

2004-2005 Fraud Report

An analysis of reported fraud in Government Departments

November 2005



HM TREASURY



HM TREASURY

2004-2005 Fraud Report

**An analysis of reported fraud in
Government Departments**

November 2005

© Crown copyright 2004

Published with the permission of HM Treasury on behalf of the Controller of Her Majesty's Stationery Office.

The text in this document (excluding the Royal Coat of Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any enquiries relating to the copyright in this document should be sent to:

The Licensing Division
HMSO
St Clements House
2-16 Colegate
Norwich
NR3 1BQ

Fax: 01603 723000

E-mail: licensing@cabernet-office.x.gsi.gov.uk

HM Treasury contacts

This document can be accessed from the Treasury Internet site at:

www.hm-treasury.gov.uk

For further information on the Treasury and its work, contact:

Correspondence and Enquiry Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558

Fax: 020 7270 4861

E-mail: ceu.enquiries@hm-treasury.gov.uk

CONTENTS

	Page
Executive Summary	3
Chapter 1 Introduction	5
Chapter 2 Main Analyses	7
Annex A Analysis of Anti-fraud Questionnaires	15
Annex B Large Value Frauds Perpetrated by Staff	17
Annex C Large Value Frauds Perpetrated by Contractors	21
Annex D External Frauds	23
Annex E Fraud Issues	25

EXECUTIVE SUMMARY

1. This report is divided into the following parts:

- **Section 1** describes the purpose of the Report and provides a definition of fraud.
- **Section 2** contains details of the main analyses of fraud data.
- **Annex A** is an analysis of anti-fraud questionnaires.
- **Annexes B, C and D** contain case summaries of high-value fraud cases (i.e. with values of £20,000 or more).
- **Annex E** contains anti-fraud guidance and advice.

2. The analysis in **Section 2** shows that overall 29 bodies reported 450 cases of internal theft or fraud with an overall value of £3,136,900. This represents a decrease over the value of fraud reported last year (£3,907,000). The following is a summary of the main observations and conclusions:

- The highest number of cases arose in the category **personnel management related fraud** (130 cases, 29%). A majority of these cases involved little or no financial loss to departments and appropriate disciplinary measures were taken against most of the perpetrators.
- In terms of value, **payment related fraud** was the dominant category accounting for losses of nearly £1.4million (45% of total losses). Individual losses in this category can sometimes be significant and this year's total included 6 cases that each exceeded £100,000 in value and totalled just over £1million. Many of the high-value cases involved staff either intercepting claims and redirecting payments to accomplices' bank accounts or processing fraudulent claims for overpayments. Collusion was a key characteristic in a lot of these cases.
- **Procurement fraud** was also a significant category in terms of both number of cases reported (53 or 12%) and overall value (£650,200, 21%). One large value fraud (over £400,000) arose because of poor supervision. This year also saw a big increase in the number of credit card/GPCcard frauds (from 4 to 41) cases mostly involving the copying of cards or using credit card details to make fraudulent purchases.
- **Theft of assets** continues to be a problem with most cases arising because of weak security at some government sites. Departments reported 96 cases in all with losses totalling nearly £790,000. Included in the total were 9 large value thefts (£20,000 or more) that accounted for over £550,000.

- The analysis of **anti-fraud questionnaires** (**Annex A** contains full details) revealed that a high proportion of organisations had measures in place to effectively manage the risk of fraud they faced. Perhaps more might consider establishing processes to continuously monitor the effectiveness of their anti-fraud policies and consider providing more fraud awareness training to operational staff and new entrants.
- Our analysis revealed three main areas that departments should consider:
 - 1. Security over assets.** Most thefts reported occurred because of poor security over assets with a significant number of personal computers being stolen from desks or meeting rooms. Thefts of personal computers carry the added risk of losing confidential information that could lead to serious criminal fraud or embarrassment to the departments concerned. Individual losses are often quite significant. Departments are advised to review their security arrangements.
 - 2. Segregation of duties/supervision.** In value terms the most significant frauds arose because the activities of some staff were not monitored closely enough or because there was a lack of segregation of duties between functions such as requisitioning, ordering and payment. Collusion was also involved in a number of these cases and again, this year, included collusion between staff and contractors or members of the public. Good management information, regular and frequent management checks, segregation and rotation of duties and well publicised avenues for reporting suspicions of fraud should go some way to reducing the risk of these types of fraud occurring.
 - 3. GPC/credit cards.** This year saw a big increase in the number of credit card frauds reported. These frauds arose despite strong internal controls with most cases involving the copying of cards or the use of credit card details to make fraudulent purchases. The credit card companies generally repaid any losses. It is important that credit card statements are examined in detail as soon as they are received in order to identify these frauds quickly so that immediate action can be taken to recover any losses.

INTRODUCTION

PURPOSE

1.1 The purpose of this Report is to raise fraud awareness within central government and to help managers strengthen processes to counter the risk of fraud as defined in “Government Accounting” and “Managing the Risk of Fraud – a Guide for Managers”.

1.2 The Report aims to inform departments of the scale and nature of certain categories of fraud which have been reported to the Treasury for the reporting year 2004-2005. This information is provided to help departments learn from the experiences of others when reviewing and developing their own control systems. The Report also aims to increase awareness of the risk of fraud and, in some areas, to suggest ways in which the risk can be managed and reduced. The categories of fraud which departments are required to report to the Treasury are described in paragraph 4 of this section. Because of the restrictive nature of these categories this report cannot be regarded as a definitive account of all frauds affecting government during the relevant period.

