

National Audit Office Good Practice in Tackling External Fraud 2005

National Audit Office Department for Culture, Media and Sport: Tackling External Fraud in Grant-Making 2006

NCIS, The National Intelligence Model. 2000

Office for Criminal Justice Reform, The Code of Practice for Victims of Crime. 2005.

Performance and Innovation Unit, Privacy and data-sharing: The Way Forward for Public Services. Cabinet Office, 2002

PriceWaterHouseCoopers, Global Economic Crime Survey 2005. PwC, 2005

Ratcliffe, Jerry H. Intelligence Led Policing. Australian Institute of Criminology, 2003.

Sentencing Guidelines Council and Sentencing Advisory Panel Annual Report 2004/ 05

Society for Advanced Legal Proceedings (Financial Regulation Working Group). Report on Parallel Proceedings 1999

Taylor, Richard D . Blackstone's Guide to the Criminal Justice Act 2003 Blackstone's, 2004

The Church Council on Justice and Corrections. Satisfying Justice: Safe Community Options that Attempt to Repair Harm from Crime and Reduce the Use or Length of Imprisonment. 2006

The Law Commission. Fraud: Report on a reference under section 3(1) (e) of the Law Commissions Act 1965, 2002

Tilley, Nick. Problem Oriented Policing, Intelligence Led Policing and the National Intelligence Model. University College London, 2003.

Websites

American Institute of Certified Public Accountants.
http://www.aicpa.org/info/sarbanes_oxley_summary.htm

Church Council on Justice and Corrections. http://www.ccjc.ca/about/index.html

Consumer Sentinel. http://www.consumer.gov/sentinel/about.htm.

Cour des Comptes. The Regional Courts of Accounts. http://www.ccomptes.fr/anglais/anglais_2.htm#5.

Federal Foreign Office. http://www.tatsachen-ueber-deutschland.de/725.0.html

Canada Fraud Prevention Forum. http://www.competitionbureau.gc.ca

Garda Bureau of Fraud Investigation. Garda Bureau of Fraud Investigation.
http://www.garda.ie/angarda/gbfi.html.

Internet Crime Complaint Centre. http://www.ic3.gov

Privacy Rights. http://www.privacyrights.org

The Organised Crime Task Force. http://www.octf.gov.uk

Royal Canadian Mounted Police. RECOL http://www.recol.ca

Scottish Business Crime Centre http://www.sbcc.org.uk/

Scott-Joynt, J. (2006). 'Hitting Back at Healthcare Graft'. BBC News.
http://news.bbc.co.uk/2/hi/business/4669532.stm. [Accessed: 04.04.2006].

Sentencing Guidelines
http:// www.sentencing-guidelines.gov.uk/docs /complete_compendium.pdf

