The Nature, Extent and Economic Impact of Fraud in the UK

Michael Levi, John Burrows, Matthew H. Fleming, and Matthew Hopkins
With the assistance of Kent Matthews

The Nature, Extent and Economic Impact of Fraud in the UK

Michael Levi, John Burrows, Matthew H. Fleming, and Matthew Hopkins
With the assistance of Kent Matthews*

Report for the Association of Chief Police Officers' Economic Crime Portfolio
February 2007

* Levi: Professor, Cardiff University; Burrows: Partner, Morgan Harris Burrows; Fleming: Senior Manager, Detica Inc.; Hopkins: Consultant, Morgan Harris Burrows; Matthews: Professor, Cardiff University. Corresponding author's email address: Levi@Cardiff.ac.uk. Opinions expressed herein are those of the authors and do not necessarily represent those of their parent organisations.

ACPO ACKNOWLEDGEMENTS

The commissioning of this report would not have been possible without the support of the following members of the ACPO Economic Crime Portfolio Group:

ACPO National Working Group on Fraud (NWGF)

APACS – The UK Payments Association

Association of British Insurers (ABI)

Bank of England

CIFAS – The UK's Fraud Prevention Service

Home Office

Prudential Plc

Serious Fraud Office (SFO)

Serious Organised Crime Agency (SOCA)

FOREWORD

It used to be said, "No one walks down the street in fear of being embezzled". Well, increasingly they do. Whereas once the average Briton dreaded being burgled or having their car broken into, they are now worried about identity fraud, mass marketing scams and other forms of financial crime that have a serious impact on their lives. Long gone is the notion that fraud is a victimless crime.

Lying to secure financial benefit is fast becoming endemic in British life. The layperson's description of fraud – "I tell you a lie, you give me the money" – has never had so much resonance. From professional criminals duping bank call centres through to inflated earnings on mortgage applications, fraud threatens to blur the boundaries between what we see as right and wrong. Unabated, fraud will undoubtedly change the way that future generations view the world and undermine many of the advances we now take for granted. How many of us, when shopping over the Internet, have paused before clicking the mouse button, hoping that we are not logged onto a fraudulent web site?

It is widely accepted that fraud causes significant harm to the UK, indeed the Serious Organised Crime Agency (SOCA) recognises this as a priority area. But estimating the size of the problem is complex. Previous attempts to scope it have varied significantly in both their findings and methodologies. Recognising this gap in our knowledge, the Association of Chief Police Officers' Economic Crime Portfolio Group commissioned Morgan Harris Burrows LLP, in association with Professor Michael Levi of Cardiff University, to undertake an independent study. Their report, supported by a wide range of public and private sector organisations, was a year in the making and represents a watershed in our understanding of fraud. I am delighted with the quality of their findings.

Professor Levi and his team have conservatively estimated that fraud cost the UK £13.9 billion in 2005. But this figure excludes some major areas of criminality, such as income tax and EU fraud, where statistics are simply not available. Adding estimates for these into the mix, it is likely that fraud represents a £20 billion annual loss to the UK. To put this figure into perspective, such losses would pay for an additional 200,000 police officers or save every man, woman and child £330 per year.

Whilst the report is very comprehensive, the findings must be seen as no more than a baseline - signalling a way forward for those involved in reducing fraud. I am heartened by recommendations made recently in the Government's Fraud Review and strongly believe this piece of work will be invaluable to those charged with implementing the UK's national response.

I sincerely hope that you enjoy reading the report and find the content an informative guide to this growing social problem.

Mike Bowron
Commissioner of Police for the City of London
Chair, ACPO Economic Crime Portfolio Group

ACRONYMS

ABI	Association of British Insurers
ACPO	Association of Chief Police Officers of England, Wales, and N. Ireland
APACS	Association for Payment Clearing Services
BBA	British Bankers' Association
BRC	British Retail Consortium
CIFAS	CIFAS – the UK's Fraud Prevention Service (formerly the Credit Industry Fraud Avoidance System.)
DCPCU	Dedicated Cheque and Plastic Crime Unit
DTI	Department of Trade and Industry
DWP	Department for Work and Pensions
FLA	Finance & Leasing Association
FSA	Financial Services Authority
HMRC	Her Majesty's Revenue and Customs
HMT	Her Majesty's Treasury
IFB	Insurance Fraud Bureau
IMF	International Monetary Fund
NAO	National Audit Office
NDPB	Non-Departmental Public Body (e.g. SOCA)
NERA	National Economic Research Associates
NFI	National Fraud Initiative, spearheaded by the Audit Commission
NHS	National Health Service
NOE	Non-observed economy
OECD	Organisation for Economic Cooperation and Development
OLAF	Organisation pour La Lutte Anti-Fraude (EC body dealing with fraud against the financial interests of the European Union)
ONS	Office of National Statistics (now 'National Statistics')
SFO	Serious Fraud Office
SOCA	Serious Organised Crime Agency

ACKNOWLEDGEMENTS

We received generous assistance from individuals and organisations—most of whom requested anonymity—from all corners of the fraud-fighting arena, for which we are extremely grateful. We would especially like to thank the members of the Fraud Review Team, particularly Steve Phillips, Wendy Hart, and Laura Davies; the members of our own Steering Group; and Josée Ratcliffe.

CONTENTS

EXECUTIVE SUMMARY

This study was commissioned by the Association of Chief Police Officers' Economic Crime Portfolio to meet the following objectives:

- to determine as accurately as possible — from existing published sources of information — the nature, extent, and cost of fraud to the public and private sectors;
- to assess critically the availability and quality of existing evidence on fraud; and
- to recommend appropriate strategies to facilitate the comprehensive and consistent recording of data on fraud (i.e. strategies for future data capture).

The study did not conduct original research to get a closer approximation to the 'true cost of fraud'.

Broad findings

There has not been the kind of centralised effort into estimating the extent of fraud that there has been into other areas of unreported and unrecorded crime: indeed it is not always obvious to victims themselves, or to outside observers, whether or not fraud has been committed. Nor has there been much effort in either private or public sectors to drill down into the social and economic costs of fraud. Nevertheless, substantial and varied data about many types of fraud in the UK are available. For each sector, this research sought to summarise data availability and deficiencies; the reasons underpinning data collection; data collection methods; and the known costs of fraud—divided into the direct (transfer) costs of the fraud, the costs of preventing fraud and the costs of responding to fraud after the event. Data on the costs of responding to fraud and of fraud prevention are particularly sparse, and for clarity, they have been kept disaggregated from fraud losses to victims.

The studies reviewed in this research encompass global surveys (from which UK data can be drawn), national level surveys (both rolling and snapshots), through to national data collection exercises drawing on administrative data compiled by umbrella organisations, often focussing on particular types of fraud (as reflects their funding and member interests). Indeed, in the absence of a more systematic overview such as this (and, to a lesser extent, the NERA 2000 study that preceded it), something of a 'free market' in information about the cost of fraud has developed. The publicity given to the ever-higher 'estimates' of fraud bears little relationship to the scientific rigour (or cost) of the studies themselves.

In analysing the cost of fraud, the study adopted a conservative position based on the lower end of estimation ranges. One consequence of that is that the aggregate cost figures in some sectors are lower than might be expected if better research were available. The data below are principally from 2005 or shortly before, but the lag in awareness of longer-term frauds (and the fact that some data such as income tax returns need to be filed only after the event) mean that some will date back years; and whereas the private sector data are generally based on calendar years, the public sector typically uses financial years, making impossible their integration into annual snap-shots. The 'health warning' on these data is that because of uneven awareness and reporting, and the different approaches adopted in surveys/ studies, they may not reflect the 'true' distribution of fraud. Moreover, the extent and nature of fraud are shaped by organisations' business and service activities as well as by their culture, transparency and prevention efforts (plus offender skills/energy).

The *minimum* extent of the losses borne by victims in the private sector was judged to be as follows:

1. *For businesses in the financial service sector* (i.e. banks, building societies, finance houses, insurance companies and their agents), some data are quite robust and some result from the administrative

record-keeping of members, which means that the data could be used tactically to prevent and/or respond to fraud. From the best evidence available, **financial services' fraud losses are estimated at £1.005 billion in 2005.**

2. *For businesses in the non-financial services sector* (the majority of businesses by volume) data are largely derived from surveys, and their value has thus to be restricted to policy development and more strategic crime reduction approaches. The coverage – both in terms of business sectors and different types of frauds—is patchy.[1] Here, **fraud losses to businesses other than financial services are estimated at £0.934 billion in 2005.**

3. However, the losses in the sectors above are complicated by the fact that a number of surveys of frauds against businesses do not separate out financial services from other sector losses in their reports. There may be some modest double-counting with the datasets above, but survey findings suggest that **at least another £1.821 billion should be added to the total costs of fraud against businesses**, mainly in 2005, though one cannot tell whether these losses are to financial services or to other businesses.

4. Fraud against *private individuals* paradoxically has received very little attention in any of the studies, being covered neither in the corporate fraud surveys nor in the public sector reviews. Although it is not certain that all 'scams' against private individuals meet the criteria of 'a crime', **fraud losses against private individuals can be estimated at £2.75 billion in 2005.**

The losses borne by victims in the public sector were judged to be as follows:

1. For *public bodies at the national level* there is much the same variation in the availability and quality of fraud data noted in the private sector. Considerable progress has been made in specific fields, notably by the NHS Counter-Fraud and Security Management Services and by the Audit Commission's National Fraud Initiative.[2] Tax fraud is (and probably always will be) a far more significant source of economic loss than any other single area of public or, for that matter, private sector fraud; and VAT/MTIC frauds and large income tax frauds may comprise the largest single categories. **National public sector fraud losses can be conservatively estimated at £6.434 billion**, mostly in 2005-06 but due to data time lags, sometimes in earlier years. But this sum excludes two major items which might be expected to make a substantial difference to the public sector fraud total. One is income tax fraud, where no valid figures are currently available and which this study has set at zero.[3] The other gap in evidence on public sector fraud is the UK's share of fraud against the EU, where annualised estimation of fraud (as opposed to irregularities and inefficiencies) is deeply problematic,[4] and against other international bodies such as the UN and World Bank.

[1]For example, although some intellectual property (IP) offences plainly cause physical as well as economic harm, the published data do not validly distinguish between cases in which purchasers were deceived as to the legitimacy of the products and those in which they were not: therefore IP fraud costs have not been included.

[2]Proposals to broaden the coverage of the NFI are included in the Serious Crime Bill 2007.

[3]HMRC (2006c, Annex C) data show that tax compliance work yielded £4.28 bn. in 2005-06, including £3.08 bn. from specialist offices and £1.2 bn. from network offices. In 2004-5, HMRC recovered £5.725 billion from tax compliance work on the revenue side (HMRC, 2005a; see also NAO, 2003). One Treasury estimate put the 'tax gap' at £30-40 billion, or around 10 per cent of revenues, compared with around 13 per cent in the US and 8 per cent in Sweden. (Hansard, HC, 8 Dec 2004: Column 1202; HM Treasury, 2004). If 10 per cent of this was fraud rather than error or avoidance, then the arithmetic would be plain, but there is no obvious way of deciding what percentage of the tax gap fraud actually constitutes. As discussed later, this is inherently difficult.

[4]EU documents assert that one can only call error 'fraud' at the conclusion of the criminal court process: this would make estimating undetected fraud (or any other crime) a logical contradiction.

2. **For public bodies at the local level, losses are conservatively estimated at £0.04 billion in 2005-06.** Some deceptions against council tax may also involve deceptions to central government departments (like DWP), so it is difficult to allocate losses to one rather than the other.

The above fraud loss figures are merely indicative. The existing sources of data on fraud are neither mutually exclusive nor collectively exhaustive. Many high value cases that appear to meet the criteria of criminal fraud are investigative by forensic accounting and law firms, and are treated as civil matters for litigation and negotiation with 'suspects' and third parties. Before an 'actual' fraud comes to be counted as such, it has to go through a process of being suspected, investigated and identified as such, whether through accident or a more formal audit process aimed at uncovering fraud. Then a decision has to be made as to whether to make the fraud public in some way, in aggregate form (as in APACS data on plastic frauds) or as an identified individual case (for example via formal reporting to a policing body). This report essentially evaluates and summarises data that reach the final stage.

It is conventional in 'cost of crime' studies to include the costs of preventing and responding to crime with the direct costs of crime. Yet even in the public sector, figures on the costs of fraud investigation are mostly unavailable outside the police, and in both public and private sectors, many fraud (and corruption and money laundering) prevention costs are bundled together with general compliance and technological systems; and also are not published. So, in this sense, the data here clearly understate the true cost. On the other side of the coin, it is clear that some data collection exercises will 'double count' some frauds.
Overall, however, available sources suggest that:

- ***excluding* the cost of doing something about them, the direct losses from frauds of all types were at least £12.98 billion (mostly) in 2005; and**
- **it would be surprising if the 'true total' was not much larger than this**.

In addition,
- **the known and separately identified private and public costs of acting against fraud – both before the event and in response to it – total £0.937 billion: this is certainly a significant underestimate.[5]**
- **Together, the known costs of fraud and of dealing with fraud were at least £13.9 billion in 2005.**

Of course, as with all crimes, the impact of fraud is more than just 'pounds and pence': victims vary in the 'collateral damage' caused and how well placed they are to recuperate from their losses, economically and psychologically. Apart from psychological damage, there are other dimensions of harm and risk such as:
- the growing attractiveness of fraud to conventional major criminals and to previously non-criminal technophiles alike; and
- the possibilities of crimes which – unlike other forms of property crime – can be committed from remote places beyond the easy reach of law enforcement or civil recovery.

However these issues were outside the brief of this study.

Problems with existing sources of data

The review highlighted the following main problems in relation to the existing sources of data:
- The neglect of some forms of fraud;
- Weaknesses and inconsistencies in defining 'fraud';

[5]There are severe difficulties in separating ongoing costs of computer systems and of compliance with anti-money laundering regulations from the costs of anti-fraud measures. Some private and public organisations also wish to keep their fraud control costs private.

- Data collection exercises that have been carried out with different purpose(s) and with poor response rates;
- Imprecision about the 'unit of analysis' (for example, whether data apply to one company or to all its related subsidiaries, including those operating abroad) and – in trans-national frauds – whether or not the fraud was committed 'in the UK';
- Insufficient concern about the implications of the variable (and sometimes considerable) time between the commission of the offence and awareness, reporting and recording – even for those frauds that are formally dealt with;
- Weak disciplines applied to the aggregation of data and in deriving UK-wide estimates.

The evidence also clearly indicates that, despite the wide variety of activities that cluster together under the label of 'fraud', there is a thread common to the commission of most offences: namely that fraudsters are able to find or create weaknesses in the systems, controls or procedures operated by victims or their intermediaries. This can be a tautology – without opportunities there can be no crimes – but as the police service cannot be expected to possess the specialist knowledge of all such systems, the primary responsibility for fraud prevention – and often for the initial identification of plausible suspects – must lie in the hands of victims. This is particularly so for the business sector, which alone must have the capacity and motivation to spend money on technology, training and staff to reduce frauds against themselves, and against others affected. The role of the police service will primarily be one of working in partnership with victims to initiate proceedings against suspects, and to assist in fraud reduction for those individual victims who have neither the funds nor the capacity to act for themselves.

Applying a victim-centric approach

Information on fraud losses is typically identified and reported by immediate and/or ultimate victims, and this recognition led the review to employ a victim centric approach to thinking about types of fraud and their measurement. This approach is critical to framing plans for improved fraud reporting, since reporting and prevention strategies are best aligned to meet the needs of those who stand to reap the dividends from these investments.

While there was a strong logic to this approach, it was not always a straightforward one to apply. Quite apart from the frauds that are poorly documented and analysed, some costs of fraud are difficult to attribute to any particular subgroup of victims, and some frauds may impact simultaneously on several sub-groups. In the final reckoning, individuals (the public-at-large) bear the costs of most fraud.

Recommendations

In looking to ways of improving the future reporting and recording of fraud, the discussion in the report is framed in the context that the Fraud Review has recommended that the appropriate response to the massive under-reporting of fraud is to establish a National Fraud Reporting Centre (NFRC), to which businesses and individuals could report frauds. The proposed NFRC would then be able to provide police and other investigative agencies with information to target individuals.

Whether or not an NFRC is endorsed in the form proposed, **the findings of the current study certainly support the case for a reasonably well-resourced, central body to 'champion' the improved reporting and recording of fraud – or at the very least the improved *study* of fraud**. This should produce dividends in both fraud reduction and the apprehension and detection of the perpetrators of fraud.

It is recommended that any such central body should work within a comprehensive framework for fraud as a whole, in that such an approach will avoid undue attention being given to 'what is currently counted' at the expense of 'what is not'. The adoption of a 'victim centric' approach, similar to that developed in the current study, could serve this purpose. Moreover, because the term 'fraud' covers such a wide and varied set of behaviours, one of the key priorities of any national centre would need to be to classify and record separately different fraud types.

The report does however caution – in the light of the very low level of current fraud reporting and the potential enormity of what might follow if victims were encouraged to report all fraud – that there is a very real danger of raising expectations for official action that might not be able to be met, whether by the police or by any other body. The overlap for regulated firms between fraud reporting and the Suspicious Activity Reports required for all offences (including fraud) by the anti-money laundering regime will also need to be examined. More specifically, separate from ongoing HMRC work on the extent of tax fraud (especially income tax fraud), the first priorities of any central coordinating and advisory centre on fraud should be:

- Where fraud data are currently being collected that can be classified as 'tactical/operational intelligence', these offer the best scope for setting up public-private partnerships to mount anti-fraud initiatives.
- Where data are currently being collected by surveys, the centre should encourage the application of tighter definitions of fraud, more rigorous methodologies and even promote some form of 'kitemarking' of data collection activities – whether they involve the pooling of administrative data or one-off surveys – that meet approved standards. Assessing the adequacy of data on fraud requires knowledge of how the data are generated.
- Where data are almost entirely absent – and notably for many sorts of fraud against private individuals – there would be a strong case for any fraud centre to initiate and commission separate studies to gain reliable insights into the extent, nature and costs of specific types of fraud.

Progress has been made in recent years in refining Home Office treatment of fraud statistics. However, irrespective of whether a national centre is established, it seems plain that given the importance of fraud to modern criminality, any ongoing analysis of the extent and nature of crime will be incomplete and inadequate unless it makes a more serious effort to incorporate data on fraud than is currently done. This report represents one step along that difficult path.

1. INTRODUCTION

Fraud costs the UK a very considerable sum of money. Recent studies suggest that the cost of fraud may fall in a rough order of magnitude of ten+ billion pounds per year (and far more in some commercial surveys): even at the lower end of the estimation range, this would place it at least 2.5 times greater than the combined cost of burglary, theft and robbery of individuals (Dubourg and Hamed, 2005). It may never be possible to work out precisely how much fraud costs because quite apart from some victims being hard-to-reach (especially if they have been involved in crime themselves), not all disputes about the presence or absence of 'dishonesty' can be resolved objectively. But in addition, information on fraud is derived from an array of diverse sources, many of which suffer from methodological weaknesses—and most of which are difficult to aggregate in any precise manner.

In response to the need for a careful review of the evidence in this neglected area of crime research, this study was commissioned by the Association of Chief Police Officers and the Home Office to meet the following objectives:

- to determine as accurately as possible – from existing sources of information – the nature, extent, and cost of fraud to the public and private sectors, including the cost of (a) fraud losses (i.e. transfer costs); (b) preventing fraud before the event (and other anticipatory costs); and (c) responding to fraud after the event;
- to assess critically the availability and quality of existing evidence on fraud; and
- to recommend appropriate strategies to facilitate the comprehensive and consistent recording of data on fraud (i.e. strategies for future data capture).

To address these aims, the study systematically reviewed all the available evidence on fraud (further details are set out under 'Methodology', below).[6] This document presents the results of the research. It is structured as follows: after this introduction, a background section contextualises the research. Then the findings of the review are summarised. The implications of the findings are discussed in the final section, along with strategies for future data capture. The report incorporates a series of annexes providing greater detail on selected issues.

[6]This research was commissioned in tandem with the Government Fraud Review (the output of which—Fraud Review, 2006 – has undergone a public consultation round). Overlap between the two studies was inescapable (e.g. the Fraud Review contains some information on publicly available information on fraud losses). The genesis of the present research lay in the concern of ACPO and the Home Office that policing and crime reduction policy in the area of fraud had been comparatively neglected and were in danger of being omitted by default from public debate on crime control, without sufficient awareness of the harms of frauds relative to each other and relative to other forms of crime. It was also recognised that many of the studies of the incidence, prevalence and impact of fraud had not been conducted according to the proper canons of empirical research, and, as such, that indiscriminate application of the results of these studies raised the risk that priorities/resources might be allocated on a misguided basis. The Fraud Review Team (FRT) was under predetermined time pressures which required it to report three months earlier than the present study. There was, of course, collaboration between the two teams, and in particular some sharing of the results of data searches: but the main understanding was that the present study would focus in particular on the validity of studies of fraud, and on the manner in which more reliable and extensive data could be collected in the future.

2. BACKGROUND

This section presents the background to the research. It discusses fraud and definitional issues; sets forth the scope of the problem; presents the study's methodology; and notes briefly the intricacies in exploring the costs of fraud.

A. WHAT IS FRAUD? A TYPOLOGY

What is fraud? At least prior to the Fraud Act 2006,[7] both legal and analytical/survey definitions and classifications were varied. As NERA (2000) put it, "the issue of defining which activities constitute fraud is the subject of considerable debate." Resolving this debate is outside the remit of the present research. To avoid confusion, for the purposes of this study, fraud is defined as follows:

> *Fraud is the obtaining of financial advantage or causing of loss by implicit or explicit deception; it is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss.*[8]

This study employs a victim-centric approach to thinking about and measuring types of fraud, set out in Table 1. Since the promotion of preventive activity underpins both the present study and the wider Fraud Review, the victim-centric approach was judged to be necessary because it is the victim (or the loser) who generally reports (or does not report) fraud and who stands to reap the dividends from any investment in fraud prevention.

Victims may be delineated into two general categories — private and public sector — and further into subdivisions within those sectors:

- victims from the private sector: financial services and non-financial services firms, and individual members of the public; and
- victims from the public sector: central bodies and local bodies.

The use of this kind of matrix makes it easier to determine where gaps exist in fraud data, and enables clearer thinking on how the costs of fraud can be aggregated (in particular, the victim-centric matrix helps to ensure that victims do not overlap, thus preventing double-counting). The third column of Table 1 includes examples of types of fraud: although by no means comprehensive in its coverage of all frauds, this column seeks to separate frauds that are mutually exclusive and collectively exhaustive for each sub-sector (although the same types of fraud and sorts of fraud technique may be used against different victim sectors).

[7]And probably thereafter, since drafting for legal purposes seldom provides the sort of behavioural categorisation that corresponds to the way individuals and businesses want to classify frauds. The Fraud Act came into force on 15 January 2007 and includes fraud by false representation, failing to disclose information to the detriment of another person, and abuse of position for dishonest gain.

[8]The aim of the provision about causing loss rather than merely causing gain is that sometimes the fraudster does not gain (or does not gain nearly as much as the losses s/he causes); the provisions also bring malicious or even 'economic terrorism' acts within the concept. From a legal viewpoint, this is important, though less significant for any economic cost analysis. Despite the cumbersome language, however, it is included for the sake of definitional completeness. The Fraud Act 2006 has a slightly broader definition than the one used in this study, involving for example the dishonest exposure to the risk of loss: but the difference is not material to this review of historical data.

Determining 'the victims' of fraud

The application of a victim-centric approach was in part driven by the sources of information available, which are mostly reports of fraud levels/losses made by or about organisations and individuals as victims.[9] Various types of fraud are perpetrated against these victims, and in Box 1, it is critical to note that types are distinct from methods.

It was recognised that some costs are difficult to attribute to any particular subgroup of victims and some frauds may impact simultaneously on several sub-groups. The brief summaries provided in Box 1 suggest that some frauds are confined to one class of victims: thus central government bears the brunt of most tax or benefit fraud, and the costs of insurance fraud are typically borne by the insurance industry. At the other end of the spectrum, every public body and private sector business is susceptible to embezzlement and procurement fraud. But in reality, the ultimate bearer of the cost of many frauds stands between these two extremes—and depends critically on the circumstances of the case. Losses from investment frauds committed by regulated persons/firms are covered by the Financial Services Compensation Scheme or, in some cases, by professional bodies like the Law Society (or by the firms themselves); but other investment frauds are compensated only if the offender can be found and made to repay (following conviction or civil recovery action). The same applies to frauds on company pension holders and to cheque frauds. In the case of payment card frauds, there are four potential losers—the card issuer, the merchant acquirer, the merchant and the cardholder. Unless the cardholder can be shown to have committed—or been complicit in—the fraud, or to have handled the PIN negligently, he or she will rarely bear the loss (albeit the introduction of 'chip and pin' technology transfers the cost of fraud to merchants who do not comply with agreed standards).

Of course, individuals (the public-at-large) are ultimately the victims of most fraud, as they generally bear the costs of fraud through higher insurance premia, reduced dividends or pensions, higher credit card fees or interest rates, higher fees for banking services, higher taxes, and so on (including psychiatric services and redundancies).[10]

Another advantage of the victim-centric approach is that it assists the distinction between:

- *primary victims:* the natural or legal persons—individual or business or public body — who initially suffer the harm of fraud; and
- *secondary victims*: those who ultimately pay for the economic component of fraud losses. In some instances these will be the primary victims; in others, they may be financial institutions, insurers or industry/professional compensation schemes who, by contract or following regulatory interventions, agree to reimburse some or all costs to primary fraud victims; plus taxpayers and/or those who are deprived of services which they would otherwise have received.

It needs to be emphasised that the label 'fraud' is not always a natural category. In many failed businesses, it may be difficult to decide whether or not the company or person has traded whilst insolvent: if it did, this could be classified as 'fraudulent trading.'[11] Part of the aim of the fraudster is to make targets believe that they and their transactions are genuine—so whether conduct is labelled as fraud

[9]A victim-centric approach is employed because it appeared to be the most sensible approach for the needs of the review; but this is not to suggest that other ways of looking at fraud (e.g. through an offender-centric approach) lack merit. Indeed, offender-centric approaches are used in several commercial fraud surveys, and sub-types of these frauds relate to whether or not offenders were employees, outsiders or both. Studies of how much fraud is committed by 'organised criminals' require us to know about both victims' losses and what sort of people have caused them.

[10]In special cases such as betting frauds, individuals may lose bets that they should have won — or occasionally, by accident, vice versa — and in electoral frauds, their right to the democratically chosen candidate.

[11]Contrary to s.458 of the Companies Act 1985 and s.9 of the Fraud Act 2006. For pragmatic, resource-constrained reasons, such potentially fraudulent trading might actually be dealt with as an administrative or civil rather than as a criminal matter.

may be a matter of some delicacy (e.g. with bad debt v. fraud, or with pyramid/high yield investment schemes). And it may be a matter of some considerable confusion for victims. Surveys of victims, for example, will often ask "have you been a victim of this or that fraud?"—yet many of these types of frauds are complex, and even seasoned anti-fraud professionals are unclear on the exact meaning of certain terms. The implication is that victim-centric measures of fraud that are drawn from victim 'knowledge' are not always precise.

Finally, it should be noted this study does not treat "identity fraud" as a separate category of fraud, as some studies have done (Cabinet Office, 2002; Home Office, 2006). Rather, such behaviour is incorporated within other fraud types.[12]

[12]Although there is some reason for aggregating the creation and circulation of fictitious or copied/misattributed personal data—for example in what might be a category of "application fraud" and/or "corporate website fraud" — there is a very significant difference between defining "identity fraud" as all conduct that involves an individual pretending to be someone he/she is not (e.g. using a stolen credit card) — in which case the word 'identity' may be redundant—and its use in APACS data to refer to more specialised acts such as "account takeover fraud", using "stolen" personal details to open accounts in the name of living or dead people without their knowledge.

Table 1. A typology of fraud by victim

Victim sector	*Victim sub-sector*	*Examples of fraud*
Private	**Financial Services**	**Cheque fraud**
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Data-compromise fraud
		Embezzlement
		Insider dealing/market abuse
		Insurance fraud
		Lending fraud
		Payment card fraud
		Procurement fraud
	Non-financial services	Cheque fraud
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Data-compromise fraud
		Embezzlement
		Gaming fraud
		Lending fraud
		Payment card fraud
		Procurement fraud
	Individuals	Charity fraud
		Consumer fraud
		Counterfeit intellectual property and products sold as genuine
		Counterfeit money
		Investment fraud
		Pension-type fraud
Public	**National bodies**	Benefit fraud
		Embezzlement
		Procurement fraud
		Tax fraud
	Local bodies	Embezzlement
		Frauds on Council taxes
		Procurement fraud
	International (but affecting UK public)	Procurement fraud [by UK against non-UK companies to obtain foreign contracts]
		EU funds fraud

Note: See below for a glossary of common fraud types.

Box 1. – A glossary of common types of fraud

Benefit fraud: Frauds of various kinds upon the social security system, ranging from widespread 'working and drawing' by employees in casual agriculture and fisheries sectors (with employer/subcontracting 'gangmaster' collusion) via housing benefit frauds (sometimes involving landlord collusion) to the more common (by volume) failure to notify benefit officials of changes in circumstances that disentitle claimants to benefits.

Charity fraud: Frauds in which donations are stripped from entirely fictitious or unregistered charities, or are embezzled from registered charities. This is distinguished from consumer fraud because the donor does not expect to receive a 'fit for purpose' product: but it may only be fraud if it can be proven that the donor was deceived as to the purpose of the donation.

Cheque fraud: Most frauds on individuals' cheques are covered by guarantees up to a particular limit, depending on the card type (£50-£200) if presented at the time; beyond that losses accrue to the firm that accepted them unless bank negligence can be demonstrated.

Consumer frauds: A broad category including lottery/prize scams; rogue dialling and other communications-based frauds; 'dishonest' mis-descriptions of products and services (such as some 'alternative health care products' or sex aids); gaming frauds (e.g. 'fixed' races and matches upon which bets (including spread betting) have been made; purchases of goods and services that are not sent by the supplier. Frauds involving the sale of cars – for example the hand over of a vehicle before full payment is received (for example, after receipt of a false banker's draft, or cheques that are then not honoured) – are also included.

Counterfeit intellectual property and products: A broad set including medicines, vehicle parts, art & antiques sold as genuine and believed by consumers to be genuine. Thus, few people buy Viagra or antibiotics or genuine Microsoft software expecting them to not to work. This should be distinguished from, say, Rolex watches bought for £10 in a street market, which almost no-one is deceived about or regards as genuine; these do not usually involve some actual financial loss to Rolex or other branded goods firm, but can do so in addition to reputational loss.

Counterfeit money: A direct loss to the individuals/businesspeople given counterfeit money.

Data-compromise fraud: Frauds on companies and on individuals (sometimes called 'phishing' and 'pharming') arising from website manipulations; these frauds include the manipulation of corporate websites to make the target believe that the firm they are dealing with (and possibly are supplying credit to) is the genuine business. Also 'traffic interception' and simulation of customers of telecommunications firms, which is not formally credit-granting but amounts to credit fraud. 'Phishing' attacks occur when the public receive a bogus email claiming to be from a legitimate site, asking the target to click on links within the email (to provide, say, access to an internet bank account password, which is then abused). 'Vishing' involves the same scam but it works over a 'voice over internet protocol' (voip) phone line.

Embezzlement: Frauds against all businesses, government departments and professional firms by staff ranging from junior clerical staff to directors & officers of the company or partners of the unincorporated firm. This normally either involves accounts manipulation or the construction of false invoices.

Gaming frauds: This refers to 'fixed' races and other forms of sport upon which spread betting and

other gaming wagers have been made. This has an effect on the profits of the gambling industry as well as on the chances of winning for individual consumers.

Insider dealing/market abuse: This category of offences is particularly difficult to classify, as it affects the general integrity of the market but may not have any directly attributable victims or – in any given individual case – even affect people's confidence in the market. In this sense, they insider dealing/market abuse might be classified as frauds against individuals/the public rather than against financial services firms. These are to be distinguished from "boiler room" and other stock manipulations that involve causing real loss to investors and that clearly belong to the class of frauds on individuals.

Insurance fraud: Insurance companies may be victims of a variety of frauds by businesspeople (e.g. arson for profit, maritime fraud) and consumers (e.g. inflated claims, fictitious claims, staged

Investment frauds: There are essentially three sub-types: (a) frauds in which investors do not believe that investments are FSA-authorised e.g. advance fee/some high-yield investment frauds involving 'secret inside information' or 'whisky/champagne' (i.e. boiler room scams); (b) frauds in which investors wrongly believe that the investments are FSA/other regulated; and (c) frauds in which investors correctly believe that investments are FSA/other authorised. Only in the third case will any compensation normally be paid: the Financial Services Compensation Scheme may be able to assist private investors if the firm with whom an investment was made is fully authorised and has gone into default and cannot pay out claims (whether or not the cause is fraud). No compensation can be sought when investment values decrease as a result of market trends or inflation. The maximum amount claimable under the FSCS is £48,000, which comprises the first £30,000 in full and 90 percent of the next £20,000.

Lending fraud: This category includes a variety of frauds involving lending funds (financial services category) and lending credit for goods and services (non-financial services category). Among sub-types are fraudulent bankruptcy (sometimes referred to as long-firm frauds); consumer credit; letter of credit (involving fictitious invoices/shipping documents against which funds can be withdrawn); and mortgage frauds (which can involve the manipulation of property prices, at one extreme, or the overstatement of applicants' income to get a loan that otherwise would not be granted, at the other). Non-financial services firms are victims of fraudulent bankruptcies by businesses from which they order goods by payment in advance or to which they supply goods on credit (long-firm frauds) and individuals to whom they sell goods on credit.

Payment card fraud: Frauds on issuers and merchant acquirers of debit, credit, and charge cards. The reason that these are also mentioned under non--financial services firms is that some card purchases that are made without authorisation by the merchant acquirer are charged back to the merchant (e.g. computers bought remotely with stolen/counterfeited cards that are not delivered to the cardholder's billing address). There may also be disputes over whether a card used at an ATM or elsewhere has actually been the victim of a fraud by an 'outsider' or whether it was the cardholder or some other person who gained access to their card and/or details, sometimes a family member.

Pension-type frauds largely fall into two categories. The first are subject to compensation from the FSCS (above) if in regulated schemes; the others are outside this protection but may receive some compensation from the Fraud Compensation Fund whether or not fraud is proven. So individuals can lose where the employer or third party steals company pensions and National Insurance contributions.

Procurement fraud: Frauds and corruption in the purchasing process, including price-fixing rings, abuse of inside information in the construction of tenders or in their application. Some of these might be prosecuted as corruption, even when committed by UK companies against overseas businesses and

government departments. Bills sent out to firms fraudulently claiming that they have ordered a placing in a business directory or similar scheme are also included here; these can affect any company.

Tax fraud involves failure to pay direct, indirect, and excise taxes. 'Direct taxes' encompass income tax and corporation tax fraud, ranging from individuals (whether on social security or not) failing to declare income from minor skilled work to large schemes involving corporate manipulation. There are also tax credits, which are a form of direct taxation involving false claims to credit. Indirect taxes include VAT fraud, particularly Missing Trader Intra-Community Fraud. Excise taxes primarily encompass alcohol and tobacco and motor oil tax evasion, from small-scale smuggling to large bonded warehouse frauds. Some tax frauds also arise at the local government level, in relation to council taxes.

B. SCOPE OF THE PROBLEM

Is fraud, in all its forms and definitions, a serious problem for the UK? In particular, where does fraud fit in relation to other costs of crime? In the event, little is reliably known about the extent and cost of fraud in an aggregate sense. This considerably complicates policymaking. Much of what policy has had to be based upon is drawn from studies carried out by National Economic Research Associates (NERA) and Norwich Union to estimate the economic cost of fraud (NERA, 2000; Norwich Union, 2005).[13] These place the cost of fraud in the UK at some 6.75 billion GBP as a lower bound and 13.82 billion GBP as an upper bound (NERA, 2000) and a (presumed mid-range) 15.78 billion GBP (Norwich Union, 2005).[14]

Neither study, however, represents the last word on the subject. Indeed, each makes clear that limitations in data quality and coverage make their figures tentative at best. NERA, for example, discusses the implications of the fact that (1) different sources provide UK-wide data, while others provide data only for England and Wales, with obvious implications for aggregation; (2) data may in many cases provide a poor understanding of the aggregate level of discovered and undiscovered fraud (perhaps in situations/sectors with little counter-fraud activity); (3) limited information on methods behind fraud extent/cost figures (e.g. surveys) precludes a deeper understanding of data quality; and (4) in many sectors insufficient data are/were available (particularly in those sectors with recoveries made after the event, which NERA,2000, nets off transfer costs).