DEFINITIONS

1.3 There is currently no precise legal definition of fraud. For the purposes of reporting fraud to the Treasury the following crimes fall within the context of the Fraud Report:

Theft	Dishonestly appropriating the property of another with the intention of permanently depriving them of it (Theft Act 1968). This may include the removal or misuse of funds, assets or cash.
False Accounting	Dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive (Theft Act 1968).
Bribery and Corruption	The offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions taken by the authority, its members or officers (Prevention of Corrupt Practices Acts 1889 and 1916).
Deception	Obtaining property or pecuniary advantage by deception (sections 15 and 16 of the Theft Act 1968) and obtaining services or evading liability by deception (sections 1 and 2 of the Theft Act 1978).
Collusion	The term “collusion” in the context of reporting fraud to the Treasury is used to cover any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes listed above.

COVERAGE

1.4 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 theft or fraud at the stage when preliminary investigations have demonstrated that fraud or theft has occurred (or that an attempt has been made to commit theft or fraud). These should be reported under the following main categories:

- Fraud perpetrated by or suspected to have been perpetrated by departmental staff;
- Frauds perpetrated by members of the public with a value of £20,000 or more but only those cases that contain generic lessons for others (i.e. not cases of fraud that relate to departments' main business areas such as benefit fraud as these normally only contain lessons for individual departments); and
- Contractor frauds.

1.5 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.

EXCLUSION CRITERIA

1.6 Fraud cases that are still under investigation or subject to legal proceedings are described in outline only. Care is also taken to exclude details that could identify fraud suspects or risk action for defamation.

1.7 The Assurance, Control and Risk (ACR) team in the Treasury collates the data reported by departments. ACR applies care and judgement where necessary to ensure, as far as possible, that the report is based on a consistent analysis and classification.

2

MAIN ANALYSES

This section contains the main analyses of data relating to fraud and theft perpetrated by staff reported by departments for the year 2004/05.

OVERVIEW

2.1 The analysis in this section is based on fraud data supplied by 46 central government bodies, including all the main departments, covering the period 1 April 2004 to 31 March 2005. Overall the analyses show:

- 17 bodies provided 'nil' returns (i.e. had no cases of theft or fraud to report);
- The remaining 29 bodies reported 450 cases of internal theft or fraud with a total value of £3,136,900 (compared to £3,907,000 last year).
- There were 28 large value cases (i.e. £20,000 or more) accounting for a total loss of £2,637,700 (84% of total losses reported). Included were 10 cases with values of £100,000 or more totalling over £1.8 million (2 cases involved the theft of assets, 2 were procurement frauds and 6 cases with a total value of £1,020,000, involved collusion with members of the public and the processing of false claims).
- The analysis of anti-fraud questionnaires (**Annex A**) shows that most bodies had taken appropriate action to deal with fraud risk such as assessing risk, allocating responsibilities for managing fraud risk, introducing fraud polices and fraud response plans.

ANALYSIS OF FRAUD DATA

2.2 The following paragraphs provide detailed analyses of the business areas in which the frauds were perpetrated.

Type of Fraud	Cases		Value	
	No.	%	£	%
T&S and Allowances	26	5.78	67,300	2.15
Pay related fraud	11	2.44	11,600	0.37
Theft of assets & information	96	21.33	788,300	25.13
Exploiting assets and Information	36	8.00	11,300	0.36
Procurement Fraud	53	11.78	650,200	20.73
Personnel Management related fraud	130	28.89	15,400	0.49

Type of Fraud	Cases		Value	
	No.	%	£	%
Payments related fraud	34	7.56	1,398,900	44.59
Income related fraud	35	7.78	95,000	3.03
Other	29	6.44	98,900	3.15
Totals	450		3,136,900	

Table I – Fraud Data 2004-05

FRAUD RELATED TO PAYMENT PROCESSES

2.3 These are frauds that involve falsely creating or diverting payments. Examples of cases reported to us this year include:

- Creating bogus customer records in order to generate false payments.
- Attempts to forge departmental cheques.
- The interception of cheques and Payable Orders and attempts to cash them. In some cases alterations were made to payee details and amounts.
- Intercepted authorised expense claims and changes to personal details.
- Creating false claims to support fraudulent claims for benefits.
- Processing false claims by accomplices for benefits or repayments.

2.4 This is the largest category in terms of total value lost (£1,398,900 or 45%) but only 34 cases were reported. Individual losses can sometimes be significant in this area and there were 11 cases that each exceeded £20,000 in value and totalling £1,337,700 (6 cases with values exceeding £100,000 totalled just over £1million.).

2.5 Many of the large value cases (i.e. over £20,000) were identified through internal control systems (e.g. monitoring management information and audit trails) or via arrangements established for staff to report their suspicions of fraud. Known perpetrators were prosecuted and action taken to recover losses.

2.6 There were a number of cases involving the interception of completed payable instruments and the alteration of payee details again this year. Also reported were some cases of forged payable instruments. Usually the banks’ control systems identify these attempted frauds before any losses occur but there were several successful attempts to remove cash. Control over this type of fraud involves holding completed payable instruments securely before despatch and regular bank reconciliations which might identify these before the payments are processed through the banking system. Electronic payments might also reduce the risk of this type of fraud occurring.

2.7 Segregation of duties between important functions such as the processing of payments, payment authorisation and bank reconciliations is a key control in this area that sometimes is rendered ineffective because of collusion between key members of staff. Many of the larger value cases involved external accomplices and the creation of false claims for repayments and arose because the officers responsible for processing

them could authorise the payments as well. Collusion can be a difficult problem to deal with and the active encouragement of staff to report their suspicions of fraud and the deterrent effect of always taking appropriate action against known perpetrators should help reduce the risk of collusive fraud.