Serious and Organised Crime Agency http://www.soca.gov.uk

ENDNOTES

[1] Association of British Insurers
[2] These offences will be repealed by the Fraud Act when it comes into force.
[3] The Law Commission. Fraud: Report on a reference under section 3(1)(e) of the Law Commissions Act 1965 2002
[4] Fraud Bill; currently before Parliament. The text can be found at: www.publications.parliament.uk/pa/cm200506/cmbills/166/2006166.htm
[5] International Auditing and Assurance Standards Board International Standard on Auditing 240 (revised). The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements 2004
[6] Jones, Lewis & Maggs, National Economic Research Associates: The Economic Cost of Fraud Home Office 2000
[7] Davia, Howard. Fraud 101 , Silverstone
[8] Shury et al Crime against retail and manufacturing premises: findings from the 2002 Commercial Victimisation Survey Home Office Online Report 37/05
[9] Fraud and Technology Crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey , p 12
[10] ACPO/MHB Study on the Nature, Extent and Economic Impact of Fraud. Interim Report , May 2006.
[11] These estimates are based on existing costs of measurement exercises undertaken by the Department of Health, which can cover large and complex spending areas.
[12] Brian Flood, 'Strategic aspects of the UK National Intelligence Model' in Rafferty (ed) Strategic Thinking in Criminal Intelligence Sydney, Federation Press, 2004. p44.
[13] SOCA website – www.soca.gov.uk/aboutUs/aims.html
[14] A number of different models have been developed designed to increase police effectiveness – intelligence led policing, problem oriented policing being just two which have been interpreted as incompatible approaches by some academics (see Tilley, 'Problem Oriented Policing, Intelligence Led Policing and the National Intelligence Model'). The Association of Chief Police Officers, who are responsible for the National Intelligence Model, had gone so far as to write guidance on how the NIM is compatible with problem solving and intelligence led approaches. Integrating the National Intelligence Model with a 'Problem Solving' Approach. ACPO 2004
[15] Jerry H. Ratcliffe 'Intelligence Led Policing' Australian Institute of Criminology, 2003.
[16] Public authorities receive and process a huge amount of information in the course of their duties. This information is subject to several legal regimes, not least the Data Protection Act. The Association of Chief Police Officers has issued details how police forces should manage and classify the information they hold. Other organisations, for example, the British Bankers Association, have issued their own guidance on how to apply the Data Protection Act. See the British Bankers Association, Data Protection: Practical Guidance for Banks. BBA, 2005 and ACPO Guidance on Managing Police Information. 2006
[17] http://www.sbcc.org.uk/
[18] The Code of Practice for Victims of Crime. Office for Criminal Justice Reform, 2005. The Code is "admissible in criminal and civil proceedings and failure to comply may be taken into account in determining those proceedings."
[19] 'The application of the Home Office Counting Rules and the National Crime Recording Standards to Offences of Fraud. ' Home Office 2005. Italics added.
[20] ACPO Guidance on The National Intelligence Model . 2005
[21] For example, the Regulation of Investigatory Powers Act, common law duty of confidentiality and so on.
[22] Taken from the ACPO Guidance on the National Intelligence Model 2005
[23] Section 2 of the Police Act (1997) stated that the functions of NCIS were:
-to gather, store and analyse information in order to provide criminal intelligence
-to provide criminal intelligence to police forces in Great Britain, the Police Service of Northern Ireland, the National Crime Squad and other law enforcement agencies
-to act in support of such police forces, the Police Service of Northern Ireland, the National Crime Squad and other law enforcement agencies carrying out their criminal intelligence activities.

[24] Reporting suspicions of criminal activity are compulsory under the Terrorism Act 2000 and the Proceeds of Crime Act 2002. Fraud reporting would be a voluntary arrangement.
[25] These would form part of a set of procedures designed to meet the requirements in the DPA that information be kept accurate and records be only kept as long as necessary.