The Fraud Review (2006) summarises the situation best when it notes "There are no reliable estimates of the cost of fraud to the economy as a whole". Moreover, no prior analyses/critiques of existing information on fraud had been carried out in any systematic sense (i.e. which systematically examine data sources and their methodology in a critical light). The need for a clear, critical assessment of the cost (and the exploration of future needs) is the motivation for the present research.

C. METHODOLOGY

To address the aims of the research, the available evidence was systematically reviewed. Initially the brief for this study was to carry out a rapid evidence assessment (REA). An REA draws on published sources of information, systematically and critically appraising identified studies against specified criteria, all in a

[13]The Norwich Union study is essentially an abridged update of the NERA research. Note also that two additional studies are of relevance, though they do not seek to paint as complete a picture of fraud as do the NERA and Norwich Union studies: Cabinet Office (2002) and Wilson *et al* (2006). The former represents an estimate of the cost to the UK of identity fraud (later updated in Home Office, 2006) and the latter conveniently incorporates a number of existing studies and administrative data sets.

[14]Each estimate is provided in current – rather than real – GBP, such that the NERA figure must be put into 2004 GBP to be strictly comparable to the Norwich Union findings. In practice, many commentators took the upper bound estimate as 'the figure'.

relatively compressed timescale. As part of an REA, a set of criteria against which to evaluate sources (to separate the 'wheat from the chaff') is established, conventionally called a Quality Assessment Tool (QAT); indeed this is a central task of all systematic analyses/REAs/meta-analyses (sources are evaluated with particular regard for the quality of the data contained therein; Annex 1 provides examples of the dimensions of data quality). The use of such criteria is intended to prevent the inclusion of research results which may be derived from questionable methods and/or which may ultimately lead to presenting data which conceals the fact that sources have been comparing apples and oranges.

Very early on in the present research, however, it became clear that subjecting the literature on fraud to a conventional QAT 'screening' would not be feasible, because of the nature of the task being undertaken and the characteristics of the available fraud literature. The difficulties faced are summarised below.

To begin, while the present research was not tremendously different conceptually from the earlier REAs sponsored by the Home Office and others (or a Campbell Collaboration report or meta-analysis along the lines of Sherman *et al* (1998)), one of the key tasks was to determine the cost of fraud to the public and private sectors in the UK. As such, the research was most interested in fraud statistics, particularly those relating to costs—while REAs typically examine evaluations of policy interventions—and therefore criteria of what makes a good study differ.[15]

The present study looked to publicly available information on fraud in the UK (from sources throughout the public and private sectors and the academic journals). The studies reviewed broadly fell into four categories:

1. those that reproduce, in a digest form, data derived from criminal justice processed cases (e.g. prosecuted frauds above a certain figure);
2. reports derived from networks of organisations (often sharing a common membership of an umbrella body) aggregating key administrative data to monitor trends and patterns;
3. surveys that aimed to generate a more general portrait of fraud or particular forms of fraudulent conduct, although almost all with far more modest investment and attention to methodological issues than in any general crime surveys since the 1970s; and
4. those that scientifically sample frauds within agencies or departments and then extrapolate from them.

But very few of these studies on fraud are derived from academic or professional analytical sources (whereas REAs of policy evaluations typically review studies conducted by research professionals). Academic sources will broadly follow accepted article/report formats—which include section(s) on methods. However in the case of many fraud studies, details of the methodology used are typically lacking. In particular, it is inescapable that while many fraud studies relating to the private sector may appear to constitute 'research', the fundamental reason the work is conducted is to raise awareness of a threat often overlooked by the business community, and/or to market the ability of the "research" sponsor to offer consultancy and/or related support services to tackle the problem. The net result is that much fraud work is based on loose methods (at best), or represents sound social science but with limited value for aggregation in any meta-analysis.

Added to this, given that the pool of relevant sources was not a deep one, a major concern was that 'setting the bar too high' would have left the study with little to review and discuss. While applying a formal Quality Assessment Tool (QAT) was not practical, the research did screen the available data, and placed a particular premium on including data that was reasonably current and that applied to the UK

[15]In other words, while most previous REAs grade research used in their meta-analyses on the evaluation methodology employed (where randomised experimental approaches are largely seen as the gold standard), the present research was concerned with statistical data quality (data quality refers to "fitness for purpose": data quality dimensions are presented in Annex 1).

only: the details of the approach adopted are presented in Annex 2. Thereafter, as indicated above, the studies on fraud that were included in the review were categorised in relation to the victim, or loser, of such frauds. One of the benefits of applying this typology was that it made it possible to determine which victim sectors were subject to considerable research, and where gaps in coverage existed. Three further dimensions were also considered.

The first key dimension was the data collection methodology typically employed in each field. The range of information sources is outlined above, but it was seen to be particularly important to separate data derived from administrative record-keeping from that obtained by sample survey methods:

- Data from *administrative record-keeping* include, for example, data on (or summarising) reports of confirmed/suspected fraud discovered/investigated by companies in the financial services sector. These data are often aggregated and provided by membership organisations (e.g. APACS) to allow for the aggregate analysis and presentation of fraud trends.
- Data from *sample surveys*, on the other hand, will have been captured through the questioning (e.g. through self-response or interviews) of a sample of the overall population of interest (where a sample frame serves as a proxy for the population of interest). Sample surveys fall into a further two categories: probability sample and non-probability sample surveys. Probability sample surveys employ some probabilistic method to select at random entities from the sample frame for participation in the survey.[16] Non-probability sample surveys employ methods other than probabilistic selection (most commonly thresholds, like all cases dealing with frauds of £100,000 or more) to determine which entities provide information.[17] Unless otherwise noted, the term "survey" in this report refers to a probability sample survey.

A second key dimension was to consider the purpose for which the data had been assembled and the implications thereof.[18] Different users may seek quite different goals in assembling fraud data. Data may be collected:

- To inform general policy-making, perhaps by indicating the volume and cost of fraud to the UK in general terms.
- To generate strategic intelligence[19] on fraud—indicating broad trends or typologies of fraud, which can assist law enforcement organisations and/or the organizations which have been defrauded to design a suitable overall response.
- To generate *tactical—or operational* — intelligence[20] products which may then be used to identify and apprehend specific individuals and/or groups of fraudsters.

---

[16]A census can be thought of as a probability sample survey in which all units within the sample frame are selected to participate with a probability of one (i.e. all units within the sample frame are asked to participate).

[17]Non-probability sample surveys also include surveys such as web-surveys which record findings of whoever responds. A consequent weakness of such non-threshold or even threshold approaches (i.e. of all non-probability samples) is that it is difficult to generalise from non-probability samples to the larger population of interest.

[18]A crucial dimension of 'data quality' refers to 'fitness for use' or 'fitness for purpose', an inherently fuzzy concept (Office of National Statistics, 2005a, hereinafter ONS, 2005). This immediately begs the critical question of what is the purpose of capturing statistics on fraud?

[19]Strategic intelligence has been defined as "an assessment of targeted crime patterns, crime trends, criminal organisations, and/or unlawful property transactions for purposes of planning, decision-making and resource allocation" (Criminal Intelligence Training Coordination Strategy Working Group, 2004: cited in Fleming, 2005)

[20]Tactical, or operational, intelligence has been defined as "evaluated information on which immediate enforcement action can be based; intelligence activity focussed specifically on developing an active case" (see CITCSWG, 2004 in note above).

In reviewing the different sources, the present study sought to separate these (and other) different purposes. Clearly the timeliness of information available is critical here: data derived from a survey of fraud affecting particular types of victim may assist general policy making and possibly serve to provide strategic intelligence, but it cannot be expected to provide any operational utility in 'nailing' a particular offender.

The third key dimension was to seek to separate the costs of fraud into different categories; this issue is discussed further below.

D. MEASURING THE COSTS OF FRAUD

Research on the costs of fraud typically disaggregates costs into various main components (see, for example, NERA, 2000). The current research was no different, and its aims included the need for the review team to "determine as accurately as possible –from existing published sources of information–the cost of fraud to the public and private sectors including the cost of (a) fraud losses (i.e. transfer costs); (b) preventing fraud before the event (and other anticipatory costs); and (c) responding to fraud after the event." This approach was largely driven by the body of literature on the economics of crime, particularly the subset focussing on the costs of crime (see, for example, Brand and Price, 2000). The costs of fraud under consideration in the present research were as follows:

- *Fraud losses (transfer costs)*: Victims face direct losses as a result of fraud (i.e. the amount defrauded). These losses are sometimes considered transfers (from the victim to the fraudster), and in the economic literature, transfers are typically excluded in analyses of the costs of crime. The present research follows Brand and Price (2000) and includes fraud losses in the costs of fraud, as these are unwanted losses (i.e. the victim has not agreed to the transfer), and as such the transfer represents one from the legal to the illegal economy.
- *Costs of preventing fraud before the event (and other anticipatory costs)*: Private and public sector entities take certain defensive measures to prevent/deter fraud, all with costs. These costs range from personal expenditures on shredders to corporate membership of (a) service organisations such as the ABI and APACS, one of whose many functions is fraud prevention, and (b) dedicated fraud prevention bodies such as CIFAS (indeed, the running costs of CIFAS itself). Costs also result from precautionary behaviour: consumers may avoid using certain services or avoid visiting certain crime-heavy locations (physically or virtually) to avoid being victims of crime in general and fraud in particular. NERA (2000) notes, for example, that customers might avoid online banking services for fear of being defrauded (which would represent a loss to them and perhaps the banks if the marginal cost of online banking is lower than that of its alternatives).
- *Costs of responding to fraud after the event:* The costs in response to fraud include costs to the criminal justice system (including police, prosecutors, courts, prison service)[21] and of civil remedies in response to fraud. Larger and more complex frauds against firms will typically incur expenditures (e.g. through internal and/or out-sourced private sector investigations) even if they are not ultimately reported to the police. In the event, very few sources provided information relating to the costs of fraud prevention and/or in response to fraud, nor do many appear to keep data in this form.

The costs of fraud (and crime in general) are sometimes disaggregated as losses, resource costs, and externalities. Resource costs may relate to expenditures both in anticipation of and in response to fraud (e.g. on fraud prevention systems, on reactive investigative teams), though these distinctions were difficult. Externalities refer to side effects from an activity which have consequences for another activity but are not reflected in market prices. Externalities can be either positive, when an external benefit is generated, or negative, when an external cost is generated. A negative externality of fraud may be the

[21]Unless the offenders have surplus assets from which costs can be paid, private sector investigative and legal costs will be deducted from compensation for victims; public sector costs are borne by contributors to council and central government taxes.

above-noted reduction in the use of online banking services (assuming that online banking commands lower marginal costs). Another might be where a corporate and/or national reputation for making or demanding corrupt payments for contracts leads to other firms or countries avoiding doing business with the suspected bribe-payer or bribe-demander. This falls into the category of fraud (as well as corruption) because where a bribe to an agent leads to the deception of the ultimate 'beneficial owner' (citizens, taxpayers, shareholders/private business owners), this is fraud. Furthermore, there is usually some false accounting that accompanies the bribes.

It should also be noted that costs may be estimated by 'bottom-up' and/or 'top-down' methods. Annex 3 explores some of the technical hurdles faced in applying the 'top down' approach in three areas where fraud is recognised to represent a significant risk: in the credit card industry, in the insurance industry and in relation to state benefits.[22]

- *A 'bottom up'* approach seeks to evaluate the costs of fraud from the perspective of the producer or defrauded organisation. An example of the bottom-up method might be the use of administrative data on payment card fraud reported to APACS (in which the annual volume/value terms simply represent the sum of all reported frauds).
- *A 'top down'* approach seeks to estimate the economic implications of fraud from a national perspective. An example of a top-down method might be as follows: X percent of cheques appear to be fraudulent (perhaps determined through some sort of audit), the mean loss per fraudulent cheque is Y GBP, and Z cheques are used in the UK annually, so X*Y*Z would yield the cost of fraudulent cheques.[23]

Additionally, the issue of 'who bears the cost' is often a complex one. It is also one reason why the likelihood of double counting is a major concern in the fraud field. An individual who has been victim of an investment or pension fraud may understandably relay this fact in the course of a survey on fraud, but so too will any body that provided all, or part of, compensation to that individual for associated losses. This presents a significant challenge to aggregating the costs of fraud to the UK economy (discussed later in the present study).

Further, determining the true costs of goods and services obtained by fraud can present difficulties. There is little consensus, for example, on whether goods obtained by fraud should be counted at their wholesale price or retail price (with or without VAT). Published data on the opportunity costs of frauds – and publicity about frauds – to businesses, individuals, and 'the public as taxpayers' are rare or largely anecdotal, yet one might expect some such costs to be substantial. Moreover, certain types of fraud – for example those that facilitate terrorism or electoral impersonation/intimidation of postal voting – may produce immense collateral damage, but their estimation will be exceedingly difficult without rafts of

[22]The benefit of the top-down approach is that it conceptually recognises that there are other 'hidden' costs (i.e. externalities) associated with fraud. That is, parties other than the fraudster and the victim are affected by fraud. For example, a fraud risk premium is borne by the population at large as a result of a small proportion who have been subject to fraud, such as payment card fraud. In the case of public sector fraud, the externality is the opportunity cost of the resources defrauded (i.e. fraud affects the incentives and choice set of all taxpayers). Three significant conclusions arise from this review. First, the top down approach includes (or should) additional costs that must be added to bottom up costs. Second, simulation is one way of attaching a monetary value to these externalities (subject to data availability and data quality). Third, the analysis provides an indication of the externality cost per GBP of fraud in any given sector, so it helps to indicate where resources should best be focussed on crime reduction.

[23]If the costs of the fraudulent cheques are initially met by banks, they would want to recoup such costs by charging more for cheque services or levying a wider interest rate spread (competitive conditions permitting). In both cases, customers end up paying more. This is an externality.

assumptions[24]. That fraud may bring such costs to bear on the UK economy, however, should not be forgotten.

Other types of fraud may be perpetrated not specifically to defraud the system (i.e. not to generate income or cause a loss directly) but rather to gain access to services. For example, a fraudulent driver's licence may be used not to obtain money or goods in some sort of identity-related fraud but rather to gain access to the UK's road network and associated services, like motor insurance. If the fraudulent licence holder maintains a perfect driving record, then the visible marginal cost of the fraud (and of this type of fraud in general) is not great (perhaps losses to the DVLA for unpaid licence fees and the marginal strain on the road network from one additional driver) – though if the fraudulent licence holder is a bad or unlucky driver, costs (which may fall upon the Motor Insurers' Bureau and then upon legitimate drivers collectively) may be easier to identify (i.e. accidents are easier to perceive as a cost).

Also, the measurement of the cost of fraud to the UK economy has some jurisdictional issues which are not commonly addressed, but which are important to note. Partly because the terms of reference of the present research refer to fraud as it affects the UK, and partly because most corporations (not least financial institutions) do not readily differentiate between the constituent parts of the UK—the criminal justice systems not being part of their core business – the present research used as its jurisdictional boundary the UK rather than (as would be normal in ACPO or Home Office terms) England and Wales.[25]

In the main, the focus of the existing literature on fraud has been on cost issues, and little attention has been directed to the characteristics of offenders, or indeed the readiness of the public at large to engage in fraudulent activities. Where these issues have been covered, they have tended to be dealt with in separate studies, rather than as part of broader studies assessing the prevalence or cost of such crime. What little is known about the organisation of fraud and how common fraud offending is from research in this area is broadly summarised in Annex 6. Our beliefs (well informed or not) about the nature of the offender population makes a difference to our judgments about how threatening a social phenomenon is: however such issues cannot usually be approached through victim studies.

[24]And if the frauds are substituted by other types of fund-raising (from legal or illegal sources), the terrorist act may not be prevented.

[25]Further, UK individuals and/or public/private sector entities may be defrauded outside the UK (e.g. mugged for credit cards, which are used abroad) or in internet transactions where, in the absence of a specified legal place of contract, it may be difficult to determine the location of the offence. Conversely, some crimes against foreigners in the UK may have their primary economic effects on foreign card issuers. In most sources other than APACS card fraud data, it is unclear whether or not costs have been incurred purely within the borders of the UK. Frauds (and other criminal acts) against UK firms or people overseas, or indeed against foreign people or firms operating in the UK affect the UK.

3. FINDINGS

This chapter reports the key findings of the literature on fraud by victim sector, following the victim-centric typology of frauds (above, in Table 1), while a fuller account of the details of individual studies is provided in allied annexes. The chapter begins by presenting findings from the private sector, focussing first on fraud against the financial services sector, then on fraud against the non-financial private sector, and finally on fraud against individuals. The spotlight is then turned on the public-sector; findings are presented, in turn, on fraud against central bodies and then against local bodies.[26] Note that those gathering data on fraud have not hitherto sought to distinguish different types of victims in the way proposed here, and while some data sources fall naturally within one categorisation, others have spanned different sectors. In view of this, the sections below do not exactly replicate those presented in Table 1.[27]

The data below are principally from 2005, but the lag in awareness of longer-term frauds mean that some will date back years; and whereas the private sector data are generally based on calendar years, the public sector typically uses financial years, making impossible their integration into annual snap-shots. Where data for 2006 have become available, this has been added in footnotes; however for sound reasons, some data on tax fraud, for example, are available only for 2004-05 or even 2003-04.

A number of sources on fraud do not appear in the pages that follow. This is the case because their methods do not appear sufficiently sound to include in this critical assessment (e.g. little is known on the underlying data generating process and/or the internal sources and methods used to estimate the extent of fraud). This is not to suggest that the estimates of fraud and fraud costs in such sources are wrong, however, only that the research methods from which they are derived do not appear sufficiently sound, including for reasons of non-availability.

It should also be noted that certain of the sources below do not ultimately contribute to the aggregate estimate of the cost of fraud presented in the final section of the report. This is the case because the costs contained in such sources, while derived from sound social science methods, may be counted elsewhere (and to include them would be double-counting).

A. Victim sector 1: Fraud against the private sector

Sub- sector 1. Fraud against the financial services sector

As Table 1 and Box 1 indicate, the financial services sector is subject to a wide range of frauds, including payment card fraud, cheque fraud, insurance fraud, lending fraud, and so forth. Annex 4 lists the sources that provide information about fraud against this sector, and provides a summary of the methodological approaches they adopted.

Headline findings

The main findings for each of the reviewed studies are presented below.

1. **Fraud: The Facts (APACS, 2006):** Plastic card fraud losses in 2005 amounted to £439.4 million, down from £504.8 million in 2004. Plastic card fraud figures for 2005 comprise the following categories: card-not-present, £183.2 million; counterfeit, £96.8 million; lost/stolen, £89 million; mail-non-receipt, £40 million; and card ID-theft, £30.5 million. Cheque fraud losses in 2005 amounted to

[26]It should be noted that certain of these sources were also described in the Fraud Review (2006).

[27]The most obvious example is that data relating both to companies in the financial services sector and those outside it have been summarised under a separate heading.

£40.3 million, down from £46.2 million in 2004. Cheque fraud figures for 2005 comprise the following categories: counterfeit cheques, £3.2 million; forged cheques, £30.9 million; and fraudulently altered cheques, £6.2 million.

2. **CIFAS Online Press Releases ("£1,400 of Fraud Prevented Every Minute"; CIFAS, 2006a)**: For the period January-June 2006, the CIFAS database identified 85,128 fraud cases (up 12.5 percent from the same period in 2005); 122,633 subjects (up 16.2 percent from the same period in 2005); and £360 million in financial benefits.[28] As noted by CIFAS: Fraud cases refer to each instance of fraud identified by CIFAS members and recorded on the CIFAS database. Members must have sufficient evidence to take the case to the police, although it is not mandatory that they do so. Subjects relate to those people involved in the fraud case, whether this be the fraudster, an accomplice, or an innocent victim. Financial benefits refer to the amount of money that members reported that they have saved through being alerted to previous frauds identified on the CIFAS database, thereby reducing re-victimisation.

3. **CIFAS Member Consultation on Government Fraud Review (CIFAS, 2006b):** The CIFAS member consultation for the Fraud Review suggests that responding members spent some £70.4 million on fraud-prevention annually (though no specifics are offered, other than noting that this does not include fraud losses — some might have included expenditure on response to as well as anticipation of fraud within "fraud prevention"). An average annual spend per respondent (£1.24 million) is then used to estimate an annual spend for the membership in total, which CIFAS suggests is of the order of £300 million. It is unclear how this total might be affected by a different grossing-up from respondents to the membership (e.g. using turnover). Having ascertained that this is not double-counting, this study has added separately the card firms' expenditure on the police Dedicated Cheque and Plastic Crime Unit or the Fraud Intelligence Bureau, and the Finance & Leasing Association's Vehicle Fraud Unit and other police bodies.

4. **UK Commercial Insurance Fraud Study 2005 (MORI/Commercial Insurance Fraud Steering Group, 2005):** The survey suggests that annual losses in the commercial insurance industry equate to some £550 million, or an estimated five percent of commercial insurance premiums. Fraud losses are due to fraudulent claims by businesses against insurers and fraudulent claims against business insurance by employees, clients, and members of the public. It should be noted that in 2005, the commercial market was about one third of total business (excluding Lloyds of London), so retail insurance fraud – about which there are no valid published studies to date – would bring this total substantially higher.

5. **Finance & Leasing Association:** Administrative data supplied quarterly to the FLA by its motor finance members total £15 million in losses annually in 2003-06 (Home Office, 2006 and personal communication). No data are available on commercial leasing fraud losses or on the sectoral costs of fraud prevention, but the FLA spends £500,000 annually on funding public policing of finance sector fraud.

Summary

Four studies and one administrative data source which focus specifically on fraud against the financial services sector have been reviewed here (see Annex 5, Table 5.1, bearing in mind that a number of

[28]CIFAS data must be interpreted with caution. While the data are useful in illustrating the extent of fraud risks, financial figures do not relate to fraud losses, but rather to the amount of money saved through the CIFAS service. For this reason, CIFAS savings data have not been aggregated into the fraud cost totals, though they constitute a net economic benefit arising from collective fraud prevention investments.

sources presented in a subsequent section discuss frauds against financial services and other sectors combined). These studies represent the publicly available, methodologically sound sources which provide data on fraud volumes/values. In sum:

- **The most dependable data derive from the administrative data products.** These appear to be the results of coordinated exercises driven by sound counting rules and with clear concepts under measurement. Of additional benefit is the fact that these sources are released on at least an annual basis, if not more often, allowing for comparisons over time on a similar basis.
- **But the administrative sources are not without limitations**. The limitations of these sources relate to 1) the fact that they are derived from membership organisations, such that figures only relate to members, not the economy in full (though such organisations include most or all relevant organisations); 2) like with other sectors, generating sector-wide aggregate figures is complicated by overlapping concepts between sources of data; 3) there are overlaps between APACS and CIFAS membership (and also CIFAS, ABI and FLA membership), with consequent double-counting if sources are not used carefully.[29]
- **Certain sources derive from surveys based on opinions.** Opinions on fraud, while useful in certain contexts, are not nearly as powerful as hard administrative data on fraud losses when trying to generate an understanding of the costs of fraud. Also, such surveys are not carried out on a regular basis, and as such findings cannot illustrate changes over time.
- **Coverage of the financial services sector is not complete**. Though not any great surprise, data on certain types of fraud are simply unavailable (largely because studies have not been carried out on certain frauds, but also because certain sources remain confidential). It is therefore unclear if these types of fraud (e.g. embezzlement, procurement fraud, commercial leasing frauds etc.) are of only limited concern, or perhaps are of considerable volume/value but are simply under-researched, sometimes because of anxieties about information-sharing.
- **Cost data relate to primarily to fraud losses**: Data tend to be collected on fraud losses, and little data are available on costs in anticipation of fraud or prevention of fraud. Only the CIFAS response to the Fraud Review presents costs beyond fraud losses.

Sub-sector 2. Fraud against the non-financial services sector

A number of surveys have attempted to measure the prevalence,[30] incidence[31]and cost of fraud against businesses. Annex 4 lists the sources that provide information about fraud against this sector, and provides a summary of the methodological approaches they adopted. Most of the studies reviewed below measured fraud only as one component of the business experience of crimes, and did not devote much refined attention to sub-types of fraud. The data that are available on fraud have been collected by using survey research instruments in which management – either in individual businesses premises or in the head offices of businesses – are asked about their victimisation experience across a number of crime types.[32]

[29]Thus, for example, to avoid double-counting, if CIFAS data on actual frauds are used, applications frauds – sometimes referred to as 'identity frauds' – should be stripped out from APACS and other organisations for those firms that are members of both.

[30]Prevalence is the percentage of businesses from the sample that are victimised over a specific recall period – usually 12 months.

[31]Incidence refers to the average number of incidents experienced by businesses over the recall period. This is usually expressed as a rate per 100 or 1,000.

[32]Such crime types typically include burglary, criminal damage, vehicle theft, employee theft, customer theft, fraud, robbery and violence.

Headline findings

The main findings for each of the reviewed studies are presented below.

1. **Fraud against retailers.** *British Retail Consortium 'Retail Crime Costs' survey (2004-05):* Total cost of fraud to retail sector was estimated to be £68.1m in 2004 (as compared to £61.7m in 2003). Twenty-four per cent of all fraud losses were from cheque fraud (£17m), 20% from card payment fraud (£14.1m) and card not present fraud (£14m). The total cost of fraud per outlet in 2004 was £1,408 and the total cost per £1m turnover was £161. (Note that the losses are for fraudulent transactions not fully authorised by card issuers and therefore are excluded from APACS data.) There are no BRC data available on costs in response to fraud, though some data are available on crime prevention capital and revenue costs. In 2004 the average expenditure per store (capital) on chip and pin was £4,130 (compared to £1,756 in 2003) – this cost should fall in subsequent years.

2. **Fraud against retailers and manufacturers**. *Home Office, 2002 Commercial Victimisation Survey: 18% of retailers (n=715) and 8% of manufacturers (n=195)* were victims of fraud by outsiders. The highest prevalence rate for any sub-category of fraud was credit card/ cheque fraud (14.7%) for retailers, and 'others' (4%) for manufacturers. In both sectors, the overall prevalence rate for fraud by employees is lower than for fraud by outsiders, with 4% of retailers (n=147) and 2% of manufacturers (n=41) experiencing an incident.[33]The mean cost of fraud by employees for retailers was £7,398 and £12,759 for manufacturers. The mean cost of fraud by outsiders was £1,278 for retailers and £10,146. No data are presented in the CVS on costs in prevention in anticipation of fraud. Some data are presented on the revenue costs of security mechanisms though these cannot be attributed to specific crime types. No data are presented in the CVS on the costs incurred in response to fraud.

3. **Fraud suffered by member businesses in the Co-operative Movement**. *Co-operative Movement survey of its members*: Estimated that 5% of all losses to business were due to fraud and these cost approximately £170K (an average of £68 per outlet). Of these losses 56% were for cheque fraud and 40% credit/ debit fraud. Some data are presented on prevention and anticipatory costs. There was £3.3m capital expenditure on security and £14.8m revenue expenditure per year. This expenditure covers a variety of equipment (such as cash protection, EAS systems, alarms, cash security services, alarm monitoring etc) and it is thus difficult to attribute a total to expenditure in relation to fraud. However, except for later expenditure on adapting computer systems for Chip and Pin, few of these systems are fraud related. No data were presented on the costs of responding to fraud.

4. **Telecommunications fraud**. *Telecommunications UK Fraud Forum (TUFF)*: The estimated industry loss to all fraud was 2.4% of £36.1 bn of telecoms retail revenue in 2004, which equates to £866m. (43% of losses are estimated to be ID related subscription fraud, which equates to £372m). The fraud data assume that the phone calls made would have been paid for at full price, which is an arguable but very far from proven assumption. To that extent, it may be considered to be a high estimate. No data were presented on prevention and anticipatory costs or on the costs of responding to fraud.

Summary

In this section some of the main findings in relation to the data on fraud against the non-financial services sector are summarised. A number of studies have been reviewed here (see Annex 5, Table 5.2) that are able to provide some data on fraud that are both contemporary and enable us to draw some conclusions as to the nature of fraud in the businesses sampled. In summary:

[33]These data show similarities to the 1994 CVS, where 20% of retailers were victim of fraud by outsiders and less than 5% of fraud by employees. Rates of fraud by outsiders were higher for manufacturers in 1993 at 17%, though fraud by employees was still below 5% at that time.

- **Data are available on fraud against the non-financial services sector from a range of sources and agencies:** However the aim of most surveys is not to measure fraud exclusively. Some global surveys such as those by PWC do concentrate on economic crime – a vague but broader category than fraud – while others (such as the CVS and BRC) measure crime in general and the subsequent costs of crime, identified fraud being only a modest part of the whole.
- **The data are not routinely collected annually in each survey:** For example, the CVS has only been commissioned twice, though the BRC has run each year since 1993.
- **The sources use different methods:** For example, the Co-operative used a postal survey and the CVS used premises interviews.
- **The surveys cover different businesses sectors and thus some business sectors have a more extensive coverage others:** There tends to be a heavy focus on the retail sector, e.g. the BRC and CVS. Other sectors are covered, though often data are not disaggregated by sector. The data appear to be non-existent for the hotel/ restaurants sector, wholesale and transport communications, at least in recent years. Some data are available for these sectors from sources (such as the Scottish Business Crime Survey and the Small Business and Crime Initiative) not reviewed here due to their geographical coverage and the age of the data.
- **The surveys focus on businesses of differing employee size and turnover:** The focus of the BRC research is larger businesses with a large number of outlets. The CVS is a premises survey and has a large sample of smaller businesses.
- **The surveys measure different types and sub-categories of fraud:** Most survey research uses the label of 'fraud', 'fraud by employees' or 'fraud by outsiders' and these are then broken-down into subcategories. These sub-categories vary from survey to survey. For example, the BRC use the labels cheque fraud, card payment fraud, application fraud, card not present fraud and counterfeit notes where the CVS uses two categories of fraud: fraud by outsiders and fraud by employees. These categories are then broken down into further subsets, such as fraud by outsiders, credit card fraud, bounced cheques, long firm fraud, counterfeit bank notes. The labels used are likely to vary according to the business sector where fraud is being measured.
- **Cost data relate to transfer loss:** Data tend to be collected on losses to businesses and little data are available on costs in anticipation of fraud or prevention of fraud.

The differing methodologies used to measure fraud in the commercial sector therefore raise questions about:

- **Data reliability:** Longitudinal comparisons of data between the same survey (say for example, the BRC in 2004/05 compared to 2003/04) might yield reliable results as the method of data collection and the definition of fraud is the same- therefore a 'like for like' comparison can be made. However, it has been observed previously that premises based surveys can generate higher incidence rates and costs of crime than head office surveys. This is because incidents are not always reported to the head office of a business. In addition to this, fraud is a 'catch all' term used in many surveys and what respondents include in this term can vary. This raises questions about reliability of data between surveys and the accuracy of pooling/ aggregating several data sources together to make national estimates of losses to fraud.
- **Data validity:** Most survey research carefully defines the concepts that are being measured and 'difficult' terms used in questions asked to respondents. However, there is always a risk that respondents might be unclear about what is being asked. This might be particularly true for when measuring fraud (and its subsets of categories), as respondent knowledge and understanding of such concepts may vary (and their matching against legal terminology will vary). This might be particularly pertinent in smaller businesses or where English is the second language of respondents. To the extent that terms like 'false pretences' are used that are not routinely collected data categories by businesses, it is far from obvious how validity or reliability can be assured.

Overall, the data show that there are large variations in transfer costs of commercial fraud when

considered for the UK as a whole and by costs per business premises.

Sub-sector 1 and 2. Fraud against companies in both the financial services and non-financial services sector

In the previous sections, a number of studies have been reviewed that examine frauds against a clearly definable victim group – such as the public sector or financial services sector. In this section, studies of fraud against companies in both the financial services sector and non-financial services sector are reviewed. Annex 4 lists the sources that provide information about fraud against both of these sectors, and provides a summary of the methodological approaches they adopted.

Headline findings

The main findings for the studies are presented below – only some of these have been included in the totals, because of concerns about response validity, double-counting and about the grossing up of small samples:[34]

1. **Global Surveys of fraud where a number of UK businesses form part of the sample.** *PricewaterhouseCoopers (2006):* in 2005, 55% of the UK sample had been victims of tangible fraud (asset misappropriation, false pretences and counterfeiting) at an average cost of $800,000 per year (costs averaged over the recall period of two years). 300 interviews were conducted so without extrapolation, total costs would be $240 million (£120 million). No comprehensive data are available on prevention/anticipatory costs or costs in response to fraud, though the study acknowledges that there is 'collateral' damage and costs as a result of fraud, and that investigations within companies occur as a result of fraud, though no estimates of costs are given.

2. **Computer related crimes experienced by business.** *Hi Tech Crime Unit (2005):* A total of 9% of the sample had been victims of financial fraud and 6% telecommunications fraud in 2004. The financial impact of both financial fraud and telecommunications fraud were measured by getting businesses to estimate the costs in ranges. It was estimated that £690m was lost to financial fraud and £77.7m to telecommunications fraud in 2004. No data were presented on prevention and anticipatory costs or on the costs of responding to fraud.

3. **KPMG fraud barometer.** *KPMG (2006):* The main costs in relation to each sector in 2005 are outlined below. The barometer shows that the total costs in all fraud cases over £100,000 charged to court (222) were £942m in 2005, a large increase on the figure of £329m for 2004 (174 cases). For the commercial sector, the costs in cases over £100,000 totalled more than £41m (a reduction from the £104m reported in 2003).[35] To avoid double-counting of the same case over successive years, these data exclude cases whose costs were included in previous surveys. No data were presented on prevention and anticipatory costs or on the on costs of responding to fraud.

---

[34]For example, a study by RSM Robson Rhodes estimated that British businesses lost £32bn in 2003 to economic crime, with FTSE 100 companies losing at least £500m. Also that £8bn was spent trying to combat economic crime, though the basis for this is not clear. No data were presented on the costs of responding to fraud. However, although the £3 billion losses to large corporate respondents in 2003 may be correct, the basis for extrapolation to the whole business population is problematic and sparse information on fraud losses was asked for in the questionnaire, which does not clearly differentiate between losses in the UK and losses to the company originating elsewhere (e.g. to foreign subsidiaries). So although there were many interesting points raised by this survey, the cost estimate has not been included (and it would anyway have been impossible to ensure that there was no double counting with other studies that have been included). Ernst & Young fraud surveys in the UK are dated and, in recent years, provide little information about methodology.

[35]Data from the KPMG 2006 survey have recently been published. The 277 cases charged to court in 2006 were worth £837m, compared to 222 cases worth £942m in 2005. The value of frauds charged to court in 2006 was the third highest in the Barometer's history, although it was down from the level recorded in 2005 – when the figures were inflated by one case worth £260m on its own. (The implication here is that, excluding this outlier, the trend is still upwards).

4. **BDO Fraud Track Report.** *BDO (2006):* During 2005, 221 cases (formally recorded or prosecuted) were reported in official press notices and/or in the media with a total value of £981m (in 2003 it was £331m). By value, half of all this fraud (£500m) was in the Financial Services Sector, and a quarter (£260m) was in the Wholesale Sector. The highest value staff frauds were revenue diversion (£40m) and procurement fraud (£14m). No data were presented on prevention and anticipatory costs or on the costs of responding to fraud.[36]

5. **SFO Annual Report.** *Serious Fraud Office (2006):* During 2005-06, the SFO began with 68 active cases involving an estimated £2.06 billion 'at risk'. This figure includes amounts judged to have been intended as well as actually obtained: the latter data are not separated out and published. The SFO is a reactive organisation that, deterrence and incapacitation notwithstanding, is not set up to play a preventative role, so its costs in anticipation and prevention are zero. Its estimated resource costs (expenditure) for 2005-06 was £41 million, which excludes costs incurred by the police and other investigators working on SFO cases. Confiscation orders made (but not necessarily paid) totalled £14 million, but an unpublished proportion of that would go to compensate victims in those cases.