2.8 Segregation of duties, good audit trails, meaningful and regularly produced management reports, good budget management, regular management or independent reviews (e.g. by internal audit) and the secure holding of blank or completed instruments of payment are all examples of the basic controls that can be applied to the payment process. The wider use of electronic forms of payment might also reduce the risk of payment fraud. Appendix 8 of “Managing the Risk of Fraud – a Guide for Managers” offers advice about the controls that should be in place to help prevent or detect fraud in this area and Treasury’s Fraud Casenotes provide advice about controlling cash handling, bill paying, electronic funds transfer and payment by cheque or Payable Order.

THEFT OF ASSETS AND INFORMATION

2.9 This category relates to the theft of physical assets, including cash. Many cases arose because of weak security and some were opportunistic thefts (e.g. items such as laptops or mobile phones stolen from peoples’ desks) demonstrating the importance of storing such items securely at all times when not in use.

2.10 In total, departments reported 96 cases (21%) of thefts with a total value of £788,300 (25%).

2.11 This is a high-risk area, in value terms - this year the second highest category. Included were 9 cases with values of £20,000 or more and totalling over £550,000. The larger value items included the theft of IT equipment, fuel and other equipment from government buildings and sites, and the theft of equipment in transit. A number of smaller items reported as stolen included mobile phones and laptop computers which carry the additional risk of loss of sensitive information.

2.12 It is important to focus on the basic physical controls that should prevent and detect these kinds of offences. Controls such as: asset registers, and inventories; regular checks and reconciliation of holdings; secure storage and movement of valuable items; and effective control of exit and entry to government sites are fundamental.

PROCUREMENT FRAUD

2.13 Procurement is the whole process of acquisition from third parties and covers goods, services and construction projects. Procurement fraud can involve contractors, sub-contractors, Crown Servants or any combination of these often colluding to perpetrate a fraud or act of corruption. This category covers tendering irregularities, credit card/GPC frauds and payment claims for goods or services that were not delivered.

2.14 This was the third highest category both in terms of number of cases reported (53, 12%) and their overall value (£650,200, 21%). This year there has been an increase in the number and value of GPC/credit card frauds reported (4 cases totalling £1,200 last year, 41 cases with losses totalling £78,600 this year). The main worries are the number of cards that appear to have been copied and used fraudulently or the number of cases where credit card details were used to make fraudulent purchases. Generally,

the credit card companies made good the losses but it is important that credit card statements are examined in detail in order to spot frauds and report them promptly to the credit card companies.

2.15 One case, with a value of over £400,000, occurred because one staff member had a number of key responsibilities and worked largely unsupervised allowing the fraud to go undetected for a long time. This case highlights the importance of rotating duties and close management monitoring where other controls such as segregation of duties cannot easily be implemented.

2.16 Examples of controls to reduce risks associated with purchasing or associated with the use of contractors can be found in Appendix 8 of Treasury's publication "Managing the Risk of Fraud – a Guide for Managers".

INCOME RELATED FRAUD

2.17 Fraud in this area can include the theft of incoming cash or cheques (which can be opportunistic or coupled with the manipulation of financial records to disguise thefts) or adjusting records of amounts owed by customers to departments in return for cash rewards or other incentives. Income was also lost by organisations that operate shops or restaurants for the public when counterfeit banknotes were used for payment.

2.18 The overall value of fraud in this category has fallen significantly from last year's total of £2,009,400 mainly because last year's total included one case with a value of over £2million. If this case is taken out then losses this year have increased (from around £9,000 to £95,000). One case accounted for nearly £58,000 where several suspicious entries in a suspense account were being investigated at the time of reporting.

2.19 Although there were relatively few cases in this category the scale of income collected by the government is vast and individual frauds can potentially be very significant. It is important that accurate debtor records are maintained, that regular management and independent checks are carried out to ensure that income is collected and brought to account and that the work of officers with responsibility for pursuing large value debts is closely supervised. Segregation of duties between those who raise debts, those who pursue them and those who bring payments to account together with good audit trails and management information will also help to reduce the risk of fraud in this area.

TRAVELLING, SUBSISTENCE AND ALLOWANCES

2.20 Fraud in this area involves such activities as the completion of fraudulent claims for payment and includes claims for journeys that were not made, overstated claims, claims for allowances for which there was no entitlement, forged signatures authorising payment and forged documentation supporting claims.

2.21 Overall, 26 cases of fraud (6% of total cases) with a total value of £67,300 (2% of total value) was reported under this category. Cases reported included one with a value of £25,000 in which three staff members colluded to by-pass departmental controls to fraudulently claim school fees.

2.22 Controls to prevent or detect fraud in this area are straightforward (e.g. clear set of rules, an approval process, management checks, finance team checks, spot checks and monitoring via the budgetary control process). To overcome collusion, as in the

large value case referred to above, good management checks and rotation of duties might reduce this risk. The key controls relating to travel and subsistence can be found in Treasury's Fraud Casenote Number 4 and in appendix 8 of Treasury's publication "Managing the Risk of Fraud – a Guide for Managers".

PERSONNEL MANAGEMENT RELATED FRAUD

2.23 Cases reported under this category were those where action taken against perpetrators involved some personal deprivation such as being downgraded, promotion bars, pay cut or dismissal. Examples of fraudulent activities reported included:

- Staff on sick leave but working elsewhere;
- Abuses of flexible working time systems;
- Misuse of official time (e.g. abusing the department's computer misuse policy);
- Deceit or misrepresentation for advantage (e.g. false references or false qualifications used to secure employment).

