

# **Fraud report 2005-06**

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

---

November 2006



HM TREASURY





HM TREASURY

---

# **Fraud report 2005-06**

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

November 2006

© Crown copyright 2006

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:

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

Fax: 01603 723000

E-mail: [hmsolicensing@cabinet-office.x.gsi.gov.uk](mailto:hmsolicensing@cabinet-office.x.gsi.gov.uk)

## **HM Treasury contacts**

This document can be found on the Treasury website at:

**[hm-treasury.gov.uk](http://hm-treasury.gov.uk)**

For general enquiries about HM 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: [public.enquiries@hm-treasury.gov.uk](mailto:public.enquiries@hm-treasury.gov.uk)

ISBN-10: 1-84532-208-8

ISBN-13: 978-1-84532-208-3

This was printed on at least 75% recycled paper.  
When you have finished with it please recycle it.

PUI15

# CONTENTS

---

	<b>Page</b>
Executive Summary	<b>3</b>
Chapter 2            Main Analyses	<b>5</b>
Chapter 3            Fraud Risk Management in Central Government	<b>11</b>
Annex A             Analysis of Anti-fraud Questionnaires	<b>13</b>
Annex B             Large Value Frauds Perpetrated by Staff	<b>15</b>
Annex C             Large Value Frauds Perpetrated by Outsiders	<b>23</b>
Annex D             Fraud Issues	<b>25</b>
Annex E             Anti-fraud Initiatives	<b>31</b>



# EXECUTIVE SUMMARY

---

1. 26 departments reported 780 cases of internal fraud or theft with losses totalling some £5,109,400. The main observations are:

- The biggest categories are **theft of assets** (225 cases, value £866k) and **personnel management related fraud** (206). A majority of cases in the latter category involved little or no direct financial loss to departments.
- In value terms two categories dominated: **payment fraud** (nearly £1.8 million) and **exploiting assets and information** (over £1.3million). Five cases, each exceeding £100k, accounted for over £2.7million.
- **Procurement fraud** accounted for 41 cases with losses totalling over £700k. One contractor fraud resulted in losses of around £600k and 24 cases involving GPC/credit cards resulted in losses of nearly £43k.
- The analysis of **anti-fraud questionnaires** revealed that a high proportion of organisations had measures in place to effectively manage fraud risk and respond to fraud when it arose, although more could be done to raise staff awareness of fraud and to improve the level of security checking of potential new employees, contractors and consultants.

2. Control issues identified in this analysis that Government bodies might bear in mind when reviewing their control processes included:

- Staff with too many key responsibilities;
- Insufficient monitoring by supervisors of staff with key responsibilities;
- Weak or no security over assets or information including assets in transit;
- Inadequate vetting of potential new staff, consultants, contractors and agency staff; and
- Insufficient attention given to the fraud proofing of new policies and programmes.



# 2

## MAIN ANALYSES

---

This section contains the main analyses of data relating to fraud and theft by staff reported by departments for the year 2005-06.

### INTRODUCTION

---

**2.1** The purpose of this Report is to inform departments of the scale and nature of certain categories of fraud which have been reported to the Treasury for the reporting year 2005-2006. 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. **Annex E** provides summaries of activities undertaken by some departments in recent years to reduce the risk of fraud which also contain useful lessons for others.

**2.2** The Report analyses data provided by central Government departments and their agencies about fraud and theft perpetrated by staff. It also includes details of some fraud cases perpetrated by members of the public or contractors with a value of £20,000 or more and containing generic lessons for others (see **Annexes B and C**). **Annex D** provides some useful information about key fraud issues which might have an impact on the anti-fraud activities in central government.

**2.3** The Report does not set out to be a complete record of all internal theft or fraud perpetrated against central Government bodies and cannot be regarded as a definitive account of all frauds affecting Government during the relevant period. 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.

### OVERVIEW

---

**2.4** The analysis in this section is based on fraud data supplied by 45 central Government bodies, including all the main departments, covering the period 1 April 2005 to 31 March 2006. Overall the analysis shows:

- 19 bodies provided 'nil' returns (i.e. had no cases of theft or fraud to report).
- The remaining 26 bodies reported 780 cases of internal fraud or theft with a total value of £5,109,400.
- There were 23 large value cases (£20,000 or more) accounting for a total loss of £4,531,700 (89% of total losses reported). Included were 7 cases each exceeding £100,000 in value with losses totalling £3,952,700 (77%).
- The analysis of anti-fraud questionnaires (**Annex A**) found that most organisations had effective measures in place to manage fraud risk although more could be done to raise staff awareness of fraud, vet potential new staff, share information with other Government bodies and fraud proof new policies and programmes.