[26] www.recol.ca
[27] www.ic3.gov
[28] EURIM, Working Draft: Grid of Data Sharing Projects. Referenced on 22 May 2006. http://www.eurim.org.uk/activities/pi/PI_DataSharingProjectsGrid.doc.
[29] Information provided by the Insurance Fraud Bureau, 2006
[30] Although Ministerial Departments can have an implied power to act under the Ram Doctrine, which only narrow statutory vires would prevent.
[31] The Bichard Inquiry Report. TSO London, 2004. p.131
[32] See BDO Stoy Hayward Fraud Track 3, and research by Martin Gill which highlight the prevalence of employee fraud and the reasons for committing it.
[33] Identity theft is distinguished in the US from identity fraud. The legislation is not comparable to the UK (see Binder and Gill.)
[34] Binder, R. and Gill, M. Identity Theft and Fraud: Learning from the U.S.A Perpetuity Research & Consultancy International (PRCI) Ltd 2005
[35] Information Commissioners Office, What Price Privacy? The unlawful trade in confidential personal information. 2006
[36] The Review has not explored the many and complex computer programmes which are available to interrogate, sift and categorise data as this would have confused the issue here.
[37] Section 29(3) Data Protection Act 1998
[38] For example, Sections 24 and 25 of the DPA provide further exemptions from the non-disclosure provisions; Section 35 is likely to be of particular relevance; Section 31 provides exemption from subject access and notification requirements in circumstances of financial malpractice. Schedule 2 details relevant Conditions for processing personal data, within which, Condition 5(d) allows for the processing of personal data "for the exercise of any other functions of a public nature exercised in the public interest by any person" and Condition 6 allows processing for "legitimate interests" and allows the Secretary of State may specify conditions under which this is satisfied.
[39] http://www.ico.gov.uk/
[40] Statutory Instrument 2000 No. 417 The Data Protection (Processing of Sensitive Personal Data) Order 2000. OPSI
[41] Department for Constitutional Affairs, Public Sector Data Sharing: Guidance on the Law. 2003
[42] Council for Science and Technology, Better Use of Personal Information: Opportunities and Risks. 2005
[43] Reproduced from the Report on Information Commissioners Annual Track 2005 http://www.ico.gov.uk/documentUploads/Final_report_individuals_6_10_05.pdf
[44] Report on Information Commissioners Annual Track 2005. and MORI survey for DCA 2003
[45] Arthur Levitt, US Securities & Exchange Commission
[46] British Crime Survey 2006
[47] Unfair Commercial Practices Directive (2005/29/EC) and Regulation on consumer protection co-operation (Dec 2005)
[48] The FSA and is responsible for taking action under the Unfair Terms in Consumer Contracts Regulations 1999 and the Distance Marketing Regulations 2004.
[49] Financial Services and Markets Act 2000
[50] The Daily Telegraph, 27.05.06
[51] NAO/HMT Tackling External Fraud
[52] NAO Department for Culture, Media and Sport. Tackling External Fraud in Grant-Making. 2006
[53] Unfortunately, because the work had to be cascaded down to departments and other bodies, there is no way of verifying what the rate of return on the questionnaire was. Responses were received from: 58 Government Agencies; 18 Government Departments; 28 Non Departmental Public Bodies (NDPBs); 6 'Other government bodies'; and 1 Special Health Authority.
[54] R v. Robin Edward Hounsham & Others 2005 WL 1396757 [2005] EWCA Crim1366 CA (Crim. Div).
[55] Respondent to Fraud Review Victim Survey, April 2006.
[56] Criminal Justice Act 2003 Section 142
[57] Attached at Annex D.
[58] Auld, LJ. Review of the Criminal Courts of England & Wales 2001
[59] Financial Regulation Working Group Report on Parallel Proceedings Dec 1999
[60] Cabinet Office, McCrory Review of Regulatory Penalties, 2006.
[61] Including the new fraud offences in the Fraud Bill 2006
[62] Cabinet Office, McCrory Review of Regulatory Penalties, 2006

[63] Criminal Justice Act 2003 Section 142
[64] Powers not yet in effect.
[65] Daily Telegraph, report of Langbar civil action 11.03.06
[66] Powers of Criminal Courts (Sentencing) Act 2000 Sections 130-132
[67] Proceeds of Crime Act 2002 Sections 48-54
[68] R v Kneeshaw 58 Cr. App. R.439 Comment in Archbold 2006 (par 5-419)"
[69] Marcel v Metropolitan Police Commissioner 1991
[70] See Annex D for full methodology and details of results.
[71] Auld, LJ. Review of the Criminal Courts of England & Wales 2001
[72] Supreme Court Act 1981. Magistrates may also sit with professional judges to hear appeals from lower courts.
[73] Criminal Justice Act 2003 Part 12 Section 142
[74] See Annex D for full methodology and details of results.
[75] Criminal Justice Act 2003 Section 154
[76] DCA costs per sitting day = Magistrates £2,072, Crown Court = £4,601
[77] EU Unfair Commercial Practices Directive will affect 28 Acts or Statutory Instruments, according to the DTI.
[78] Including the new wider fraudulent trading offence.
[79] Missing Trader Intra Community, Office for National Statistics May 2006
[80] Other than restraint orders in connection with criminal confiscation (POCA 2002 & earlier legislation)
[81] I.e. samples. The new provisions for multiple offending in Section 17 Domestic Violence, Crime and Victims Act 2004 are not yet in force.
[82] Review of the Criminal Courts of England and Wales Sept. 2001; Recs 147 & 148
[83] Published December 1999
[84] Specific sector authorisations to conduct business are contained in FSMA 2000, Enterprise Act 2002 and various legal & accountants' Professional bodies' regulatory arrangements.
[85] Cabinet Office, McCrory Review of Regulatory Penalties, 2006
[86] Section 203 - see Archbold 2006 par 5-139 for fuller explanation.
[87] For offences of theft and those to be replaced by the Fraud Bill.
[88] Currently undergoing scrutiny by a Joint Committee of both Houses, May & June 2006
[89] See for example the Langbar case; shareholders are taking civil action, alleging conspiracy to defraud, within weeks of the start of the criminal investigation. If the civil investigation fails to uncover all the evidence available to the Police/SFO there will be a risk of subverting the criminal trial, as happened in R v Baxendale-Walker 2004.
[90] High Court judges on circuit are seldom used for longer trials but are routinely assigned to high profile but essentially simple murders and child abuse cases, which might more appropriately be deal with by Crown Court judges.
[91] POCA 2002 Section14 provides for postponed confiscation up to 2 years beyond the date of conviction, even longer in exceptional circumstances.
[92] As noted above, the accountancy profession has no single statutory regulator.
[93] Art 6 ECHR and Section 19 Courts Act 1971 require that a criminal trial be determined within a reasonable time, including the sentencing process.
[94] Since CJA 2003, revision of the so called hearsay rule, provision for bad character evidence etc.
[95] Chapter 9, par 52 (page 384).
[96] "The feasibility of a Unified Approach to proceedings arising out of major city fraud"
[97] Society for Advanced Legal Proceedings (Financial Regulation Working Group). Report on Parallel Proceedings 1999
[98] Section 17 Domestic Violence, Crime and Victims Act 2004
[99] KPMG Fraud Survey 2005
[100] All C&E offences, not just frauds.
[101] 2004/5
[102] Not known whether individuals or cases, or whether Crown Court or below.
[103] DCA, Judicial Statistics Annual Report 2005
[104] Sections 297-299
[105] Specific orders obtainable under Financial Services & Markets Act (FSMA) 2000 e.g. R v Martin and Others 2005.
[106] CPS lawyers are confined to conducting criminal work under Prosecution of Offences Act 1985
[107] Constitutional Reform Act 2005 amends title of Supreme Court Act 1981 to Senior Courts Act
[108] Enterprise Act 2003