2.24 The highest number of cases (130, 29%) was reported under this category but most involved little or no loss to the departments concerned. In all cases action had been taken or was planned to be taken against perpetrators. Action taken included: dismissals; demotions; and loss of spine points and/or bar on promotion.

2.25 Whilst these cases are low-risk in terms of value, it is nevertheless important that departments try to detect them as staff who get away with this type of fraud may be tempted to attempt much more serious frauds. They can also reflect badly on a department's ethical standards. Closer checking of data supplied in order to gain employment, more frequent management checks of sick leave records, close scrutiny of flexi records and independent monitoring of staff accesses to official data are all examples of controls designed to detect these types of frauds.

PAY RELATED FRAUDS

2.26 These frauds were perpetrated via the payroll process. Examples of frauds reported included falsification and/or unauthorised amendments of timesheets, false claims for working unsociable hours and the deliberate failure to repay salary overpayments,

2.27 There were 11 cases (2%) with an overall value of £11,600 reported. This is potentially a high-risk area as was proven last year when losses totalled over £250,000. Some simple housekeeping controls (see paragraph 3.27 of last year's Fraud Report) can go a long way to reducing fraud risk in this area.

EXPLOITING ASSETS AND INFORMATION

2.28 This type of fraud involves using the assets of the organisation for other than official purposes and/or supplying information to outsiders for personal gain. Many of these cases had no reported value as assessing losses is not always possible. Departments are required to report only those cases where the action taken against perpetrators goes beyond the oral or written stage (e.g. dismissal, downgrading, promotion bar).

2.29 Although figures are fairly low this year (36 cases, £11,300) this is potentially a high risk area as was shown two years ago when £2.7 million was lost as a result of information sold to a criminal gang.

2.30 Clear rules about how assets can be used, appropriate segregation of duties, effective audit trails and regular management checks on the existence and use of assets can be effective in discouraging or identifying the misuse of assets. To reduce the risk of staff providing information to outsiders that can then be used to perpetrate fraud, reliance should be placed on good detective controls such as staff reporting their suspicions (there will need to be clearly advertised avenues for staff to do this), the use of IT checks (e.g. data mining or data matching) to provide indicators that fraud might be occurring and spot checks of claims for large refunds (e.g. tax and VAT) from members of the public.

OTHER FRAUD

2.31 This category accounted for 29 cases (6% of the total) and a total value of £98,900 (3%). Two cases, each exceeding £20,000 in value, resulted in a total loss of £64,000. One case involved a member of staff in their capacity as a member of the public making false claims against their department. Departments that make payments to the public are particularly vulnerable to this type fraud where staff could use their knowledge of departmental processes to make fraudulent claims. Processes should be designed to identify members of staff that make claims against their departments for benefits so that they can be checked to confirm entitlement.

CONTRACTOR FRAUDS

2.32 As third party providers deliver more essential services, it becomes increasingly important that departments are aware of the fraud risks and the need to take appropriate action to minimise them. **Annex C** provides details of frauds perpetrated by contractors where individual losses exceeded £20,000. These cases are excluded from the main analyses. Cases involving staff working in collusion with contractors are, however, included in the main analyses.

EXTERNAL FRAUDS

2.33 Departments are asked to report any external frauds that contain lessons for other bodies. These are not included in the main analyses but summaries of individual cases where losses exceeded £20,000 can be found in **Annex D**. This annex should not be interpreted as being a complete record of all fraud perpetrated by members of the public against government. Most external fraud is related to the main work of individual departments (e.g. benefit payments) and these cases are not reported to us because they contain lessons for those departments only.

2.34 A lot of good work has been undertaken by departments to reduce external fraud. Examples include:

- The actions taken by DWP in recent years that have resulted in a reduction of fraud in the benefit system from £2 billion in 2001 to around £0.9 billion in 2004. Actions taken included: creating a professional, intelligence-led detection force equipped with new powers through the Social Security Fraud Act 2001; introducing a national advertising campaign to deter people from committing benefit fraud; increasing the capacity of the National Benefit Fraud Hotline; making the process for checking

new claims and monitoring existing claims more rigorous; and working more closely with other bodies such as HMRC and Local Authorities. DWP will continue to push forward its anti-fraud agenda including an increased use of data matching (including private sector data) and new technology. Detailed future proposals are given in 'Reducing Fraud in the Benefit System - Achievements and Ambitions' published on 13 October 2005.

- The work of the NHS Counter Fraud Service (CFS) which became operational in 1999 and has the remit of tackling all losses to fraud and corruption in the NHS in England and Wales. Since their inception they have reduced patient fraud from £171 million to £78 million. These figures include dental and optical patient fraud, reduced from £40 million to £21.5 million and £13.25 million to £10 million respectively. They have also reduced fraudulent claims by NHS professionals: these have fallen by around 50% after processes were improved to reduce the risk of fraud. A stronger counter fraud structure has been developed across the NHS by creating more than 480 professionally trained counter fraud specialists via their comprehensive counter fraud-training programme. Over 980,000 NHS staff and professionals are now covered by Counter Fraud Charter agreements. These agreements with organisations such as regulatory bodies, professional associations and trade unions, demonstrate a commitment to work with the CFS to counter fraud and corruption in the NHS. There have been 292 successful prosecutions and 324 successful civil, legal and disciplinary cases with a successful prosecution rate of 96%. The NHS CFS has provided a financial benefit to the NHS totalling £675 million - a continuing 13:1 return on the budgetary investment made in this area of work.