## ANALYSIS OF FRAUD DATA

**2.5** The following paragraphs provide analyses of the business areas in which the frauds/thefts were perpetrated.

Fraud Category	Cases		Value	
	Number	%	£	%
Travel, Subsistence & Other Allowances	50	6.41	38,700	0.76
Pay or Allowances Paid Via the Payroll	36	4.62	55,600	1.09
Theft of Assets	225	28.85	866,100	16.95
Exploiting Assets and Information	72	9.23	1,314,900	25.73
Procurement Fraud	41	5.26	708,500	13.87
GPC/Credit Card Fraud	24	3.08	42,900	0.84
Personnel Management Related Fraud	206	26.41	82,200	1.61
Payment Fraud	75	9.62	1,758,800	34.42
Receipt Fraud	19	2.44	144,100	2.82
Other	32	4.10	97,600	6.56
<b>Total</b>	<b>780</b>		<b>5,109,400</b>	

## PAYMENT FRAUD

**2.6** These are frauds that involve falsely creating or diverting payments. Examples of cases reported included:

- Creating bogus customer records and bank accounts in order to generate false payments;
- Intercepting cheques and Payable Orders and attempts to cash them. In some cases alterations were made to payee details and amounts;
- Creating false claims to support fraudulent claims for benefits;
- Processing false claims by accomplices for benefits, grants or repayments;
- A member of staff authorising payments to himself.

**2.7** This is the largest category in terms of value lost (£1,758,800 or 34%) although only 75 cases were reported. Individual losses can sometimes be significant in this area with 4 cases (each exceeding £100,000 in value) accounting for losses totalling £1,458,700 (83% of total losses in this category). One large-value case with losses of over £860k involved a consultant using his expert knowledge of an accounting system to create false payments to his personal bank account (the consultant was also employed on the basis that he was a qualified accountant when he was not).

**2.8** All of the large value frauds arose because some individuals with key responsibilities worked largely unsupervised allowing the frauds to go undetected for a time. These cases highlight the importance of rotating duties and effective monitoring where other controls such as segregation of duties cannot easily be implemented. Once someone is in a position to affect the processing of payments, they can have a significant impact. It is not just payments to suppliers that are at risk. Central Government staff are often in a position to affect grant and benefit payments as well as collecting and administering taxes.

**2.9** 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. 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 can help reduce the risk of collusive 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 HM Treasury's *Fraud Casenotes* provide advice about controlling cash handling, bill paying, electronic funds transfer and payment by cheque or Payable Order.

## EXPLOITING ASSETS AND INFORMATION

---

**2.10** 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).

**2.11** This year departments reported 72 cases (9%) in this category with losses totalling £1,314,900 (26%). This is potentially a high risk area as is clearly demonstrated this year by one case where losses totalled £1,250,000 and involved a Government employee providing details of departmental records to an external accomplice to perpetrate the fraud.

**2.12** Clear rules about how assets can be used, appropriate segregation of duties, effective audit trails, effective supervision of employees and regular management checks on the existence and use of assets can be effective in discouraging or preventing the misuse of assets or information. 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 can be effective as well.

## THEFT OF ASSETS

---

**2.13** This category relates to the theft of physical assets, including cash. Many cases arose because of weak security but 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.

**2.14** In total, departments reported 225 cases (29%) of thefts with a total value of £866,100 (17%).

**2.15** This is a high-risk area and was the highest category in terms of number of cases reported and third highest in terms of value. Included were 2 cases with values of £20,000 or more and totalling over £668,000 (77% of this category's total value). The larger value items included the theft of two satellite phones that were used to run up bills of over £600,000. A number of smaller items reported as stolen included cash, mobile phones, palmtop and laptop computers (which carry the additional risk of loss of sensitive information).

**2.16** 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. Where mobile phones are stolen, it is important to identify the thefts quickly and to take prompt action to minimise losses due to their illegal use.

## **PROCUREMENT FRAUD & GPC/CREDIT CARD FRAUD**

---

**2.17** 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. These categories cover tendering irregularities, unauthorised use of the Government Procurement Card (GPC) and payment claims for goods or services that were not delivered.

**2.18** These two categories accounted for 65 (8%) cases of fraud with a total value of £751,400 (15%). This included 24 GPC/credit card frauds with losses totalling £42,900. One case accounted for losses of £600,000 and involved collusion between staff and a contractor that resulted in payments for work that had not been completed satisfactorily.

**2.19** A number of cases were reported where staff colluded to award contracts in return for incentives or where friends or family members were awarded contracts. Losses to departments were not provided in these cases because the goods or services had been satisfactorily provided but it is possible that better value for money might have been achieved through proper competition. In one case, a contract was let to a company owned by a departmental employee who was appointed to his post on the basis of a false qualification. In all these cases the key control was segregation of duties but collusion between the parties rendered this control ineffective. Rotation of duties and effective monitoring should help reduce the risk of collusive fraud.