[109] Cabinet Office, McCrory Review of Regulatory Penalties , 2006
[110] Consumer Contracts Regulations 1999 & Distance Marketing Regulations 2004
[111] R v Martin & others Oct 2005. Victims were compensated from the offenders firm which was found to have been "knowingly concerned" in the offence
[112] The FSA brought 1 prosecution in 2005 and this was for market abuse.
[113] These relate to all Regulators and concentrate on non fraud offences, so any detailed read across to the Fraud Review is limited.
[114] Understood to be under consideration in HMRC following its merger.
[115] Huber, Dr Barbara. Tribunal for Serious Fraud Max Planck Institute 2005
[116] Published July 2005
[117] 22nd March 2005
[118] Updated April 2005
[119] Published April 2006
[120] Protocol for the Provision of Advance Information, Prosecution Evidence and Disclosure of Unused Material in the Magistrates' Court, effective from 15 may 2006.
[121] R v Rayment and others, Central Criminal Court, June 2003-March 2005
[122] Review of the Investigation and Criminal Proceedings Relating to the Jubilee Line Case, published June 27 2006; http://www.hmcpsi.gov.uk
[123] page 1, LCJ Protocol – Control and Management of Heavy Fraud and Other Complex Criminal Cases 22 March 2005
[124] The opening lasted 205 days but itself constituted the bulk of the Plaintiff's case, for which no witnesses were to be called.
[125] R v K [2006] EWCA Crim 724
[126] R v Sampson, Hurley, Watts and Soklazzo (GWT01), Wood Green Crown Court Feb-July 2005.
[127] Para 4 (iv), LCJ Protocol
[128] Para 27, Attorney General's Guidelines on Disclosure, updated April 2005
[129] Para 107-109, Improving the Investigation and Prosecution of Serious Fraud, published 25th May 2006
[130] Levi . M Sentencing Frauds: A Review 2006. p 2
[131] Levi M Sentencing Frauds: A Review 2006. p 11
[132] A term coined by Edwin Sutherland in 1939- defined as a crime committed by a person of respectability and high social status in the course of his occupation.
[133] Fraud: Law Practice and Procedure p 32
[134] For summary of fraud guidelines see Annex 2, Levi, M. Sentencing Frauds: A Review 2006.
[135] Ashworth (2005) Sentencing and Criminal Justice, p 73
[136] BDO Stoy Hayward, Annual Survey 2006, p8
[137] Levi .M Sentencing Frauds: A Review 2006 p 27
[138] http://www.timesonline.co.uk/article/0,,200-2174449,00.html
[139] Ashworth (2005) Sentencing and Criminal Justice, p84
[140] Levi. M Sentencing Frauds: A Review 2006. p17
[141] Levi. M Sentencing Frauds: A Review 2006.
[142] Levi. M Sentencing Frauds: A Review 2006. p 4
[143] Levi. M Sentencing Frauds: A Review 2006.p 11
[144] Rose. Rt.Hon.Lord Justice: Sentencing Guidelines Complete Compendium, (foreword).
[145] Gill. Martin, Learning From Fraudsters. Protiviti Ltd, 2005 p9
[146] Flood Page, Claire and Mackie, Alan. Sentencing Practice: An examination of decisions in magistrates courts and the Crown Court in the mid 1990's. Home Office, 1998. p. 85
[147] FAP(2006) Victims of Fraud p5
[148] Ashworth (2005) Sentencing and Criminal Justice p 301
[149] Levi. M Sentencing Frauds: A Review 2006p13
[150] Home Office, A Five Year Strategy for Protecting the Public and Reducing Re-Offending 2006
[151] These figures are for adult males only - Her Majesty's Prison Service Annual Report and Accounts 2004-05
[152] Ashworth, Andrew. Sentencing and Criminal Justice . Cambridge University Press, 2005, p180
[153] Levi. M Sentencing Frauds: A Review 2006
[154] Levi. M Sentencing Frauds: A Review 2006 p20
[155] Levi. M Sentencing Frauds: A Review 2006 p 61
[156] AG's Guidelines on Disclosure reissued 2005
[157] [2005] EWCA 888
[158] (1970) 54 Cr.App.R. 352