2.35 A great deal of good advice about managing external fraud risk effectively can be found in the joint Treasury and NAO publication “good practice in tackling external fraud”¹.

ANTI-FRAUD MEASURES

2.36 Annex A provides an analysis of anti-fraud questionnaires that were completed by 38 government departments, 30 Agencies and 93 sponsored bodies (NDPBs mostly). The questionnaires seek to identify, in broad terms, the actions taken by central government bodies to manage the risk of fraud.

2.37 Nearly all bodies had either carried out a separate fraud risk assessment (24%) or had included fraud risk in their overall assessments of risk. A majority of bodies (72%) said that they had assessed the size of the threat from external fraud and had identified the areas in their organisations that were most vulnerable to fraud (83%). As a result of this work, 32% of organisations assessed the threat of internal and/external fraud as medium or high.

2.38 It was encouraging to note that a majority of organisations had taken measures proportionate to the fraud risks they faced to tackle the threat of fraud (e.g. 32% had developed comprehensive measures to tackle fraud risk, 90% had allocated responsibility for their fraud strategies to named individuals, 73% had allocated responsibilities for managing specific fraud risks, 89% had a fraud policy, 73% had a fraud response plan, 88% had clear avenues for staff to report their fraud suspicions and 32% employed their own anti-fraud experts). Two possible areas of concern were

¹ <http://hm-treasury.gov.uk/fraud>

that only 43% of organisations said they measured the effectiveness of their anti-fraud policies and 53% provided fraud awareness training to new entrants.

2.39 It is important that organisations, particularly those with a medium or high risk of fraud, have systems in place to continuously measure the effectiveness of processes to manage fraud risk and that all new staff are at least made aware of their organisations' anti-fraud policies and what is expected of them should they discover or suspect fraud. Ideally, organisations should identify the areas most vulnerable to fraud and put in place measures to manage fraud risk proportional to the risk they face such as allocating responsibility for managing fraud risk in those areas, having a fraud policy and response plan, establishing avenues for staff to report their suspicion of fraud, measuring the effectiveness of their anti-fraud processes and promoting anti-fraud cultures.

A

ANALYSIS OF ANTI-FRAUD QUESTIONNAIRES

Completed anti-fraud questionnaires were received from 38 departments, 30 Agencies and 93 other bodies (NDPBs mostly). The table below summarises the data provided.

Organisations that:	Departments & Agencies		Other bodies		Total	
	No.	% of Total	No.	% of Total	No.	% of Total
1. Assessed the size of the threat from external fraud	43	63	73	78	116	72
2. Assessed <u>external</u> fraud risk as being:						
High	5	7	3	3	8	5
Medium	17	25	17	18	34	21
Low	46	68	73	79	119	74
3. Assessed <u>internal</u> fraud risk as being:						
High	2	3	0	0	2	1
Medium	14	21	17	18	31	19
Low	52	76	76	82	128	80
4. Undertook a fraud risk assessment.	24	35	15	16	39	24
5. Identified areas most vulnerable to fraud.	57	84	77	83	134	83
6. Developed measures to tackle fraud risk.	29	43	22	24	51	32
7. Allocated responsibility for fraud strategy/policy.	65	96	80	86	145	90
8. Allocated responsibility for fraud risks.	53	78	64	69	117	73
9. Had a <u>Fraud Policy</u>	63	93	81	87	144	89
10. Had a <u>Fraud Response Plan</u>	57	84	61	66	118	73
11. Communicated their policies & changes to staff	64	94	74	80	138	86
12. Had avenues for staff to report fraud	63	93	78	84	141	88
13. Measured the effectiveness of anti-fraud policies	28	41	41	44	69	43
14. Employed their own anti-fraud experts	29	43	22	24	51	32
15. Had access to anti fraud expertise	37	54	61	66	98	61
16. Provided fraud awareness training to new entrants	38	56	48	52	86	53
Total Number of Questionnaires completed	68		93		161	

B

LARGE VALUE FRAUDS PERPETRATED BY STAFF

The following summaries relate to cases with values of £20,000 or more which were perpetrated by or involved staff in some way (e.g. collusion with outsiders). These cases are included on the main analyses.

Travelling, subsistence and allowances frauds

£25,000 Following information received via a departmental fraud hotline it was discovered that three individuals had been providing false documentation to support claims for school fees. Collusion between the three individuals resulted in normal controls being by-passed. Criminal charges have been brought against the three individual involved in the fraud.

Thefts of Assets and Information

£356,515 Departments reported 6 separate cases of thefts of assets (e.g. IT equipment, fuel, training equipment) from various government sites. All of these cases were under investigation at the time of reporting so it was not known whether staff were involved in the thefts or not. In all cases physical security at the sites was improved to reduce the risk of similar thefts occurring.

£115,000 Weak security on a contractor's premises resulted in the theft of Crown equipment. Action has been taken to improve physical security. The case was still under investigation at the time of reporting.

£40,625 This case involved the theft of equipment whilst in transit. The case was still under investigation at the time of reporting.

£40,000 Weak security at a government building resulted in the theft of equipment by a contractor. A whistleblower reported the theft which lead to the arrest of the perpetrators and the recovery of the equipment. The contract was terminated and a prosecution is pending.

Procurement Fraud

£417,076 During routine management checks it was discovered that a member of staff had been inflating charges for customs clearance of certain items at an overseas location. It was also discovered that the same staff member had been tampering with annual bonus awards. The fraud arose because insufficient management checks were carried out and as a result better rotation of duties and closer monitoring have been introduced. A criminal prosecution is pending.