Summary

In this section some of the main findings in relation to the data on fraud against multiple victim types are summarised. Three studies have been presented and two help to highlight the total charges in such cases heard by crown courts. In summary:

- Both of the commercial studies add the total costs of frauds charged to or tried in criminal courts over the course of a year, though these frauds may have occurred over a variety of previous years. The KPMG study estimated that losses charged to court in 2005 totalled £942m (or £494m if the Government sector is excluded). The BDO Fraud Track Report estimated that the total in confirmed recorded or prosecuted frauds involved £981m. in 2005.
- The surveys allow for some comparison over time, given that data are collected on a consistent basis. Both studies suggest that fraud losses in cases dealt with rose in 2005. KPMG data showed a cost increase of 2.5 over 2003, whereas BDO data trebled in cost over 2003.
- Some of the data are routinely collected: the KPMG survey is conducted every six months, while the BDO data are collected annually.
- The sources use different measurement thresholds: The KPMG survey considers cases over £100,000 and BDO over £50,000.
- The SFO does not present cost of fraud data over time or broken down by victim categories (in aggregate form), and its cost of fraud data include sums held to be 'at risk' rather than actually lost: the ratio between the two is unknown.

A summary of the studies is presented in Annex 5, Table 5.3. Overall, the data presented here have a number of problems in terms of their reliability and validity in measuring the cost of fraud over a set period of time. As stated above, the KPMG and BDO studies only measure cases above certain value each year, and both would include SFO cases which by organisational working definition of 'serious or complex fraud' have a threshold of over £1 million (though including sums at risk as well as actual losses). More importantly, these data are sometimes misleadingly reported in the media to suggest that they represent trends in fraud: they do not. They represent trends in the recording and/or taking to criminal court of frauds that were committed at various times, investigated over varied lengths of time, and may have been prosecuted after varied elapsed times due to delays in the availability of evidence

[36]Data from the BDO 2006 survey have recently been published. Media-reported business fraud over £50k is up almost 40 per cent by value to £1.37 billion in 2006 (from just under £1 billion in 2005), and the number of media-reported frauds worth over £50,000 rose by a third to 295.

from overseas or of suspects for interview or trial. They therefore cannot properly be compared with surveys or administrative data involving frauds happening within a particular year.

Sub-sector 3. Fraud against private individuals

As Table 1 and Box 1 indicate, individual members of the public are subject to a wide range of frauds, notably the broad range of categories covered under the label 'consumer fraud' (from 'phishing' to 'pharming'), through to frauds involving counterfeit money, investment and pension-type frauds. While many of these frauds are widely documented in the electronic and print media and specialist press[37], the frequency with which they occur and the loss that results is very poorly researched. This seems to owe much to the fact that while assessment of the extent of fraud in the corporate sphere can – if perhaps indirectly – yield business opportunities, any similar 'payback' from such endeavour in relation to crimes against particular individuals is unlikely, though collectively, the purchase of anti-virus software and shredders amounts to significant sums[38] (which are not readily deduced from published corporate accounts).

Another particular difficulty with a number of the frauds against private individuals is that there are blurred lines of responsibility. The banking industry, for example, is generally keen to promote internet banking as a means of reducing costs and typically assure the users/potential users of their services that they will not be liable to the costs of any fraud (unless, of course, the customer is complicit in this or is negligent, for example writing down their PIN).[39] On-line banking fraud attacks are however proliferating rapidly – to the extent that an estimated 150 million spoof 'pfishing' emails are sent each month in an attempt to obtain passwords.[40] In consequence, APACS has led a campaign of public awareness (alongside its awareness-raising around identity theft); indeed at least one bank now offers free anti-virus software to bolster its customers' defences. A growing issue that affects the distribution of costs but not perhaps the total amount of fraud[41] is whether customers or banks will pay losses in cases where customers – despite warnings on bank websites and in the mail not to do so – give out their full bank and/or other personal details to phishers.

Some frauds against private individuals fall within compensation schemes that tend to be the only data reported, since traditionally, there has been no common receptacle/reporting body for unauthorised high

[37]An example is that those selling cars through Exchange and Mart receive warnings that they should not part with their vehicles until any personal or building society cheques have cleared (not just shown in their account) and moreover that they are very likely to receive offers from buyers who will send agents to collect the vehicle and provide apparently secure bankers drafts in payment: drafts that will then prove to be fraudulent. The resource costs of such media warnings will be very modest but the prevention benefits may be substantial.

[38]One might try to obtain these from the published accounts of firms such as Fellowes, Argos, etcetera, but the task of separating sales motivated by fear of fraud from sales motivated by the desire to keep computers going or preserve confidentiality of papers would not be deducible in this way. One could look at the increased sales following 'identity fraud awareness week' (for shredders) and 'get safe online week' (for computer security, though the effects of the latter might expect to be phased in more slowly). Omnibus or BCS interviews could be used to examine the extent to which fear of fraud motivated anti-fraud measures.

[39]This situation is analogous with the position of credit card providers who are keen to promote usage of their product but also have to bear the bulk of losses: under the Consumer Credit Act, section 75, credit card companies are "jointly and severally" liable with providers for the goods the customer buys.

[40]"Don't feed the phishers". The Sunday Telegraph, September 24, 2006.

[41]Frauds may be reduced if having customer liability makes customers more careful at keeping documents and personal identification details safe. There is insufficient published evidence to enable people to know whether it does have this effect. Of course, financial institutions and other bodies sometimes send out literature containing personal information that can be misused: measures to reduce such information should also have an impact on the scale of fraud by opportunity reduction.

yield investment schemes or other scams. Although the demographics of individual victims add something to data available from APACS and CIFAS, the most recent review of crime statistics asserts (Walker *et al*., 2006: 161) that "fraud is mainly a crime against commercial organisations and therefore not thoroughly investigated by the BCS." [42] (Though the Office of Fair Trading, 2006, subsequently estimated that 6.5% of people fall victim to scams annually, suggesting that this view may require revision. A study of EU countries in the 2004 International Crime Victimisation Survey indicated that the percentage of people experiencing consumer fraud was 7.7 per cent in England and Wales, 7.8 per cent in Northern Ireland and 6.4 per cent in Scotland -van Dijk *et al*., 2007; see also van Kesteren *et al*., 2001).

Indeed, neither the BCS nor the OCJS review anything approaching a broad spectrum of fraud experiences, and the Bank of England data do not distinguish between losses of counterfeit money to private individuals and those to banks and retail businesses.[43] Other uncosted areas of socially significant fraud against private individuals include charity frauds: the latter also has collateral damage or externalities, insofar as if such frauds are exposed and/or believed to be likely, people may stop future donations.[44] Whether the consequences fall within the UK depends on how this is constructed: poverty reduction in the developing world is an objective of the Department for International Development (DFID), so this might be an argument for relevance.

Annex 4 lists the sources that provide information about fraud against individuals, and provides a summary of the methodological approaches they adopted.
Headline findings

1. **OFT Scams Survey (OFT, 2006):** Some 6.5% of the population fell victim to scams in the previous year. In repeat victimisation terms, victims had a 30 per cent chance of falling for another scam in the following year. The average loss was £850 per scam (per person losses are affected by repeat victimisation), though this average was distorted by some very expensive losses, and half the losses were £14 or less. Average losses varied from £5,660 for high risk investment, £5,000 for African advance fee and £3,030 for holiday club scams to less than a hundred pounds per scam for premium rate telephone and miracle health scams. On the basis used by the OFT of multiplying victimisation levels by average cost, the total cost of scams was £3.5 billion in 2005 (with a 95% confidence interval, range from £2.75 to 4.26 billion): this report has taken the low end figure of £2.75 billion.

---

[42]The BCS is not particularly helpful to this research exercise on fraud costs and will not be reviewed in detail here. One might count worry about crime as a cost of crime, but though the 49 per cent of cardholders who in 2003-04 worried about fraud may be of concern to government as well as to the private sector, they are not a cost to economic welfare unless they need psychiatric or medical care. (Though if economic welfare were measured by the sense of well-being, this would constitute economic harm – see Layard, 2006.) Recent surveys (e.g. for GetSafeOnline, 2006) have shown increased concern about identity fraud, but the questions do not differentiate whether this leads some to total or just occasional avoidance of e-commerce. Three per cent of the BCS respondents had actually been victims of card fraud during 2003-4, and though the combined victimisation/ offending report (Wilson *et al*., 2006) does not state whether their losses were gross or net, they were almost certainly gross: however there would have been (uncounted) telephone, letter and opportunity costs in addition. Unavailable data on the future behaviour of cardholders might throw some light on the externalities with respect to financial services industry, suppliers of goods and services, and cardholders themselves. (Expenditure on shredders and on anti-virus software would be part of the costs of responding to future fraud: but these costs are not available in the literature.)

[43]Informal judgment suggests that around three quarters of counterfeit notes recovered (and not destroyed by recipients in the knowledge that they are worthless) are losses to banks and their cash-handling intermediaries. The remainder will be to private individuals and retailers, most likely the latter.

[44]Though there are no hard data, interviewees from charities in related areas have noted falls in donations following revelations about fraudulent operators (e.g. BBC radio 4 programme 'You and Yours' 28 September 2006 on alleged fraud involving a Scottish breast cancer charity operator).

2. **FSA 'boiler room' study (FSA, 2006):** The average loss of those motivated to complain to the FSA and fill in the questionnaire was £20,000, with substantial regional variations that might be due to chance. It is not possible to deduce from this what total UK actual losses are from boiler room operations.

3. **CIFAS identity fraud study (Pascoe *et al.*, 2006):** No cost data were obtained. Over three quarters of victims had experienced more than one offence against them (though this may have been why they ended up registered as an identity fraud victim). Over half of the respondents spent less than 24 hours rectifying the situation, significantly less than times given in US-based studies: but 11 per cent took longer than a week and given the small number of respondents, this skewed the average time to 201 hours. About a half of the victims (but fewer victims over 61 and with higher incomes) said that their experience had a big impact on their stress and health levels, and slightly more claimed that it caused them great inconvenience. Levels of inconvenience caused and impact on health or stress levels increased with the time it took to rectify the situation. When asked about personal losses, 17 per cent stated that they had suffered financial repercussions through having to pay postage, make telephone calls, or use printer ink/fuel etcetera in contacting agencies about their case and in replacing documentation.

4. **Fraud involving solicitors and company pensions:** On conservative inference from mixed fraud/ solicitors' insolvency data, a minimum of £16.5 million per year is lost by private individuals as a result of fraud involving solicitors. In the seven years to 2004, only four cases of fraud were discovered and less than £600,000 was paid out to company pension fraud victims by the (then) Pensions Compensation Board.[45]

Summary

Very patchy data are available on the costs of fraud against individuals. One of the professional motives for assessing fraud against business – the scope for service provision in investigation and prevention – is normally absent in this sector, except for due diligence in the wealth management of high net worth individuals (which is tantamount to a business operation). The 'scams', 'boiler room' and 'identity fraud' studies reviewed here show evidence of levels of fraud that are substantial in relation to other types of crime, but it is not possible currently to extrapolate from these exercises to losses in general, since it is not known what proportion of victims or people who are annoyed at being pressurised contact the FSA. Unlike crime victims, who may be motivated to report (genuine or false) crimes so that they can claim on insurance, there is no financial benefit to reporting cases 'outside the perimeter' to the FSA, since the Financial Services Compensation Scheme only covers losses to FSA-authorised bodies. Additionally:

- Only the OFT study has good data on the economic cost of these frauds (and does not deal with the externalities arising therefrom).
- Administrative data from compensation bodies are sometimes difficult to attribute to fraud, since they are primarily concerned with compensating for the insolvency of authorised firms.
- Radio and television programmes on 'rogue trading' reveal widespread deception of customers by a variety of trades, none of which activities appear to be costed by surveys (including the OFT 'scams' study) and which are not the 'property' of any particular agency other than local Trading Standards Authorities.
- Largely business-loss focussed studies of intellectual property and other counterfeiting by 'organised crime' and terrorist financiers do not differentiate between the overall crimes/losses to business and the deception of/direct harm to customers. Though product quality is sometimes lower than they expect,

[45]Parliamentary Debates HC 20 May 2004: Column 1139. The episodic nature of such events illustrates the perils of using a purely annualised basis for fraud risk calculations. If recent European legal rulings are translated into UK practice, the payouts may increase substantially, but although some failed companies may be dealt with for wrongful or even fraudulent trading, the attribution of company pension losses to fraud would remain controversial.

most consumers of counterfeits know that they are not buying genuine products and therefore are not deceived. Since there are no separate data on the amount of deception in this context and because industry estimated losses make the implausible assumption that most purchases of counterfeits would have taken place for legitimate products at full price, they have been excluded from this review.
- Some frauds against individuals (such as pension fund and other long-term 'mis-selling') may take years to materialise, if the victims are ever aware (in the less egregious cases) that they have been deceived 'dishonestly', as the criminal law requires. Pragmatically, in terms of getting ongoing businesses to compensate wronged individuals, it may be better to treat deception of financial services customers as 'mis-selling' rather than fraud: but difficulties with corporate criminal liability apart, the extent of fraud may be significantly greater than that identified.

B. Victim sector 2: Fraud against the public sector

The public sector has become more complex, with the relative autonomy of Non-Departmental Public Bodies, and with the growth of anti-fraud bodies such as the Audit Commission's National Fraud Initiative and the NHS Counter-Fraud and Security Management Services. Within the classic public sector, bodies are either classified as 'central' (audited by the National Audit Office) or 'local' (audited by the Audit Commission).

Sub-sector 1. Fraud against national bodies

As Table 1 and Box 1 indicate, the national bodies in the public sector are subject to a wide range of frauds, notably benefit and tax fraud, procurement, insurance fraud, lending frauds and payment card frauds. Annex 4 lists the sources that provide information about fraud against this sector, and provides a summary of the methodological approaches they adopted.

The identification of fraud in the public sector is affected powerfully by data-matching, and the biennial National Fraud Initiative operated by the Audit Commission can data-match 100 per cent of local (but – subject to enhancements proposed in the Serious Crime Bill 2007 – not all central) government expenditure against all subscribing sources, looking for example at people who are claiming benefit without disclosing that they are receiving other benefits or are working in another geographic area. In 2004/05 the number of participating public sector bodies contributing data was just under 1,300, an increase of 12.7 per cent on the NFI 2002/03. Unless fraudsters are deterred or simply stopped from earlier matching exercises, it should be surmised that this expansion alone should produce more identified public sector fraud.

Headline findings

1. **Frauds against government departments.** *(HM Treasury, 2006):* Excluding other areas of benefit and tax fraud (discussed separately below), the total volume of identified and reported (to HM Treasury) fraud against central government, 2005-06, is very modest in scale, as it has been in the past:
   - 26 departments reported 780 cases of internal fraud or theft with losses totalling some £5,109,400;
   - 19 bodies stated that they had no cases of fraud or theft to report.[46]

2. **Benefit fraud.** *(Department of Work and Pensions (2005a, 2005b, 2005c; 2006a, 2006b, 2007):*[47] During 2005-06, benefit fraud losses were estimated at £0.5 bn. (based on the low point, as per the

[46]In 2004-05, 17 out of 46 central government bodies provided 'nil' returns (i.e. had no cases of theft or fraud to report); 29 bodies reported 450 cases of internal theft or fraud with a total value of £3,136,900.

[47]The DWP (2007) definition of fraud includes all cases where: (i) the basic conditions for receipt of benefit, or the rate of benefit payment, are not being met; (ii) the claimant can reasonably be expected to be aware of the effect on entitlement; and (iii) benefit stops or reduces as a result of the review.

practice adopted here), or £0.7 bn. (based on the mid-point of the range). More specifically, these included:

- £140m in income support
- £20m in jobseekers allowance
- £40m in pensions credit
- £0m on State retirement pensions
- £10m to incapacity benefit
- £70m in housing benefit
- £40m in disability living allowance
- £40m. in carers' allowance
- £20m. in instrument of payment fraud
- £10m. in interdependencies

Benefit fraud estimated by the DWP halved between 2003-4 and 2004-5 to £0.9 billion and then fell further in 2005-06 to £0.7 billion (or £0.5 bn. on the low point estimate used in this report's summary). The decrease results from a combination of the overall improved accuracy of the estimates (historically, the Department of Work and Pensions' now abandoned estimates of suspected fraud dwarfed confirmed fraud), plus an unknown amount of reduction resulting from anti-fraud activities. Given a stable and improved methodology, future fraud levels may be a better reflection of changes in underlying behaviour.

3. **Tax credit fraud.** *(National Audit Office, 2006; HMRC, 2006b):*
   - £70 million was lost in 2003-04 due to 'likely fraud' by individuals
   - £131 million was lost in 2005-6 due to organised fraud
   - 143,000 suspected fraudulent tax credit claims were stopped, indicating the scale of potential loss, claimed to be £409 million in 2005-06
   - HMRC estimates that claimant error and fraud resulted in between £1.06 billion and £1.28 billion (8.8 to 10.6 per cent by value) being paid to claimants to which they were not entitled.

4. **Indirect tax fraud: Missing Trader Intra-Community Fraud.** *(National Audit Office, 2006c; HMRC, 2005b, 2006b)*: The results for the net theoretical tax liability, receipts and revenue loss for 2003-04 and 2004-05 show that in 2004-05 there was a revenue loss gap of £11.3bn, an unknown proportion of which is fraud.

   The impact upon receipts from MTIC fraud in 2005-06 seems to lie between £2 bn. and £3bn. It is widely acknowledged that losses rose much higher in 2005-6, albeit falling in the latter part of 2006. No individual piece of research could be used to make improvements to the methodology for MTIC carousel fraud adjustments to the trade statistics, but collectively all the research undertaken suggests that HMRC is on the right lines. With so many legitimate but unquantifiable causes of differences between the various available data sources, it was impossible to develop a robust methodology for generating even an aggregate estimate for acquisition fraud let alone a commodity by country breakdown; whereas for MTIC carousel fraud, information uncovered during HMRC's operational activity help with the estimation. HMRC's on-going asymmetries studies – comparing another country's declared trade with the UK's trade statistics – produce an analysis of annual asymmetries for the ONS, updated each quarter, which provides indications of changes in the reported discrepancy, which could be fuelled by MTIC. It can also identify changes in the product make-up of any discrepancies. However, the review indicates the importance (not solely to the UK) of more rigorous pan-European trade statistics and checks.

5. **Indirect tax fraud: Fraud relating to alcohol, tobacco and hydrocarbon oil consumption.** *(HMRC, 2005b, 2006b):* In 2004-05, fraud involving cigarettes was estimated at £1.9 bn; Hand-Rolled

Tobacco, £0.832 bn; and hydrocarbon oils, £0.350 bn. (HMRC 2006b, 2006c).[48] Customs' estimate of spirits fraud in 2001-02 ranged between £330 million and £1,080 million; Scotch Whisky Association estimates ranged between £10m and £260 million, though Goddard and Compton (2005) pointed to an error in its analysis of underlying data which could affect the validity of this estimate. The National Audit Office (2006c) concluded that the underlying data used and the modelling undertaken by both Customs and the Scotch Whisky Association in estimating spirits fraud were defensible in their own terms, and Goddard and Compton (2005) stated that closer judgment was not yet appropriate.

6. **Frauds relating to vehicle excise duty.** (Driver and Vehicle Licensing Agency, 2005, 2006): In the June 2005 survey, the evasion rate was 3.6%, equating to a revenue loss of £0.147 bn.[49]

7. **TV licence evasion.** (TV Licensing, 2004): In 2004/05, £2.94 bn. was collected and the evasion rate was an estimated 5%, with estimated losses totalling £0.145 bn.[50]

8. **NHS Fraud.** *(Fraud Review, 2006; National Health Service, 2006, 2007):* In total, it is estimated that £76m (£0.076 bn.) was lost to patient fraud in 2005-06.[51] In more detail, it is estimated that:

   - £47m was lost to pharmaceutical patient fraud in 2005-06, compared to £117m in 1998-99.
   - £21.1m was lost to dental patient fraud, compared to £40.3m in 1998-99.
   - £8.2m was lost to optical patient fraud, compared to £13.2m in 1998-99.

   Against these fraud costs, in 2004-05, the amount of money recovered by the NHS CFSMS was £26.9m (up from £7.1m the previous year, largely due to successful civil actions against pharmaceutical companies for breach of duty.) It is also estimated that the NHS spends £22.2m (based on 2004/05 costs) on countering fraud, which is 0.028% of expenditure (Fraud Review, 2006); of this, £8,412,021 was spent on local counter-fraud work in 2005-06, a million more than the previous year (NHS, 2007).

9. **EU fraud.** (European Court of Auditors, 2006, National Audit Office, 2006d; Rural Payments Agency, 2006; DARDNI, 2006; OLAF, 2006): There are no readily deducible plausible estimates either of the scale of fraud against the financial interests of the EU or of the economic impact of this upon the UK. In terms of frauds investigated by UK agencies, DARDNI (2006) data for Northern Ireland indicate that in 2005-6, the counter-fraud unit dealt with £84,000 of internal fraud that was agriculture-related and 42 cases of external fraud and irregularity costed at £370,000, totalling £454,000. No equivalent data are published for England and Wales, nor are resource costs of dealing with fraud and irregularities published separately. During 2004, the United Kingdom reported to the European Commission's anti-fraud body OLAF 841 cases of irregularities (including fraud), representing some €48 million (£33 million), a drop of six per cent compared to 2003. There is no separate figure available for the level of possible or proven fraud.[52]

[48]These losses for 2003-04 were estimated to be: for Spirits, £250m; for Cigarettes and Hand-Rolled Tobacco £2.9bn; and for Hydrocarbon Oils, £0.6 bn.

[49]In 2004, 3.4% of vehicles were not licensed, equating to a loss in revenue of £0.129 bn.

[50]In 2003/04, £2.798 bn. was collected in licence revenue, and the evasion rate was an estimated 5.7%.

[51]This compared to £170.5m in 1998-99.

Summary

Frauds against the public sector can fluctuate wildly, depending on the state of internal controls and offenders' capacities. Departmental annual reports may conceal large variations within any year and be only a modest guide to fraud levels in the previous or in the next year. Some major initiatives – such as Individual Learning Accounts – have had to be closed down altogether partly because of fraud levels and are too old to be included here; others, such as tax credits and VAT/MTIC, have had to be drastically altered in their service delivery as a response to the (late) identification of, and/or response to, fraud risks. So because of the dynamics of fraud and the elapsed time to official awareness, forecasting of fraud costs (and of demand for policing, whether or not involving 'the police') is hazardous.

The main findings in relation to the data on fraud against central government are summarised in the table below. A number of sources of data have been reviewed (detailed in Annex 5, Tables 5.4 and 5.5). These studies are those that are both contemporary and enable some tentative conclusions to be drawn as to the cost of fraud across a number of public sector bodies. In summary:

- Data are available on fraud from a range of government departments and NDPBs;
- The data are not however comprehensive, especially in relation to income tax evasion and some of the difficult-to-determine boundary between legitimate corporate tax avoidance and evasion;
- The data are not routinely collected annually;
- The sources use a range of different methods to assess the frequency and cost of fraud;
- Many of the figures are based around 95% confidence levels and are thus broad estimates;
- In the field of benefit fraud, it is often difficult for people other than the claimants themselves to determine in any one instance what is fraud and what is error (for example on 'failure' to notify 'change of circumstances');
- There is a general absence of data both on the resource costs of responding to fraud and on the externalities generated by these responses (e.g. controls on VAT registrations and VAT reimbursement, taken in order to reduce the direct costs to taxpayers of MTIC fraud).

[52]Reviewing data on the EU as a whole, during 2004, the 25 Member States reported to OLAF 9,475 irregularities, including possible fraud, with a value of €983 million (£667 million). Excluding those reported by the ten new Member States, the total was £664 million, five per cent by value up on 2003. There was a decrease in reported fraud costs in the categories Traditional Own Resources and the Common Agricultural Policy. However, there was a 40 per cent rise in the value of cases of irregularities reported for Structural Measures, in part due to more reports from Italy and Greece. It is not possible to infer whether this represented a real rise or merely a rise in awareness and/or willingness to take action. In its report for 2004, OLAF assessed the effect of fraud on the Community budget based on estimates provided by Member States and its own analyses. OLAF estimated that, for agriculture, suspected fraud amounted to some €11 million (£7 million) and for Structural Measures to some €118 million (£80 million). During 2004, therefore, the estimated value of reported fraud in these areas was at least €129 million (£87 million), spread between the member states. In reporting these figures, OLAF noted that it was difficult to attribute specific fraud levels to specific years when projects are spread over several years.

OLAF (2006) asserts that one can only attribute losses to 'fraud' at the end of legal proceedings: on this logic, the fewer the prosecutions (especially in large, expensive cases), the lower the fraud. As regards own resources, suspicions of fraud account for approximately 20% of the cases of irregularities notified in 2005 and involve an amount of some €95.2 million. For agricultural expenditure, suspicions of fraud account for approximately 13% of the cases of irregularities notified, involving an amount of some €21.5 million, equivalent to 0.05% of the total EAGGF Guarantee Section appropriations. For the Structural Funds, approximately 15% of the irregularities notified and involving an amount of €205 million were attributed to fraud and accounted for some 0.53% of the total appropriations for the Structural Funds and the Cohesion Fund. For pre-accession funds, fraud accounted for approximately 18% of the irregularities notified and involving an amount of some €1.77 million, equivalent to 0.06% of the total appropriations under the PHARE, SAPARD and ISPA funds. This estimate is based on the information reported by the Member States, but must be treated with caution. Divided by the number of member states and taking into account complex funding formulae, it will be appreciated that these sums represent quite modest totals for the UK's share of EU fraud. Given the haphazard ways in which the data were generated and the difficulty of finding an appropriate formula, this study excludes the EU fraud data from the total.

Sub-sector 2. Fraud against local bodies

As Table 1 and Box 1 indicate, local bodies in the public sector are subject to relatively few specific forms of fraud that have not been highlighted in the previous commentary. Local authorities do however act as distributors of housing benefit and therefore are a conduit for controls of housing benefit fraud. They are moreover as vulnerable as any corporate entity to the normal range of frauds, from procurement fraud or embezzlement through to payroll frauds such as payment of 'ghost workers'. Annex 4 lists the sources that provide information about fraud against both of this sector, and provides a summary of the methodological approaches they adopted.

Headline findings

Council tax fraud. *(DWP, 2006a, 2007):* Council Tax fraud is estimated at £40 million – 1 per cent of expenditure (DWP, 2007), but this has not been measured by the DWP and it is simply assumed to have the same levels of fraud as housing benefit, on the grounds that it shares many characteristics with it.

Summary

All local authorities operate anti-fraud and corruption strategies and, as a part of this strategy, internal audit sections investigate suspected cases of fraud and financial irregularities in relation to benefits, council tax and other payments. But while it is clear that local authorities experience fraud, details of the extent, nature and cost of any such fraud are not routinely published: anti-fraud units only investigate individual cases and do not make overall estimates of resource costs to the authority. Some of these losses are accounted for in central government statistics, but there also appear to be significant omissions.

There are also no details of the costs incurred in fraud detection and prevention.

4. DISCUSSION AND RECOMMENDATIONS

So what does the REA indicate about the nature, extent and costs of fraud in the UK? What evidence is available about these issues, and is this 'fit' for any policy-making, strategic or operational purposes for which it might be needed? This section first sets out the implications of the REA. It then addresses strategies for future data capture.

A. IMPLICATIONS OF THE REA

The fraud literature is reasonably substantial and certainly heterogeneous. The sources of data reviewed in this study included:

- Global surveys of crime, which tend to focus upon larger enterprises, from which UK data can be drawn.
- National level surveys, which often but not always consider smaller enterprises.
- National administrative data collection exercises compiled by umbrella organisations, focussing on particular types of fraud within their remit.
- Data on 'fraud trends' derived from the value of fraud cases heard in court.
- Public sector fraud studies derived from samples of activity, some developed over several years, and from data-matching across public sector bodies.
- Studies of fraud against individuals, based around reported cases and, occasionally, general victimisation samples and data from trading standards and anti-counterfeiting trade bodies.

Self-evidently, there has not been the kind of centralized effort into estimating the extent of fraud that there has been into other areas of unreported and unrecorded crime, nor has there been significant effort made to drill down into the social and economic costs of fraud. The financial services industry – the employer of around one in five working Britons – has been neglected by both sweeps of the Commercial Victimisation Survey, while the British Crime Survey and the more recent Offending, Crime and Justice Survey have only recently focused on fraud, and then largely on payment card fraud, intellectual property violations and low to medium-tech crimes. In this climate, it is not surprising that something of a 'free market' in information about the cost of fraud has developed, with each successive study—however carefully or poorly conducted – being acclaimed for its news about the rise in fraud (and particularly 'hi-tech' forms of fraud): putting pressure on bodies never to come up with a lower figure, even if that lower figure is still much greater than the cost of other sorts of crime. In the context that the government has already faced some difficulties in persuading the media and the public to take at face value even the most carefully conducted analysis of crime trends (see Statistics Commission, 2006), it is not surprising that most of the data available have to be viewed as highly deficient.

Coverage of fraud against different types of victim

'Fraud' is a misleadingly simple term that, in reality, covers an extremely wide and varied set of:

- behaviours (involving direct personal contact at one extreme, to global impersonal contact at the other);
- victim characteristics and impacts;
- length of time to awareness as crime/loss by victims or bystanders;
- investigative costs and time before deciding to report/not to report;
- ages, and criminal backgrounds, of offenders;
- jurisdictions (in the process of offence commission and/or in the laundering of the proceeds).

To impose a logic on the task of cutting a path through this jungle, this study adopted a 'victim-centric' approach to reporting the literature on fraud, driven primarily by the fact that it is the loser who has the motivation to tackle the problem, but also to enable readers to think through the extent to which 'ignoring fraud' is the result of a rational decision either that 'it' is not important, or that there is some kind of 'market failure' in current responses. The victim-centric typology has often proved difficult to apply retrospectively (largely because studies seldom neatly deal with one class of victim) and indeed the task of identifying the loser in a fraud is often far from straightforward. But the approach has facilitated a systematic assessment to be carried out of what is known, and what is not known, about this crime.

The data on frauds suffered by the private sector are—in some spheres—highly informative and useful. Some private sector bodies (notably APACS and CIFAS) have worked hard to provide reliable and valid data on the frauds faced by their members, and the ABI is following on this path, though with a more diversified industry and inherently more difficult judgements to make about where conduct lies along the axis of confirmed fraud/suspected fraud/honesty.

The data from APACS and CIFAS are virtually unique in that they result from the administrative record-keeping of members (summary data filed with APACS, and from specific reports filed with CIFAS, who therefore act as direct 'data administrators'). These data appear to represent faithfully the frauds faced by their members, and are suggestive of the fact that administrative data could be (and are, in the case of CIFAS) used tactically to prevent fraud/in response to fraud. APACS receives data in more summary form from its members, who forward their own selected cases to the police for their consideration for action;[53] APACS (and the card schemes) also use the summary data to evaluate strategic interventions and policy.

By contrast the data available on fraud affecting businesses outside the financial services sector are largely derived from surveys, and their value has thus to be restricted to policy development and more strategic crime reduction approaches. The coverage of these data—both in terms of business sectors and different types of frauds—is patchy.

Fraud against private individuals has received very little attention in any of the studies, being covered neither in the corporate fraud surveys nor in the public sector reviews. The BCS has examined a limited range of victimisation (mainly card and other 'identity fraud'), and the International Crime Victimisation Surveys (ICVS) included questions to individuals about consumer frauds and corruption (though on a modest sample size). The FSA study of market abuse (Dubow and Monteiro, 2006) does relate to fraud on individuals but at a fairly abstract level. The work on 'scams' by the OFT (2006) is promising but does not cover some slower-developing forms of fraud, and quite apart from any issues of when (if at all) 'knowledge' that one has been defrauded crystallises, the sample size may be too small to pick up rarer types of scam.

In the public sector, while the issues are somewhat different, there is much the same variation in the availability and quality of data on fraud. Tax fraud is (and probably always will be) a far more significant problem than any other single area of public or, for that matter, private sector fraud.[54] VAT/MTIC frauds appear to be the largest single category, although estimates of the extent of MTIC – which in recent years has been highlighted as a cause of significant distortion in the balance of payments – have fluctuated by billions of pounds in recent years, making historic data a poor guide to an understanding of the

[53] This usage was demonstrated in March 2002 with the establishment of the Dedicated Cheque and Plastic Crime Unit (DCPCU), a specialist police unit – then jointly funded by the Home Office and APACS, and drawing primarily on the latter's data sources – to target these forms of crime (see Burrows *et al*, unpublished). Currently, the DCPCU is funded entirely by APACS at £2 million p.a.

[54] But dedicated resource costs in investigating it are harder to identify than in the DWP and in housing benefit investigations in local authorities.

contemporary scale of problem, while non-PAYE income tax fraud (see NAO, 2003) does not appear to have received much attention in recent HMRC or Public Accounts Committee reports.[55] Though MTIC fraud rose dramatically in recent years, it would be surprising if the total of income tax fraud were much lower than VAT fraud 'normally', and the inclusion of income tax fraud figures (as was done in the NERA study) would make a significant difference to the total fraud figure. Levels of fraud reported by government departments and NDPBs to HM Treasury (2005, 2006) seem very low, and reporting criteria may have been interpreted very cautiously by respondents: this might include defining contractor fraud as 'corruption' rather than 'fraud'.

Considerable progress has been made in specific fields. The Counter-Fraud and Security Management Services of the NHS have made very significant strides in analysing their fraud problems and the Audit Commission's National Fraud Initiative has demonstrated fraud levels by data-matching all local government, NHS and London Transport payrolls and payments against benefit claims and against each other. This would be even more accurate (and offer preventative dividends) if more central government departments were included in this matching (as proposed in the Serious Crime Bill 2007). Although the latter strategy continues to show dynamic benefits, however, by revealing patterns of contract-getting in different parts of the country, it cannot easily pick out very costly procurement corruption and price-fixing.[56]

Estimating the overall cost of fraud?

Despite the shortcomings in the data on fraud, the sources referred to in this report give an indication of the scale of fraud losses experienced (that is, transfer costs – as opposed to costs of prevention and of responding to fraud after the event [57]) in each of the five 'victim fields' that have been highlighted. It suggests that – taken from studies that are reasonably well designed and applying figures at the lower end of the error range[58] – losses amounted to:

- For businesses in the financial service sector: £1.005 billion
- For businesses in the non-financial service sector: £0.934 billion
- For businesses generally (not distinguishing sector, additional to those given above): £1.821 billion
- For private individuals: £2.75 billion (though not all of these would have met criminal fraud proof standards)
- For public bodies at the national level: £6.434 billion (excluding income tax fraud[59])
- For public bodies at the local level: £0.04 billion.

[55]Tracking the results of random enquiries is the most robust way of measuring the impact of controls, but there are long time lags from behaviour to enquiry to aggregation that mean inevitable delays in assessment of evasion levels. It is difficult to work out what is the correct multiplier for judging the unknown income of known evaders, and what proportion of undeclared income is fraudulently undeclared. Other areas of income tax fraud are more difficult to estimate: e.g. by law, HMRC cannot conduct random enquiries on those who have not been sent tax returns.

[56]Initiatives have begun in which procurement is matched against Companies House data to pick up cases in which company directors and/or addresses are the same as those of employees (but nominee directorships might not be picked up in this way without some high-level data mining). Price-fixing is an area of activity in which national and local police intelligence-gathering historically has been undeveloped, since many offenders stem from areas of criminality which fall outside of performance indicators for policing. This also applies to bribery by UK companies of overseas public officials, which is also one of the more difficult areas for the regulated sector to pick out for suspicions of money laundering.

[57]Transfer costs only are included simply because data is so sparse on other forms of costs: see Annex 7.

[58]With some minor exceptions of public sector fraud where the lower end is zero: these have no material distorting effect on the overall category.

[59]HMRC has given sound analytical reasons for its reluctance to generate a single figure for tax fraud (NAO, 2003). In 2004-5, HMRC recovered £5,725 million from tax compliance work on the revenue side (HMRC, 2005a), an unknown amount of which was fraud.

Annex 7 provides a table that summarises these various costs and which suggests the aggregate costs of fraud are currently, at a minimum, of the order of £13 billion, excluding the costs of responding to fraud and any externalities.

There are however very considerable problems associated with aggregating these figures to provide an overall estimate of 'fraud in the UK'. Some could, for example, dispute the criteria applied to include or exclude studies from the current review.[60] Added to this, the existing sources of data on fraud are neither mutually exclusive nor collectively exhaustive. The commentary in this report has frequently highlighted the problem of double-counting. To give an example, although APACS and CIFAS data are good, they very likely partly overlap. Equally, many of the cheque and payment card frauds mentioned by members of the public in surveys may already be accounted for in the data captured by the above bodies, whose members largely compensate them for their economic costs. Added to this, the existing sources of data on fraud can be shown to suffer from a range of different shortcomings (some of which are listed in the next section), so that quite legitimate differences on opinion can exist about the validity of any particular conclusion drawn. The recent highly-publicised differences between the Treasury, opposition parties and BBC investigators over the extent of MTIC fraud offers a telling example, as does the disagreement over the cost of spirits fraud.