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

## **PERSONNEL MANAGEMENT RELATED FRAUD**

---

**2.21** Examples of fraudulent activities reported under this category 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).

**2.22** The second highest number of cases (206, 26%) was reported under this category but most involved little or no loss to the departments concerned. One case where losses amounted to £35,000 related to the employment of somebody who provided false educational qualifications in order to gain employment and who also failed to declare a criminal record. Similar situations have arisen in previous years and highlight the importance of good recruitment processes that should include carrying out effective checks into potential new employees. In all cases action had been taken against perpetrators that included: dismissals; demotions; and loss of spine points and/or bars on promotion.

**2.23** Whilst these cases are usually 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.

## RECEIPT FRAUD

**2.24** 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.

**2.25** The overall value of fraud in this category was £144,100 involving 19 cases. Cases included the manipulation of records in order to reduce the amount owed by an individual to a department (£31,000)

**2.26** 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.

## TRAVEL & SUBSISTENCE, PAY AND OTHER ALLOWANCES

**2.27** Fraud in this area involves such activities as the completion of fraudulent claims for payment or the creation of false payroll records. Examples of fraud include claims for journeys that were not made, overstated claims, claims for allowances for which there was no entitlement, forged signatures authorising payment, forged documentation supporting claims or applications for employment, falsification and/or unauthorised amendments of timesheets, false claims for working unsociable hours, deliberate failure to repay salary overpayments and the creation of non-existent personnel on payrolls

**2.28** In total there were 86 (50 T&S, 36 pay) with losses totalling £94,300 (£38,700 t&s, 55,600 pay). There were no high-value frauds (i.e. £20,000 or more) reported under these categories.

**2.29** 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 HM Treasury's *Fraud Casenote Number 4* and in **appendix 8** of HM Treasury's publication *Managing the Risk of Fraud – a Guide for Managers*.

## OTHER FRAUD

---

**2.30** This category accounted for 32 cases (4% of the total) and a total value of £97,600 (2%). Total losses included one high-value case (£27,500) that involved a member of staff stealing funds from a deceased customer's account.

## EXTERNAL AND CONTRACTOR FRAUDS

---

**2.31** Departments are asked to report any high value (i.e. £20,000 or more) external frauds including fraud perpetrated by contractors that contain lessons for other bodies. These are not included in the main analyses, however, cases involving staff working in collusion with outsiders are included in the main analyses.

**2.32** In all, 9 external fraud cases were reported with losses totalling nearly £300,000. Summaries of individual cases can be found in **Annex C**. This annex should not be interpreted as being a complete record of all fraud perpetrated by contractors or 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.

**2.33** Two cases, each exceeding £20,000 in value, resulted in a total loss of £58,000 involved members of staff in their capacity as a member of the public making false claims against their department. Both cases were discovered as a result of other investigations into the activities of the individuals (who were both dismissed and action taken to recover losses). 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.

**2.34** A great deal of good advice about managing external fraud risk effectively can be found in the joint HM Treasury and NAO publication *Good Practice in Tackling External Fraud*<sup>1</sup>.

---

<sup>1</sup> <http://hm-treasury.gov.uk/fraud>

# 3

## FRAUD RISK MANAGEMENT IN CENTRAL GOVERNMENT

This section contains an analysis of anti-fraud questionnaires completed by 194 central Government bodies. These questionnaires sought to determine how fraud risk is managed and what new controls/processes had been put in place in recent years to reduce the risk of fraud.

### OVERVIEW

**3.1** The analysis in this section is based on information supplied by 38 Government Departments, 41 Agencies, 86 NDPBs and 29 other bodies (e.g. Special Health Trusts), 194 bodies in all.

**3.2** Overall the analysis revealed that fraud is taken seriously across central Government bodies and that organisations have measures in place (or are planning to install them), proportional to the fraud risk they face, to manage fraud risk effectively and to respond to fraud when it arises. Government bodies have also carried out a lot of work in recent years to improve their management of fraud risk and anti fraud initiatives in some bodies have resulted in big reductions in fraud losses (e.g. benefit fraud has been reduced from around £2billion a year to just under £1billion and DWP is working to reduce losses further). **Annex E** provides more details of measures taken by departments to reduce losses due to fraud.

**3.3** The analysis revealed some possible areas where more might be done to reduce the risk of fraud including:

- Raising staff awareness of fraud through training and communication (e.g. via Intranets);
- Carrying out basic security checks of all potential new staff, consultants, contractors and agency staff and higher security checks of those destined to be employed in more sensitive areas;
- Reviewing policies and controls following major frauds;
- Ensuring that the risk of fraud is always considered when developing new policies, programmes and projects;
- Sharing information with other organisations about frauds in order to allow Government bodies to check whether the same fraudsters are targeting their systems; and
- Sharing financial information with a view to identifying possible fraudulent activity (e.g. data matching or data mining).