[159] 1986 (updated 2002)
[160] Para 67 R v Goodyear 2005
[161] SGC Guideline - Reduction in Sentence for a Guilty Plea, published 16 December 2004
[162] Sections 71-74 Serious Organised Crime and Police Act 2005
[163] United States Sentencing Commission, Guidelines Manual, 3E1.1 (Nov.2005)
[164] U.S. v Booker 543 U.S. 220 (2005)
[165] Levi M (2006) Sentencing Frauds: A Review.
[166] US Sentencing Commission Sourcebook 2001
[167] Found in The United States Attorneys' Manual Section 9-27,000 et seq.
[168] USAM 9-27.310
[169] USAM 9-27.410
[170] USAM 9-27.410
[171] Para 6B1.2
[172] Rule 48(a), Fed.R.Crim.P
[173]Para 6A1.1
[174] Para 6B1.4
[175] http://www.cdpp.gov.au/Prosecutions/Policy/ProsecutionPolicy.pdf
[176] Beckett, Sophia. 'Criminal Case Processing: practice and procedure of indictable matters set for reform.' Law Society of NSW Journal, June 2005, p32.
[177] Review of the Criminal Courts of England & Wales Sept.2001
[178] http://.homeoffice.gov.uk/documents/cond-caution-cop
[179] Sections 71-74 Serious Organised Crime and Police Act 2005
[180] Identity fraud may be included in some of these estimates of the cost of fraud, so there may be potentially be a prevalence of duplicate counting.
[181] Association of Certified Fraud Examiners. 2004 Report to the Nation on Occupational Fraud and Abuse. 2004:1. This figure is an estimate of occupational fraud which the ACFE defines as 'The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.'
[182] Ibid.
[183] Göpfert, A . 'The German Problem with Corruption' DW-World.de 2005.
[184] This figure has been calculated using the figures for the cost of fraud and GDP in 2004.
[185] The Legal Secretariat to the Law Officers. The Conduct of Fraud Trials: The Case for Reform. 200
[186] Scott-Joynt, J. BBC News. 2006.
[187] Estimation of Don Holmes (Ernst & Young fraud investigator) cited in Gutstein, D. (2000).
[188] This figure is calculated using the figures for the cost of fraud and GDP in 2004.
[189] Oakes, P. The Post IE. 2005. This figure refers to the amount of money lost to money laundering – not fraud exclusively.
[190] This figure is calculated using the figures for GDP in 2004 and the cost of fraud per annum.
[191] SMITH, R. G., 2003. Serious Fraud in Australia and New Zealand. Cited in Caslon Analytics, ' Caslon Analytics profile: identity crime'. Canberra: Australian Institute of Criminal Justice. [http://www.caslon.com.au/idtheftprofile6.htm] [Accessed 24 February 2006].
Also: KPMG, 2004. Cited in Money Management, Fraud Rife Across Corporate Australia http://www.moneymanagement.com.au/articles/34/0c028e34.asp [Accessed 27 February 2006].
[192] For a comparable list of health expenditure per capita in international dollars ($) in each country, see Appendix II.
[193] We were able to obtain figures on bank card fraud although this is not significant enough o to base a national estimate upon.
[194] Consumer Sentinel. Consumer Sentinel: The Cybertool for Fraud Busters. (2005).
[195] Internet Crime Complaint Centre. About Us. No date provided.
[196] £5.6 million.
[197] £5.1 million.
[198] Centrelink. Program Protocol: Pay-As-You-Go (PAYG) Data Matching. May 2004. p.17.
[199] Resulting in a cost-benefit ratio of 1: 2.61.
[200] Resulting in a cost-benefit ratio of 1: 13.74.
[201] The cost of the reviews amounted to £495,652 (AUS $1.2 million).
[202] The remaining two types of criminal activity were vehicle crime and immigration crime.
[203] A penalty of unlimited imprisonment is imposed in lieu of non-payment.
[204] Ibid.