It also needs to be pointed out that just because specific types of fraud have not been subject to measurement, this does not mean they don't exist. One unintended effect of the present 'free market in information of fraud' may be to emphasise cognitively those types of fraud (like payment card fraud) that are relatively well analysed, and are committed against articulate 'repeat victims', as against the more diffuse and less well-analysed or predictable frauds affecting other parts of the business community, the public sector or individuals.

Moreover where fraud figures are available, they tend to focus primarily on the direct (transfer cost) of fraud: the table in Annex 7 provides a breakdown of the known losses 'by type' and the direct costs comprise 93% of the total. It was pointed out at the beginning of this report that very few published sources provided information relating to the costs of fraud prevention and/or in response to fraud. No data are published in the proportion of compliance and regulation costs attributable to dealing with fraud as contrasted with other crimes or prudential issues. In this sense, again, the figures clearly understate the true cost, and probably by a substantial margin.

Weaknesses relating to the current data on fraud

In broad terms, the studies that have been reviewed have paid scant regard to adopting rigorous research methods; they have paid insufficient attention to the problematic interpretation of the term 'fraud' and—to the extent that fraud is a crime targeted on organisations as much as individuals—the survey exercises carried out share many of the problems associated with corporate surveys (e.g. the CVS) rather than with the better tested surveys of individuals and/or households (e.g. the BCS). Weaknesses in current fraud data can be grouped together around several key issues:

Defining 'fraud'. Questions about fraud often lack specificity. This does not matter greatly in the simpler forms of fraud, whether against individuals, businesses or public sector. If individuals pay direct for goods from someone they have encountered on e-Bay, by-passing normal controls, and the goods never arrive and the vendor cannot be found, then this clearly is fraud; likewise the data collected by APACS on

[60]Different decisions could have dramatic consequences on the aggregate total quoted here. One survey of 'economic crime' suffered by major corporations, for example, estimated that businesses lost fully £32 bn. in 2003. It cannot be ruled out that this estimate was of the correct order of magnitude. However, 'economic crime' is a far broader construct than 'fraud'. This particular survey was deemed to have been based on a small postal survey covering an ambiguous period of time; it was heavily biased towards major companies which may not have separated out their losses in the UK from those suffered elsewhere; and the extrapolation methods used to derive aggregate estimates were not explained.

payment card and cheque frauds are relatively unambiguous reflections of crime. (Though APACS data under-count the more ambiguous 'first party' fraud by genuine card-holders and do not include frauds committed in the UK upon the holders of non-UK cards, though they do include frauds committed abroad on UK-issued cards). Where data have been collected by means of a survey, however, assumptions are often made that all recipients will share a common understanding of what specific forms of fraud entail. These problems are compounded where a broader set of victims is included, and a telephone call (or paper/on-line questionnaire) involves just one corporate representative. In such circumstances the validity of the judgement as a measure of fraud across the business can be even more in doubt, if only because liaison between security and group audit departments is not always perfect, and the former may not always be aware of major frauds from external sources or from very senior insiders[61]. The issue of separating 'bad debt' from 'fraud' also remains a major difficulty[62]. There is no obvious case for including money-laundering as a separate category in any fraud survey, since even when using false identity documents, it is either double-counting (when the predicate offence is fraud)[63] or should be excluded because it is not fraud. On the whole, very little information describing the underlying fraud data-generating process (i.e. the process through which individuals/organisations are made aware of whatever fraud they face in the first place) is captured in fraud surveys — and it is not clear that the data-generating process is even understood by many or all survey respondents.[64]

Accounting for the different purpose(s) of each data collection exercise. The different objectives behind different data collection exercises create differences in methodological strategies, even if these are seldom clearly apparent. Strong caution has, in particular, to be expressed about the interpretation of surveys initiated, or conducted, by the private sector (most of which were not designed with the sorts of purposes for which government departments and policing agencies would normally expect). It is not obvious why the government or wider public should expect the private sector to fund the representative estimation of fraud unless private sector entities are likely to benefit from it: there is a danger of confusing the pro bono work of some professional firms with the marketing impetus that lies behind certain sources and that in part accounts for their proliferation[65]. It is thus not surprising that the large accounting firms should focus on the larger companies: they are their clients for audit, consulting and forensic services in ways that members of the Forum for Private Business or private individuals are unlikely to be.

Readiness to participate in fraud surveys. Distrust of sharing data on fraud does not seem to affect fraud survey findings as much as it might have done 10 or more years ago. Arguably, to be defrauded is no longer stigmatising for companies, although in areas – such as e-banking – fear of individual business reputational risk might be generated if there is distrust of the anonymity of responses

[61]The professionalisation of security in major corporations – financial services and others – will have reduced this communications gap. The better surveys will contact the representative (or their PA) in advance to give them time for consideration, but there is no guarantee that they have done so in every case. Categories such as 'identity fraud' are particularly prone to slippage in formal or operational definition.

[62]By re-analysis of its bad debt book, one consumer credit grantor more than tripled its ratio of fraud to write-offs: but whether this ratio is generalisable across the credit industry remains unknown.

[63]Technically, where the offence is fraud overseas but the laundering takes place in the UK and false documents are used, this could be construed as the evasion of a debt by deception practised upon the bank, but the launderers have not obtained funds or property by deception in the UK.

[64]The data generating process typically involves various types of computer systems which flag up anomalous behaviour, investigator experience, and tip-offs. Of course, the data generating process itself may affect the amount of fraud reported: advanced systems will likely out-perform basic systems, and as such will identify more fraud.

[65]Though not suggestive of much, it is interesting to note that informal discussions indicate that almost no private sector firm spends as much money on their fraud/economic crime surveys as does the government on any of its studies.

(ONS, 2006b). There is however no discussion of this as an issue in any of the surveys, nor is there evidence of awareness of it in any of the interviews conducted with the survey firms.

Ensuring full survey participation by victims. There often seems to be variable commitment by respondents to answering survey questions seriously. Since business surveys became vogue in the 1990s, interviews suggest that they may be regarded as a chore by firms and response quality is probably uneven, but difficult to assess by the survey firms or by readers. It is not suggested that fraud surveys uniquely suffer from this or other difficulties mentioned above — the British Crime Surveys may have difficulty with interviewee fatigue and locating hard-to-reach inner city/council estate residents—but this does not diminish the problem here. The OFT found that answers to the short omnibus survey were significantly different from those given in the more intensive, probing follow-up questionnaire, suggesting poor reliability and validity in the first survey.[66]

Determining the unit of analysis. The unit of analysis is often not clarified in data collection exercises and equally often appears to be taken for granted by data providers, not least in questionnaire surveys (written or telephone). For example, with surveys of businesses, it is very seldom clear whether the questionnaire response speaks for the company as a whole (e.g. it has been circulated around different divisions before completion) or simply the person/section asked. Some surveys take care to give advance notice but in many telephone questionnaires, particularly, it seems to be taken for granted that the person answering the questions has full, immediate knowledge of the issues at hand. There are reasons to be sceptical about whether this is always so. The summary of fraud studies outside the financial services sector suggests that different responses will be obtained depending on whether it is Head Office or local branches answering questions (and there are positive and negative aspects of both). In financial services, especially but not exclusively, different consequences may arise for bonuses and for staff accountability if a loss is classified as bad debt or as fraud. This may distort the data by the time it reaches the person filling in the questionnaire and/or considering whether to file administrative reports on bad debt or fraud.

Determining where the fraud was committed. It is inherently difficult in the case of trans-national frauds to determine where the fraud has occurred, since the answer might be in more than one country. Thus, in the case of international companies, where there is a group audit for the business as a whole (or a region of the world such as Europe and the Middle East), it is far from clear in which country the fraud occurred. This may not matter to the company – which may want to know only what its risks are – but it is relevant to assessing 'the impact on the UK', which was the objective of this research. Moreover, frauds affecting part of a business in another country might have an impact on the UK (e.g. loss of capital for investment in the UK = negative; or perceived relative attractiveness of the UK compared with untrustworthy country = positive).

Accounting for the time lapse between the commission and reporting of fraud. The duration of the process by which frauds come to light creates difficulties for the placement of fraud within an annualised time frame, let alone real-time 'hot-spotting' of fraud events. There are of course modest lagged effects in relation to some frauds—such as payment card frauds, where the cardholder may become aware of the fraud only weeks after the event, generally when his/her statement arrives (although proactive card scheme and issuer detection systems may spot these much sooner). However, the events themselves are tightly time-bound. Procurement frauds and cartels involve particular timed events which may require 'retrospective allocation' when learned about some time later (as did the Harold Shipman murders).

[66]Information provided by personal communication.

Aggregating data and deriving UK-wide estimates. The task of extrapolating—from limited data—the extent of fraud affecting a particular business sector, or even country, requires much more sophistication than is commonly recognised. Some extrapolations clearly test the bounds of credibility: though there was a caveat in its original report, the much-publicised Association for Certified Fraud Examiners (ACFE, 2002, 2004) study was a membership survey in the US that had only a 10 per cent response rate, so to extrapolate from that even to the US let alone the UK would defy the normal canons of research. Likewise, the frequent absence of ranges in fraud estimates may make clear newspaper headlines, but cannot possibly be defended when it comes from a research study other than one which, like the KPMG Fraud Barometer and the BDO Fraud Track, reports cases that are coming or have come to court. The question of whether different surveys could 'double count' the same fraud events has been discussed earlier, and represents a major risk when attempting to pool the results of different data collection exercises.

The irregularity in data collection exercises. The studies (particularly surveys) that have been cited as sources of information on fraud have seldom been carried out with the same regularity as their counterparts investigating other personal or household crimes. The BCS, for example, has been conducted biennially since 1982 and annually since 2001, whereas in that period only two Commercial Victimisation Surveys have been carried out, each covering victimisation experience only in the preceding year and neither including financial services firms.

B. STRATEGIES FOR FUTURE DATA CAPTURE

The final key objective of this study was to recommend appropriate strategies to facilitate the comprehensive and consistent recording of fraud. Given what is known about the generally low quality of data on fraud volumes and costs, then, this section seeks to outline a possible strategy for future data capture[67]. It first explores the similarities and differences between fraud and other recorded crime, then addresses the crucial question of 'how' fraud can be controlled and – in the light of this – why better recording of fraud data are needed. In the light of this discussion a general framework for improved reporting is presented, followed by a summary of the key principles that should underpin improvements in fraud reporting[68].

This discussion has been drawn up in the context that the Fraud Review (2006) has recommended that the appropriate response to the massive under-reporting of fraud is the establishment of a National Fraud Reporting Centre (NFRC), to which businesses and individuals could report frauds. The Fraud Review proposed that this should be a public/private partnership, jointly staffed and financed. Its role would be to "receive these reports, analyse them, identify patterns and trends and provide police and other investigative agencies with information to target individuals".

---

[67]It is informed primarily by the findings of the studies reviewed, but also by the data quality issues noted earlier in this report—in particular the six dimensions of data quality set out in Annex 1—as well as information from sources addressing statistical agencies/systems in their entirety; the measurement of the non-observed economy; conversations with relevant parties throughout the statistical arena; and the proposals made in the Fraud Review (2006).

[68]Interestingly, as an indication of the fact that countries share similar issues generating dependable statistics on fraud, the Coalition Against Insurance Fraud in the US (no date) suggests a number of steps that should be taken to improve data quality. These include the following:

- Develop concise definitions of fraud for the purposes of uniform measurement, and promote the understanding and use of the definitions with industry, government, academia and the media. Terms might include "suspected fraud," "referred fraud" or "convicted fraud," depending on the action taken.
- Investigate securing the aggregate reporting data insurers file annually with state insurance departments, to determine whether data could be extrapolated for measurement purposes.
- In the interim until more accurate measurements can be ascertained, major anti-fraud organizations should seek agreement on more-consistent estimates, or perhaps resist publishing estimates that are not based on some level of scientifically valid empirical studies.

Fraud and other crime: similarities and differences

In legal terms, fraud constitutes just one of many different notifiable crimes and it can easily be assumed that encouraging improved reporting and recording of this offence will require actions little different from those designed to improve, say, the reporting of any other acquisitive offence. In thinking about the proposals for the NFRC it helps to consider how the proposed way of reporting might differ from that applied to other forms of crime, what lies behind the very large underreporting of fraud and how fraud can be viewed as qualitatively different from many other forms of crime.

Conventionally, most crimes experienced by individuals, their households or corporate bodies are reported to the police rather than to any other body. The timeliness of any report is important, as crimes with a short time lapse between their commission and reporting tend to offer the greater likelihood of being detected (see Burrows *et al*, 2005 in respect of 'volume crimes'), although this is not necessarily true of those frauds where there are other (for example, documentary) links between events and suspects.[69] In terms of the labels applied earlier in this report, it is hoped that crimes reported quite rapidly might provide tactical or operational intelligence with which to identify and detect the perpetrator(s) – or, failing that, strategic intelligence with which to plot broad trends in crime and frame future responses, some of which may be handled by business without any government or police action. At appropriate intervals the key aspects of the recorded crimes are relayed by the police to the Home Office and aggregated to inform broader crime reduction policy agendas.

The implicit assumption behind the proposal made by the Fraud Review is that this conventional sequence is reversed: in other words that victims, nationally, submit reports to the NFRC in the first instance and that it, in turn, will 'process' them and then provide police and other investigative agencies with – it is assumed – actionable tactical intelligence, plus information that is simply noted to inform a broad understanding of patterns of crime. This could be warranted by the perception that fraud constitutes more of a 'cross border' crime than do most other forms of criminality.

The Fraud Review points out that fraud is massively underreported because this offence is "not a national police priority and, even when reports are taken, little is done with them". But the proposals in relation to the NFRC are explicitly based on the expectation that (as with the reporting of suspicions of money-laundering through suspicious activity reports, or 'SARs'[70]) the Centre will not anticipate that every report submitted to it will be 'individually investigated'. This could prove 'difficult to sell' to those victims that are not routinely at major risk from fraud, particularly as it is known that (insurance claims notwithstanding) the expectation that 'the police will do something' constitutes one of the main drivers for reporting any crime to the police, and – conversely – that recognition that they are often unable to fulfil this expectation constitutes one of the main reasons for non-reporting. As for individual victims, repeat victimisation (OFT, 2006) notwithstanding, they are currently unlikely to report frauds and may not be inclined to do so to an NFRC unless they consider they will have a chance of getting their money back or at least of putting an end to the offending. To the extent that reporting to the proposed NFRC proves to be partial and uneven, their 'intelligence map' derived from this data would be similarly flawed.

Finally it is worth observing that because the term 'fraud' covers such a wide and varied form of behaviours, one of the key priorities of any national reporting centre would need to be to classify and

[69]Elapsed time may have a substantial effect on the prospects of recovering proceeds of crime, and this affects the net costs of fraud – but this issue is outside the scope of this report.

[70]The FSA require 'significant' frauds to be reported to them for regulatory risk assessment purposes, but how this is defined in practice remains uncertain: however in any event, only a sub-set of these would be reported to the police. By no means all frauds against all sectors that are reported to SOCA by financial institutions as 'suspicious activity reports' are reported separately as crimes to the police or to any other law enforcement bodies.

record separately different fraud types. In respect of volume crimes like domestic burglary and vehicle crime, for example, it could be said they are defined primarily in terms of their targets (homes and cars, respectively) and that while the modus operandi adopted in any single crime can, and occasionally does, assist detection, it does not serve to distinguish quite different forms of behaviour. Such a statement could not, however, be applied to fraud. As this report has shown, this generic title – covering the "obtaining of financial advantage or causing of loss by implicit or explicit deception" (see page 2) – really means very little on its own. As the glossary of common types of fraud (Box 1) indicates, financial advantage can be obtained by activities as wide ranging as selling a product that is not genuine, the failure to pay appropriate taxes, claiming to an insurer to have suffered a loss which did not actually occur, the adoption of someone else's identity, the 'fixing' of a sporting event on which bets have been placed or much wider set of quite discrete behaviours. In these cases these various modus operandi in reality separate quite different forms of types of fraud, each of which might require a quite different investigative or preventive response.

How can fraud be controlled?

The review of the literature clearly indicates that, despite the heterogeneity of fraud, there is a thread common to the commission of most fraud offences: namely that it is typically weaknesses in the systems, controls or procedures operated by victims or their intermediaries (whether they be in the public arena, or private) that allow the fraudster to obtain financial advantage or cause loss by implicit or explicit deception. The extent and nature of fraud represents a combination of these situational opportunities and motivated offenders with the skills to take advantage of those opportunities (Annex 6 provides an account of what is known about perpetrators).

It may be a tautology to state that without opportunities there can be no crime; but this simple fact can often be overlooked, as can the direct implication that must be drawn from it: that the prevention of fraud lies, above all, in the discipline of subjecting to rigorous risk assessment systems or procedures that can be manipulated to give any financial advantage, both before they are implemented and regularly thereafter. This discipline must be 'scenario specific' and exercised by the organisation or individual at risk. Most corporate victims are aware of this and, indeed, financial services firms in particular spend substantial (although largely unquantified) software and staff resources on managing those risks.

These observations—which form the basis of any 'threat assessment' approach to fraud – have profound implications for the role that the police service can play in controlling this form of crime. Put simply, while it is appropriate to expect the police and other security professionals to dispense advice to potential victims of—say—burglary and car crime, it is not reasonable to expect such generalists to possess the specialist knowledge to enable them to, say, advise on how retailers might prevent frauds against their electronic funds transfers at point of sale (EFTPoS), or advise on procurement fraud risks in global advanced technology industries.

The question of who should take prime responsibility for the management of fraud affecting the private sector has long been a 'political football', and this position is unlikely to change. Businesses can be viewed as both crime victims and active agents in crime prevention, but they can be viewed also as 'crime generators'– either of offences against themselves as businesses or of offences against others, by their creation of new services and products (see Burrows, 1997)[71]: and this naturally colours their relationship with law enforcement agencies. In reality, partnership arrangements constitute the only practical way forward, but the terms of this partnership need clarification lest both different business sectors and

[71]This description was initially coined by Brantingham and Brantingham (1995) and developed further by Felson and Clarke (1997).

[72]Partnership discussions occur also at European and international levels too, consuming more resources in liaison whose effects need to be evaluated (and can lead to 'partnership attrition' if their consequences are not seen to be mutual).

policing agencies waste time in pure 'talking shops' that fail to progress either direct action or intelligence development that leads to improved policy or action.[72] Applying this principle to cheque and payment card fraud, for example, it is clear that banks and other private bodies (separately or, better, with pooled data) do take prime responsibility for identifying fraud, instigating initial investigations and doing all they can to identify suspects and set out the nature of the fraud they have committed. With this support, the police are then in a position to call on their additional powers of investigation (where appropriate and where they have the resources) and initiate proceedings that will bring the perpetrators of fraud to justice. In doing so, they are likely — as does the Serious Fraud Office (SFO) — to need to enlist the services of financial experts, specialist lawyers and others.

In short, partnership is fundamental to effective action. Although industry groups themselves can and sometimes do collect better data for internal sharing, this review has been focused on the requirements of society as a whole. This stark reality is central to the issue of why data collection could be improved in future, which is discussed next.

The case for improving the data on fraud?

While it did not fall within the formal remit of this study – which was simply to recommend how consistent and comprehensive recording of fraud could be achieved – the question of 'why' this is necessary or desirable must first be addressed. Clearly the comprehensive reporting and recording of fraud would be desirable in principle, and indeed serve to reveal the costs borne by both primary and secondary victims as well as 'UK plc', but – as the discussion above has indicated – it would be neither practicable nor, arguably, desirable to promote the view that the police could assume full responsibility for the prevention of all fraud.

Three observations can be made in this context.

The key parties interested in this change must define the goal: the purpose of capturing statistics on fraud[73]. The critical question of the purposes for which current data are collected was considered in the conduct of the current review. While it was not for the research team to impute reasons where these were not explicit, the review has sought to shed light on this motivation, by trying to separate where data has been collected to inform general policy-making, to generate strategic intelligence on fraud, or to generate tactical intelligence products which may then be used operationally.[74] The review has concluded that there is currently very little data available that could be classified as providing operational intelligence, despite the fact that the principal goal of the proposed NFRC appears to be to obtain and 'process' this type of information, on which others could act. It has also pointed out that the time lapse between the commission and discovery of many frauds presents a challenge that needs to be recognised, even if it cannot be fully overcome. To the extent that the proposed NFRC were set up and accepted as the agreed 'owner' of fraud statistics, clearly its first task should be to consult on the purpose of obtaining any fraud statistics and how more timely and actionable data could be secured[75].

[73]Defining the purpose of data capture on fraud relates in turn to the data quality dimension of relevance, defined as "the degree to which the statistical product meets user needs for both coverage and content" (ONS, 2005). The ONS goes on to note that "any assessment of relevance needs to consider: who are the users of the statistics; what are their needs; how well does the output meet these needs".

[74]Consumers (i.e. users) of fraud data wish to use fraud statistics for all of these purposes, but generally it can be assumed that different user groups will have different needs (e.g. Home Office for policy-making; law enforcement for strategic/tactical intelligence).

[75]Interviews with some North Americans in connection with this study suggest that more complex cases are not often reported electronically.

Different purposes command different levels of specificity from fraud-related information, of course—and will require different approaches to data capture. General data on overall fraud volume and cost – say to inform policy making or broad tactical direction – will not need to be event-specific; but data from which to generate strategic and tactical intelligence will require such specificity. If truly specific information is required, then certain approaches may be most appropriate. For example, general data on fraud volume and cost may be best obtained through the pooling of administrative data by umbrella organisations (such as APACS) or certain surveys. Specific data on fraud events may require, however, more specialised responses. It should be further considered that different entities within the anti-fraud spectrum will be better placed to provide information to assist prevention rather than information to assist detection. Information to assist prevention will likely come from those entities 'at the coalface '— the managers/owners of systems/controls (as the situational crime prevention literature recognises). Information to be used tactically (to generate actionable intelligence against operational targets) may come from slightly different sources.

The purposes underlying data capture will also have implications for the timeliness of data-collection, and their availability to users. Tactical intelligence requires relatively current information collected at a relatively high frequency, while strategic intelligence needs may be met by somewhat older information collected at lower frequencies. This consideration is absolutely critical in the context that the ability to provide up-to-date, actionable, information may not be within the control of 'the system' or indeed of the victims of fraud: this may require internal or external private investigation before the suspicion becomes crystallised to the extent that a decision may be made to report it to the police or regulators (and/or to SOCA as a suspicious activity report). Except where there is a rapid increase in levels of crime exploiting security weaknesses (as in MTIC and some other e-frauds), information to underpin policy-making may not need to be gathered on much more than a yearly basis, with a realistic lag between information collection and release to users[76].

An incremental approach to improved fraud reporting and recording?

The findings of the current study certainly support:

- the need for a centralised and reasonably well-resourced, central body to 'champion' the improved reporting and recording of fraud; and
- that, if this body were to be charged with some of the range of responsibilities proposed for the National Fraud Strategic Authority (the proposed parent organisation which would house the NFRC: see Fraud Review, 2006), it should be able to produce dividends in terms of both the apprehension and detection of the perpetrators of fraud (as shown by the evaluation of the DCPCU: see Burrows *et al*, unpublished) and its prevention.

It does however seem appropriate to caution that – in the light of the very low level of current fraud reporting and the potential enormity of what might follow if victims were encouraged to report all fraud[77] – there is a danger of raising expectations that might not be able to be met by the police or by any other body charged with law enforcement, harm reduction, and/or regulation.

[76]So, for example, while the Home Office, or proposed NFRC, may not require information on frauds in 2005 until early 2006, the use of such information would be undermined were such data not to be available until late 2006 or 2007.

[77]The current data does not allow any realistic estimates to be drawn, but there are serious warning signs. Victims of crime are, for example, encouraged to report attempts to – say – burgle their homes, or steal their cars. If only a modest proportion of the 150 million spoof emails sent each month (see above) were reported to the authorities, there would be some difficulties!

There is a need for any central body to work within the framework of a comprehensive typology, of the sort developed in this study, in that such an approach will avoid undue attention being given to 'what is counted' at the expense of 'what is not'. The victim centric approach adopted here has served to do this and while there are other typologies that may work, the benefits of retaining a clear vision of 'who loses' (in the end) – and therefore who will be inclined to take remedial action or require others to do so – are significant. Losses can of course be looked at in terms of individual incidents or in terms of cumulative harm over a period.

Based on the broad findings of this review, the first priorities of any central coordinating and advisory centre on fraud might be:

- Where fraud data are currently being collected that can be classified as 'operational intelligence' then – following the APACS-funded DCPCU and FLA-funded Vehicle Fraud Unit models – these circumstances would offer clear potential of areas where police/private partnerships should be set up or altered to make fuller use of the information available, provided that there is a capacity and willingness of the enforcement agency to do so. When any such initiatives are set up, they should be subjected to independent evaluation that will help not only to improve and develop their performance, but to make the business case to potential sponsors in relation to other types of fraud. The central body should moreover seek to rapidly identify additional umbrella organisations and others capable/keen to develop operational intelligence – so more could follow.
- Where data are currently being collected in the so-called 'free market of information on fraud', there is a vested interest in the government trying to encourage the application of tighter definitions of fraud, more rigorous methodologies and indeed in trying to promote some form of 'kitemarking' of data collection activities – whether they involve the pooling of administrative data or one-off surveys – that meet approved standards. It is to be expected that these standards may initially need to be set quite low and it should be recognised that those conducting surveys, for example, can only work within the budgets available to them (although the injection of 'pump priming' funding could be an important means of driving up standards). While the personal/ household victimisation surveys carried out in the US, UK and other developed countries (like the BCS) took many years and substantial funding to reach their current levels of reliability, there has been very limited investment in developing similar methodologies in respect of corporate fraud surveys or other methods, and these remain – by comparison – in their infancy.
- Where data are almost entirely absent – and notably in the area of frauds against private individuals – then there would be a strong case for any fraud centre to initiate and commission separate studies to gain reliable insights into the extent, nature and costs of specific types of fraud.

Key principles that should underpin any initiative to improve fraud reporting and recording

If consensus can be reached that changes should be made to ensure fraud reporting in future should be rendered more consistent and comprehensive, then it is highly desirable that this drive should be centrally coordinated, even though one method does not fit all data needs. The key principles[78] recommended by the current study are presented in more detail below.

To begin, at the risk of considerable repetition, the measurement of fraud should be coordinated and driven by one entity at the top: one owner. Given that the UK needs to understand the problem of fraud as it affects the UK — across all sectors and geographic regions (fraud doesn't discriminate by location) — the measurement of fraud needs to handled in a comprehensive, system-wide, coordinated fashion. This coordination must come from a single body.

It would not be the role of the owner of the measurement issue to be fully responsible for all data collection (i.e. the point is not to suggest that the owner be responsible for all fieldwork, etc.); rather, existing data providers should be maintained to the extent they provide quality, useful information (e.g.

APACS). But the owner should coordinate nationwide activity — treating fraud statistics as a system, not isolated statistical products — ensuring that measurement exercises adhere to the canons of social science (i.e. produce data of high quality). Along these lines, measures should be designed/handled in concert, and to ensure effectiveness, the owner of the measurement issue should maintain subject-matter experts, survey statisticians, and field-work specialists on staff (good practice as recommended by UNSD, 2003). The owner should aim to build consensus and an atmosphere of cooperative working with the private and public sector victims of fraud who ultimately provide data (e.g. by establishing a group or groups of data providers meeting on a semi-regular basis). The owner should also coordinate periodic independent reviews of statistics produced in the system, not least to ensure that statistics remain credible.

In coordinating any fraud statistical system, the owner of the fraud statistical system should clearly define the concepts to be measured and promulgate consistent counting rules and measurement methodologies. A system-wide use of clearly defined concepts with established counting rules would go a considerable way to properly recording known and reported fraud. The key principles should be:

- To preclude double-counting, the concepts should be collectively exhaustive and mutually exclusive. It is important that no other concepts in the data-collection exercise overlap. It also seems imprudent, except in special circumstances, to move beyond the use of the generic word "fraud" without first defining the boundaries of the term.
- Concepts/counting rules should be elaborated and distributed to all data providers to set forth clear and uniform standards and procedures for recording and disseminating statistics to appropriate authorities. The concepts/counting rules should be informed by the purpose of data collection and should steer data providers toward the use of sound social science methods (e.g. administrative data collection or probability sampling over non-probability sampling as appropriate), bearing in mind the dimensions of data quality.[79]
- Counting rules and strategies should also be designed to capture better information on resource costs (i.e. resource costs in anticipation of and response to fraud). Strategies in this regard might include clarifying the accounting information requested of public and private sector entities on expenditures on anti-fraud systems, investigative teams, measurement teams, et cetera.
- Similarly, strategies should be designed to better capture information on the externalities of fraud (perhaps in occasional surveys of specific victim sectors to measure willingness to pay/willingness to accept measures of the importance of avoiding fraud).

The owner of any fraud statistical system will need to devote time/resources to educational outreach activities to ensure that data providers have the full capacity to provide quality data. That is, the owner should ensure that data providers understand the concepts/counting rules set forth. Some data providers may also have to be motivated to take seriously data quality issues, since they may not see any personal benefit from so doing.

The owner of any statistical system should seek to remove the disincentives of reporting fraud. At present, these are considerable: the Fraud Review (2006) states that "a comprehensive measurement exercise must increase the reporting of known but unreported fraud".[80] Victims of fraud, be they

[79]For example, data providers should provide metadata/information on methods along with any statistical products, or at least be prepared to release such information to the public upon request.

[80]This seems reasonable on the face of it—though, of course, reporting of known but unreported fraud should be done in line with the stated purposes of the statistical system. After all, if the purpose of fraud statistics is exclusively to inform policy-making, then while known but unreported frauds should in fact be reported, it may be the case that only aggregate, low frequency reporting is necessary.

[81]This should not be taken as a harking back to some Golden Age of Fraud Policing, which has never existed in the UK: however it is a matter of degree and the data on declining Fraud Squad staffing speaks for itself (Fraud Review, 2006).

individuals, firms from within and outside the financial services sector, perhaps even public sector entities are currently reluctant to report fraud—or at least feel that reporting fraud carries little benefit. As pointed out earlier, years of neglect from law enforcement, whose priorities have shifted dramatically away from fraud in recent years[81], have generated an atmosphere of 'why bother' at best. At worst, law enforcement has been unwilling to accept reports of fraud. Further, private sector entities face the potential for reputational risk (which could increase as the information increases in specificity): though 'the public' might vary in their behavioural reactions to reports in the media on different types and levels of fraud. Banks and other corporate entities need to be sure that information they (and their customers) provide is kept confidential and secure from misuse.

How, then, can data providers/reporters be encouraged to report? The United Nations Statistics Division (UNSD) notes that there are four mutually compatible methods which may enhance cooperation with respect to data provision:

- legal instruments to force compliance or discourage disobedience;
- appeals to respondents' sense of morality to encourage cooperation;
- assurances that the information will not be misused; and
- a variety of incentives are being used increasingly in some countries (UNSD, 2003).

Some of the arguments in support of, and against, applying these different approaches are outlined in Annex 8.

The owner of the fraud statistical system should encourage data providers to explore options to expose and better estimate undiscovered fraud. This has the benefit of both generating better information on fraud as it exists and — more importantly—helping to prevent/respond to it. Industry-wide data pooling approaches (like the Insurance Fraud Bureau or CIFAS) have been successful in this regard. And businesses might also consider subjecting their procedures and protocols to regular spot checks (as 'mystery shopping' serves to check for systemic weaknesses). Once discovered, of course, previously undiscovered frauds should be reported in the appropriate manner.

Lastly, the owner of the fraud statistical system should encourage data providers to employ proportionate/cost-effective data-collection approaches. Given the purposes of data collection (i.e. the needs of users) — which will drive the specific concepts to be measured and the timeliness of data collection—any strategies introduced to improve data capture will, of course, need to be proportionate and cost-effective. This is the case not least because of perceived imbalances in the effort to fight fraud (with the perception that more effort/resources are being expended by the private sector than the public, particularly law enforcement). Further, as with all data-gathering good practice, efforts must be made to minimise respondent burden (certainly there is every reason to avoid data-collection fatigue). In this regard, it is imperative to:

- Maximise the use of existing data. Existing data from select sources may be used in innovative ways (see, for example, OECD (2002) for a discussion of potential approaches to the reconciliation of various data sources to illustrate NOE activity). Further, it would seem impractical (to say the least) to require financial services firms to report frauds to APACS and to a proposed National Fraud Reporting Centre. Dual reporting is a disincentive to data provision and should be avoided to the extent possible.
- Where possible — and not impractical and/or distracting — consideration should be given to introducing measures of fraud in existing surveys. It may not be overly difficult to introduce appropriately probing questions on fraud in surveys like the British Crime Survey.
- Ensure that any new and existing measurement exercises/approaches fit sensibly into a comprehensive system. All component parts of the fraud statistical system need to work in tandem, not in conflict. Measurement exercises/approaches need to be mindful of the push and pull of different reporting chains, responsibilities, allegiances, etc.

Regardless of whether new measurement approaches are taken or existing approaches are leveraged, it is imperative that the right approach – with sound methodology – is used for the problem at hand. If results must be precise, for example, then things like postal surveys may not be appropriate (given their typically low response rates). Or if the result of a survey will ideally be generalised to a broader population, then the appropriate sampling frame must be employed. In an environment of scarce resources, it is important to recognise the strengths and weaknesses of certain measurement approaches – and to act accordingly.[82] If response rates are poor, then the appropriate level of caution must be employed in data aggregation, in preference to making heroic guesstimates that may induce more fraud prevention action but may also distort private and public sector expenditure and legislation.

[82]Perhaps the best roadmap for improving fraud statistics should include the ingredients of a non-observed economy (NOE) implementation strategy as stated in the OECD's Measuring the Non-Observed Economy: A Handbook. Annex 9 provides an overview of this.

5. CONCLUDING COMMENTS

The process of compiling, plausibility testing and then aggregating data has been a dense, and in some respects, an unenviable exercise involving difficult judgment calls. However, this review makes a significant contribution to clarifying what is currently known about fraud. The patchiness of the data is self-evident, and some results have been left out altogether because aggregation even within victim categories has been impossible. An unintended effect may be to present patterns of fraud that reflect the level of data-gathering effort and ease of compilation, rather than the portrait that might appear if careful and rigorous assessment were attempted across the peace. A better and truer picture of fraud will have to await improved fraud awareness and collection strategies within business as well as by trade bodies, regulators and the public police. In recent years, the rates of non-violent acquisitive crimes other than fraud have been falling in the UK. This study shows that fraud is currently a very significant crime problem, and there is no reason whatever to suppose that its costs, level or significance will diminish naturally over time.

REFERENCES

Alessie, R., Hochguertel, S. and Weber, G (2005), 'Consumer Credit: evidence from Italian micro data', Journal of the European Economics Association, 3(1), 144-178.

Association of British Insurers (2005), UK Commercial Insurance Fraud Study 2005.

Audit Commission (1988) Protecting the Public Purse, London: Audit Commission.

BDO Stoy Hayward (2006) 'Inside Job': Fraud Track 3: Rising Fraud in the Spotlight: Annual Survey 2006. BDO Stoy Hayward UK.

Bhattacharyya, D. (1990), 'An econometric method for estimating the "hidden" economy. United Kingdom (1960-1984)', Economic Journal, 100, 703-717.

Brackstone, G. (1999) 'Managing Data Quality in a Statistical Agency.' Statistics Canada-Survey Methodology 25.

Brand, S. and Price, R. (2000) The Economic and Social Costs of Crime, Home Office Research Study no.217, London: Home Office.

British Broadcasting Corporation (2005) Annual Report and Accounts 2004-05.

British Retail Consortium (2006) Retail Crime Survey 2004-2005: BRC, London.

Burrows, J. (1997) 'Criminology and business crime: building the bridge'. In Felson, M and Clarke, R (eds.) Business and Crime Prevention.

Burrows, J., Anderson, S., Bamfield, J., Hopkins, M, and Ingram, D. (1999) Counting the Cost: Crime Against Business in Scotland. Edinburgh: Scottish Executive.