### New or Altered Fraud-risk Management Processes

**3.4** The anti-fraud questionnaire asked central Government bodies to describe details of any new or altered fraud risk management processes that were implemented in the last 3 years. Some departments undertook major initiatives to reduce fraud and these are described in detail in **Annex E**. The main actions taken to combat fraud are summarised below:

- A large number of bodies (61) created new or reviewed and updated their existing anti-fraud strategies, anti-fraud policies, fraud response plans and user guidance. A further 21 bodies had established or were developing whistle blowing arrangements.
- All of the above bodies and at least 21 more had implemented processes to raise awareness of fraud. This was achieved by establishing anti-fraud intranet websites (21 bodies), disseminating anti-fraud information to staff, running fraud workshops and fraud awareness programmes, including fraud awareness in induction training for new staff and arranging presentations for senior managers. Other activities included notices on payslips, on forms used to claim benefits or grants and general advertising campaigns. One organisation had provided fraud awareness training to all GPC cardholders and administrators.
- All organisations where major fraud was discovered had implemented new controls to reduce the risk of similar fraud occurring in future. Additionally, a number of organisations had enhanced their budgetary and financial controls by installing new accounting systems. New controls/processes implemented included paying most suppliers via BACS, improved procurement procedures including better segregation of duties, improved authorisation procedures and checks over payroll processes and better security arrangements over physical assets.
- At least 21 bodies had reviewed the risk of fraud either for the first time or as part of a periodic review of risk. These reviews included the allocation of overall responsibilities for fraud risk management and for managing specific fraud risks.
- One large organisation had introduced central reporting requirements for all fraud cases to ensure that all cases were dealt with consistently.
- A number of bodies (8) had taken on anti-fraud specialists or had arranged for existing staff to receive appropriate professional training.
- Some bodies (6) each with a large number of distinct business areas had established working groups to coordinate the sharing of intelligence and best practice between themselves and subsidiary bodies. There was also some evidence of intelligence sharing across Government bodies where organisations were engaged in similar activities or faced similar risks (e.g. the payment of grants, reducing the risk of identity fraud) with 3 organisations implementing more effective data matching or data mining techniques.
- At least 5 organisations had established new Audit and Risk committees.
- Several bodies had carried out independent reviews of counter-fraud arrangements, including organisational policies and fraud awareness activities (e.g. by internal audit).

# A

## ANALYSIS OF ANTI-FRAUD QUESTIONNAIRES

Completed anti-fraud questionnaires were received from 38 Departments, 41 Agencies, 86 NDPBs and 29 other central Government bodies. The table below summarises the data provided.

Organisations that:	Departments & Agencies		Other Bodies		Total	
	No.	% of total	No.	% of total	No.	% of total
<b>Total number of Questionnaires completed</b>	<b>79</b>		<b>115</b>		<b>194</b>	
Carried out regular risk assessments	76	96.2	100	86.96	176	90.72
Carried out regular fraud-risk assessments	46	58.23	61	53.04	107	55.15
Had anti-fraud and theft policies	72	91.14	104	90.43	176	90.72
Had a fraud response plan	62	78.48	77	66.96	139	71.65
Operated a policy of zero tolerance	56	70.89	70	60.87	126	64.95
Had whistleblowing arrangements or fraud hotline	72	91.14	100	86.96	172	88.66
Had other avenues for reporting fraud	55	69.62	69	60.00	124	63.92
Recorded and investigated all suspicions of fraud or theft	76	96.20	105	91.30	181	93.30
Monitored all fraud investigations	73	92.41	98	85.22	171	88.14
Took appropriate action against known fraudsters	74	93.67	104	90.43	178	91.75
Allocated overall responsibility for anti-fraud strategy	60	75.95	98	85.22	158	81.44
Allocated responsibility for managing specific fraud risks	51	64.56	78	67.83	129	66.49
Reviewed policies and controls following major frauds	63	79.75	96	83.48	159	81.96
Used appropriate personnel to investigate fraud	64	81.01	100	86.96	164	84.54
Provided fraud awareness training to staff	27	34.18	26	22.61	53	27.32
Made staff aware of anti-fraud policy	68	86.08	94	81.74	162	83.51
Made members of the public aware of anti-fraud policy	20	25.32	24	20.87	44	22.68
Covered anti-fraud policy in induction training	44	55.70	65	56.52	109	56.19
Applied basic security checks to all potential new staff	70	88.61	81	70.43	151	77.84
Applied higher security checks destined to work in sensitive areas	61	77.22	55	47.83	116	59.79
Applied security checks to contractors	46	58.23	43	37.39	89	45.88
Applied security checks to consultants	47	59.49	39	33.91	86	44.33