£100,000 A resettlement trainer was charged and committed to trial for forging official correspondence to support false visa applications to various government departments. The fraud arose because of an absence of control and was reported via internal arrangements. Management control has been improved.

£45,000 An allegation was made that a contract had been awarded to a company owned by an individual who was in a relationship with the department's contracts officer. There had been no declaration of interest and all the usual tendering rules appeared to have been by-passed or not recorded. Although there was a late attempt at asking other companies to tender, the decision regarding who won the tender had in effect already been taken and work commenced. The work tendered for was satisfactorily completed. All parties to the contract were interviewed under caution but there was insufficient evidence to substantiate a charge of corruption. The officer was disciplined.

£39,063 Purchases were made and charged fraudulently to 20 individual Visa cards. There was a number of transactions involved ranging in value from £5 to £3,500. The cards had not been stolen but it is suspected that card details were used to make the purchases. The credit card company refunded the total loss to the department. More detailed information is now provided to cardholders on monthly statements to allow expenditure to be checked more easily and for fraudulent purchases to be spotted more quickly.

Fraud Related to Payment Processes

**£200,000,
£180,000,
£200,000** In all three cases officers hijacked claims, adjusted them and redirected payments to external accomplices. Weak procedures allowed the frauds to be perpetrated which were discovered as a result of routine internal checks. Internal audit has reviewed procedures and have made recommendations to reduce the risk of similar frauds arising. At the time of reporting, the department was awaiting the outcome of internal investigations before taking action against the employees but the likelihood is that the perpetrators will be prosecuted.

**£20,332,
£100,000,
£220,000** A department's monitoring system detected a number of cases involving the creation of false records and repayment claims. Staff colluded with members of the public to whom false repayments were made. The perpetrators were suspended from duty and, at the time of reporting, cases were being prepared with a view to taking criminal proceedings. A study has been commissioned to identify controls to overcome the weaknesses highlighted by these frauds.

£120,000 A member of staff processed two repayment claims for non-existent minors paying the money to his partner. Investigations revealed four similar cases. In all cases the repayments were not supported by appropriate documentation. The officer was suspended from duty and further action will be taken on completion of departmental investigations. At the time of reporting it was not known what control weaknesses allowed the fraud to be perpetrated and internal audit was asked to review systems with a view to improving control.

£90,000 A Payable Order for £8.53 had been fraudulently altered and cashed. The bank discovered the alteration. The case is still under investigation.

£83,418 An officer working in collusion with 3 members of the public and two commercial entities abused his position to help the perpetrators claim refunds to which they were not entitled. The fraud came to light as a result of information provided by internal detective controls. The officer was dismissed and he and the other perpetrators were prosecuted and received custodial or suspended prison sentences. Management have introduced better rotation of duties and improved record control.

- £70,000** An officer hijacked genuine claims redirecting all payments to the same bank account. The case was discovered when non-receipt of a payment was queried. The officer was suspended from duty and further action will be taken on completion of the department's investigations.
- £53,991** A member of staff created false repayment claims and duped friends into accepting payments into their bank accounts. The fraud was discovered as a result of the department's payments monitoring system. The officer was suspended from duty pending an internal investigation. Management has since taken some corrective action which will provide additional control over similar repayment cases and are working with internal audit to discover whether any additional measures are required.

Income Related Fraud

- £57,697** A management inspection of a suspense account identified several suspicious transactions. The fraud arose because management checks were not carried out on a regular basis. The perpetrator was prosecuted, received a custodial sentence and was dismissed. The overall control system was being reviewed at the time of reporting.

Other

- £36,000** An employee of a department made a mistake in grading certain items that were sold to an overseas buyer. To cover up the mistake the employee falsified test results. The error was discovered during administrative checks. The officer received a written reprimand, was taken off certification duties, required to retrain, denied a pay award and placed under quarterly review procedure.
- £28,000** A member of staff made a number of false claims for benefits against a department and failed to declare certain income. The frauds came to light as a result of the department's internal checking system. The staff member's appointment was terminated.

C

LARGE VALUE FRAUDS PERPETRATED BY CONTRACTORS

The following summaries relate to cases with values of £20,000 or more that were perpetrated by contractors. These cases are not included in our main analyses.

£197,422

An allegation was made that a contractor was claiming public funding for services that were not provided. The investigation revealed that signatures to support claims had been forged. The department has taken action and it is in the process of recovering losses from the contractor.

£133,000

A department received an invoice from a company that claimed it had organised a conference on behalf of the department. No such conference had been organised and the department identified the attempted fraud before any payment was made.

£66,000

A contractor had submitted invoices for work at a number of locations which had not, it was alleged, been carried out. The alleged fraud arose because management checks had not been carried properly. At the time of reporting the department was awaiting the outcome of its investigation before taking action against the contractor. The department took action to improve its internal procedures which included better communication between offices where contractor services are provided and better scrutiny of work claims before authorising payments.

£50,000

A contractor performed services for a department and submitted payment requests. Payments began being made on the basis that the payment requests were valid. Further substantiation was requested from the contractor to support the payment requests. Some of the supporting documentation appeared to have been altered and departmental signatures appeared to have been forged. Management controls were not properly applied because the work was carried out during an emergency. An investigation by the police and other bodies is ongoing. The department is awaiting the outcome of these investigations before deciding whether to try to recover losses. The department has improved the control procedures to be applied during emergency situations.