Burrows, J., Levi, M. and Webb, S. (unpublished) An Evaluation of the Dedicated Cheque and Plastic Crime Unit. London: Home Office.

Burrows, J.; Hopkins, M; Hubbard, R; Robinson, A; Speed, M. & Tilley, N. (2005) Understanding the Attrition Process in Volume Crime Investigations, London: Home Office Research Study 295.

Bussman, K. and Werle, M. (2006) 'Addressing crime in companies: first findings from a global survey of economic crime', British Journal of Criminology, 46, 1128-1144.

Butler, G., Hodgkinson, J., Holmes, E. and Marshall, S. (2004) Evidence Based Approaches to Reducing Gang Violence, Government Office for the West Midlands and Home Office Regional Office.

Butler, G., Deaton, S., Hodgkinson, J., Holmes, E. and Marshall, S.. (undated) Quick but not dirty: Rapid Evidence Assessments as a Decision Support Tool in Social Policy, http://www.gsr.gov.uk/downloads/gsr_news/quick_dirty.pdf#search=%22butler%20%20quick%20but%20not%20dirty%22

Cabinet Office (2002) Identity Fraud. London: Cabinet Office.

Cabinet Office (2003) The Magenta Book: Guidance Notes for Policy Evaluation and Analysis. London: Cabinet Office.

Cagan, P. (1958) 'The demand for currency relative to the total money supply', Journal of Political Economy, 66, 303-328.

Calzaroni, M. (2000) The Exhaustiveness of Production Estimates: New Concepts and Methodologies. Italy: Istat.

Coalition Against Insurance Fraud (no date) Measuring Fraud.

Committee of Public Accounts (2004) 32nd Report: HM Customs and Excise Standard Report. HC 284. London: TSO. NAO. (2001). Losses to the Revenue from Frauds on Alcohol Duty. .HC178. TSO.

Cooperative Movement (2004) Cooperative Movement Retail Crime Survey 2003/04. Cooperative Movement: Manchester.

Core, J. (1997) 'On the Corporate Demand for Directors' and Officers' Insurance', The Journal of Risk and Insurance, 64, 1, 63-87

Crocker, K and Morgan J. (1998) 'Is Honesty the Best Policy? Curtailing Insurance Fraud through Optimal Incentive Contract', Journal of Political Economy, 106, 2, 355-375

DARDNI (2006) Counter Fraud and Enforcement Activities Annual Report 2005/06, Belfast: Department of Agriculture and Rural Development. http://www.dardni.gov.uk/index/publications/pubs-dard-strategies-reports-and-accounts/publications-strategies-reports-and-accounts-counter-fraud-and-enforcement-activities-2005-06.htm

Davidson III, Wallace N, Cross M, Thornton J (1992) 'Corporate Demand for Insurance: Some Empirical and Theoretical Results', Journal of Financial Services Research, 6, 1, 61-72.

de Vries, W. (1998) 'How Are We Doing: Performance Indicators for National Statistical Systems.' Netherlands Official Statistics, 13: 5-13.

Department of Work and Pensions (2005a) Fraud and error in Income Support, Jobseekers Allowance and Pension Credit from April 2004 to March 2005.
Department of Work and Pensions (2005b) Reducing fraud in the benefit system, www.dwp.gov.uk/publications/dwp/2005/fsu/reducingfraud.pdf
Department of Work and Pensions (2005c) Fraud and error and other Incorrectness in Disability Living Allowance: The Results of the Benefit Review of Disability Living Allowance.
Department of Work and Pensions (2006a) Resource Accounts, 2004-05,
Department of Work and Pensions (2006b) Fraud and error in Housing Benefit from April 2002 to March 2005. http://www.dwp.gov.uk/asd/asd2/fem/fem_apr05_mar06.pdf

Department of Work and Pensions (2007) Fraud and Error in the Benefit System from April 2005 to March 2006.
http://www.dwp.gov.uk/publications/dwp/2006/dwp_resource_account.pdf#search=%22dwp%20resource%20accounts%22

Dijk, J. van, Manchin, R., Kesteren, J. van, Nevala, S., and Hideg, G. (2007) The Burden of Crime in the European Union. http://www.gallup-europe.be/euics/Xz38/downloads/EUICS%20-%20The%20Burden%20of%20Crime%20in%20the%20EU.pdf.

Doig, A. (2006) Fraud. Cullompton: Willan.

Driver and Vehicle Licensing Agency (2005) Annual Accounts 2004-2005.

Driver and Vehicle Licensing Agency (2006) Annual Report and Accounts 2005-2006

Dubow, B. and Monteiro, N. (2006) Measuring market cleanliness, Occasional Paper Series 23, London: Financial Services Authority.

Emery, H and Gerrits, K (2005) 'The demand for private health insurance in Alberta in the presence of a public alternative', University of Calgary discussion paper.

European Court of Auditors (2006) Annual Report on the Implementation of the Budget in the financial year 2004. http://europa.eu.int/comm/anti_fraud/reports/olaf/2004/en.pdf

Fleming, M. (2005) UK Law Enforcement Agency Use and Management of SARs, London: UCL/JDI.

Fraud Act, 2006.

Fraud Review (2006) Final Report, London: Attorney General's Office.

Freixas, X. and Rochet, J. (2002) Microeconomics of Banking. Cambridge, Mass: MIT Press.

GetSafeOnline (2006) The GetSafeOnline Report. http://www.getsafeonline.org.

Gill, M. (2005) Learning from Fraudsters. Leicester: Perpetuity.
http://www.perpetuitygroup.com/prci/pdfs/learning_from_fraudsters.pdf

Goddard, E. and Compton, S. (2005) Evaluation of the use of household survey data on spirits consumption for estimating the level of spirits fraud. ONS.

Government Social Research Unit. "Rapid Evidence Assessment: A Tool for Policymaking." Webpage accessed 17 April 2006. <http://www.gsr.gov.uk/new_research/archive/rae.asp>.

Gross, D and Souleles,N (2002), 'Do liquidity constraints and interest rates matter for consumer behaviour? Evidence from credit card data', Quarterly Journal of Economics, 117, 149-185.

Hi Tech Crime Unit (2005) Hi Tech Crime: The Impact on UK Business 2005. Hi Tech Crime Unit, London.

HM Revenue and Customs (2004) Measuring Indirect Tax Losses.

HM Revenue and Customs (2005a) Annual Report 2004-05, London: TSO.

HM Revenue and Customs (2005b) Measuring Indirect Tax Losses,
http://www.hmrc.gov.uk/pbr2005/mitl2005.pdf

HM Revenue and Customs (2006a) Tackling Error and Fraud in the Child and Working Tax Credits.

HM Revenue and Customs (2006b) Measuring Indirect Tax Losses,
http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageLibrary_ConsultationDocuments&propertyType=document&columns=1&id=HMCE_PROD1_026423

HM Revenue and Customs (2006c) Annual Report 2005-2006, London: TSO.

HM Treasury (2005) 2004-05 Fraud Report: An analysis of reported fraud in Government Departments.

HM Treasury (2006) 2005-06 Fraud Report: An analysis of reported fraud in Government Departments.

Home Office (2006) Updated Estimate of the Cost of Identity Fraud to the UK Economy, 2nd February 2006, London: Home Office (accessible via www.identity-theft.org.uk).

Hopkins, M. and Tilley, N. (1998) 'Commercial Crime, Crime Prevention and Community Safety- A Study of Three Streets in Camden, North London'. In Gill, M., Crime at Work- Increasing the risk to offenders. Volume II. Leicester: Perpetuity Press.

House of Commons Committee of Public Accounts (2003) Tackling Fraud against the Inland Revenue: First Report of Session 2003-04.

International Monetary Fund. "Data Quality Reference Site." Webpage accessed 17 April 2006. <http://dsbb.imf.org/Applications/web/dqrs/dqrsintroduction/>.

Karstedt, S. and Farrall, S. (2006) 'The Moral Economy of Everyday Crime: Markets, Consumers and Citizens', British Journal of Criminology, 46, 1011-1036.

KPMG (2006) KPMG Fraud Barometer- Press release appendix.

Kesteren, J. van, Mayhew, P. and Nieuwbeerta, P. (2001) Criminal Victimisation in Seventeen Industrialised Countries: Key Findings from the 2000 International Crime Victims Survey. http://www.unicri.it/wwd/analysis/icvs/pdf_files/key2000i/index.htm.

Laliberté, L, Grünewald, W. and Probst, L. (2004) Data Quality: A Comparison of IMF's Data Quality Assessment Framework (DQAF) and Eurostat's Quality Definition. Washington, DC: IMF.

Lander, S. (2006) Review of the Suspicious Activity Reports Regime, London: Serious Organised Crime Agency.

Law Commission (1999) Company Directors: Regulating Conflicts of Interest and Formulating a Statement of Duties (LC261).

Law Commission (2002) Fraud (LC276).

Layard, R. (2006) Happiness – the New Science, London: Penguin.

Levi, M. (1981) The Phantom Capitalists: the Organisation and Control of Long-Firm Fraud, London: Heinemann.

Levi, M. (1987) Regulating Fraud. London: Routledge.

Levi, M. (1988) The Prevention of Fraud, Crime Prevention Unit Paper 17, London: Home Office.

Levi, M. (1992) 'White-collar crime victimization', in K. Schlegel and D. Weisburd (eds.), White-Collar Crime Reconsidered, Boston: Northeastern University Press.
Levi, M. (1998) 'The craft of the long-firm fraudster: criminal skills and commercial responses', Crime at Work, Volume II [Editor M. Gill] Leicester: Perpetuity Press, 155-168.

Levi, M. (2002) 'The Organisation of Serious Crimes', The Oxford Handbook of Criminology [Editors M. Maguire, R. Morgan and R. Reiner], Third Edition, Oxford: Oxford University Press. 878-913.

Levi, M. (2003) Organising and controlling payment card fraud: fraudsters and their operational environment, Security Journal, 16(2), 21-30.

Levi, M. (2007) 'Organised crime and terrorism', The Oxford Handbook of Criminology [Editors M. Maguire, R. Morgan and R. Reiner], Fourth Edition, Oxford: Oxford University Press.

Luttikhuizen R and Kazemier B (2000) A Systematic Approach to the Hidden and Informal Activities. Voorburg: Statistics Netherlands.

Lyssiotou P, Pashardes P and Stengos T (2004), 'Estimates of the Black Economy based on consumer demand approaches', Economic Journal, 114, 622-640.

Martin, G., Klein, R. and Kleindorfer, P. (2000), 'The demand for homeowners insurance with bundled catastrophe coverages', Wharton project on managing catastrophe risks.

Matthews, K. (1982), 'Demand for Currency and the Black Economy in the UK', Journal of Economic Studies, 9, 2, 3-22

Mayers, D. and Smith, C (1990), 'On the Corporate Demand for Insurance: Evidence from the reinsurance market', Journal of Business, 63, 1, 19-40

Mirrlees-Black, C. and Ross, A. (1995) Crime against Retail and Manufacturing Premises: Findings from the 1994 Commercial Victimisation Survey. Home Office Research Study no. 146. Home Office: London.

National Audit Office (2001). Losses to the Revenue from Frauds on Alcohol Duty. HC178. TSO.

National Audit Office (2003) Tackling Fraud against the Inland Revenue. London: National Audit Office.

National Audit Office (2004) Measuring the level of Spirits Fraud. London: National Audit Office.

National Audit Office (2006a) National Insurance Fund Account 2004-05, London: National Audit Office.

National Audit Office (2006b) Department for Work and Pensions Resource Accounts 2004-05: Report by the Comptroller and Auditor General, London: National Audit Office.

National Audit Office (2006c) The Comptroller and Auditor General's standard report on the accounts of HM Revenue & Customs 2005-06, London: National Audit Office.

National Audit Office (2006d) Financial Management in the European Union. HC 999 2005-2006 Session. London: National Audit Office.

National Health Service (2005) Counter Fraud and Risk Management Service Annual Report 2004-05.

National Health Service (2005) Countering Fraud in the NHS: Protecting Resources for Patients 1999-2005 Performance Statistics.

National Health Service (2007) Countering Fraud in the NHS: Protecting Resources for Patients, 1999-2006 Performance Statistics. www.cfsms.nhs.uk.

NERA (2000) The Economic Cost of Fraud, London: Home Office.

Office of National Statistics (2000) Framework for National Statistics. London: ONS.

Office of National Statistics. (2005a) Guidelines for Measuring Statistical Quality (Version 2.0). London: ONS.

Office of National Statistics (2005b) Fraud, Error and other Incorrectness in Disability Living Allowance, http://www.dwp.gov.uk/asd/asd2/dlafraudjuly05.pdf.

Office of National Statistics. (2006a) Fraud and Error in Housing Benefit April 2002 to September 2005, http://www.dwp.gov.uk/asd/asd2/fraud_hb/HBR_Report_Jul06.pdf.

Office of National Statistics (2006b) International Benchmark of Fraud and Error.

OLAF (2006) Protection of the Communities' financial interests – Fight against fraud – Annual report 2005. COM(2006) 378 final. European Commission.
http://ec.europa.eu/anti_fraud/reports/commission/2005/en.pdf

Organisation for Economic Co-operation and Development (2002) Measuring the Non-Observed Economy: A Handbook. Paris: OECD.

Organisation for Economic Co-operation and Development (2003) Quality Framework and Guidelines for OECD Statistical Activities. Paris: OECD.

Pascoe, T., Owen, K., Keats, G. and Gill, M. (2006) Identity Fraud: What about the Victim? London: CIFAS.

Pissaridis, C. and Weber, G. (1989), 'An expenditure-based estimate of Britain's black economy', Journal of Public Economics, 39, 17-32

PriceWaterhouseCoopers (2005) Global economic crime survey- United Kingdom. London: PWC.

Robson Rhodes (2004) Combating Economic Crime. Robson Rhodes LLP.

Ruffles, D. and Williams, T. (2005) Report on further research into the impact of Missing Trader Fraud on UK Trade Statistics, Balance of Payments and National Accounts, ONS

Schneider, F. and Enste, D. (2000), 'Shadow Economies: Size, Causes and Consequences', Journal of Economic Literature, 38, 1, 77-114

Serious Crime Bill, 2007.

Serious Fraud Office (2006) Annual Report 2005/06, London: Serious Fraud Office.

Sherman, L., Gottfredson, D., MacKenzie, D., Eck, J., Reuter, P. and Bushway, S.. (1998) Preventing Crime: What Works, What Doesn't, What's Promising. Washington, DC: National Institute of Justice.

Shury, J., Speed, M., Vivian, D. and Kueachel, A. (2005) Crime against retail and manufacturing premises: findings from the 2002 Commercial Victimisation Survey. Supplementary web report 1: costs of crime. Home Office, London.

Shury, J., Speed, M., Vivian, D., Kueachel, A.. and Nicholas, S. (2005) Crime against retail and manufacturing premises: findings from the 2002 Commercial Victimisation Survey. Home Office Online Report 37/05. Home Office, London.

Statistics Commission (2006) Crime Statistics – User Perspectives, Report No.30. London: Statistics Commission.

Telecommunications UK Fraud Forum (2006) Cost of ID Related Telecoms Fraud and Case Studies. TUFF.

Tilley, N, and Hopkins, M. (1998) Business as Usual: An Evaluation of the Small Business & Crime Initiative. Police Research Series Paper 95. Home Office: London.

TV Licensing (2004) Annual Review 2003-04.

United Nations Statistics Division (2003) Handbook of Statistical Organization, Third Edition, New York: UNSD.

Van Dijk, J. and Terlouw, G. (1995) 'Fraude en Criminaliteit Tegen het Bedrijfsleven in Internationaal Perspectief'. Justitiele Verkenningen 4.

Weisburd, D. and Waring, E., with Chayet, E. (2001) White-Collar Crime and Criminal Careers, Cambridge: Cambridge University Press.

Wilson, D., Patterson, A., Powell, G. and Hembury, R. (2006) Fraud and technology crime: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources, London: Home Office

Wood, J., Wheelwright, G. and Burrows, J. (1996) Crime Against Small Business: Facing the Challenge. Crime Concern: Swindon.

Yamori, N (1999), 'An Empirical Investigation of the Japanese Corporate Demand for Insurance', The Journal of Risk and Insurance, 66, 2, 239-252

ANNEX 1. Six dimensions of data quality

The table below, drawn from the ONS, indicates data quality is typically discussed (and evaluated) along six dimensions: relevance, accuracy, timeliness/punctuality, accessibility/clarity, comparability, and coherence (ONS, 2005).[83]

Three of these in particular assist in judging individual data products—accuracy, timeliness/punctuality, and accessibility/clarity; the current REA criteria focussed on accuracy and accessibility/clarity (timeliness, while important, is less of an issue here: given the paucity of data on fraud: put simply, older figures may be better than nothing).[84] The other dimensions—relevance, comparability, and coherence — are typically used in evaluating a statistical system (i.e. a country's national statistical office or national statistical programme) in the holistic sense. These dimensions of data quality are of greatest importance when aggregating figures on fraud from different sources and when exploring strategies for future data capture.

[83]Data quality as an issue has received considerable attention from a number of national statistical offices and international organisations around the world in the last five+ years (see, for example, ONS, 2005; Laliberté *et al*, 2004; OECD, 2003; Brackstone, 1999). Though these efforts focus on national statistics, many of the issues raised are relevant here. For more information on data quality, see the International Monetary Fund, which maintains a comprehensive data quality reference website: <http://dsbb.imf.org/Applications/web/dqrs/dqrsintroduction/>. Note also that certain authors/organisations employ five dimensions of data quality, and others seven or eight—but the concepts are the same (numbers differ due to the amalgamation or expansion of certain quality dimensions).

[84]Further, the elapsed time between the occurrence of fraud and its realisation by the victim or bystander, as well as the elapsed time for the report to be made to the authorities, has an impact on timeliness. This renders analysis/understanding of fraud trends more difficult in principle than analysis/understanding of the trends seen with other sorts of offences: changes in levels of fraud over time may result from changes in underlying fraudulent behaviour and/or from changes in the realisation/reporting of fraud (a similar point is made in NERA, 2000).

Dimension and definition	Key components
1. Relevance	
The degree to which the statistical product meets user needs for both coverage and content.	Any assessment of relevance needs to consider: • who are the users of the statistics • what are their needs • how well does the output meet these needs?
2. Accuracy	
The closeness between an estimated result and the (unknown) true value.	Accuracy can be split into sampling error and non-sampling error, where non-sampling error includes: • coverage error • non-response error • measurement error • processing error • model assumption error
3. Timeliness and punctuality	
Timeliness refers to the lapse of time between publication and the period to which the data refer. Punctuality refers to the time lag between the actual and planned dates of publication.	An assessment of timeliness and punctuality should consider the following: • production time • frequency of release • punctuality of release
4. Accessibility and clarity	
Accessibility is the ease with which users are able to access the data. It also relates to the format(s) in which the data are available and the availability of supporting information. Clarity refers to the quality and sufficiency of the metadata, illustrations and accompanying advice.	Specific areas where accessibility and clarity may be addressed include: • needs of analysts • assistance to locate information • clarity • dissemination
5. Comparability	
The degree to which data can be compared over time and domain.	Comparability should be addressed in terms of comparability over: • time • spatial domains (e.g. sub-national, national, international) • domain or sub-population (e.g. industrial sector, household type)
6. Coherence	
The degree to which data that are derived from different sources or methods, but which refer to the same phenomenon, are similar.	Coherence should be addressed in terms of coherence between: • data produced at different frequencies • other statistics in the same socio-economic domain, and • sources and outputs

Source: ONS, 2005.

ANNEX 2. Quality assessment criteria

In the light of the very substantial difficulties outlined in the Methods section of the report, a more 'flexible' approach to assessing data quality was called for. Following the conventions set in other REAs, the study team generated a QAT to guide the systematic assessment of sources. The QAT, however, was used strictly as a roadmap, not a pure grading template.[85]

The criteria applied are set out in the QAT form below. Note that a particular premium was placed on including data that was reasonably current and that applied to the UK only. In short, the QAT was used strictly as a roadmap, not a pure grading template.

Table 2.1. Quality assessment criteria

Criterion	Options
Data-collection methodology	Census/administrative records
	Probability sampling
	Nonprobability sampling
	Not reported
Type of frauds measured	Confirmed frauds
	Suspected frauds
	No distinction drawn (confirmed + suspected frauds)
	Not reported
Use of counting rules	Counting rules employed
	No counting rules employed
	Not reported
Sources of error/bias addressed	Adequately addressed
	Not adequately addressed
	Not addressed at all
	Not reported
Secondary data analysis (if any)	Employs appropriate methods or no secondary analysis
	Employs inappropriate methods
	Not reported
Timeliness of data capture	Data collected since 2004
	Data collected 2000 to 2004
	Data collected pre 2000

In sum, the research shaped up as follows:

- The relevant databases were searched using a wide range of keywords.
- A first sift of the available sources was conducted based on (1) their relevance to an understanding of the nature, extent, and cost of fraud; and (2) their status as primary (as opposed to secondary) research. Only relevant primary sources were considered.

[85]The criteria highlighted in the QAT proved important not only in assessing existing sources of data, but also in looking to future data needs.

- The sources surviving the first sift were then judged against the QAT roadmap. Sources judged to have insufficient data quality were excluded from the next stage of the research.
- Those sources (and their findings) judged to have sufficient data quality were subsequently described.
- Finally, informed by the available data — and by the topics and areas found to have no or weak information — strategies for future data capture were developed and set out.

Limited information about the way data were assembled[86] and analysed meant that the research team had to make numerous clarifying requests to authors—many of whom were found to be subcontractors, requiring multiple metadata requests from different organisations.[87] But authors were often reluctant to release underlying methods, sometimes for understandable confidentiality reasons (not least to ensure fraudsters would not use such information to their advantage). When information on methods was absent or was insufficiently detailed, it was not an entirely straightforward decision on whether or not certain studies should be discussed in the research.

[86]Somewhat beyond the requirements of a typical REA, the study also looked to the broad range of public and private sector organisations who are affected by fraud and/or who are tasked with fighting fraud to request existing, if unpublished, information on fraud and fraud response costs. Of course, given the sensitivities of fraud (e.g. relating to reputational risk), all information providers were promised that confidential information would only be presented in aggregate, without identifying characteristics.

[87]Spending a great deal of time speaking directly to authors appears to fall well outside the bounds of a typical REA; the research team is unaware of any other REA which allowed sources to comment and provide clarifying information - albeit, it was fair and sensible to give authors the opportunity to provide information that their initial audiences might not have needed/wanted.

ANNEX 3. The 'top-down' approach to measuring fraud losses[88]

The NERA (2000) study identified a top-down approach to estimating the economic implications of fraud from the country-risk premium on the cost of capital. As the study stated, this is not a straightforward process as the existence of any risk premium would include other types of risk (such as inflation and capital risk) and identifying what is specific to fraud (as contrasted with default risk) would not be a trivial exercise. Insofar as corruption and fraud are connected, external assessments of corruption put the UK as the 11th least corrupt nation to do business in, with a higher rank than Germany, France, Canada and USA. A low corruption index suggests that a country-specific fraud risk premium is negligible and does not cause serious economic harm to the UK.[89] Previous studies of the UK market risk premium identify that inflation risk was the main factor in explaining the higher cost of capital UK firms faced in the global capital market. Since the independence of the Bank of England and the recent history of low inflation, the risk premium measured in various ways has declined to negligible figures.[90] This suggests that the aggregate fraud-specific risk premium would be relatively low and would not be significant in the country cost of capital.

However, this does not mean that the fraud risk premium is insignificant in all markets. An alternative approach is to focus on measures of fraud-specific risk in particular industries where fraud has been known to be significant. In this note we will examine the economic costs of fraud in three areas; Credit Cards, Insurance, and Benefits.

Methodology

Ultimately the costs of fraud in an economy fall on the consumer. The NERA bottom-up approach evaluates the cost of fraud from the perspective of the producer. The costs of fraud will include the actual losses incurred by the producer and the resource costs of fraud prevention and investigative/legal costs of reactions to fraud. The proportion of resources devoted to fraud prevention will be dictated by its marginal cost relative to marginal benefit which provides for an optimal level of fraud pass-through.[91] These costs are part of the producer's 'bottom-line' which will be passed through to the consumer in the aggregate pricing contract. The rise in the price of the specific product as a result of a fraud-specific risk premium will reduce market demand to the extent of the price sensitivity of demand for the product. The economic

[88]This Annex has been prepared primarily by Professor Kent Matthews.

[89]Corruption Perception Index http://www.transparency.org/policy_research/surveys_indices/cpi/2005 for 2005. The UK has a score of 8.6 jointly with the Netherlands on a 10-point scale of 'cleanness'. The highest rank is Iceland with 9.7 and the lowest are Bangladesh and Chad with a joint score of 1.7. There is significant intellectual controversy over the TI corruption index, only partly because of its cumulative compilation from a variety of surveys. See http://www.icgg.org/corruption.cpi_2005.html for an exposition of the rationale.

[90]For a recent examination of the market risk premium see HM Treasury (2003)

[91]Normally the term pass-through refers to the extent to which an exchange rate change is reflected in the prices of imported goods. With full pass-through, a currency depreciation, which increases the price of foreign currency, would increase the prices of imported goods by the same amount, and vice versa. With no pass-through, prices of imports remain constant. Here we use the term pass-through as indicating a certain amount of fraud that is expected and therefore tolerated. In the case of insurance fraud, this could be conducted through an optimal incentive contract which recognises that the best strategy is to allow all claimants to over-claim. See Crocker and Morgan (1998).

cost can be decomposed into the loss of potential business for the market as a whole and the loss of consumer surplus (welfare cost) to the consumer. The concept of loss of business for the market and the net welfare loss to the consumer is shown below in Figure 1.

Figure 1

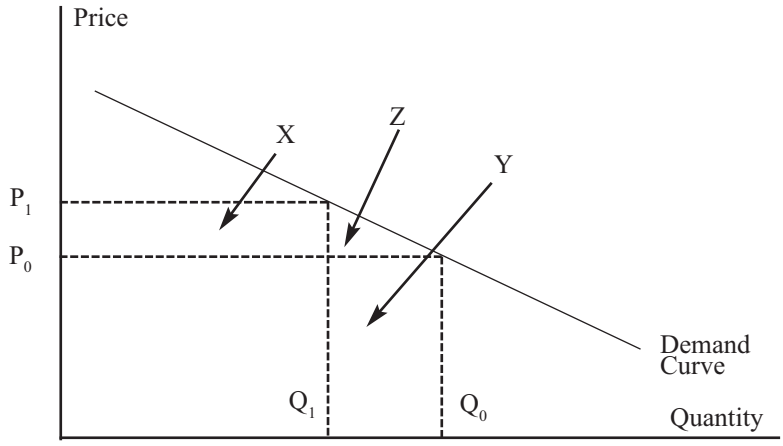

Figure 1 shows a demand curve for a product and the quantities demanded for given prices P_1 and P_0. The value of the loss of market business from a rise in price due to a fraud-specific risk premium is given by the rectangle Y. The value of the gain in market business is shown by the rectangle X. The net loss (or gain) to the particular market will depend on the price elasticity of demand.[92] However, there is also a non-monetary loss to the consumer which is shown by the triangle Z (approximated by $= {}^1/_2(P_1 - P_0)(Q_0 - Q_1)$). In terms of welfare losses the amount Y is the displacement from the particular market which is assumed to be transferred to other areas of the economy (substitutes) and is therefore not thought of a net loss to the economy. The area X represents the cost of the fraud which is passed on to the consumer and corresponds to the producer's cost. The triangle Z is the welfare loss. The net loss to the economy is given by X+Z, which represents the loss of 'consumer surplus'.

The above analysis is purely a partial equilibrium (which means that it is concerned with the particular market in question) and fails to account for the general equilibrium implications of the cost to households (in terms consumption of other goods foregone or wider externalities) of meeting the costs of fraud. However, in the case of benefit fraud it is possible to get closer to a general equilibrium perspective with the aid of a macroeconomic model.

A partial equilibrium analysis of unemployment benefit fraud would suggest one of two possibilities. First, the receipt of fraudulently obtained benefits would have sufficient income to allow the recipient to consume maximum leisure and not work. Second, some recipients of fraudulently obtained benefits would prefer to receive the benefits even at the expense of lower pay in the black economy than consume maximum leisure. Whether they work in the black economy at lower than market wages per hour or at the same rate, the assumed preference for leisure would mean that they would substitute work hours for leisure and work a less than normal week.

[92]The revenue loss in continuous time is $dQ(P)$ and the revenue gain is $dQ(P)$. There is a net revenue loss if $|dQP| > |dQP|$, which occurs when the price elasticity of demand is greater than unity

$$\left|\left(\frac{dQ}{dP}\right)\right|\left(\frac{P}{Q}\right)\Bigg| > 1$$

What the above analysis suggests is that people on low wages constrained to work a full week may prefer to obtain state benefits that subsidize their income and work a less than standard working week. Therefore the output loss from withdrawal from the labour market is less than 100%. However, this is only a first-round effect. Second-round effects stem from the recognition of the general equilibrium nature of the issue.

The second-round effects can be decomposed into fiscal effects and further supply-side effects. Benefit fraud is a drain on the public purse. One could think of the fraudulent claim as a transfer from another area of public spending or an extra amount of revenue generated from taxation or borrowing (future taxation). If the extra revenue to meet fraudulent benefit claims is met out of income tax, there is a further second-round effect from incentives in the labour market and supply-side responses. If it is funded from borrowing, the second round effects will depend on whether the fraud is a one-off or sustained. If it is a one-off the externality effects are negligible. If it is sustained then, the permanent level of borrowing increases resulting in some level of the crowding out of private expenditure with resulting output effects.

'Top-down' estimates

Credit Cards

Total plastic card fraud in 2004 was £504.8 million and around half (£259.3 million) of this amount was due to Credit and Charge card fraud[93]. With 71.9 million credit cards in circulation in 2004, this is an annual average fraudulent use of £3.60 per account (not per person). The total aggregate credit outstanding of Visa and Mastercard in 2004 was £64,518 million of which 73% incurred interest charges. Therefore the aggregate net credit card debt outstanding at end 2004 was £47,098 million. This figure stands close to the Bank of England seasonally adjusted end year figure for net credit card debt at £47,334 million. In the calculation that follows, the Bank of England figure for net credit card debt will be used.

There have been remarkably few studies that have examined the responsiveness of credit card usage to interest rate changes, though the development of microfinance research has begun to change this. Using Italian micro data Alessie *et al* (2005) estimate median interest elasticities of demand in the range -1.510 to -2.142 with further variations according to type of credit card, geographical region and individual characteristics. These estimates can only be a guide to the responsiveness of UK credit card consumers to interest rate changes, however they indicate what is a generally accepted view, which is that the demand for consumer credit is strongly interest elastic. These elasticities can be used as a range to estimate the credit business foregone as a result of a fraud risk premium on the interest charge and the potential welfare loss.

It can be assumed that the aggregate cost of fraud falls on the card providers, which will raise the interest charge on credit cards through an explicit risk premium or an increase in unit costs[94]. The calculation of the fraud risk premium relating to credit cards is shown in Table1

Table 1 Calculation of fraud risk premium

Credit card losses from fraud in 2004	£259.3 million
Net outstanding credit card debt 2004	£47334 million
Losses as % of net debt	0.55%

[93]British Bankers' Association – Abstract of Banking Statistics 2005

[94]The rate of interest rate charged on a credit loan will depend on the cost of funds, unit costs of the provider, market power and a risk premium. See Freixas and Rochet (2002)

A risk premium of 0.55% (55 basis points) is used in combination with the range of elasticities to estimate the equilibrium credit business foregone and the loss of consumer surplus – shown in Table 2.

Table 2 Externality cost of credit card fraud premium

Elasticity	Supply cost of Fraud (Area X) £ million	Welfare Loss (Area Z)	Net cost to economy: loss of consumer surplus (Area X+Z)	Loss of Market to industry (Area Y)	Overall cost to Industry (Area X+Y+Z)
-1.510	259.3	1.1	260.4	393.1	653.5
-2.142	259.3	1.5	260.8	557.6	818.4

Table 2 shows the long-run loss of extra credit card business (area Y) which represents a stock equilibrium. However, the adjustment of a stock to full equilibrium within one year is a strong assumption. One usually thinks that an increase in the cost of borrowing takes more than one year to take full effect on the stock of borrowing. To move towards the flow decrease in net lending in the year requires further assumptions relating to the short-run and long-run elasticities. Gross and Souleles (2002) use confidential credit card data issued in 1995 to study the responsiveness of credit card debt to changes in interest rates and credit limits in the USA, within a dynamic setting. Short-run and long-run elasticities were estimated to be -0.8 and -1.3 respectively. These estimates provide ball-park estimates of the speed of adjustment of the stock equilibrium that will in turn give an indication of the total flow of credit business lost in 2004 as a result of credit card fraud[95].

For illustration of this point, let y_t be the stock of credit in period t, let x be the rate of interest and b the β interest elasticity. The flow of net credit card spending in the period t to t-1 is z_t and described by equation (1);

$$z_t = y_t - y_{t-1} \qquad (1)$$

$$y_t - y_{t-1} = \lambda\left(y^* - y_{t-1}\right) \qquad (2)$$

$$y^* = \beta x_t$$

Equation (2) describes a partial adjustment of stock equilibrium to the long-run desired equilibrium given by y^* where $(0 < \lambda < 1)$. Re-parameterising equation (2) gives;

$$y_t = \lambda\beta x_t + (1-\lambda)y_{t-1}$$

where $\lambda\beta$ is the short-run elasticity and λ is the speed of adjustment in each time period. From the study by Gross and Soulules (2002) $\lambda\beta = -0.8$ and $\beta = -1.3$, hence $\lambda = 0.615$, which says that 61.5% of the stock adjustment occurs in the first year, a further 61.5% of the remainder in the second year and so on. Table 3 gives an estimate of the net flow of extra credit card lending lost from fraud in 2004.

[95]The total volume of credit lost as a result of a fraud-risk premium is an equilibrium stock adjustment. This adjustment may take more than one year to occur, in which case only a proportion of the total credit lost will have occurred in the first year, with the rest occurring in the years following.

Table 3 Estimate of equilibrium loss of credit card business and loss of credit card business in first year.

Decrease in equilibrium Credit Card Debt	Loss of net credit business in 2004
£393.1 million	£255.5 million
£557.6 million	£362.4 million

The total gross cost of credit card fraud to the private sector in 2004 is in the range £353- £558 million – significantly more than the amount of direct card fraud alone. In the long-run, the total gross cost to the private sector is shown in Table 2 and is in the range £653 – £818 million. The net cost to the economy as a whole in the long-run is £260.4 – £260.8 million.

Insurance Fraud

UK commercial insurance fraud is estimated to be in the order of £550 million a year.[96] The cost of fraud equates to 5% on a typical insurance premium. If there is significant price responsiveness in the demand or commercial insurance, a 5% increase in premiums would be expected to create a strong element of under-insurance.

There have been numerous theoretical studies relating to corporate demand for commercial insurance but relatively few empirical studies[97]. These studies typically identify the corporate characteristics of the purchaser that influence demand and if the purchase of insurance influences the cost of capital for the firm. However, none of the studies estimate the price responsiveness of corporate insurance demand, largely because the data on individual insurance payments are not usually declared in company accounts. Empirical studies do not confirm or deny the existence of price responsiveness, but corporate finance theory suggests that the demand for corporate insurance is likely to be price inelastic. Standard theory suggests that corporate purchases of insurance protect stockholders against risk of loss and therefore insurance acts as a signal to investors. While modern financial theory argues that investors can hedge against insurable risks through diversification, only large institutional investors have this capability and the signalling theory remains a powerful argument.

Assuming price inelasticity in the corporate insurance market means that the risk premium from fraud creates less of a misallocation of resources, but it could create significant 'wealth effects' for the firm that could result in under-investment in other areas of enterprise (including distributed profits). In the case of a perfectly price inelastic demand for corporate insurance, the full cost of the fraud is passed on to the purchaser. The dead-weight loss to the purchaser is offset by underinvestment by the firm or an equivalent reduction in dividend payments to households. Simulations with the aid of a macroeconomic model suggest that such redistribution has a negligible effect on the wider economy.[98]

Other areas of potential insurance fraud are in automobile, housing and health.[99] In each of these cases, both theory and empirical evidence tends to support a price inelastic demand, so that the welfare cost created by the fraud premium is minimised.