Organisations that:	Departments & Agencies		Other Bodies		Total	
	No.	% of total	No.	% of total	No.	% of total
Applied security checks to temporary staff hired through employment agencies	53	67.09	50	43.48	103	53.09
Carried out regular data-matching/mining	35	44.30	46	40.00	81	41.75
Set targets to reduce fraud	6	7.59	10	8.70	16	8.25
Reviewed the effectiveness of anti-fraud arrangements	41	51.90	58	50.43	99	51.03
Publicised their determination to stamp out fraud	26	32.91	31	26.96	57	29.38
Fraud-proofed new programmes	31	39.24	32	27.83	63	32.47
Had Boards that endorsed Anti-fraud policy & practices	72	91.14	101	87.83	173	89.18
Provided regular reports about fraud to Boards	65	82.28	94	81.74	159	81.96
Had Boards that assumed responsibility for fraud risk	55	69.62	81	70.43	136	70.10
Embedded fraud-risk assurance principles in contracts	53	67.09	65	56.52	118	60.82
Shared information on fraud with others.	48	60.76	61	53.04	109	56.19

# B

## LARGE VALUE FRAUDS PERPETRATED BY STAFF

The following summaries relate to cases with values where losses exceeded £20,000 and which were perpetrated by or involved staff (e.g. collusion with outsiders). These cases are included in the main analyses.

### PAYMENT FRAUD

- £867,200**
- B.1** A department recruited a consultant via a recruitment agency to act as a SAP accounting system expert. He assisted line staff in improving their knowledge and use of SAP and was given access to the department's IT system and SAP accounting system in order to carry out his duties. He subsequently transferred to another area within the department.
- B.2** During his time in central finance he authorised a form to set up a company (a Housing Association) on the departments SAP vendor database. The individual was a director of this company along with his wife and it was registered at their home address. The individual then created a 'ghost' person to be added to the department's IT systems, which enabled him to set up the 'ghost person' on SAP. Once the contractor (using both his own and 'ghost' identities) had access to SAP he was able to create purchase orders, approve them, enter goods received and invoice details for payment.
- B.3** A number of purchase orders (for consultancy services and equipment) for values less than £1,000 were raised before others up to £100,000 were raised. A total number of 21 purchase orders were raised resulting in payments to the value of £867,200 being made to the Housing Association.
- B.4** The area of the department where the individual worked had no legitimate business relationship with any Housing Association. The payments were made from a cost centre with a large budget, which was being under spent and where the fraudulent payments went unnoticed. The individual left the department before the fraud was detected although his line manager had started asking leading questions about his activities. The fraud was detected when a review of capital expenditure was undertaken within the line.
- B.5** The fraud was reported to Internal Audit as soon as it was discovered and was investigated by its specialist fraud unit. Internal Audit reported the case promptly to the Metropolitan Police and continued their investigation into the lessons learnt and made a number of recommendations to prevent a similar fraud being repeated. Key issues that arose from the investigation included:
- The perpetrator claimed to be a qualified accountant, but according to the ACCA he was only registered as a trainee. No checks on his educational and professional qualifications were made;
  - Insufficient control was exercised over the setting up or amending of vendor records on SAP;
  - Insufficient control over the setting up of individuals on the department's IT and accounting systems;
  - Lack of post payment checks being carried out;

- Lack of effective supervision of agency staff; and
- Failure of employment agency to carry out effective basic checks.

**B.6** The police charged the individual and his wife under the Proceeds of Crime Act 2002 (Money Laundering) and the Companies Act of 1985 (Fraudulent Trading). He was sentenced to four years and his wife was sentenced to six months imprisonment in March this year. At the time of writing this case £500,000 worth of assets had been identified for recovery. Recovery action remains on going with a Court hearing due.

**£672,200 B.7** Five similar cases were reported in which members of staff created false records so that fraudulent payments would be made to bank accounts set up for this purpose. In one case the fraud involved outside accomplices. The frauds were detected by the department's payments monitoring system or as a result of information received from informers. In all cases, the officers were dismissed and criminal proceedings planned or taken against them and their accomplices. Inadequate preventive controls allowed the frauds to be perpetrated and the department concerned was reviewing its procedures with a view to reducing the risk of similar frauds occurring in future.

**£81,222 B.8** A member of staff employed in a finance post exploited access to and knowledge of the Supplier Database and payment systems to create a new supplier record including a new bank account which appeared to relate to a satellite site for an existing supplier (though it was actually one for a similarly named company registered by the employee) and to raise and pay two illegitimate invoices for circa £81K to the newly registered bank account. In addition it is believed that the staff member inadvertently changed the bank account details of the original supplier and caused two legitimate payments intended for the original supplier to be redirected to the newly registered bank account. These redirected payments totalled £9.2 million. The failure of these to reach the intended recipient caused enquiries to be made which brought the matter to light.