£42,299

A consultancy company was employed to manage funding on a project but weak financial control allowed consultancy employees and beneficiaries to divert monies. The fraud was reported via arrangements set up by the department for reporting fraud. All the perpetrators were dismissed by the consultancy that agreed to repay around £18,000 to the department. The consultancy has reviewed its procedures for financial monitoring and has made improvements to the control environment.

£37,219

As part of an overseas project to provide mobile banking services a payment was made to a local bank to cover the purchase of a vehicle and software. The department received no confirmation that the purchases had been made and allegations of fraud were made against the director of the bank. At the time of reporting the director was being investigated by the parent bank. It was also

alleged that the contract to provide the vehicle had been awarded by the bank director to a supplier with whom he had personal links. The department has recovered the vehicle, value around £15,000. The department's internal procedures were under review at the time of reporting.

£34,141

This case involved the fraudulent activities of a sub-contractor who manipulated timesheets to falsify records of attendance. The main contractor claimed funding from a department to cover the fraudulent claims of the sub-contractor. Investigations further revealed that official sub-contracting arrangements did not exist between the two providers. The fraud was discovered during a departmental audit of contractor records. The department has recovered all losses and has introduced more frequent management checks.

£21,868

A department telephoned the office of a consultant to say that a cheque for payment for services provided was available for collection. It is thought that the perpetrator of the attempted fraud took the telephone call, collected the cheque producing official identification and a receipt book and paid the cheque into an account opened by the perpetrator for this purpose. The bank identified the attempted fraud and alerted the department before any losses occurred. The police are planning to prosecute the perpetrator.

D

EXTERNAL FRAUDS

Members of the public perpetrated the following thefts and frauds against central government bodies. This is not a complete list of all external frauds but only those cases that contain general lessons for other government bodies (note: most external frauds against government bodies relate to the business of the organisation such as benefit payments, income tax, and VAT and contain lessons for those departments only. Details of fraud in these areas are not reported to us). These cases are not included in our main analyses.

£113,175

A department was made aware of a small grant fraud involving multiple applications in another government department. Following a data matching exercise and local enquiries it was found that this department's grant schemes had also been targeted. The police have been provided with all salient information. A revised regime has been put in place for new grant applications and new guidance produced.

£108,500

In March 2005, fraudulent transactions started to appear on a department's credit card statements. In all 21 cards were affected. The cards were used for purchases in Japan mainly but some purchases were also made in Spain and the UK. Barclaycard was informed immediately and all affected cards were cancelled and new cards issued. It appears that a criminal gang in the Far East had obtained a card number and from it generated a series of card numbers some of which matched some of the department's GPC numbers. Five government departments were affected and Barclaycard estimate that around £1 million worth of fraudulent transactions were made. Barclaycard assured the department that the criminal gang had been arrested and all losses have been refunded.

£51,000

A processing error led to a payment being made to the wrong supplier. The error was discovered when the intended recipient complained of non-payment. The recipient kept the payment, was arrested, had his bank account frozen and is awaiting trial. At the time of reporting £30,000 had been recovered.

£45,647

A Payable Order was intercepted in the post, payee details were removed and replaced. The Payable Order was cashed.

£31,269

Several GPC cards were 'cloned' and used to purchase goods. Losses were recovered from Barclaycard.

£28,040

A standard pre-printed bank generated form for requesting payments to overseas suppliers was received by a bank but was rejected because it contained only one signature when two were required for the amount requested. Further investigation revealed that the form was a forgery. Electronic payment methods have been recommended for future payments.

£25,000

A departmental cheque was forged and presented for payment at a bank. The attempted fraud was discovered when the bank implemented an agreed procedure and contacted the department preventing any loss.

GOVERNMENT FRAUD REVIEW

E.1 Legislation is currently before Parliament to introduce a single offence of fraud and the Government has proposed regulations to implement Section 43 of the Criminal Justice Act 2003 which would allow a limited number of very serious and complex fraud trials to be tried without a jury if both the trial judge and Lord Chief Justice concur.

E.2 In addition, the Government has set up an inter-departmental review of fraud to report to the Attorney General and Chief Secretary to the Treasury by late spring 2006. The review will consider the prevention, detection, investigation and prosecution/punishment of fraud. It will consider the scope for improving the current arrangements with the objective of reducing the amount of fraud and the harm it causes to the economy and wider society. The Review Team will consult widely with stakeholders in the public and private sector before delivering its report.

CFSMS FORENSIC COMPUTING UNIT

E.3 The National Health Service's Counter Fraud and Security Management Service Forensic Computer Unit provides a comprehensive, professional service to recover digital evidence for use in criminal, civil, and disciplinary proceedings. They also provide a data recovery service for lost documents and an auditing service to assist in compliance of corporate policies.

E.4 Data can be recovered onsite or across a network when a system is still in use. A full forensic investigation can be carried out while allowing the organisation to maintain business continuity. The investigating officers will endeavour to carry out the work at a time convenient to an organisation's investigation. Throughout any examination process, investigators will receive regular updates of progress and, at the end will be given a final detailed report of all findings and witness statements.

E.5 If you think you would benefit from this service or want more information about it then contact CFSMS (tel: 020 7895 4999; fax: 020-7895 4379; Email: forensics@cfsms.nhs.uk).