[96]Association of British Insurers (2005)

[97]Mayers and Smith (1990), Core (1997), Davidson III *et al* (1992) and most recently Yamori (1999)

[98]The Quarterly Liverpool Macroeconomic model was used to conduct the simulations but the use of an alternative model such as the Treasury model is unlikely to result in a significant difference.

[99]Automobile insurance is a legal requirement and is therefore a complementary demand for vehicles, whereas empirical studies of non-catastrophe home insurance and health insurance in the presence of a public health system shows price insensitivity. See for example Martin *et al* (2000) and Emery and Gerrits (2005).

Benefit fraud

Benefit fraud is estimated to cost the Exchequer £960 mn a year. This figure amounts to nearly 0.8% of the total benefit expenditure in Great Britain in 2005. While 40% of the £960 mn represents official error, total payments – whether planned or unplanned – have been made to recipients who would otherwise have had to engage in the labour market to make up some of the fraudulently obtained income (or adjust their lifestyles downwards).

Two simulations were conducted to evaluate the wider economic costs of benefit fraud. In the absence of benefit fraud and official error, the expected benefits to the representative household (think of this as the average household) would be 99.2% of the actual benefit payments made. The fiscal implication of the benefit fraud is the £960 mn on benefit expenditure which should be viewed as extra revenue generated through taxation, which would otherwise remain in the hands of the private sector.

There are several ways simulation analysis can be used to evaluate the implications of benefit fraud. First, the total benefits defrauded have to be funded. They could be funded first by borrowing, second by an increase indirect taxes and third, by an increase in direct taxes. Each simulation would produce different outcomes. Furthermore the outcomes would differ from its impact effect and its long-run effect (over a number of years) depending on whether the fraud is treated as a one-off or a continuous level for the indefinite future. The Liverpool Macroeconomic model is used to conduct two simulations; an increase in expected benefits and a rise in taxes of the equivalent of £0.9 bn. Because a simulation is the artificial injection (positive or negative) of an impulse to an economic model we can treat the numbers as assumptions. The ratio of output to impulse remains roughly the same for any level of impulse. If £0.9 bn is thought to be too high and a lower figure of 50% is considered more realistic, the output effects would be commensurately 50% less.

The increase in expected benefits produces the supply-side effects on GDP on the assumption that recipients of benefit fraud do not work in the unrecorded economy and therefore all the output losses from withdrawal from the recorded labour market represents a net output loss to society. The analysis of section 2 above suggests that this not a likely scenario. Recipients of fraudulently obtained benefits are likely to work part-time and possibly at a lower than market wage rate.

Table 4 below shows the results of the simulations. It is assumed that benefit fraud recipients work 50% of a working week in the 'black economy' so that the estimated output loss from labour market withdrawal is offset by some black economy activity.

Table 4 Estimated Output Effects of Benefit Fraud

Simulation	Net output loss – short run	Net output loss – long run
Benefits	£47 million	£168 million
Fiscal effect	£434 million	£2,763 million
Total £481 million	£2,931 million	

The results of the simulation suggest that the impact effect of the fraud in terms of net output losses in current prices is £481 million. The long run or equilibrium net loss is £2.9 billion.

The ratio of fraud to net economic losses provides an indicator of the areas resources should be directed in anti-fraud operations. Table 5 illustrates.

Table 5 Ratio of victim cost to fraud

SectorFraud	Net cost*	ratio
Benefit	£960 m	£2,931 m 3.05
Credit Card	£259.3 m	£260.6 m 1.01
Insurance	£550 m	£550 m 1.00

* long-run. Note that net cost does not include the cost to the defrauded person or sector as this is a transfer from one individual or sector to another individual or sector. The net cost represents the cost to the economy as a whole.

In the case of credit card fraud, the mid-point of the range was taken as representative. In the case of insurance fraud, the general finding of price inelasticity suggests that the economic loss from a fraud risk-premium would be less than the total fraud losses. Table 5 suggests that anti-fraud resources should be allocated in the order of net output loss to total fraud, which puts benefit fraud at the top and insurance fraud at the bottom.

Other areas for investigation

The British Bankers' Association estimates that non-plastic related fraud (e.g. cheque fraud) totalled £107.6 million in 2004. This is the amount of undetected fraud that managed to bypass security systems and staff vigilance and get through to the banking system. Total potential (or perhaps, more accurately, attempted) fraud was in the order of £1,152 million, of which around 90 per cent was intercepted by staff and security systems. It is not possible to obtain estimates of resource costs devoted by the banks to fraud detection. If these resource costs are significant, then it would be reflected in interest rate spreads and the cost of credit to borrowers. However the actual amount of loss from fraud is less than 0.4% of gross income of the banking sector in 2004.[100]This is well inside the recommended capital requirement for operational risk under the Basle 2 rules and will therefore not create any marginal capital charges. The NERA report referred to estimates of the 'hidden economy' but concluded that measurement is difficult, as different methodologies yield different estimates. However, we would argue that different methodologies and measures are ways of obtaining triangulation, which provides ball-park figures of the size of the black economy relative to GDP.

The earliest studies of the hidden economy in the UK used the currency demand method pioneered by Cagan (1958). These studies have tended to produce highly variable estimates of the size of the hidden economy as a percentage of GDP. More recently, researchers have utilised family expenditure survey and estimation of Engel curves to obtain measures of the hidden expenditure by comparing the 'risky' groups with safe benchmark groups.

[100]Gross income is defined by the Bank for International Settlements as net interest income and fee income which corresponds to total revenue. Total revenue of the banking sector in 2004 was in the order of £30 billion.

Table 6 below presents a sample of estimates using different methods. The currency demand method (which tries to isolate currency used for recorded transactions from unrecorded transactions) shows rising estimates of the hidden economy through the 60s to mid 1980s. The consumer demand method shows a similar rise in the estimates from the 1980s through to the first half of the 1990s. Pooling a number of methods, the review paper by Schneider and Enste (2000) show estimates in excess of 10% of GDP.

Table 6 Published Estimates of the size of Unrecorded Economy

Source	Method	Data period	% of GDP
Matthews (1982)	Currency demand	1979	5.8 – 7.1
Bhattacharyya (1990)	Currency demand	1984	7.9
Pissarides and Weber (1989)	Consumer demand	1982	5.5
Lyssiotou *et al* (2004)	Consumer demand	1993	10.6
Schneider and Enste (2000)	Various methods	1994-95, 1996-97	12.5 – 13.0

The mean figure for the estimates is 8.7% with a standard deviation of 3. These estimates confirm the NERA conclusion that methods of measuring the hidden economy produce widely differing estimates. However, to fall on the hurdle of measurement is no reason to ignore it. The hidden economy is a significant part of the UK economy that is probably in the region of 10% of GDP or roughly £122 billion. However, not all of this is valid unrecorded economic activity (meaning activity that could be produced in the legal recorded economy). Strictly, illegal activity would be the trade in sex and narcotics. There are no reliable estimates of the economic activity in these areas (the BBC reported a figure of £1 billion for the sex industry in a series of programmes aired between March and April 2005) and the Home Office has several unpublished studies of the levels of 'organised crime' harm in the UK (see also SOCA, 2006). It is therefore possible that the dominant share of the unrecorded economy is due to activities that could be reproduced in the regular economy. The purpose of presenting measures of the hidden economy is to demonstrate that unrecorded economic activity due to tax and benefit fraud would be included in the estimate but there is no way of identifying specifics.

Summary

1. There is no evidence that the UK faces a general fraud risk premium on the cost of capital. However, that does not mean that individual markets do not face significant fraud that may be reflected in the price of particular trades. We examined three areas where fraud is thought to have had a significant impact; the credit card market, the insurance market and the labour market (unemployment benefit fraud).

2. The cost of credit card fraud is passed through to the consumer of credit card services in the form of a fraud risk premium which raises the price of credit above what it would have been in the absence of fraud.

3. The higher price of credit in the credit card market is likely to reduce the demand for credit over time. There is empirical evidence to support the view that the credit card market is responsive to changes in the price of credit.

4. The cost to the consumer is measured by the loss of consumer surplus. This is measured by the costs incurred by the producer of credit (assumed to have been passed on to the consumer) and the welfare loss to society.

5. n addition to the loss of consumer surplus, the higher cost of credit has led to a decline in demand for credit which is a loss of business for the credit market.

6. In economic welfare terms this loss of business is assumed to be offset by an increase in business elsewhere in the economy and is therefore not seen as part of the net costs to society. However, from the credit card industry point of view this is a valid 'opportunity cost' – business that otherwise would have occurred.

7. The higher price of credit caused by fraud may take some time to influence the credit card market. Estimates of time adjustment suggest that the market would adjust by 61.5% in the first year, 61.5% of the remainder in the second year and so on.

8. We have not unearthed any evidence that the market for insurance as a whole is price sensitive. Naturally we would expect the demand for individual suppliers of insurance will be price sensitive but there is no evidence that insurance as a whole is price sensitive.

9. The finding of price insensitivity means that the loss of consumer surplus corresponds to the cost of fraud faced by the supplier. There is also no loss of aggregate business in this market as a result of a higher price of insurance caused by fraud.

10. In the case of benefit fraud we conducted a simulation based on a full macroeconomic model. A simulation is an artificial evaluation of a scenario. We ask the question, what is the overall economic effect of benefit fraud totalling £960 m? The actual numbers produced are less interesting than the ratio of input to output. Because the economic model used is generally linear in small impulses, the inputs and outputs remain in proportion.

11. Benefit fraud affects the labour market through the impact on the recipients of benefit fraud. People receiving benefits fraudulently may withdraw from the labour market altogether or work part-time in the unrecorded economy. In the latter case the output loss from withdrawal from the labour market is partially offset by work in the black economy. In the simulation, we assume that only 50% of the output is lost due to withdrawal from the labour market.

12. Externalities occur due to the funding of the benefit fraud. These externality effects need to be distinguished between a 'one-off' benefit fraud and a sustained level of benefit fraud. Furthermore the output effects caused by the externalities will depend on the assumptions made about the funding of the benefit fraud.

13. If it is assumed that the benefit fraud is one-off and is funded from borrowing or general taxation, there will be negligible effects on the economy.

14. If it is assumed that the benefit fraud is sustained over a number of years, then the output effects will be significant and the magnitude will depend on the funding assumption.

15. In the case of funding from income taxes, there is an effect on work incentives and the market wage in the labour market which results in a marginal reduction in labour supply. In the case of funding from indirect taxes there is a marginal effect on private expenditure which leads to a contraction in demand.

16. In the case of borrowing, there is a marginal effect caused by expected future taxes and a rise in government bond interest rates which causes some crowding out.

17. The numerical magnitude of the output losses are largest in the case of funding from income taxes and smallest from an increase in borrowing.

ANNEX 4. Studies reviewed and their methodological approaches

Victim sector 1: Fraud against the private sector

Sub- sector 1. Fraud against the financial services sector

Sources available

Published sources of information on fraud against the financial services sector are few in number, though in the scheme of things are fairly wide ranging and may represent some of the best sources on fraud. Data are typically collected through administrative record-keeping. For example, the most comprehensive sources – from APACS (which uses an acronym in absence of the underlying words, instead calling itself "the UK payments association") and CIFAS (which similarly uses an acronym but has abandoned the underlying words, instead calling itself "the UK's Fraud Prevention Service") – are derived from administrative data at the membership-organisation level. Administrative data are captured both to inform policy-making (APACS) and for tactical intelligence purposes (CIFAS, whose data inform the credit-granting decisions of its member institutions).

Survey work on fraud against the financial services sector also exists, including work carried out by the FSA, that commissioned by the Association of British Insurers (ABI), and several UK or even global surveys of fraud directed by various professional services firms (e.g. PriceWaterhouse Coopers, Ernst & Young, KPMG, BDO Stoy Hayward, RSM Robson Rhodes, Mishcon de Reya). Those of the latter sources that are recent enough and pass over the methodological threshold are discussed in a subsequent section, as they also relate to fraud against multiple victim sectors (i.e. not exclusively financial services victims). Surveys are typically designed to illustrate the scope of the problem for policy-making purposes or to describe the views of respondents with regard to their attitudes on fraud.

The administrative and survey data relate to the volume and value of fraud losses. Perhaps not surprisingly, information on costs in anticipation of/response to fraud is much harder to come by. The only source which addresses anticipatory/response costs in any collective manner is the CIFAS response to the Fraud Review.

Studies reviewed and their methodological approaches

The main studies reviewed and their respective methodological approaches are outlined below[101].

1. **Fraud: The Facts (APACS, 2006):** APACS releases cheque and plastic fraud figures which are

[101] Note that this research has focussed on publicly available information. A number of sources exist which are not available in the public domain (for example, detailed firm-by-firm information gathered in the course of Financial Services Authority (FSA) work on firms' high-level management of fraud risks (FSA, 2006) was not released to the project team– understandably so, given likely commitments made by the FSA to keep detailed findings confidential). Additionally, certain anti-fraud initiatives gather information on fraud and fraud reports, but have yet to produce/release relevant statistics on volumes/values (and may never do so); these include the FSA initiative on the voluntary reporting of intermediary mortgage fraud; the FSA Financial Crime Information Network (FIN-NET, formerly the Financial Fraud Information Network, or FFIN); the UK insurance industry's Insurance Fraud Bureau (IFB); and work underway at the ABI. Along similar lines, APACS is assembling what it calls the Fraud Dashboard, which will summarise fraud volumes/values for a larger number of frauds than its standard cheque and plastic publication; this source is in development, and should be publicly available in due course. Note also that the annual reports of various financial services firms (and indeed organisations in other sectors) occasionally provide information on annual spends on a compliance departments, bad debt estimates, and so forth. Because there is no clear mention of fraud costs (i.e. there is no clear activity-based costing which specifies the proportion of spends attributed to anticipatory/response costs), such annual reports have not been included here.

summarised in the Fraud: The Facts publication (and which may be found in other APACS statistical releases). The information presented relates to fraud volumes and values with respect to losses. The publication is based on the administrative records of APACS members (as noted by the APACS website, APACS has 31 members with 97 percent of the total UK payments market by traffic volumes). According to APACS (information on methods is not included in this publication, and was provided directly by APACS staff), aggregate data are provided monthly by members in accordance with APACS guidelines, which spell out the concepts and counting rules to be followed. For plastic card fraud, members provide aggregate information on total numbers of cards in issue; the circumstance of card loss or compromise; and place of misuse. For cheque fraud, members provide aggregate information on counterfeit, forged, and altered cheques. The 2006 publication presents annual data for 2005 and includes historical data for ten years for plastic fraud and four years for cheque fraud.

2. **CIFAS Online Press Releases ("£1,400 of Fraud Prevented Every Minute"; CIFAS, 2006a):** CIFAS, the "UK's Fraud Prevention Service", is a membership organisation of some 230+ entities from the financial industry, including those in banking, credit cards, asset finance, retail credit, mail order, insurance, and the like. CIFAS members file details of fraud or attempted fraud on the CIFAS database; members employ this shared database (delivered via Experian, Equifax, Callcredit, and MCL Software) when deciding whether or not to grant credit to an applicant. CIFAS releases statistics on its website (www.cifas.org.uk) on a quarterly basis (a number of different reports/press releases are available, which often slice the CIFAS data in slightly different ways, and which present findings quarterly, semi-annually, or annually).[102] Statistics include the number of fraud cases and subjects identified, and the financial benefit of the CIFAS database for a certain period of time (e.g. January-June 2006).

3. **CIFAS Member Consultation on Government Fraud Review (CIFAS, 2006b):** As with virtually all trade bodies, CIFAS prepared an official response to the Fraud Review.[103] In so doing, CIFAS undertook a census of its membership (which it calls a "membership consultation") to estimate annual expenditures on fighting fraud; the percentage of "successful" frauds reported to the police; views on whether or not all frauds should be reported to the police; preferred methods of reporting frauds to the police; and steps members would like to see to design fraud out of the system. Seventy of the 230 member organisations replied; it is not clear what percentage of total membership this seventy represents when considering turnover. The respondent pool is not summarised, save for comments on how the 70 represent a "fair cross section of organisations both in terms of size of organisation and business sector".

4. **UK Commercial Insurance Fraud Study 2005 (MORI/Commercial Insurance Fraud Steering Group, 2005):** To gain an understanding of fraud in commercial insurance lines (e.g. commercial property and motor vehicle fleet insurance), the ABI and a syndicate of insurers commissioned MORI to conduct a survey of businesses and employees. The intent of the project was to ascertain the scale and nature of fraud against the commercial insurance sector. MORI conducted two [probability sample] surveys in 2005: a business survey and an employee survey. The business

[102]CIFAS has also commissioned various research projects over the years, the results of which are summarised on the CIFAS website. While interesting, most are not of direct relevance to an understanding of fraud volumes/values, and are not included in the body of this report. One piece worth mentioning briefly is a study on deceased frauds (CIFAS, 2004), which is the result of data-matching with CIFAS data and deceased lists; results suggest that deceased fraud figures previously published by CIFAS understated the problem, and that deceased fraud costs some £250 million/year (though the methodology behind this estimate is unclear). Though understated, the thrust of the problem was stated in earlier CIFAS statistics. Another piece of research, a study on employee fraud (CIFAS, 2003) surveyed a sample of 127 CIFAS member organisations, with what appears to be a third responding. Among other things, the research suggests that employee fraud may exceed £40 million (though, again, the methods and the basis for extrapolation from a one third response rate are not clear).

[103]The official responses of other trade bodies to the Fraud Review typically did not make mention of fraud volumes/values (save for simply restating previous estimates/hypotheses), and as such are not included here.

survey explored the opinions of 1,102 individuals responsible for arranging commercial insurance with their organisation. The employee survey explored the opinions of 323 employees (through face-to-face interviews) covered by their organisations' commercial insurance policies. Survey data on attitudes towards fraud were then combined with ABI figures on insurers' claims to derive an estimate of commercial fraud losses.[104]

Sub-sector 2. Fraud against the non-financial services sector

Sources available

The surveys that have been conducted can be broken down into three main categories. These include:

1. **International:** Surveys conducted for the purpose of making international comparisons of crimes against business: Such surveys include The International Crimes against Business survey (Van Dijk and Terlouw, 1995) and the International Crime Business Survey (2000).[105]

2. **National:** National surveys covering either the United Kingdom or individual countries within the UK: Such surveys include the British Retail Consortium Surveys (which covers the UK), the Home Office Commercial Victimisation Survey (which covers England and Wales) and the Scottish Business Crime Survey (which covers Scotland). There is no corresponding survey for Northern Ireland.

3. **Local:** Local surveys covering specific streets, areas of towns/cities, or specific 'themes', such as crimes against business in a particular sort of location or type of business: Such surveys include The Small Business and Crime Initiative Surveys (Wood *et al*, 1996, Tilley and Hopkins, 1998) which was based on businesses in Leicester and Camden Three Streets Survey (Hopkins and Tilley, 1998) based on three streets in North London.

For the purpose of this research, data have been reviewed that are seen as being most relevant to this study both in terms of timeliness and the geographical location of the achieved sample. Therefore data prior to 2000 have been excluded, and the focus is on national level data relating to England/ Wales or the UK as a whole. It was considered that however good earlier studies such as the Scottish Business Crime Survey 1998 (Burrows *et al*, 1999) were, such data might not reflect accurately contemporary patterns of fraud against businesses. (Any methodological lessons for future data capture strategies are incorporated elsewhere.) In addition to this, the studies reviewed are also from national surveys. Though some local studies (such as the Small Business and Crime Initiative studies) have yielded good data, they are more useful for highlighting localised victimisation patterns, and may not represent national patterns.

Studies reviewed and their methodological approaches

The main studies reviewed and their respective methodological approaches are outlined below.

1. **Fraud against retailers: British Retail Consortium 'Retail Crime Costs' survey (BRC, 2005):** Annual survey that began in 1993. The main aim of the BRC surveys is to measure the costs of crime for retail outlets. The methodological approach is based upon collecting data from the head offices of businesses rather than interviewing individual premises (unlike the CVS- see below). Postal surveys are distributed to the head officers of all major multiples in the UK that trade through a number of outlets: in 2004 this totalled 13,360. The survey data are collected over a 12-month recall

[104]Note that the ABI commissioned a study on public attitudes to insurance fraud in 2002 (ABI/Frank, 2002). As this study focused exclusively on attitudes—and makes no mention of volumes or values of fraud—it has not been included here, though attitudes or willingness to commit fraud affect behaviour.

[105]It should be noted here that in the 2000 ICBS there is no UK sample.

period that matches the financial year and covers: Cheque fraud, Card payment fraud, Application fraud, Card not present fraud, Counterfeit notes and 'other fraud'.

2. **Fraud against retailers and manufacturers: *Home Office, 2002 Commercial Victimisation Survey (Shury et al, 2003),*:** Directly interviewed business premises (through telephone interviews) and broadly replicated the approach of the 1994 survey (see Mirrlees-Black and Ross, 1995). The overall sample for the study was 6,516, of which 3,955 were retail and 2,561 manufacturing business premises. Two broad categories of fraud were considered in the CVS: 'fraud by outsiders' and fraud by 'employees'.

3. **Fraud suffered by member businesses in the cooperative movement: Cooperative Movement survey of its members: Cooperative Movement (Cooperative movement, 2004):** The most recent survey (presented data for April 2003/2004 and published in June 2004) was the fourth completed by the Co-op and generated a sample of 2,498 businesses. The sample covered 59,398 staff and a total business turnover of £5bn. The survey considered losses for cheque fraud, credit/ debit card fraud, 'card not present fraud' and 'other' fraud. Though the actual numbers of incidents are not presented for these fraud types, some data on costs (losses) are.

4. **Telecommunications fraud: Telecommunications UK Fraud Forum (TUFF, 2006):** An estimate of the total loss to telecommunications fraud 2004 was made through figures supplied by TUFF. Losses to fraud in telecoms range from 3 to 15% of turnover, with higher figures being typically generated by 'start up' firms, so large firms predominate. TUFF estimate that the industry average for fraud is 2.4% and as a proportion of retail revenue figures for 2004 from OFCOM, the figure of £866 million is reached. The figures assume that the calls made illicitly would all have been paid for at full price had fraudulent opportunities not been available, and in this sense represent genuine opportunity costs, although the direct marginal costs to the businesses of the frauds were typically very modest, since the telecoms facilities are there whether used or not.

Sub-sector 1 and 2. Fraud against companies in both the financial services and non-financial services sector

Sources available

PricewaterhouseCoopers (2005); Hi Tech Crime Unit (2005) KPMG (2006); BDO (2006); and SFO (2006).

Studies reviewed and their methodological approaches

The main sources of data available in relation to fraud against multiple victim types relate to surveys of businesses (PWC, Robson Rhodes and Hi Tech Crime Unit), fraud cases that have been charged to appear in or have been heard in UK courts (KPMG fraud barometer and the BDO Fraud Track survey) and the Serious Fraud Office annual reports, which contain cases that would be included in the KPMG and BDO reports.

The studies reviewed and their respective methodological approaches are outlined below:

1. **Global Surveys of fraud where a number of UK businesses form part of the sample: PricewaterhouseCoopers (2005):** The global economic survey (2005) was based upon interviews with 3,634 chief financial officers (CFOs) and chief executive officers (CEOs) in 34 countries, randomly selected from the top 1000 in each country – there were 300 UK companies sampled. The businesses included were drawn from financial services (17%), manufacturers (28%), services (28%),

technology (10%) and trade (wholesale/retail) (17%). 'Fraud' is broken down into a number of categories including asset misappropriation, false pretences, financial misrepresentation, insider trading and counterfeiting. The survey has a two-year recall period.[106]

2. **Computer related crimes experienced by business: Hi Tech Crime Unit (2005):** Third survey of businesses completed in 2005 (with data relating to 2004). A total of 200 telephone interviews were completed with businesses. The sample breakdown included: manufacturing businesses (25%), retail/ wholesale (15%), professional services (13%), financial services (11%), transportation (11%), construction/ engineering (10%), others (6%), IT sector (5%), Utilities (3%) and telecommunications (3%). The focus was on businesses with over 100 employees. It is not clear how many outlets are covered by the survey.

3. **KPMG fraud barometer (KPMG, 2006):** The KPMG fraud barometer has been published every year since 1990, and is now published twice a year (see UK KPMG Fraud Barometer, 2006). This considers fraud cases in excess of £100,000 with defendants charged to appear in UK courts: those under £100,000 are not included. The barometer considers cases in relation to financial services, non-financial services company, government, investors and 'other'.

4. **BDO Fraud Track Report (BDO, 2006):** Similar to the KPMG fraud barometer, but with less cross-checking of sources, the BDO collates data about all confirmed business related fraud cases with losses of over £50,000. The most recent study reports on data from 1st January 2005 to 31st December 2005.[107] Data are drawn from press releases. This included a variety of fraud including breach of regulations, employee fraud[108], financial misstatement, non-corporate, tax, third party fraud and unauthorised use. The data are not broken down in to these categories of fraud, though some data are presented by business sector.

5. **Serious Fraud Office Annual Reports (SFO, 2006):** These do give data on high-value cases accepted after vetting, involving different sorts of victims, but not cost breakdowns per victim sector. The data include sums considered to be at risk of fraud, which are not separated from actual losses.

Sub-sector 3. Fraud against private individuals

Sources available

Sources used here include: Office of Fair Trading (2006) 'scams' survey, parts of which are unpublished but made available to this study; the FSA 'boiler room' study, of which only a public notice communication is available[109]; a CIFAS-funded study of identity fraud (Pascoe *et al*., 2006) and data derived from the Solicitors' Indemnity Fund/Compensation Scheme.

[106]For more details of methodology in the PWC study, see Bussman and Werle (2006).

[107]There was also a survey of public attitudes to fraud (sample of 1,360) and attitudes to fraud (sample of 2,010), though this is beyond the scope of this study and is not included here.

[108]Employee fraud was further broken down into procurement fraud, payment fraud, revenue diversion fraud, cheque fraud, payroll fraud and expenses fraud.

[109]See http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/053.shtml

Studies reviewed and their methodological approaches

The main studies and their respective methodologies are reviewed below:

1. **The Office of Fair Trading scams survey (OFT, 2006):** The OFT has not historically examined the cost and incidence/prevalence of frauds. The survey used a combination of focus groups and larger scale probability sample surveys in two stages, an omnibus survey and then a follow up of 1,900 people who stated that they had been a scam victim, knew someone who had, or had been unsuccessfully targeted.[110] The study examines the correlates and costs of scams.

2. **The Financial Services Authority (FSA)'s 'boiler room' study (FSA, 2006):** Over a five month period, callers to the FSA who reported being targeted by boiler rooms were asked to complete an online survey about their experiences. The target sample size was 100, and when the reports reached that total, the study stopped. A sub-set of 58 of those who filled in the survey were actual victims who reported losses by purchasing shares via boiler rooms, and costs were analysed with regional demographics.

3. **CIFAS study of identity fraud victims (Pascoe *et al*, 2006):** This involved sending questionnaires to a total set of victims of identity fraud registered on the CIFAS database, plus a non-probability sample of individuals registered as either 'innocent victims' or 'impersonated' on the databases of six CIFAS member organisations.

4. **Fraud involving solicitors:** administrative data from unpublished but not confidential information from the Law Society Compensation Fund and Solicitors' Indemnity Insurance, and from the (now defunct) Pensions Compensation Board.[111] Financial services and law firms themselves would normally compensate, or be expected to compensate, individuals defrauded by them, and such data are not published or even collated, outside the payment card/cheque sectors.

Victim sector 2: Fraud against the public sector

Sub-sector 1. Fraud against national bodies

Sources available

A number of reports consider public sector fraud. Most of these reports are produced by individual government departments, reflecting their responsibilities, and through National Audit Office reports on departmental work, and it is seldom possible to conduct any read-across for categories such as procurement fraud. Intelligence sharing is uneven and sometimes is restricted by legislation (for example from HMRC to other bodies).

The coverage of frauds against national bodies is however uneven. Income tax fraud, for example, is relatively ill-analysed, due to greater methodological difficulties. As the Public Accounts Committee (2004)

[110]In discussion with the current authors, the OFT researchers expressed much more confidence in responses to the second detailed interviews than responses to the first rather superficial recruiting omnibus surveys. A significant proportion of people who had originally classified themselves as "knowing others" or "targets, but not victims" in response to the omnibus questions recognised themselves as having actually been victims when subjected to deeper probing. The origins of these changes merit some exploration and reflection.

[111]In the future, the Fraud Compensation Fund within the Pension Protection Fund will be included, but it became operational only in September 2005. The Financial Services Compensation Scheme is an independent body that pays compensation to consumers if a regulated firm is unable to pay claims against it, but its data have been excluded because they do not distinguish (and for institutional purposes do not need to distinguish) whether or not those losses are due to fraud. The FSCS is mandated not to pay out on frauds committed by unregulated legal or natural persons

noted: "The Revenue…have not estimated the level of fraud or the "tax gap", the difference between full compliance with tax regulations and actual compliance…. The Revenue have not been able to use a similar approach [as VAT] for direct taxes as no independent baseline exists to assess the level of income or profits that should be declared and the level of tax due. …. The Revenue have therefore been identifying areas of particular risk through programmes of random enquiries on tax returns for individual tax streams. Having strengthened their analytical capacity they were now seeking a better way of estimating the tax gap." The progress made in this respect has not been reported. A variety of different methods are used. Most estimates are based upon operational evidence from random enquiry programmes and risk assessments, but supplemented by other intelligence sources including Suspicious Activity Reports made by professionals and financial institutions.

Fraud against the financial interests of the European Union has a less direct, but nonetheless significant effect upon the UK taxpayer. Although OLAF has some investigative and prosecutorial staff, it is mainly reliant on investigations conducted by the member states, and much variation is experienced between them. Here, however, it is important to take into account the complexity of interests in identifying fraud. On the income side, customs duties (including anti dumping duties) for exports accrue 100% to the EC budget: so if this is lost, it is lost to the EC budget and has to be made up through GNP-based contributions by all Member States, who thus become *pro rata* victims. A difficulty is that customs duties are often lost alongside national excise and VAT frauds (a proportion of which is contributed to the EC budget). On the expenditure side, programmes are often co-financed by member states and the EC, so fraudulent losses through structural funds, external programmes such as foreign aid, subsidies of various types, and direct costs of the European Commission can affect both budgets. Perhaps surprisingly, in the light of political concerns about 'EU fraud', there are no readily available data on this issue, as on the specific fraud costs to any Member States. The European Court of Auditors (2006) and the National Audit Office (2006d), *inter alia*, have pressed the European Commission to make methodological improvements in distinguishing fraud from irregularities, but as the UK Public Accounts Committee Chair has observed, this is almost impossible to do in an absolute sense. OLAF (2006) reports total identified fraud cases involved €323.47 million for the EU25, mostly the EU17. However given the difficulties of knowing, defining, reporting and prosecuting frauds, this would seem to be a modest total.[112] There are no data published on the UK's share of frauds against UN and World Bank budgets: a less complex issue than EU fraud, but one where most of the offending would occur outside the UK.

Studies reviewed and their methodological approaches

The main studies reviewed, and their respective methodological approaches, are outlined below:

1. **Frauds against government departments (HM Treasury, 2005, 2006):** Chapter 5 of Government Accounting 2000 requires departments to make an annual return to the Treasury, for themselves and their agencies, of all cases of confirmed actual or attempted thefts or frauds, classified by contractor frauds, staff fraud, and frauds by the public that are both £20,000 or more and are

[112]The strategy for investigating possible frauds and irregularities varies over time and between member states. To the extent that there is no prioritisation, intelligence and follow-up are mostly derived from scrutiny visits and whatever technology is in place. Responsibility for reporting irregularities (including fraud) in the United Kingdom is shared between the Department for Trade and Industry for Structural Measures and the Rural Payments Agency for the Common Agricultural Policy (CAP). They have significant scrutiny and compliance staff and send to OLAF quarterly reports detailing the number and value of the irregularities detected, what follow-up action they have taken, and whether the case has been resolved. They also produce an annual report listing any money that has been recovered from the previous year and explaining what has been done with the money that has been recovered. In the past, the European Court of Auditors used to publish a global error rate for the whole budget (the last occasion being 5.4 per cent for the 1996 budget), but it discontinued this practice as: (a) any figure quoted was inevitably misinterpreted as relating to fraud rather than error; (b) no account was taken of amounts which were later recovered; and (c) the fact that the data were derived from randomly selected samples meant that the activity and geographic areas varied, making them not simply comparable over time.

deemed to contain generic lessons for others. The annual reporting exercise covers fraud affecting departments and 'their' agencies. Non-Departmental Public Bodies (NDPBs) are not required to complete an annual return. However, details of frauds or thefts perpetrated against NDPBs with a value of £20,000 or more that contain valuable lessons for others should be reported to the Treasury via their sponsor departments.

2. **Benefits fraud (National Insurance Fund Account (NAO, 2006a), Department of Work and Pensions (2005a, 2005b, 2006a, 2006b, 2007), Office of National Statistics (2005b).**[113] The methodological approach used by DWP to assess fraud and error is evolving, although their accounts (not uniquely) are 'qualified' annually by the NAO because of what the latter refer to as an unacceptable level of fraud and error. There has been a recent improvement in methodology (NAO, 2006b), so older studies will not be reviewed: furthermore, recent competent reviews summarise the sectoral methods and findings so, given space constraints, there is no advantage in analysing them all individually. As stated in DWP (2006, p80 and 2007), the robustness of estimates vary according to the methodological approach taken. At present there are three groups:

- Estimations made through continuous non-probability sampling exercises. (Fraud and error in income support, jobseekers allowance, pension credit and housing benefits are all now measured by using such methods.)
- Estimations made through one-off snapshot exercises (disability living allowance, incapacity benefit, instrument of payment and retirement pension)
- Areas where there is no reliable figure (council tax, attendance allowance).

In the latest National Audit Office report (NAO, 2006) the rounding and overall accuracy levels used throughout the estimation process were tightened and the resulting details more transparent. The fraud and error estimate – which was previously reported as an overall total and rounded to the nearest £0.5 billion – was reported in tabular format that reflects the more extensive details from the underlying estimation work and is rounded to £0.1 billion. Furthermore, the overall degree of tolerance in the total estimate, which provides a good measure of accuracy, also improved to +/-£0.3 billion from closer to +/-£0.5 billion. The methods used in DWP (2005b) led to a reclassification of some frauds as non-fraud (see also DWP 2007 for a fuller discussion of methodology and more refined data). Benefits where there has not been any recent measurement activity make up around 15% of total DWP expenditure. For most of these benefits, a flat rate of 2.7% overpaid expenditure is assumed as this was the average overpayment in the benefits the DWP could measure in 2003/4, when the methodology was first developed.

3. **Disability Living Allowance frauds (DWP, 2005c):** To complement the continuous measurement exercises in other areas, the DWP conduct a periodic individual 'snapshot' probability sample review of 1,200 claims within areas selected for geographical spread, to examine the correct entitlement of each. As in other DWP studies, conduct was classified as 'fraud' if there is overpayment and:
- there was evidence, by admission or third party verification, that the customer could reasonably have been expected to know either that they had provided incorrect information at the start, or something had changed in their circumstances that they should have informed the Department about; and
- there was a (judged) probability of intent to defraud on the customer's part.

4. **Tax credit fraud (National Audit Office, 2005c and HM Revenue and Customs 2006).** In addition to the routine checks on all tax credit claims, HMRC carried out compliance work in specific high risk-assessed areas (NAO, 2005c). In 2003-04 and 2004-05, HMRC carried out two special

[113]Additionally, there are abundant annual and periodic surveys of sectors, monitored by the National Audit Office and the House of Commons Public Accounts Committee, which are omitted here unless they add to the portrait of fraud.

exercises to check child care costs with the providers who were contacted to verify the details provided by all claimants whose award included an element for child care costs, though these checks were reduced the following year. Patterns of claiming via the e-portal showed that a rapid rise in claims (from 10,000 to 30,000 per week in 2005) indicated rapid exploitation of opportunities coinciding with large scale leaking of identities, to the extent that the e-portal had to be closed, though the portal with DWP has subsequently been reopened (HMRC, 2006a). HMRC tests a probability sample of enquiries against claimant records and then extrapolates to an estimate of combined fraud and error. A separate report by HMRC analysed approximately 4,500 randomly selected 2003-04 awards that were paid for the full year (HMRC, 2006a). The random enquiry programme checked whether the information used to determine the claimant's entitlement to tax credits at the end of year (during which period circumstances may have changed) was a true reflection of the claimant's circumstances. (See NAO, 2005c, above).