**B.9** The size of these payments also triggered anti money laundering procedures in the recipient bank, which froze the monies. All the funds except approx £51K, which was withdrawn before the bank froze the funds, were recovered direct from the bank.

**B.10** The member of staff was suspended and then dismissed. Police were immediately informed and, at the time of reporting, the former member of staff was on Police bail while their enquiries continued. In a civil action, the Department obtained a freezing order from the High Court freezing assets, including properties and the proceeds of their sale to the sum of £130k (£51k stolen, plus interest on £9.3 million for the time it was out of the department's account, plus costs). Having issued a claim against the former staff member the Department obtained summary judgment against them in the High Court for the amounts misappropriated and redirected (less the amount recovered directly from the bank), plus interest and costs in full. The Department subsequently returned to Court to increase the value of assets frozen to £160k to protect the value of the summary judgment. At the time of reporting the Department was waiting to see whether the former member of staff would apply for and obtain permission to appeal against the summary judgement.

**B.11** Immediate, interim, amendments were made to supplier record and payment procedures to prevent any recurrence and work is continuing to identify sustainable safeguards to address the system vulnerabilities.

**£33,781 B.12** An accounts assistant, in collusion with a contractor, generated fraudulent payments which involved forging signatures on cheques and adjusting accounting records. Weak internal controls allowed the fraud to be perpetrated. These included bank statements being received directly by accounts staff and insufficient management controls over cheques. The fraud was discovered when the bank questioned a transaction. Action has been taken to recover losses. The majority of the amount lost was recovered from the contractor and the accounts assistant dismissed.

**£30,822 B.13** An absence of control allowed a member of staff working in a department's finance section to obtain blank cheques and make payments to themselves. There were several weaknesses that contributed to this:

- Copy sheets were not always used when a clerical giro was issued.
- National Insurance numbers were not recorded on the clerical giros.
- There was no segregation of the Finance duties - the same person performed all of the duties relating to the control and issue of clerical giros and no additional checks were issued to compensate for the lack of segregation.
- The person (cashier) who held the stock of giros, prepared and issued the giros also performed the monthly-unmatched giro return with no supervision.
- Selection of giros for test checking was not made from a source document but from supporting documentation. As there was no supporting documentation for the giros under investigation, by selecting in this way none of the fraudulent giros were ever selected for test checking.
- Inadequate training for Finance staff was identified.

**B.14** The fraud was discovered through departmental payment monitoring arrangements and action has been taken to recover the losses. The officer was dismissed. The Police were involved in the case and the member of staff was charged and pleaded guilty to the theft. The case was heard at Crown Court and the individual was sentenced to 1 year's imprisonment. The weaknesses were fully discussed locally with management during the investigation and changes were implemented at that time to address most of them.

**£20,000+ B.15** A fraud against a charitable fund from which compensation payments could be made to members of the public was under investigation by a department. The fraud arose because a member of staff had total responsibility for administering the fund (e.g. checking application forms, authorising and making payments) and took advantage of the lack of segregation of duties in order to create fictitious forms and make payments to his own bank account. The charity has obtained a freezing order on the perpetrator's assets and criminal proceedings were underway at the time of reporting. New processes have been implemented to reduce the risk of similar fraud in future including separation of duties between the functions of checking claims, authorising and making payments.

## THEFT OF ASSETS

---

**£644,000 B.16** Two satellite phones were stolen from a batch of phones sent to an overseas location and were used for a period of 17 months resulting in bills to the department

totalling £644,000. The fraudulent use of the phones was allowed to continue over such a long period because the thefts had not been identified at the time and the bills paid in the UK were assumed to relate to official usage (which was not checked).

**B.17** The department investigated the incident and made recommendations to reduce the risk of similar incidents arising in the future. The main weaknesses identified by the investigation included:

- Staff at the locations where the phones were sent were not informed that they had been despatched;
- No record of what was received or issued was maintained at the overseas location;
- There was a lack of secure storage to house the equipment when it arrived;
- The phones had been activated before despatch so they could be used immediately by anybody with possession of them;
- There was no credit limit on the phones; and
- Bills were paid without compliance with proper procedures and adequate budget monitoring.

**£24,000 B.18** An accountant at an overseas post was able to steal cash and hide the theft through false accounting. The fraud arose because managers at the post had not received adequate training regarding the computer-based accounting system in place at the time so did not fully understand information produced which would allow them to monitor transactions. The fraud was discovered when the accountant was made redundant as a result of staff restructuring. The accountant could not continue hiding the fraudulent transactions and they were found during a routine monthly check of the account. The officer was dismissed and terminal gratuities withheld reducing the loss to around £24,000. At the time of reporting, criminal proceedings had begun against the officer, a new computerised accounting system installed and staff trained to use and understand it.