MANAGING THE RISK OF INTERNAL FRAUD IN HMRC

E.6 HMRC undertakes a pro-active approach to the detection of internal fraud and abuse of its corporate systems (including those accessed via the internet) and established in 2002 an Anti-fraud Assurance Team which is part of Internal Audit. Publicising the role of the team within the Department (via presentations at induction training for managers, presentations to staff and articles in HMRC publications) plays an important part in promoting anti-fraud awareness and in deterring fraud. Since the introduction of the Anti-fraud Assurance Team a number of long term internal frauds have been identified resulting in positive action being taken against offenders (e.g. prosecutions, dismissals) and the Department has seen a reduction in the number of misuse cases (e.g. of the Internet, IT systems, HMRC data).

WHISTLE BLOWING

E.7 The Committee on Standards in Public Life has stressed that whistleblowing¹ is “both an instrument of good governance and a manifestation of a more open culture” and that “here, more than in any other area we have considered the principle of leadership is paramount”. The Committee calls on all public bodies to ensure that staff are aware of whistleblowing avenues, that they have access to advice and that the policy is regularly promoted and reviewed. To this end the Committee has updated and expanded its good practice on whistleblowing. The Committee endorsed the following key elements of good practice:

- Ensuring that staff are aware of and trust the whistleblowing avenues. Successful promotion of awareness and trust depend upon the simplicity and practicality of the options available, and also on the ability to demonstrate that a senior officer inside the organisation is accessible for the expression of concerns about wrongdoing, and that where this fails, there is recourse to effective external and independent oversight.
- Provision of realistic advice about the whistleblowing process. While requests for confidentiality and anonymity should be respected, there may be cases where a public body might not be able to act on a concern without the whistleblower’s open evidence. Even where the whistleblower’s identity is not disclosed, this is no guarantee that it will not be deduced by those implicated or by colleagues.
- Continual review of how the procedures work in practice. This is a key feature of the revised Code on Corporate Governance, which now places an obligation on the audit committees of listed companies to review how whistleblowing policies operate in practice. The advantage of this approach is that it ensures a review of action taken in response to the expression of concerns about wrongdoing; it allows a look at whether confidentiality issues have been handled effectively and whether staff have been treated fairly as a result of raising concerns.
- Regular communication to staff about the avenues open to them. Creative approaches to this include the use of payslips, newsletters, management briefings and Intranets, and use of Public Concern at Work’s helpline, to which employees can now subscribe.

BUSINESS AND BUYER’S PUBLICATIONS SCAMS

E.8 Government bodies should be on the alert for a scam that often involves an individual approaching a receptionist asking for the organisation’s compliments slip and some basic details that are available to the general public. The receptionist is asked to sign to say that the individual attended the premises and leaves. Next, an invoice comes through for an entry on their website with a copy contract document containing the receptionist’s signature. A number of similar scams have originated in Austria.

¹ Source: the Whistleblower issue 5 published by Public Concern at Work (www.pcaw.co.uk)

IT FRAUD AND ABUSE

E.9 The Audit Commission's report IT Fraud and Abuse 2004² includes, for the first time data provided by central government departments and NDPBs. The report is produced every three years and provides a snapshot of the level of ICT abuse, the reasons for its occurrence and the risks that organisations need to address. The overall conclusion of the report is that ICT abuse continues to be a threat and that fraud, viruses, and accessing inappropriate material on the internet present the greatest risks to organisations.

Other conclusions included:

- Organisations have improved their governance arrangements with 96% having ICT security policies, 82% employing email filtering and 85% employing staff with specific IT security responsibilities.
- There has been less commitment in providing users with robust guidance and unambiguous statements of users responsibilities (only 50% of organisations had initiated ICT security awareness training; only 20% of staff had been provided with copies of organisations' ICT security policies; only 33% of staff knew where to find written procedures for reporting security incidents).
- There was a failure to communicate to users their ICT security responsibilities which has led to: a significant increase in inappropriate use of the internet and email; virus infections continuing to represent a major risk; and ICT fraud still being a problem across organisations.
- Organisations appear to be complacent about the risks of newer technology with two thirds regarding wireless technology as being a medium to low risk and three quarters regarding PDAs as only medium to low risk.

E.10 In all 407 organisations contributed to the survey which included 61 government departments/ agencies and 62 NDPBs.

PAC AND NAO REPORTS

E.11 The following PAC and NAO Reports relate to or contain information on fraud.

- Tackling VAT Fraud (HC512 – 29 July 2004);
- HM Customs and Excise Standard Report (HC284 – 22 July 2004);
- DVLA Trust Statement (HC336 – 1 July 2004);
- Financial Management of the European Union (HC498 – 4 April 2005);
- Fraud and Error in Benefit Expenditure (HC411 – 11 October 2005).

The Reports are available on the following websites:

<http://www.publications.parliament.uk/pa/cm/cmpubacc.htm> (PAC Reports)

http://www.nao.org.uk/publications/nao_reports/chronindex.asp?type=vfm

² The report is available on the Audit Commission's website:

<http://www.audit-commission.gov.uk/reports/NATIONAL-REPORT.asp?CategoryID=&ProdID=2F4CC95D-4BC6-4e40-89FA-829C9D73438D>

(NAO Reports)

USEFUL WEBSITES

- <http://www.hm-treasury.gov.uk/fraud> - contains anti-fraud advice produced by the Treasury.
- <http://www.hefce.ac.uk/finance/assurance/fraud/> - contains a number of interesting fraud case studies.
- <http://www.ipf.co.uk/governance/counterfraud/> - CIPFA's counter fraud website.
- <http://www.iaa.org.uk/knowledgecentre/keyissues/fraud.cfm?StartRow=6> - IIAUK.
- <http://fraudadvisorypanel.org> - the Fraud Advisory Panel.
- <http://www.cfsms.nhs.uk/> - NHS Counter Fraud Security and Management Services.