[205] The Church Council on Justice and Correction is a national faith-based alliance of eleven churches which promotes a restorative approach to criminal justice.
[206] The Church Council on Justice and Corrections. Satisfying Justice: Safe Community Options that Attempt to Repair Harm from Crime and Reduce the Use or Length of Imprisonment. 1996: 89.
[207] The savings to fraud are calculated in different ways.
[208] First person card transactions are not recorded as APACS record this as classed as bad debt.
[209] Figures released on 07/03/06 in press release - total card fraud losses fell by 13% on 2004 figures – mainly due to chip and pin technology.
[210] www.abi.org.uk
[211] The British Retail Consortium's Retail Crime Survey 2004/5
[212] The syndicate is made up of major insurers, ABI and insurance industry partners. For full report go to http://www.abi.org.uk/BookShop/ResearchReports
[213] Capita Insurance Services – Commercial Insurance Fraud: Additional Findings, 8 September 2005.
[214] Azure Solutions are a global revenue-assurance company.
[215] Figures received from Jack Wraith, Chairman of TUFF.
[216] KPMG Forensic 30 January 2006. www.kpmg.co.uk/news
[217] http://www.mishcon.co.uk/inp/inp_c/fraudreport2005/fraudreport2005.htm
[218] ODPM holds this data as they are responsible for housing matters.
[219] Information received on the telephone, awaiting email confirmation.
[220] Tackling External Fraud, NAO, 2004.
[221] TV Licensing Annual Review 2003/4
[222] BBC Annual Accounts 2004/5, p.94.
[223] Fraud and Error in Income Support, Jobseekers Allowance and Pension Credit, Office of National Statistics and DWP, 2005, p2. These confidence intervals do not account for other uncertainties that do not arise from the sampling process.
[224] Reducing fraud in the benefit system, achievements and ambitions, DWP, October 2005, p.7.
[225] DVLA Annual Accounts 2004/5, p53.
[226] HMRC Filing of Income Tax Self Assessment returns – 22 June 2005
[227] Identifying the nature and scale of the problem, www.cfsms.nhs.uk. A copy of the full methodology can be obtained from the NHS Risk Measurement Unit.
[228] See Derry v Peek (1889) 14 App Case 337, [1886-90] All ER Rep 1. House of Lords and Westminster City Council v Croyalgrange Ltd [1986] 2 All ER 353
[229] Based on costs in 2004-05
[230] Expenditure being £76,400,000 for 2005-06
[231] All figures as published.
[232] Jones, S., Lewis, D. and Maggs, P. National Economic Research Associates: The Economic Cost of Fraud. Home Office, 2000 www.nera.com