## EXPLOITING ASSETS AND INFORMATION

**£1,250,000 B.19** An officer was suspected of providing information from a department's records to outside accomplices to claim payments from the department. The fraud was detected by the department's payments and legal proceedings commenced.

## RECEIPT FRAUD

**£31,000 B.20** A departmental employee created false records for their partner's business and provided false information about expenditure incurred by the business. The fraud came to light as a result of information supplied by a member of the public and resulted in the member of staff being suspended whilst legal proceedings were being considered.

## PROCUREMENT FRAUD

**£600,000 B.21** During a routine review meeting concerns were raised over the management of a spare parts contract and the apparent payment of approximately £480k (excluding VAT) for work that had not been completed. The investigation identified evidence of collusion between members of staff and the contractor and it also appeared that no

monitoring of the work was undertaken. At the time of reporting prosecutions were pending and recovery action instigated.

**£43,719 B.22** This case arose when employees working on an overseas project voiced concerns about the conduct of the Project Director. The outcome of the Department's investigation was a Crown Court case involving two men, one of them formerly employed by the Department. The men received custodial sentences for conspiracy to defraud (i.e. one of them awarded contracts to a company he jointly owned with the other for goods which were largely not necessary). Also, the Departmental employee was found guilty of deception for gaining employment on the basis of a false qualification. Confiscation Orders were also served on both men for the recovery of all losses. This was a one-off incident and local management have been instructed to be more alert to the risk of something similar happening in future.

**£35,875 B.23** An employee arranged for an education contract to be let with an ex-associate. Normal contractual arrangements were by-passed. The Procurement department identified the fraud when the company began to invoice for their services, payment was stopped and the contract cancelled. An investigation revealed that the work being proposed was already being performed under a separate contract. Although the Department incurred no financial loss, the potential loss was nearly £36,000. The employee resigned and for health reasons no further action was taken against him.

**£56,958+ B.24** An allegation was received from an office concerning regular payments that were being made to an outside company for a service that was allegedly being provided to two Departmental offices. An initial enquiry by the office failed to establish a reason for these payments. After extensive investigations it was established that the invoices were false and that no company detailed on the invoices existed. Although no member of staff could be identified as perpetrating this offence there were further lines of enquiry that could be pursued but were outside the legislative powers of the Investigator, therefore the matter was passed to the Police to continue the investigation.

**B.25** The control weaknesses identified were as follows:

- The Remote Processing Centre set-up an account for a company and subsequently credited money into a bank account on the basis of receiving an invoice. This was the incorrect procedure, as the office should have submitted a separate form for this purpose.
- The office did not pick up the rogue payments for approximately 6 months despite reports being issued showing these payments.
- No checks were made to confirm that the signature authorising payment was that of an authorising officer.
- The issue of official authorisation stamps were not recorded nor were they held securely.
- There was no official mechanism for the submission of payment forms to the Remote Processing Centre which meant they could be sent by any means without the need for official acknowledgement.
- It is believed that an electronic payment form was downloaded and transferred to a floppy disc for use outside of business premises. It was recommended that consideration should be given to the number of individuals who have their floppy disc facility enabled.

## PERSONNEL MANAGEMENT RELATED FRAUD

---

**£35,000 B.26** An officer was employed but from information received from an informer was subsequently found to have provided false educational qualifications and had not declared a criminal record. The police investigated the matter and the officer was charged under the Theft Act, pleaded guilty and was fined £500 plus £55 costs. New checks have been implemented in the recruitment process to prevent similar situations arising. These new checks include an automatic check for a criminal record, only allowing original qualification certificates and seeking references from all previous employers in the last 5 years.

**£20,000+ B.27** A number of consultants conspired to ensure that a colleague/friend was also recruited at an inflated rate. The fraud arose because there was no proper separation of duties and too much reliance was placed on the consultants who were able to influence management decisions about recruitment. The three consultants had their contracts terminated and procedures for the recruitment of consultants.

**£20,000+ B.28** A Programme Director failed to exercise proper control over a high-profile programme. An investigation by the department into programme delays revealed a number of shortcomings in the management of the project including:

- Department rules relating to the appointment of consultants had been circumvented (e.g. in one case a consultant's contract had been extended by transferring the contract to an NDPB in order, it appears, to circumvent the Department's procurement rules);
- Very little control was exercised over payments to consultants (e.g. claims were not checked properly re time spent on the programme and quality of work);
- Misuse of Assets;
- Abuse of Department's computer policy.

**B.29** The Programme Director was suspended pending the outcome of investigations. The Department also terminated the contracts of two consultants and put a hold on the payment of some invoices. Appointing an interim Programme Director and revising project reporting arrangements has significantly strengthened the shortcomings identified in the management of the programme.