5. **Indirect tax fraud: Missing Trader Intra-Community Fraud (Ruffles and Williams, 2005):** This type of fraud takes two forms: (1) acquisition fraud, where the goods are imported from the EU by a trader who then goes missing without completing a VAT return or Intrastat declaration after selling the goods to an internal buyer. The 'missing trader' therefore has a VAT free supply of goods, as they make no payment of the VAT monies due on the goods; and (2) Carousel fraud, which is similar in the first stage, but the goods are not sold for consumption on the home market but through a series of companies and then re-exported to another Member State (or can be merely paper transactions without real transfer of goods). As part of the VAT return which firms over the VAT threshold complete each quarter, there is a declaration of the total value of dispatches of goods to customers in other EU Member States and the total value of arrivals of goods from suppliers in other EU Member States. These returns provide a direct estimate of the size of UK dispatches to and arrivals from the EU. The detailed measurement of trade in goods within the European Union is based on the Intrastat system. Any trader whose annual trade for either arrivals or dispatches is above a given threshold (£221,000 in 2004) is required to submit an Intrastat form each month, set such that a required percentage (at least 97 per cent) of all trade is collected. In MTIC fraud, the importing missing trader does not submit VAT returns, and in virtually all cases these traders also submit no Intrastat returns. This has a corresponding impact on the trade statistics.

6. **Indirect tax fraud: MTIC fraud relating to alcohol, tobacco and hydrocarbon oil consumption (HMRC Annual Report 2004-2005):** This annual report (HMRC, 2005a) presents data for indirect tax fraud/ loss from missing trader intra-community fraud and excise losses relating to alcohol, tobacco and hydrocarbon oil consumption, discussed also in more methodological detail in HMRC (2005b, 2006b) and National Audit Office (2006). In the case of VAT, the total fraud/loss is calculated by estimating VAT theoretical tax liability – the total level of VAT that would be received in the absence of any loss – ONS national accounts are used to calculate total amount of national expenditure liable for VAT (based on commodity breakdowns) and any legitimate reductions in the VAT liability occurring through schemes and relief are made. This gives the net theoretical liability. The actual annual receipts of VAT are then subtracted to give a tax gap. The gap is assumed to be the VAT loss due to non-compliance (error), non-payment, avoidance and fraud. HMRC (2005b, 2006b) discusses estimating total UK consumption of each good from time series of the results of surveys of consumers.[114]

[114]For alcohol and tobacco, where survey respondents have a tendency to underreport consumption, identifying a period during which it is anticipated that little or no fraud took place and then comparing the survey estimate of consumption during this period with total legitimate consumption to obtain an uplift factor to adjust for underreporting; applying the uplift factor to the trend in survey reported consumption to obtain an estimate of total actual consumption in each year; deducting legitimate UK Duty-Paid consumption using HMRC clearance data which, as this is not derived from a survey, is considered accurate; deducting legitimate cross-border shopping from survey data collected from international passengers, and data from the trade on sales of duty free goods; assuming that the residual element – the gap – represents the level of fraud in the good.

7. **Spirits Fraud (Goddard and Compton, 2005):** This study reviewed the difficult arguments about the level of spirits fraud, in which HMCE's estimates of spirits fraud were about five times higher than those from the Scotch Whisky Association. The method used for estimating spirits fraud is to subtract HMRC data on clearances from bond (on which tax has been paid) from survey estimates of spirits consumption, which in theory would include consumption of illicit spirits on which tax had not been paid. The survey sources available are of two types: those based on respondents keeping a diary of expenditure and/or consumption, and those based on a questionnaire in which quantity and frequency of drinking are asked. For the diary based approach, the Expenditure and Food Survey is a better source than the National Food Survey, capturing double the off-licence spirits consumption.

8. **TV licence evasion (TV Licensing Annual Review 2003/04, BBC Annual Reports and Accounts 2004/05).** An estimate is made of the loss to the BBC annually in relation to TV licence fee evasion (see TV Licensing Annual Review 2003/04, BBC Annual Reports and Accounts 2004/05). The estimates are derived by first calculating the number of households that should have a valid TV licence (this is done by using ODPM household data and BARB data on the supposed 'TV penetration rate': for example, in 2003/04 there were just over 28 million households in the UK and the TV penetration rate was 98%. Therefore 98% of the 28 million households should have a TV licence). The total raised revenue from licensing is calculated and from this an estimate is made of the 'evasion' rate.

9. **Frauds relating to vehicle excise duty (Driver and Vehicle Licensing Agency Annual Accounts, 2004-05, 2005-06).** The Driver and Vehicle Licensing Agency Annual Accounts (DVLA, 2005, 2006) make an estimate of the total loss to vehicle excise duty evasion, basing these on periodic roadside surveys of 1 million vehicles that are on the highways. The licence numbers were run against the agency's records to estimate the percentage of vehicles on the road that were not licensed.

10. **NHS Fraud (Countering Fraud in the NHS: Protecting Resources for Patients: 1999-2005 Performance Statistics):** No estimates of the total value of fraud to the NHS are available, though a series of Risk Measurement Exercises (run by the Risk Management Unit) are currently being run by the NHS Counter Fraud Service (CFSMS) to estimate total losses in various areas across the service (Fraud Review, 2006).[115] The Risk Management Unit focuses on an area where there are known losses in relation to fraud and validates the data available, on a case-by-case basis, to ascertain if fraud has actually occurred. The data are analysed and extrapolated for the whole population within the area being investigated and statistically validated (to a +/-1% figure). It is estimated that by 2008, the NHS will have figures for losses contained in 75% of NHS spend.

Sub-sector 2. Fraud against local bodies

Sources available

There are no published data that focus specifically on fraud in local authorities. NERA (2000) considered local government fraud in the light of data in Audit Commission (1988)[116], but currently, all local government fraud is flagged up in the Comprehensive Performance Assessments, introduced in 2003-04. Each single tier, county council and district council is audited every 12 months, although the assessment is in relation to provision of services and does not routinely publish details of fraud in the authority. The National Fraud Initiative data-matching exercise accounts for some but not all local authority frauds,

[115]Data on the Risk Management Exercises to date have been published through the NHS Counter Fraud and Security Management Service (see Countering Fraud in the NHS: Protecting Resources for Patients 1999-2005 Performance Statistics).

[116]This included identified fraud in relation to student awards, renovation grants and fraud by local authority employees.

for example working while claiming, or claiming relief from council tax at the same time as receiving another benefit inconsistent with that: matches are sent to the local authority (who may act on them or not).

Studies reviewed and their methodological approaches

Some of the main costs in relation to fraud in local authorities are accessible through central Government reports, but these have been reviewed in other sections of this report. For example, the resource costs in relation to housing benefit and council tax costs are published in DWP resource account reports (see DWP, 2006a). However, there are other fraud costs to local authorities (such as fraud in relation to student awards, renovation grants and fraud by local authority employees) where it is unclear if these are included in national estimates of costs. For example, DWP publish some 'unreviewed' estimates on fraud in relation to 'other' benefit payments; though it is unclear what this actually measures.

ANNEX 5. Tables summarising fraud losses against the different sectors

Continued on next page

Table 5.1: Summary of data for financial services sector losses

Source	Method	Costs 1: Transfer Loss Data	Cost 2: Costs in Response to fraud	Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
Fraud: The Facts (APACS, 2006)	Data based on aggregate administrative information provided monthly to APACS by APACS members	Plastic card fraud losses in 2005 amounted to £439.4 million, down from £504.8 million in 2004. Cheque fraud losses in 2005 amounted to £40.3 million, down from £46.2 million in 2004.	No data	No data	One year recall period (with historical data), completed annually, APACS membership only
CIFAS Online Press Releases ("£1,400 of Fraud Prevented Every Minute"; CIFAS, 2006a)	Administrative records of use of the CIFAS database by CIFAS members	For the period January-June 2006, the CIFAS database identified 85,128 fraud cases (up 12.5 percent from the same period in 2005); 122,633 subjects (up 16.2 percent from the same period in 2005); and £360 million in financial benefits	No data	No data	Quarterly, semi-annual, and annual recall period (depending on CIFAS press release; with historical data), CIFAS membership only
CIFAS Member Consultation on Government Fraud Review (CIFAS, 2006b)	Census of CIFAS members for aggregation and inclusion in the official CIFAS response to the Fraud Review (2006); responses received from 69 of the 230 members	No data	Not clear if data on "fraud prevention" include response to fraud	The 70 responding members spent some £70.4 million on fraud prevention (average annual spend per respondent of £1.24 million). Average spend is used to estimate an annual spend for the membership in total of £300 million. Unclear how this total might be affected by grossing-up based on turnover	One-year recall period, one-off data-collection exercise
UK Commercial Insurance Fraud Study 2005 (MORI/ Commercial Insurance Fraud Steering Group, 2005)	Two surveys: a business survey of 1,102 individuals responsible for arranging commercial insurance with their organisation; and a employee survey of 323 employees covered by their organisations' commercial insurance policies. Survey data were combined with ABI figures to derive an estimate of commercial fraud losses	Commercial insurance fraud estimated at £550 million	No data	No data	One-year recall period, one-off data-collection exercise

Table 5.2: Summary of data for the non-financial services sector losses

Source	Method	Costs 1: Transfer Loss Data	Cost 2: Costs in Response to fraud	Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
British Retail Consortium- Retail Crime Costs Survey 2004-2005 (BRC, 2005)	Random sample of postal surveys with head offices of UK businesses representing 13,360 retail outlets.	Costs 1: Transfer Loss Data £68.1m in relation to cheque fraud, card payment fraud, application fraud, card not present, counterfeit notes and other fraud for all retail sector (grossed up). Each outlet loses £1,408 to fraud per year.	No data	Some data on chip and pin costs. In 2004 the average expenditure per store (capital) on chip and pin was £4,130 (compared to £1,756 in 2003).	One year recall period, survey completed annually, focus on retail business only
Commercial Victimisation Survey (Shury *et al*, 2003)	Random sample of telephone interviews with 3,955 retail and 2,561 manufacturing premises (total of 6,516) in England and Wales.	18% retail/ 7.6% man victim of fraud by outsiders. 3.7% retail and 1.6% man victims of fraud by employees. Average cost of last incident- fraud by outsiders £1,278 (retail), £10,146 (man). Fraud by employees- £7,398 (retail), £12,759 (man).	No data	No data	One year recall period, survey not annual, focus on retail and manufacturing premises.
Co-operative Movement Retail Crime Survey 2003/04 (Cooperative Movement, 2004)	Random sample of postal and email surveys with 2,498 member outlets.	5% of all losses to businesses are fraud. Estimated loss of £170K to businesses in survey (an average of £68 per outlet).	Some data on capital and revenue expenditure on security- no breakdown to specific crimes.	No data	One year recall period, annual survey, samples only members of co-operative movement.
Telecoms UK Fraud Forum Data (TUFF, 2006)	TUFF membership data on loss to fraud in telecommunications industry	£866m lost to all fraud, £372m of this is ID fraud.	No data	No data	One off estimate of costs in 2004.

Table 5.3: Summary of data for studies of fraud embracing both the financial services and non-financial services sectors

Source	Method	Costs 1: Transfer Loss Data	Cost 2: Costs in Response to fraud	Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
PWC global economic crime survey (PWC, 2005, Bussman and Werle, 2006)	Telephone survey of random sample of finance directors or other personnel in 300 UK businesses across financial services, manufacturing, services, technology, wholesale and retail sectors.	Tangible fraud- 55% of sample victims. Costs available for asset misappropriation, false pretences, counterfeiting. Loss on average US$800,000 p.a. to each business, totalling around £150 million.	No data	No data	Two-year recall period, survey completed bi-annually, focus is on large businesses.
KPMG Fraud Barometer (KPMG, 2006)	Measures fraud cases over £100,000 in cases charged to appear in Courts. Published each year since 1990.	In 2005 charges were £942m.	No data	No data	Twice yearly and 6 months recall period. Published at least annually since 1990
Hi Tech Crime Unit Survey 2004 (Hi Tech Crime Unit, 2005)	Sample of 200 telephone interviews with businesses across manufacture, retail/ wholesale, professional services, financial services, transportation, construction/ engineering and 'others.'	Financial Fraud- £690m Telecommunications Fraud- 77.7m [to all UK business]	No data	No data	One year recall period, annual survey, focus on large business with over 100 employees.
BDO Fraud Track (BDO, 2006)	Collates data on all media-reported business related fraud cases of over £50,000.	In 2005 charges were £981m.	No data	No data	Annually and 12-month recall period. Published annually since 2003.
SFO Annual Report (SFO, 2006)	Collates information on sums at risk of being defrauded in cases accepted for investigation.	Sums at risk estimated £2.06 billion at beginning of FY 2005.	£41 million gross (excluding police costs)	N.A.	Annual reports, though cases mentioned may stretch over several years' reports

Table 5.4: Overview of costs of fraud against central government

Source	Method	Costs 1: Transfer Loss Data (proportion of spend in brackets)	Cost 2: Costs in Response to fraud	Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
National Insurance Fund Account 2004-2005 (NAO, 2006a)	Draws together work from DWP resource accounts 2004-05.	Retirement pension- £60m Incapacity Benefit- £80m Contribution Based Jobseekers allowance- £30m Other benefits- £30m	NERA used Beating Fraud is Everyone's business (1998): the current DWP view is that all staff have mainstreamed anti-fraud work	No data	Annual
DWP Resource Accounts 2004-05	Based upon continuous rolling sampling exercises	Carer's allowance - £40m. (3.9) State pension - £30m. (0.1) Incapacity benefit - £10m. (0.1)	No data: see above	No data	Annual
DWP Fraud and error in claims for Income Support, Jobseekers allowance and pension credit from April 2004 to March 2005	Based upon continuous rolling sampling exercises	Income support working age- £240m (2.3) Jobseekers allowance- £50m (2.2) Pension credit- £60m (1.0)	No data: see above	No data	Annual
DWP Fraud and error in claims for housing benefit	Based on continuous rolling sampling of 10,000 to 14,000 cases per year	Housing Benefit- £140m; £170m for full extrapolation (1.3)	No data: see above	No data	Annual
DWP Fraud and error in and other inaccuracies in Disability Living Allowances 2005	Random sample of 1,200 claims across 33 geographical areas	Disability Living Allowance- £40m (0.5)	No data: see above	No data	Periodic

Table 5.4: Overview of costs of fraud against central government – continued

Source	Method	Costs 1: Transfer Loss Data (proportion of spend in brackets)	Cost 2: Costs in Response to fraud	Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
HM Revenue and Customs Annual Report 2004-05; **HM Revenue and Customs Measuring Indirect tax loss 2005**	Loss estimated by calculating the VAT theoretical tax liability	MTIC – £1.12bn to £1.90bn (acknowledged to be out of date – recent media reports suggest £8 bn.) Spirits £250m [03/04] Cigarettes 2.2bn [03/04] Hand-rolled tobacco £700m [03/04] Hydrocarbon Oils – £600m [2004]	Investigations = £428m (though merger of HMRC and extra focus on MTIC will probably have altered this)	No data	Annual
HM Revenue and Customs Annual Reports, income tax fraud	No data at present, but combination of random enquiries and intelligence from other sources, including SARs	Total revenue loss- £11.3bn But no specific calculation of fraud	Resource costs in NERA, now outdated but not updated	No data	Report annual
Driver and Vehicle Licensing Agency Annual Accounts 2004-2005	Roadside survey at 256 sites in June 2004	£129m in 2004-2005	No data	No data	Annual
HM Treasury Fraud Report: An analysis of reported fraud in Govt departments 2004-2005	Reports to Treasury Assurance, Control and Risk Team groups	£3.1m in 2004-2005	No data	No data	Annual

Table 5.5: Overview of fraud cost data against other public sector bodies

Source	Method	Costs 1: Loss Data / Costs 2: Transfer in Response to fraud		Costs 3: Data on prevention and anticipatory costs	Frequency and recall period
NHS Annual Report 2004-2005; Countering Fraud in the NHS: Protecting Resources for patients 1999-2005 Performance Statistics	Based on analysis of data case by case in each area to ascertain if fraud has occurred	£72.2m lost in 2004/05 / £22.27m in patient fraud (2003-04) £47m to pharmaceutical patient fraud (2003-04) £21.1m dental patient fraud (2003-2004) £10.17m optical patient fraud (2003-04)		No data	Annual
BBC Annual Report 2005-2006	Number of households that should have TV license against actual number and gap is considered fraud/loss	No data / £145 million (4.7% evasion rate) in 2005-06		No data	Annual

ANNEX 6. Information on fraud offenders

The criminal backgrounds of offenders and the way that they relate to each other – both now and plausibly in the future – are a key component of a threat assessment model for fraud (and 'organised crime') that should influence the preventive tactics and strategies of both (a) public and private sector organisations at risk from fraud and (b) the wider enforcement authorities. (They may also influence individuals if they are in a position to do something about the risks to which they are exposed.) The extent and nature of fraud represents a combination of situational opportunities and motivated offenders with the contacts and/or skills to take advantage of those opportunities. Both the numbers motivated, and their skills, can change – not least via contacts and training. One way of illustrating this point is to ask what active and passive factors are necessary to enable particular sorts of fraud to happen at all and/or to flourish: not just on 'shoulder surfing' spy cameras and false ATM fronts, or concealed connections between traffic 'accidents' for insurance frauds, but also deeper issues like wilfully blind legal services to hide beneficial ownership of companies; or (in procurement fraud and in payment card fraud by merchants) active insider corruption/failures in cross-border database integrity checks. In a sense, the wrong question has often been asked about 'organised crime', which is to ask if 'it' is organised in a particular way, whereas the more sensible question is to ask what factors over time shape the ways in which crimes of certain types are organised and who gets involved in them? We might expect this to vary according to the types of frauds and the need for expert assistance from other offenders or from innocent professionals who facilitate the creation of nominees/corporate fronts.

There are issues of general prevalence and incidence of fraud offending in the general population, but also of offender organisation, that are relevant to the choice of appropriate policing and prevention strategies. Neither the Home Office nor any other UK government department has ever conducted or sponsored any specific study of fraud offenders. Most of the few fraud offender studies that have been carried out have been done by snowball non-probability sampling totalling fewer than 20 offenders (Gill, 2005; Levi, 1981, 1988, 2003)[117]and while the findings have often been interesting, they can hardly be authoritatively presented as representative.

The Home Office Offending, Crime and Justice Survey examines the incidence and frequency of a very limited range of relatively low-value fraud offences among a representative sample of the general population. No financial benefits for offenders were estimated, nor did the survey ask about co-offending, which is necessary in order to understand criminal and social networking. One per cent of 12- to 25-year-olds reported using someone else's card or card details without the owner's permission in the last 12 months. The level of card fraud by offenders aged 18 to 25 years remained broadly stable (2% in 2003 and 1% in 2004, but – given sampling error – not a statistically significant change). Moreover, among eligible 18- to 25-year-olds, claiming falsified work expenses and committing insurance fraud was relatively common, by 16 per cent and 10 per cent respectively. Less than one per cent of all 10- to 25-year-olds reported that they had made a false insurance claim for a mobile phone in the last 12 months, with no differences between males and females or across age groups. Benefit fraud and income tax evasion were less common (each at 2%). Moreover, one per cent of all 10- to 25-year-olds admitted sending computer viruses and computer hacking; illegal downloading of software, music or films was committed by around a quarter of Internet users in this age group in 2004. As for offending diversity,

[117]One of the very few studies worldwide (Weisburd and Waring, 2001) examines the criminal careers of convicted US federal offenders, but on a sample from the 1980s. Though described as 'white-collar criminals', many are 'blue collar' as the offence category includes social security fraudsters.

around a quarter of fraud and technology offenders had committed either a serious or frequent offence (or both) in the last 12 months: so although the majority were not generalist offenders, a substantial minority bridge fraud, technology and 'normal' offending. Whether this pattern is true for older offenders is unknown.

There have been attitude surveys that shed some light on the motivation/willingness to offend, if not on actual offending rates. Retail insurance fraud is the area in which this has been done with greatest sampling accuracy (see, for example, ABI/Frank Research, 2002), but the early Ernst & Young surveys from 1985 did ask a probability sample of senior executives in FTSE-500 quoted companies for their attitudes to a range of frauds (Levi, 1987, 1988, 1992). Response rates for sub-sectors were not kept, so the surveys' representativeness cannot be assessed; and executive attitudes may have changed since the 1980s and early 1990s, after which these questions were dropped. Karstedt and Farrall (2006) discuss both general attitudes and self-reported offending data in relation to a range of everyday 'market offences' for general non-probability samples of 1,807 25-65 year olds in England and Wales (and Germany). The restriction of the age range should help to target mainly individuals who as adults and part of the active work force were confronted with a roughly equal set of opportunities to commit 'everyday crimes' when selling cars, dealing with tradespeople or taking out insurance.[118]

Although the development of multi-crime type 'serious/major crime units' looks as if it takes into account the complexity of criminal activities of crime networks, in practice such squads are dependent on where they can get human and technical intelligence from, and these may more likely come from the anti-drugs than from the anti-fraud arena. If the same criminal personnel are active in both types of crime, this may not matter (except in crime statistics) but if they are not, then this advantages some groups – particularly specialist fraudsters – against others.

Data on offender self-reports and organisation are best triangulated with data on victimisation to help to test their explanatory power, but more extensive data mining of victimisation data may (as in the payment card and insurance industries, and with applications frauds generally) yield insights into commonly unseen connections between cases that in turn generate reasonable suspicions of well-organised fraud. Whether such frauds are or should be dealt with by prosecution may depend on resources and attitudes, and also (as dealt with elsewhere in this report) on whether the corporate victims see that there is any point in reporting these connections to the authorities. Policing bodies historically have been poor at developing Covert Human Intelligence Sources (CHIS) or more open source information on financial crimes on the UK mainland, but in tax and banking crimes, this has begun to change and represents a further arena of improving knowledge, though one presenting challenges to the police, HMRC and SOCA. However, as with snowball offender interviews, there is a danger in generalising from the 'previously unknown but now known knowns' to the wider population. A CHIS can normally only tell us about persons involved in co-offending, whereas many frauds (and other crimes) can be perpetrated without active co-offending; and penetration by more generic crime networks may vary between fraud business sectors e.g. may be

[118]Intentions to offend were measured by scaling the strength of such intentions. Respondents were asked if they "would consider", "would never consider", or "depending very much on the situation" consider doing each of the following: "agree to pay or to be paid 'in cash' in order to avoid paying VAT or other taxes"; "during an insurance claim, add items which had not been lost, damaged or stolen, or increase the value of any items claimed"; "when selling second hand hide or not disclose faults in what you were selling"; and "try to claim for replacement items, refunds or compensation from a shop, small business or travel agent's which you were not entitled to". These items covered large as well as small business, and private exchanges. The scale of intentions to offend is a sum score of these items and strongly correlated with a scale of actual offending, which measures if respondents had ever committed any of ten offences (r= .55), indicating that specific intentions to offend are easily generalised to other opportunities if these present themselves. Correlations between intentions and actual offending for the individual items range between r= .55 for paying cash in hand, and r=.26 for cheating on an insurance claim (coefficients for the total sample). Altogether, looking at 'ever committed offences', 34% admitted that they paid cash in hand to avoid taxation; 11% wrongly used identity cards for their own gain (e.g. student prices); 7% 'padded an insurance claim' and 3% 'deliberately mis-claimed benefits for own gain'.

stronger in payment card merchant, ATM-tampering, retail insurance, spread-betting and telemarketing scams than elsewhere, for example in individual embezzlement by senior company officers, Enron-type executive conspiracies, or price-fixing cartels. Intelligence on some of the latter may be enhanced by whistleblower policies, whether active and reward-based (as in the UK Enterprise Act 2002 and the US False Claims Act 1863 and plea-bargaining models) or profit-neutral (as under the UK Public Interest Disclosure Act 1998), which may reduce the stigma from being a 'sneak'. A more acute awareness of the difficulties of extrapolating modes of organising fraud would be healthy, and the data on the levels and nature of fraud victimisation reviewed in this study are a helpful corrective for this.

ANNEX 7. Summary of estimated fraud losses

Principally but not exclusively in 2005 or 2005-06

£ million

Sector and study	Cost 1 Transfer loss	Cost 2 In response	Cost 3 Prevention and anticipatory	Overall sector costs	% by sub sector
Financial Services					
Fraud - the facts (APACS)	£439.70	£2.00			
CIFAS member consultation			£300.00		
FLA motor insurance fraud	£15.00	£0.50			
UK Commercial Insurance fraud	£550.00				
Sector sub-total	*£1,004.70*	*£2.50*	*£300.00*	*£1,307.20*	*9.4%*
Non-Financial Services					
BRC, 2004-5 survey	£68.10				
CVS					
Co-op Movement	£0.17				
Telecoms UK	£866.00				
Sector sub-total	*£934.27*	*£0.00*	*£0.00*	*£934.27*	*6.7%*
Private individuals					
OFT Scams Survey	£2,750.00				
Sector sub-total	*£2,750.00*			*£2,750.00*	*19.8%*
Both FS and non-FS					
PWC UK economic survey	£150.00				
BDO Fraud Track	£981.00				
Hi-Tech Crime Unit	£690.00				
Sector sub-total	*£1,821.00*	*£0.00*	*£0.00*	*£1,821.00*	*13.1%*
Public bodies, national level					
National Insurance Fund account	£200.00				
DWP - Benefit Fraud Total (low end)	£500.00				
HMRC VAT/MTIC etc.	£2,000.00	£428.00			
HMRC Income tax fraud					
HMRC indirect tax frauds	£3,230.00				
HMRC tax credit	£131.00				
DVLA	£147.00				
Rural Payments Agency (EU fraud)		£3.00	£23.00		
HM Treasury -fraud in govt depts	£5.11				
NHS	£76.00		£22.30		
BBC	£145.00				
Police, Prosecution and Courts		£156.50			
Pensions Fraud Compensation Fund		£0.64			
Sector sub-total	*£6,434.11*	*£588.14*	*£45.30*	*£7,067.55*	*50.8%*
Public bodies, local level					
Council tax	£40.00				
Audit Commission NFI			£1.40		
Sector sub-total	*£40.00*	*£0.00*	*£1.40*	*£61.40*	*0.4%*
	£80.00				
OVERALL TOTAL	**£12,984.08**	**£590.64**	**£346.70**	**£13,921.42**	100.1%
% by cost	93.3%	4.2%	2.5%	100.0%	

ANNEX 8. Approaches that could be adopted to improve fraud reporting

The commentary set out in the main text of the report points to four methods which may compel or enhance cooperation with respect to data provision, as suggested by the United Nations Statistics Division (UNSD). These are addressed in turn:

- Compliance enforcement. It seems that a legal compliance regime would in this case be far too draconian (not to mention expensive for all involved). After all, numerous entities in years past wanted to provide the authorities with fraud statistics (in the form of reports of fraud) but were told not to. To install a compliance regime now would seem hypocritical. Further, a suspicious activity reporting (SARs) regime already exists for money laundering—and SARs may already be filed on fraudsters (e.g. if the fraudster's activity lends itself to suspicion of money laundering). Introducing another separate compliance regime could complicate matters (though making use of the SARs regime to further fraud reporting may represent a good use of limited resources).
- Appeals. Fraud reporters are also unlikely to whole-heartedly reply to appeals to their sense of morality. Where was the morality when they were telling the police that they had been defrauded—and the police did little in response?
- Assurances that the information will not be misused will, however, be of some benefit to commercial data providers, who might be the most affected by reputational damage with the inappropriate release of their fraud information. Any recipients of fraud statistics (e.g. National Fraud Reporting Centre) should be housed in secure facilities with properly vetted staff. Along these lines, public confidence in the system should be encouraged. Notes UNSD (2003): "In order for the public to trust official statistics, a statistical agency must have a set of fundamental values and principles that earn the respect of the public. These include independence, relevance and credibility as well as respect for the rights of respondents."
- Incentives have a role to play here. Outright incentives are probably unlikely to be introduced (it's difficult to imagine that favourable tax incentives or subsidies would be introduced for corporate entities which play their part). But indirect incentives could be quite powerful. They might include government attention on fraud (e.g. desired legislative changes); police responsiveness to fraud reports (i.e. investigations launched, arrests made, etc.—though in the absence of a strong increase in resources and training any increase in police responsiveness will be modest); increased budgets for fraud prevention (driven by a spend-to-save mentality); advice and guidance on how to identify/control fraud. On this last incentive, the owner of the fraud statistical system should leverage the experiences of the SARs regime by learning the lessons publicly addressed in recent reports on the regime (e.g. Lander, 2006; Fleming, 2005).

ANNEX 9. Essential ingredients of a non-observed economy implementation strategy

Perhaps the best roadmap for improving fraud statistics includes the ingredients of a non-observed economy (NOE) implementation strategy as stated in the OECD's Measuring the Non-Observed Economy: A Handbook. These ingredients, designed for improving the measurement of certain aspects of the economy, like illegal activities and informal sector production—all for inclusion in national accounts statistics—are presented in Box 9.1. The acronym NOE could/should be exchanged for the word fraud.

Box 9.1. Essential Ingredients of a NOE Implementation Strategy (from OECD, 2002)
Improved measurement is most likely to result from a number of incremental steps undertaken within the context of an overall framework that links them in some way. What is important is that the statistical office adopts an implementation strategy that is systematic, comprehensive, and tuned to local circumstances. The strategy should, as a minimum, contain the following elements:

a comprehensive programme of consultation with internal and external users on their needs and priorities with respect to the measurement of the NOE;

a set of clear, realistic, broad objectives indicating what the statistical office is trying to achieve in terms of NOE measurement and how this will address the needs of major data users;

a well defined conceptual and analytical framework appropriate for NOE measurement;

an assessment of the sources and outputs of the existing basic data collection programme and the national accounts compilation procedures with the aim of identifying NOE related problems and their magnitudes;

a prioritised set of possible short and long short term initiatives for improving the statistical infrastructure and outputs of the existing basic data collection programme, and for improving the national accounts compilation processes;

an implementation plan providing clear targets, milestones and an allocation of responsibilities and expectations for all the various players in the national statistical system;

a data revision strategy for preventing breaks in macro-economic data outputs resulting from NOE related improvements;

documentation procedures that ensure proper recording of: the results of the NOE assessment; estimates of the magnitude of the NOE activities by type; and the existing and planned data sources and compilation procedures;

documentation and evaluation of the NOE measurement programme.

Source: OECD, 2002.

ANNEX 10. References found in initial database searches[119]

ABI – Association of British Insurers. 2003. Facts on fraud No.1. London: Association of British Insurers.

Accountancy Age. 2002. Business must get tough on dirty dealing. [WWW] <URL: http://www.nera.com/MediaCoverage.asp?pr_ID=1513> [Accessed 24 March 2006.]

Ailisto, H., Vildjiounaite, E., et. al. 2006. Soft biometrics – combining bodyweight and fat measurements with fingerprint biometrics. Pattern Recognition Letters 27, pp. 325-334.

Al-Hawamdeh, A. and Snaith, I. 2005. Is "Private Briefing" Illegal in the United Kingdom? Corporate Governance: An International Review 13(4), p. 489.

Annesley, C. 2005. Banking Compliance and security threats increase burden on bank IT staff. Computer Weekly 13 December, p. 10.

Anonymous. 1990. The Guinness affair. The Economist 316(7670), p. 72.

Anonymous. 1992. Software theft. Royal Canadian Mounted Police Gazette 54(11), pp. 7-14.

Anonymous. 2004. Card fraud down but worries persist. Credit Management Jan, p. 10.

APACS. 2005. Card fraud: the facts 2005. London: APACS Administration Ltd.

APACS. 2005. Phishing scams cost UK banks £12m in 2004. [WWW] <URL: http://www.finextra.com/fullstory.asp?id=13337> [Accessed 25 March 2006.]

APACS. 2006. Card fraud facts and figures. [WWW] <URL: <http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html> [Accessed 8 March 2006.]

APACS. 2006. UK card fraud losses in 2005 fall by £65m – to £439.4 from £504.8m in 2004. [WWW] <URL: http://www.apacs.org.uk/media_centre/press/06_03_07.html?print=yes&print=yes&print=yes#top> [Accessed 20 March 2006.]

APACS. Fraud losses on UK-issued cards split by fraud type. [WWW] <URL: http://www.crimereduction.gov.uk/fraud9.htm> [Accessed 13 March 2006.]

[119]The sources in this study used as part of the REA derive from specific searches of various social science databases. These include: ABI Inform/ Proquest, Cambridge Scientific Abstracts (CSA) Internet Database Service, CSI Illumnia, EconLit, GMID (Global Market Information Database), ISI Web of Knowledge Service for UK Education, JSTOR, LexisNexis Executive, NCJRS - National Criminal Justice Reference Service, ScienceDirect, Social Care Online. The websites of various trade associations, government bodies, and relevant organisations were also searched. Search terms employed include: fraud, forgery, counterfeiting, plastic cards, false accounting, cheque [check], conspiracy to defraud, benefit fraud, deception, making off without payment, insider dealing/trading, market abuse, and white-collar crime. The additional sources which inform the background, discussion (in particular, the strategies for future data capture), and various annexes are interspersed in the list of references. Furthermore, some sources appeared only after the search was done, and where used, these are included in the bibliography to the main document.

Arreymbi, J. 2005. Online banking: Spoofing scams exposes security loopholes. In: Paulus, S., Pohlmann, N., et. al. eds. Isse 2005 – securing electronic business processes. Wiesbaden, Germany: Friedrich Vieweg & Sohn. pp. 289-300.

Arthur, C. 2004. Online banking fraud soars as fake e-mails trick customers. The Independent 2 October, p. 20.

Artis, M., Ayuso, M. and et. al. 2002. Detection of automobile insurance fraud with discrete choice models and misclassified claims. Journal of Risk & Insurance 69, pp. 325-340.

Bainbridge, S. M. 1986. The insider trading prohibition: a legal and economic enigma. University of Florida Law Review 38, 35-36.

Bainbridge, S. M. 2000. Insider trading: an overview. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=132529> [Accessed 24 March 2006.]

Bainbridge, S. M. 2001. The law and economics of insider trading: a comprehensive primer. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=261277> [Accessed 24 March 2006.]

Bajada, C. 2005. Unemployment and the underground economy in Australia. Applied Economics 37(2), pp. 177-189.

Bank Marketing International. 2004. New site to help counter phishing. Bank Marketing International 31 October, p. 5.

Bank Marketing International. 2004. Who's in the dark over online security? Bank Marketing International 30 November, p. 6.

Bank Marketing International. 2005. Banks start to offer anti-virus software to stop online crime wave. Bank Marketing International 31 July, p. 1.

Bateman, N. 1999. Welfare rights: lies, damned lies and benefit fraud statistics. Community Care p.23.

Bateman, N. 2000. Welfare rights: the fraud of fraud reporting. Community Care p.31.

BBA – British Bankers' Association. 2005. New ammunition in war against financial crime. [WWW] <URL: http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=145&a=5300> [Accessed 8 March 2006.]

BBC News. 1999. Internet fraud to cost UK business billions. [WWW] <URL: http://news.bbc.co.uk/1/hi/business/the_economy/342644.stm> [Accessed 24 March 2006.]

Belfast News Letter. 2005. Counting the cost of growth in cybercrime. Belfast News Letter 12 April, p. 2.

Benston, G. J. 2000. Consumer protection as justification for regulating financial-services firms and products. Journal of Financial Services Research 17(3), pp. 277-301.

Beny, L. N. 2004. A comparative empirical investigation of agency and market theories of insider trading. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=193070> [Accessed 24 March 2006.]

Bequai A. 2002. White collar crime: a handmaiden of international tech terrorism. Computers & Security 21(6), pp. 514-519.

Berwick, I. 2005. Crime doesn't pay? Dream on fraud: investigators fear that companies don't have the stomach to go the whole way in cracking down on theft. Financial Times 15 October, p. 2.

Berwick, I. 2005. In the doghouse ID theft insurance. The boom in insurance protection for identity fraud is justified by some dubious statistics. Financial Times 30 April, p. 25.

Bhattacharya, S. 2002. Conditional probability of actually detecting a financial fraud – a neutrosophic extension to the application of Benford's law. In: Callaos, N., Whymark, G., et. al. eds. 6th world multiconference on systemics, cybernetics and informatics, Vol XIII, proceedings – concepts and applications of systemics, cybernetics and informatics III. Orlando, Fl: Int Inst Informatics & Systemics. pp. 86-92.

Bhattacharya, U. and Daouk, H. 1999. The world price of insider trading. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200914> [Accessed 24 March 2006.]

Biagini, F. and Oksendal, B. 2005. A general stochastic calculus approach to insider trading. Applied Mathematics and Optimization 52(2), pp. 167-181.

Blickle, G., Schlegel, A., et. al. 2006. Some personality correlates of business white-collar crime. Applied Psychology 55(2), p. 220.

Bolton, R. J. and Hand, D. J. 2002. Statistical fraud detection: a review. Statistical Science 17(3), pp. 235-249.

Bowe, M. and Jobome, G. 2001. Fraudulent activity in financial institutions and optimal incentive structures for managing operational risk. Bank of Valletta Review 24, pp. 1-19.

Brand, S. and Price, R. 2000. The economic and social costs of crime. [WWW] <URL: http://www.homeoffice.gov.uk/rds/pdfs/hors217.pdf> [Accessed 23 March 2006.]

Brindle, D. 1998. NHS treats unhealthy fraud levels; financial irregularities in the health service are tackled only too rarely, says a new study. David Brindle reports. The Guardian 8 December, p. 19.

British Retail Consortium. 2005. Retail crime survey: key facts 2004-2005. [WWW] <URL: http://www.brc.org.uk/Downloads/12th_BRC_Crime_Survey_Key_Facts.pdf> [Accessed 23 March 2006.]

Brown, K. and Garnham, P. 2004. Theft of credit cards in post rises by 50%. Financial Times 20 September, p. 6.

Bunn, D. W. 2003. Evaluation of market power using agent based simulation. In: 2003 IEEE Power Engineering Society general meeting, vols 1-4, conference proceedings. New York, NY: IEEE. pp. 506-508.

Burger, H. K. White collar crime – a report on the methods and tricks of offenders.

Business Wire. 2006. Consumers vote for biometrics in the battle to beat identity fraud; Unisys survey reveals 2 out of 3 UK consumers would opt for biometric technologies to combat fraud problem. Business Wire 8 March.

Cabinet Office. 2002. Identity fraud: a study. [WWW] <URL: http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf> [Accessed 13 March 2006.]

Cao, C., Field, L. C., et. al. 2002. Does insider trading impair market liquidity? Evidence from IPO lockup

expirations. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=372220> [Accessed 24 March 2006.]

Calavita, K. Tillman, R. et. al. 1997. The savings and loan debacle, financial crime, and the state. Annual Review of Sociology 23, pp. 19-38.

Carozza, D. ed. 1999. Fraud in Europe: survey offers insight to crime trends. White Paper 13(5), p. 27.

Caunter, N. 2001. The real cost of fraud to e-tailers. Computer Fraud & Security 8, p. 17.

CBI. 2001. Business leaders warn of cybercrime threat to internet development. [WWW] <URL: http://www.cbi.org.uk/ndbs/press.nsf/0/eff1596523e1653f80256aaf00338dac?OpenDocument> [Accessed 25 March 2006.]

Cerullo, M. J. and Cerullo, V. 1999. Using neural networks to predict financial reporting fraud: part 2. Computer Fraud & Security 6, pp. 14-17.

Chakraborty, A. and Yilmaz, B. 2004. Manipulation in market order models. Journal of Financial Markets 7, pp. 187-206.

Chapman, A. 2001. Controlling fraud in the financial services sector. In: Fraud Prevention and Control. Canberra, Australia: Australian Institute of Criminology. pp. 1-7.

Chapman, A. and Smith, R. G. Controlling financial services fraud.

Chapman, B. and Denniss, R. 2005. Using financial incentives and income contingent penalties to detect and punish collusion and insider trading. Australian and New Zealand Journal of Criminology 38(1), pp. 122-140.

Chilvers, M. 2002. What lies behind the growth in fraud? Crime and Justice Bulletin 71, pp. 1-8.

CIFAS. 2004. Deceased frauds – research results – December 2004. [WWW] <URL: http://www.cifas.org.uk/reports_deceased_fraud.asp> [Accessed 8 March 2006.]

CIFAS. 2004. Employee fraud – the enemy within. [WWW] <URL: http://www.cifas.org.uk/reports_employee_fraud.asp> [Accessed 8 March 2006.]

CIFAS. 2004. Stockbroking & sharedealing – fraud prevention solutions. [WWW] <URL: http://www.cifas.org.uk/reports_stockbroking.asp> [Accessed 8 March 2006.]

Clark, A., Kenyon, W., et. al. 2005. 55% of UK companies are victims of economic crime, says PricewaterhouseCoopers survey. [WWW] <URL: http://www.pwcglobal.com/gx/eng/cfr/gecs/PwC_GECS05_UK_PR.pdf> [Accessed 23 March 2006.]

Clayton, H. 2003. Hole-in-the-wallet machines: Card fraud: criminal gangs targeting users of plastic cards are costing the banking industry more than Pounds 400m a year. Financial Times 2 August, p. 22.

Cloninger, D. O. and Waller, E. R. 2000. Corporate fraud, systematic risk and shareholder enrichment. Journal of Socio-Economics 29, pp. 189-201.

Coke, DeeDee. 2004. Office hours: sleuthing in cyberspace: the modern form of crime needs a different kind of criminal and a different kind of PC. DeeDee Coke on how the rise of computer forensics is

changing the face of internet crime. The Guardian 16 February, p. 2.

Cole, L. S. 1984. Claims, cost and crimes – a study of insurance frauds from invention to prevention. Novato, CA: Lee Books.

Computer & Security Fraud. 2006. Regulator warns banks to face up to online fraud. Computer & Security Fraud 2, p. 4.

Courtney, K. 2005. Home Office identity fraud reduction programme. London: Identity Fraud Steering Committee.

Cox, J. D. and Thomas, R. S. 2003. SEC enforcement actions for financial fraud and private litigation: an empirical inquiry. Vanderbilt Law and Economics Research Paper No. 03-08. Nashville, TN: Vanderbilt University.

Cumbo, J. 2004. Rise in personal banking e-fraud. Financial Times 2 October, p. 1.

Darling, S. P. A. 2004. Nineteenth survey of white collar crime. American Criminal Law Review 41(2), pp. 215-215.

Datamonitor CommentWire. 2005. Cryptomathic: driving customer authentication; Lloyds TSB has installed identity/access management solution the Cryptomathic Authenticator. Datamonitor CommentWire 24 November.

Datamonitor NewsWire. 2005. Internet card fraud is on the increase. Datamonitor NewsWire 8 November.

Datamonitor. 2004. UK card sector takes a swipe at the fraudsters. Datamonitor Expert View 6 September.

Datamonitor. 2005. UK cards: declining fraud means issuers can look to product development; APACS has reported a fall in plastic card fraud for the first half of 2005. Datamonitor CommentWire 9 November.

Datamonitor. 2006. BT offers identity theft insurance. Datamonitor NewsWire 22 February.

Davis, B. 1995. Crimes against business: an overview. Criminology Australia 6(4), pp. 23-26.

Davies, P., Francis, P. et. al. ed. 1999. Invisible crimes: their victims and their regulation.

del Brio, E. B., de Miguel, A., et. al. 2001. Insider trading in the Spanish stock market. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=267011> [Accessed 24 March 2006.]

Delisi, M. and Gatling, J. M. 2003. Who pays for a life of crime? An empirical assessment of the assorted victimization costs posed by career criminals. Criminal Justice Studies: A Critical Journal of Crime, Law and Society 16(4), pp. 283-293.

Derrig, R. A. 2002. Insurance fraud. The Journal of Risk and Insurance, 69(3), pp. 271-287.

Dessain, A. 2001. The liabilities of financial institutions for the fraud of third parties: the Jersey, Channel Islands experience. Journal of International Banking Regulation 3(2), p. 145.

Doig, A. and Coles, E. 1997. Local authorities and housing benefit: cost and control of fraud. Local Government Studies 23(2), pp.103-26.

Donnelly, A. 2000. Online credit card fraud outpaces physical world. Computer & Security Fraud 10, p. 9.

DWP Information Directorate. 2006. Fraud and error in housing benefit April 2002 to March 2005. London: Crown copyright.

DWP, Department for Work and Pensions Information Directorate. 2005. Fraud and error in income support, jobseeker's allowance and pension credit from April 2004 to March 2005. London: Crown copyright.

DWP, Department for Work and Pensions Information Directorate. 2005. Fraud, error and other incorrectness in disability living allowance. London: Crown copyright.

Ernst & Young. 2003. Fraud the unmanaged risk: 8th global survey. [WWW] <URL: http://www.ey.com/global/download.nsf/South_Africa/Jan03_8th_Global_Fraud_Survey/$file/8th%20Global%20Survey.pdf> [Accessed 23 March 2006.]

Essinger, J. 1995. Fraud prevention and computer security for financial institutions – part 2. Computer Fraud & Security Bulletin 3, pp. 16-19.

Euromonitor. 2004. Financial cards in the United Kingdom. London: Euromonitor Plc.

Euromonitor. 2005. Credit and charge cards in the UK. London: Euromonitor.

Euromonitor International. 2005. Retail banking services in the UK. London: Euromonitor International.

Evason, E. and Woods, R. 1995. Poverty, deregulation of the labour market and benefit fraud. Social Policy and Administration 29(1), pp.40-54.

Ferrarini, G. A. 2004. The European Market Abuse Directive. Common Market Law Review 41(3), pp. 711-741.

Financial Services Authority. 2005. Financial crime newsletter 2005. [WWW] <URL: http://www.fsa.gov.uk/pubs/newsletters/fc_newsletter4.pdf> [Accessed 23 March 2006.]

Financial Services Authority. 2006. Financial risk outlook 2006. [WWW] <URL: http://www.fsa.gov.uk/pubs/plan/financial_risk_outlook_2006.pdf> [Accessed 23 March 2006.]

Financial Services Distribution. 2005. The rise of online crime. Financial Services Distribution 27 May. p. 14.

Fischer, N. E. Big rip-off – what crime costs you.

Fishe, R. P. H. and Robe, M. A. 2004. The impact of illegal insider trading in dealer and specialist markets: evidence from a natural experiment. Journal of Financial Economics 71, pp. 461-488.

Fridson, M. S., Picket, J. M. 2002. Financial crime investigation and control. Financial Analysts Journal 58(5), p. 99.

Garfinkel, J. A. and Nimalendran, M. 2003. Market structure and trader anonymity: An analysis of insider trading. Journal of Financial and Quantitative Analysis 38(3), pp. 591-610.

Gartner. 2004. Phishing alliance formed as Gartner study unearths big losses. [WWW] <URL: http://www.finextra.com/fullstory.asp?id=12016> [Accessed 25 March 2006.]

Gartner. 2004. Phishing scams cost US financial firms $1.2 billion. [WWW] <URL: http://www.finextra.com/fullstory.asp?id=11778> [Accessed 25 March 2006.]

Gaudin, S. 2002. Online fraud growing in scale, sophistication. [WWW] <URL: http://www.internetnews.com/ec-news/article.php/1552921> [Accessed 25 March 2006.]

Geis, G. and Jesliow, P. eds. 1993. White-collar crime. Annals of the American Academy of Political and Social Science National 525.

Gerety, M. and Lehn, K. 1997. The causes and consequences of accounting fraud. Managerial and Decision Economics 18(7/8), pp. 587-599.

Gips, M. A. 1998. Where has all the money gone? Security Management 42(2), pp. 32-36.

Givens, B. 2000. Identity theft: how it happens, its impact on victims, and legislative solutions. [WWW] <URL: http://www.privacyrights.org/ar/id_theft.htm> [Accessed 13 May 2006.]

Godefroy, T. and Laffargue, B. Cost of crime in France in 1976 and 1977.

Graboksy, P. 2000. Computer crime: a criminological overview. [WWW] <URL: http://www.aic.gov.au/conferences/other/grabosky_peter/2000-04-vienna.pdf> [Accessed 13 May 2006.]

Green, B. P. and Reinstein, A. 2004. Banking industry financial statement fraud and the effects of regulation enforcement and increased public scrutiny. Research in Accounting Regulation 17.

Green, S. P. 2004. The concept of white collar crime in law and legal theory. Buffalo Criminal Law Review 8(1), pp. 101-134.

Griffin, J. 1999. Headline: Midland fraud bill hits Pounds 26.5m. Birmingham Evening Mail 24 February, p. 27.

Griffiths, M. 2003. Internet abuse in the workplace: issues and concerns for employers and employment counselors. Journal of Employment Counseling 40(2), pp. 87-96.

Gupta, G., Mazumdar, C. et. al. 2006. Paradigm shift in document related frauds: characteristics identification for development of a non-destructive automated system for printed documents. Digital Investigation 3, pp. 43-55.

Hale, C. 2002. Cybercrime: facts & figures concerning this global dilemma. Crime & Justice International 18(65), pp. 24-26.

Hallam-Baker, P. 2005. Prevention strategies for the next wave of cyber crime. Network Security 2005(9), pp. 12-15.

Harris Interactive. 2003. Identity theft new survey & trend report. [WWW] <URL: http://www.bbbonline.org/idtheft/IDTheftSrvyAug03.pdf> [Accessed 23 March 2006.]

Harvey, F. 2003. Online crime set to rise: Cyberspace: the fight against hackers is a big burden. Financial Times 3 December, p. 3.

Hegde, S. P., Malone, C. B., et. al. 2003. The financial impacts of fraud and securities class action suits. [WWW] <URL: http://207.36.165.114/Denver/Papers/10b5.pdf> [Accessed 23 March 2006.]

Hill, J. 2005. Scots fraud soars 300 per cent to record GBP 28.56m. The Scotsman 31January, p. 52.

Hillier, D. and Marshall, A. P. 1997. The impact of the London stock exchange model code on insider trading in the UK. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=41036> [Accessed 24 March 2006.]

Hodgeson, P. W. 2005. The threat to identity from new and unknown malware. BT Technology Journal 23(4), pp. 107-112.

Holtfreter, K. 2005. Is occupational fraud "typical" white-collar crime? a comparison of individual and organizational characteristics. Journal of Criminal Justice 33, pp. 353-365.

Home Office. 2004. Government sets out decisions on fraud law reform. Hermes Database 19 October.

Home Office Identity Fraud Steering Committee. 2006. Updated estimate of cost of identity fraud to UK economy. [WWW] <URL: http://www.identitytheft.org.uk/ID%20fraud%20table.pdf> [Accessed 13 March 2006.]

Houlder, V. and Tiesenhausen Cave, F. 2005. Distorted trade data point to massive tax fraud. Financial Times 10 August, p. 1.

Huang, M. Y. 2005. Critical information assurance challenges for modern large-scale infrastructures. Computer network security, proceedings lecture notes in computer science 3685. Berlin, Germany: Springer-Verlag Berlin. pp. 7-22.

Hung, M. and Trezevant, R. 2003. Insider trading and corporate governance structure: evidence from Southeast Asia. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374422> [Accessed 24 March 2006.]

Hurst, T. R. 2001. Securities fraud and the internet: adapting existing regulatory schemes to regulation in cyberspace. Journal of Financial Crime 8(3), pp. 226-233.

Hyder, K. 2000. Sinister menace of the cyber saboteurs hell-bent on bringing us to our knees. Sunday Express 27 February.

Jain, N. and Mirman, L. J. 1998. Real and financial effects of insider trading with correlated signals. [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=85908> [Accessed 24 March 2006.]

Jarrett, T. 2005. Who knows what you know? Sunday Times 27 November, p. 10.

Jeng, L. A., Metrick, A., et. al. 2003. Estimating The Returns To Insider Trading: A Performance-Evaluation Perspective. The Review of Economics and Statistics 85(2), pp. 453-471.

Jesilow, P., Klempner, E. *et al*. 1992. Reporting consumer and major fraud: a survey of complainants. Boston: Northeastern University Press.

Johnson, S. 1995. On the fiddle. Police Review 103(5331), pp. 22-4.

Jones, G. 2004. The bank r@iders; internet conmen try to trick cash from millions of online customers. The Mirror 3 June, p. 9.

Karamouzis, F. and Hallawell, A. 2005. Fraud case focuses unwelcome attention on Indian outsourcing. Stamford, CT: Gartner Inc.

Karl, A. 2001. The perception of "benefit fraud" and the acceptance of benefits for unemployed people. Soziale Welt-Zeitschrift fur Sozialwissenschaftliche Forschung und Praxis 52(3), p. 341.

Kennedy, J. G. 1981. Forgery and credit card fraud. In: Grau, J. J. and Jacobson, B. ed. Criminal and civil investigation handbook. New York, NY: McGraw-Hill Publishing Co. pp. 6-81 – 6-101.

Kerley, K. R. and Copes, H. 2004. The effects of criminal justice contact on employment stability for white-collar and street-level offenders. International Journal of Offender Therapy and Comparative Criminology 48(1), pp. 65-84.

Kingston, J., Schafer, B., et. al. 2005. No model behaviour: ontologies for fraud detection. In: Law and the semantic web lecture notes in computer science 3369. Berlin, Germany: Springer-Verlag Berlin. pp. 233-247.

Kirchner, S. 2005. Subsidy fraud in German criminal law and the protection of the financial interests of the European Communities. [WWW] <URL: http://www.ssrn.com/author=343201> [Accessed 24 March 2006.]

Kirkos, E., Charalambos, S. et. al. 2006. Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications 1659, pp. 1-9.

Klotter, J. C. Criminal law. 7thed.

Klotter, J. C. J. D. Criminal law and criminal law study guide. 6th ed.

Knight, R. 2005. Fraudsters favour brandy and one-way tickets credit cards: a fraud prevention company has crunched the numbers to come up with software to help retailers stop the card cheats. Financial Times 27 August, p. 24.

Knowles, A., Moore, S., et. al. 2005. Internet crime: Personal experience of internet crime and trust in the internet for financial transactions. Australian Journal of Psychology 57, pp. 221-221.

Kohatsu-Higa, A. 2004. Enlargement of filtrations and models for insider trading. In Akahori, J., Ogawa, S., et. al. eds. Stochastic processes and applications to mathematical finance. Singapore: World Scientific Publ Co. pp. 151-165.

Kshetri, N. 2005. Pattern of global cyber war and crime: a conceptual framework. Journal of International Management 11(4), pp. 1-38.

Langevoort, D. C. 2001. Cross-border insider trading. Journal of Financial Crime 8(3), pp. 254-263.

Lee, J. and Soberon-Ferrer, H. 1997. Consumer vulnerability to fraud: influencing factors. The Journal of Consumer Affairs 31(1), pp. 70-89.

Leonard, K. J. 1995. The development of a rule based expert system model for fraud alert in consumer credit. European Journal of Operational Research 80, pp. 350-356.

Levi, M. (ed) 1999. Fraud: organization, motivation and control volume 1: extent and causes of white-collar crime and volume 2: the social, administrative and criminal control of fraud. Aldershot: Ashgate.

Lewis, M. K. 1999. Counteracting fraud: the case of BCCI revisited. The Globalization of Financial Services pp. 614-32.

Litan, A. 2006. Fraudulent ATM withdrawals reflect a widespread threat. [WWW] <URL: http://www.gartner.com/resources/138400/138479/fraudulent_atm_withdrawals_r_138479.pdf> [Accessed 25 March 2006.]

Litan, A. and Pescatore, J. 2004. Stolen credit card case should prompt card companies to act. [WWW] <URL: http://www.gartner.com/DisplayDocument?doc_cd=113282> [Accessed 25 March 2006.]

Litan, A. and Pescatore, J. 2005. Bank transfer delays show awareness of 'Phishing' danger. Stamford, CT: Gartner Inc.

Liu, K., Li, J. A., et. al. 2005. Analysis of monitoring and limiting of commercial cheating: a newsvendor model. Journal of the Operational Research Society 56(7), pp. 844-854.

Lo, K. H., Wang, K., et. al. 2005. Insider transfer trading of banking companies around exchange listing. Journal of Financial Intermediation 15, pp. 215 – 234.

Loxton, L. 2005. Be aware of the tricks and sleights of hand of the fraudster's trade. The Times 20 September, p. 58.

Lunnitt, M. 2004. Credit card fraud: your card in their hands. Fraud Magazine 18(3), pp. 26-29-48.

M2 Presswire. 2004. UK Government – OPRA successfully prosecutes company director for pensions fraud. M2 Presswire 9 August.

M2 Presswire. 2005. Citizens Advice: New guidance from Citizens Advice urges people to 'Get Safe Online'. M2 Presswire 28 October.

M2 Presswire. 2005. Infosecurity Europe: survey reveals that people will give away their identity for a chance to win theatre tickets. M2 Presswire 24 March.

M2 Presswire. 2005. Philippsohn Crawfords Berwald: EU set to take on phone lottery fraudsters tomorrow. M2 Presswire 24 February.

M2 Presswire. 2005. StreamShield Networks: StreamShield outlines three step approach for stamping out phishing scams; Innovative new approach will close net on phishing. M2 Presswire 18 August.

M2 Presswire. 2005. UK Government: Benefit Fraud Inspectorate (BFI) inspection report on Cherwell District Council. M2 Presswire 19 July.

M2 Presswire. 2005. Vogon Initernational: fighting cyber crime. M2 Presswire 28 April.

M2 Presswire. 2006. GeoTrust: GeoTrust joins the anti-phishing working group steering committee to help combat online fraud. M2 Presswire 1 March.

M2 Presswire. Thales: Thales UK survey shows identity management to be top transaction security concern for UK banks Internet threats raise identity management to number one concern. M2 Presswire 16 November.

Marshall, A. M. and Tompsett, B. C. 2002. Spam 'n' chips – A discussion of internet crime. Science & Justice 42(2), pp. 117-122.

Matsumura, E. M. and Tucker, R. R. 1992. Fraud detection: a theoretical foundation. The Accounting Review 67(4), pp. 753-782.

Maug, E. 1999. Insider trading legislation and corporate governance. Brussels, Belgium: European Corporate Governance Institute (ECGI).

Maybury, R. 2005. Bootcamp top traumas solved by Rick Maybury top 10 internet scams, part 1. The Daily Telegraph 26 April, p. 35.

McBarnet, D. 1991. Whiter than white collar crime: tax, fraud insurance and the management of stigma. The British Journal of Sociology 42(3), pp. 323-344.

McCall, T. and Moss, R. 2005. Gartner survey shows frequent data security lapses and increased cyber attacks damage consumer trust in online commerce guarantees on web site security sought from merchants, banks, other businesses. [WWW] <URL: http://www.gartner.com/press_releases/asset_129754_11.html> [Accessed 25 March 2006.]

McDonald, G. 2005. Cybercrime costing firms millions, new study claims. Irish News 6 April, p. 43.

McGee, R. W. 2004. Ethical issues in insider trading: case studies. In: Proceedings of the global conference on business economics, Association for Business and Economics Research, July 9-11, 2004. Miami Shores, FL: Barry University. pp. 712-721.

Meadowcroft, P. 2005. Combating cardholder-not-present fraud. Credit Control 26(8), p. 60.

Merrell, C. and Seib, C. 2004. Phishing attack on NatWest halts online services. The Times 18 November, p. 7.

Miller, T. R. and Cohen, M. A. et. al. Extent and costs of crime victimization: a new look.

Money Management. 2005. Security alert. Money Management 1 April.

Monks, H. 2005. Tricks of the ID thieves – and how to foil them; Helen Monks on how to beat the conmen who steal your identity. The Independent 12 February.

Monnet, C. 2005. Counterfeiting and inflation. [WWW] <URL: http://www.ecb.int/pub/pdf/scpwps/ecbwp512.pdf> [Accessed 23 March 2006.]

Moore, J. 2004. E-mail fraudsters target Citibank World's biggest bank warns of 'phishing' scam to trick customers into giving away private details on hoax website. The Daily Telegraph 19 January, p. 32.

Moore, J. and Uhlig, R. 2003. Bank of England falls victim to e-mail hoaxers. The Daily Telegraph 31 December, p. 2.

Morgan, J. 2006. Don't be caught in the net by cyberstalkers. The Times 25 February, p. 10.

Morris, N. 2005. International gangs target British businesses in 'cyber crime' surge. The Independent 4 August, p. 6.

Morrison, S. and Nuttall, C. 2004. Gone phishing fraud based on bogus e-mails is causing concern among banks and online retailers, write Scott Morrison and Chris Nuttall. Financial Times 23 June, p. 1.

Muncaster, P. and Bennett, M. 2005. Banks vet staff to reduce e-fraud. VNU NET 31 October, p. 1.

Nacha. 2004. Phishing losses total $500 million – Nacha. [WWW] <URL: http://www.finextra.com/fullstory.asp?id=12568> [Accessed 25 March 2006.]

Nairn, G. 2005. Make it someone else's problem managed security services: Market: torrents of spam and phishing scams are time-consuming for businesses, writes Geoff Nairn. Financial Times 15 June, p. 2.

National Statistics. 2006. Social trends: crime & justice highlights. [WWW] <URL: http://www.statistics.gov.uk/cci/nugget.asp?id=1363> [Accessed 15 March 2006.]

National White Collar Crime Ctr. 2005. Internet fraud – crime report. Richmond, VA: National White Collar Crime Ctr.

NCIS – National Criminal Intelligence Service. 2006. UK threat assessment: the threat from serious and organized crime 2004/5 – 2005/6. London: National Criminal Intelligence Service.

Neal, D. 2005. Internet week – Phishing scams report – e-crime fighters discuss new; new laws and better authentication are being developed to combat. VNU NET 7 November, p. 24.

Nejat Seyhun, H. and Bradley, M. 1997. Corporate bankruptcy and insider trading. The Journal of Business 70(2), pp. 189-216.

Newman, G. R. 2003. Check and card fraud. [WWW] <URL: http://www.cops.usdoj.gov/mime/open.pdf?Item=965> [Accessed 13 May 2006.]

Newton, J. 1995. Organised plastic counterfeiting. London: Her Majesty's Stationery Office.

NHTCU – National Hi-Tech Crime Unit. 2004. Hi-Tech crime: the impact on UK business. London: NOP Business.

NHTCU – National Hi-Tech Crime Unit. 2005. Hi-Tech crime: the impact on UK business 2005. London: NOP World Business and Technology.

North Carolina Dept of Crime Control and Public Safety. Business crime prevention: security pays.

North, S.E. 1973. Fraud in industry – detection, prevention and prosecution. London: Industrial and Commercial Techniques Ltd.

OFT. 2006. Impact of Mass Marketed Scams. London: Office of Fair Trading.

Oujo, I. 2003. Privacy & American business survey finds 33.4 million Americans victims of ID theft; consumer out-of-pocket expenses total $1.5 billion a year. [WWW] <URL: http://www.pandab.org/id_theftpr.html> [Accessed 23 March 2006.]

Pain, S. 2005. E-business: headache of hi-tech cops. Birmingham Post 25 October, p. 23.

Paisley, J. 2006. Chip and pin a winner at beating card fraud; new system deters crooks with 16-per cent drop in plastic crime. Evening Times (Glasgow) 7 March, p. 3.

Pathak, J., Vidyarthi, N., et. al. 2005. A fuzzy-based algorithm for auditors to detect element of fraud in settled insurance claims. Managerial Auditing Journal 20(6), pp. 632-644.

Pettey, C. 2003. Gartner says identity theft is up nearly 80 percent 7 million U.S. adults were identity theft victims in the past 12 months. [WWW] <URL: http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp> [Accessed 25 March 2006.]

Phillippsohn, S., Thomas, S., et. al. 2003. E-fraud – what companies face today. Computer Fraud & Security 1, pp. 7-9.

Podgor, E. S. 1993. White collar crime in a nutshell. St. Paul, MN: West Publishing Co.

Pontell, H. N. 2005. Control fraud, gambling for resurrection, and moral hazard: accounting for white-collar crime in the savings and loan crisis. The Journal of Socio-Economics 34, pp. 756-770.

Pontell, H. N. 2005. White-collar crime or just risky business? The role of fraud in major financial debacles. Crime Law and Social Change 42(4-5), pp. 309-324.

Porter, D. 2003. Insider fraud: spotting the wolf in sheep's clothing. Computer & Security Fraud 4, pp. 12-15.

Porter, D. 2004. Identity fraud: the stealth threat to UK plc. Computer Fraud & Security 7, pp. 4-6.

Post Magazine. 2005. Risk report; penny pinching. Post Magazine 9 June, p. 33.

Precision Marketing. 2005. Special report – email marketing: pest control. Precision Marketing 19 August, p. 15.

PricewaterhouseCoopers. 2005. Global economic crime survey 2005. [WWW] <URL: http://www.pwcglobal.com/gx/eng/cfr/gecs/PwC_GECS05_United_Kingdom.pdf> [Accessed 23 March 2006.]

Pujas, V. 2003. The European Anti-Fraud Office (OLAF): a European policy to fight against economic and financial fraud? Journal of European Public Policy 10(5), pp. 778-797.

Rhode Island Governor's Justice Cmssn. White collar crime: Rhode Island's narrative and statistical study tracking the growth of this crime category, both state and nation-wide.

Rider, B. A. K. 2001. Cyber-organised crime: the impact of information technology on organised crime. Journal of Financial Crime 8(4), pp. 332 – 346.

Rogers, M. K. and Seigfried, K. 2004. The future of computer forensics: a needs analysis survey. Computers & Security 23, pp. 12-16.

Royal Canadian Mounted Police Ottawa. 1995. Examination of altered payment cards. Gazette 57(11&12), pp. 18-20.

Rutledge, G. P. 1998. Internet and US financial markets. Journal of Financial Crime 6(2), pp. 129 – 141.

Searjeant, G. 2005. The swift rise and fall of the Bank of Crooks & Cocaine. The Times 3 November, p. 54.

Shelley, L. I. 1998. Crime and corruption in the digital age. Journal of International Affairs 51(2), pp. 605 – 620.

Shin, J. 1996. The optimal regulation of insider trading. Journal of Financial Intermediation 5, pp. 49-73.

Simon, C. P. and Witte, A. D. Beating the system – the underground economy.

Sinith, A. 2002. White-collar crime. Singapore Academy of Law Journal 14, p. 231.

Slotter, K. 1997. Plastic payments. FBI Law Enforcement Bulletin 66(6), pp. 1-7.

Smith, R. G. Best practice in fraud prevention.

Smith, R. G. 2001. Controlling cross-border economic crime [WWW] <URL: http://www.aic.gov.au/conferences/outlook4/SmithCBC.pdf> [Accessed 13 May 2006.]

Smith, R. G. 2003. Serious fraud in Australia and New Zealand. Canberra, Australia: Australian Institute of Criminology.

Song, W. 2003. Financial infrastructure, underwriter reputations, and securities fraud. Baton Rouge, LA: Louisiana State University.

Spalek, B. 2001. Regulation, white-collar crime and the Bank of Credit and Commerce International. Howard Journal of Criminal Justice 40(2), pp. 116-179.

Sunday Mail. 2006. Lotto plotto; Scam: the official-looking headed notepaper featuring lotto logos used in the con online players warned as identity crooks bid to fleece them in Pounds 500,000 email scam. Sunday Mail 29 January, p. 43.

Swindon Crime Reduction Initiative Partnership. Retail theft – the facts. [WWW] <URL: http://www.scrip.org.uk/retailtheft.html> [Accessed 23 March 2006.]

Szockyj, E. and Geis, G. 2002. Insider trading patterns and analysis. Journal of Criminal Justice 30, pp. 273-286.

Tait, N. 2005. Computer records provide 80% of fraud case evidence. Financial Times 18 October, p. 6.

Taylor, R. 2005. Average cost of business crime now £5,000 a year. [WWW] <URL: http://press.iod.com/newsdetails.aspx?ref=5&m=2&mi=62&ms= > [Accessed 24 March 2006.]

Tennyson, S. 1997. Economic institutions and individual ethics: a study of consumer attitudes toward insurance fraud. Journal of Economic Behavior and Organization 32(2) pp. 247-65.

Thal Larsen, P. 2005. Gang targeted Sumitomo in UK. Financial Times 17 March, p. 17.

The Fraud Advisory Panel. 2005. The human cost of fraud. [WWW] <URL: http://www.fraudadvisorypanel.org/newsite/PDFs/annualreports/FAPreview2004-5.pdf> [Accessed 23 March 2006.]

The Independent. 2002. Companies lose billions to criminals. [WWW] <URL: http://www.nera.com/MediaCoverage.asp?pr_ID=1511&login=6923124> [Accessed 24 March 2006.]

The Irish Times. 2005. Chip and pin cards brought in to tackle fraudsters. The Irish Times 18 March, p. 6.

The Journal. 2001. The fight to pin down credit card fraudsters -payment card fraud is costing £ 300m a year and rising. Crime correspondent Helen Charlton looks at how the industry is fighting back. The Journal (Newcastle, UK) 19 March, p. 8.

The Times. 2000. Working hard for a healthy economy. The Times 22 March.

Tillman, R. and Pontell, H. 1995. Organizations and fraud in the savings and loan industry. Social Forces 73(4), pp. 1439-1463.

Topkara, M., Kamra, A., et. al. 2005. ViWiD : Visible watermarking based defense against phishing. In: Digital watermarking, proceedings lecture notes in computer science 3710. Berlin, Germany: Springer-Verlag Berlin. pp. 470-483.

Total Telecom. 2004. Cybercrime costing U.K. business billions police. Total Telecom 24 February.

TowerGroup. 2004. Phishing fraud losses exaggerated – TowerGroup. [WWW] <URL: http://www.finextra.com/fullstory.asp?id=12937> [Accessed 25 March 2006.]

Treanor, J. 2003. Hoaxer hijacks Bank's name: Latest cyber fraudster dons Old Lady's disguise to draw 100,000 responses. The Guardian 31 December, p. 15.

US Dept of Justice Criminal Division Fraud Section. 1995. Fraud victimization – the extent, the targets, the effects. Rockville, MD: National Institute of Justice/ NCJRS.

US Dept of Justice Criminal Division Fraud Section. 2005. Special report on "phishing". Rockville, MD: National Institute of Justice/ NCJRS.

Van Dyke, M. T. ed. 2005. Identity fraud survey report 2005. Pleasanton, CA: Javelin Strategy & Research.

Viaene, S. and Dedene, G. 2004. Insurance fraud: issues and challenges. Geneva Papers on Risk and Insurance 29(2), pp. 313-333.

Victorian Drugs and Crime Prevention Cmtte. 2004. Inquiry into fraud and electronic commerce: final report [WWW] <URL: http://www.parliament.vic.gov.au/dcpc/Reports/DCPC_FraudElectronicCommerce_05-01-2004.pdf> [Accessed 13 May 2006.]

von Tiesenhausen, F. 2004. Computer hackers strike at 80% of large businesses: cyber crime. Financial Times 25 February, p. 6.

Wales, E. 2003. E-commerce counts cost of online card fraud. Computer & Security Fraud 1, pp. 9-11.

Wall, M. 2005. E-doubters miss out on a mint. Sunday Times 22 May, p. 12.

Walsh, N. 2005. ATM fraud prompts card rethink? Card Technology Today 17(2), p. 10.

Ward, S. 2004. Crackdowns cutting Scots credit fraud. The Scotsman 5 March, p. 28.

Warren, P. and Streeter, M. 2005. Life: online: Stealing the limelight: Global gangs are infiltrating our computers, which could threaten the success of the internet. Peter Warren and Michael Streeter report. The Guardian 17 March, p. 32.

Watkins, J. 2005. Fighting fraud on the home front. Financial World Aug, p. 7.

Webb, B. 1996. Preventing plastic card fraud in the UK (United Kingdom). Security Journal 7(1), pp. 23-25.

Wellford, C. F. and Ingraham, B. L. White-collar crime: prevalence, trends, and costs. In: Albert R Roberts, A. R. ed. Critical issues in crime and justice. pp. 77-90.

Wheeler, S., Weisburd, D. et. al 1988. White collar crimes and criminals. American Criminal Law Review 25(3), pp. 331-357.

White Paper. 1999, fraud in Europe: survey offers insight to crime trends. White Paper 13(5), pp. 27.

Wiggins, L. M. 2002. Corporate computer crime: collaborative power in numbers. Federal Probation 66(3), pp. 19-29.

Witherell, W. 2004. Combating financial crime through international standards and cooperation. [WWW] <URL: http://www.oecd.org/dataoecd/28/1/33866667.pdf> [Accessed 23 March 2006.]

Yeo, V. C. S. 2001. A comparative analysis of insider trading regulation – who is liable and what are the sanctions? [WWW] <URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=260884> [Accessed 24 March 2006.]

Zhang, W., Cahan, S. F., et. al. 2005. Insider trading and pay-performance sensitivity: an empirical analysis. Journal of Business Finance & Accounting 32(9)&(10), pp. 1887-1919.

Zimring, F. E. and Johnson, D. T. 2005. On the comparative study of corruption. British Journal of Criminology 45(6), pp. 793-809.