## OTHER FRAUD

---

**£38,464 B.30** In this case a clerical error resulted in the significant overpayment of a refund to a member of the public. The repayment was made because the officer who processed the repayment and the line manager failed to recognise the unusually large value of the refund where most refunds tend to be in the range £100 to £500. At the time of reporting recovery action against the person who received the overpayment was on-going and £19,000 had been recovered. New procedures have been put in place to reduce the risk of similar errors in future which include the use of control totals and the referral of large value refunds to senior staff for checking.

**£27,468 B.31** During a random security check by a department's audit and risk management team it was revealed that an employee had authorised a BACS payment transferring £20,000 from a deceased customer's account to an account owned by her husband. Further investigations revealed a number of other similar fraudulent transactions. In total £27,468 was written off as a loss to the department. The employee was dismissed and £10,000 recovered. It was decided not to take any further action against the ex-employee on the grounds of ill health.

**B.32** The fraud arose because the officer was in a position of trust, had complete access to all Death Claims records and no checks were carried out into her activities. All papers relating to Death Claims are now held in a secure area with limited access to them and on-going checks by Audit and Risk management have been implemented.



# C

## LARGE VALUE FRAUDS PERPETRATED BY OUTSIDERS

Members of the public or contractors perpetrated the following cases. This is not a complete list of all external fraud cases but only those that contain general lessons for other Government bodies. These cases are not included in the main analyses.

### CONTRACTOR FRAUD

- £20,000+** **C.1** A contractor employed to provide training to members of the public had secured a high number of contracts on the basis, it is alleged, of false information supplied about staffing levels and qualifications of trainers. The training provider is also alleged to have submitted false claims for participants in training courses, provided inadequate training or submitted claims for training provided when in fact courses were cancelled due to staff shortage.
- C.2** The situation was allowed to continue because of lack of independent validation of the quality of services provided and failure by the department to apply basic management checks, like authenticating the services and documentation provided by the contractor in support of securing a contract. Recovery action has been taken against the contractor and District Performance Quality Monitoring Teams (DPQMT) will monitor all remaining contracts more closely to ensure they comply with the terms of their contracts and agreed variations to the contract documented and held in the contract file.
- £29,315** **C.3** A scheme to help disabled people find employment suffered a number of frauds including:  
**£52,187**  
**£20,899**
- An employer submitting a false invoice for the purchase of a vehicle;
  - Falsified timesheets submitted by workers employed to provide support to disabled staff;
  - Fraudulent claims for services that were not provided;
  - False travelling expense claims.
- C.4** The frauds came to light as a result of monitoring arrangements or following information received from third parties alleging fraud. They arose because checks of claims had not always been carried out properly. One case was referred to the police and action was being taken in all cases to recover losses. Improved local monitoring arrangements have been put in place to monitor funding more closely.
- £34,141** **C.5** Two organisations employed to provide training to members of the public sub-let the contracts contrary to the terms and conditions of contracts and without notifying the Department. Allegations against the sub-contractors included sub-standard training and the submission of fraudulent time sheets. Also, there was no evidence of monitoring by the main contractors of sub-contractor activities. Recovery action was taken against the main contractors.
- £37,031** **C.6** As a result of the investigation recommendations have been made to the District Performance Quality Monitoring Teams (DPQMT) to ensure that any changes in contract terms and conditions should be discussed with the appropriate Procurement

Team before agreement with the provider. The DPQMT will also notify contractors that more robust method of monitoring sub contractors is required and followed up with regular checks.

## EXTERNAL FRAUD

---

**C.8** A criminal gang established 55 fictitious construction companies in different parts of the country in order to be able to submit applications for training grants for non-existent employees. Suspicions were aroused in the department by the large number of companies claiming these grants and by the large numbers of people for which the grants were claimed. Also, bank staff became suspicious when they were approached to open accounts and reported their concerns to the department.

**C.9** Initial investigations revealed similarities between the applications for registration from the different fraudulent firms (e.g. same mobile phone numbers, same e-mail; addresses, trading from rented office space, same handwriting on different applications).

**C.10** In total £163,940 was claimed by 12 fictitious employers, £48,230 was paid out before the fraud was discovered. At the time of reporting the case had been handed over to the police for investigation.

**C.11** To reduce the risk of similar frauds occurring in future, the department established more robust controls over grant applications which included:

- Requiring firms to provide clear evidence of construction activity when applying for registration;
- Additional checks to verify the authenticity of firms (e.g. on-line checks, credit agency checks, postcode searches on trading addresses);
- Cross checking to other applications to look for similarities which might indicate fraud.

**£58,000 C.12** Two cases were reported where members of staff, in their capacity as members of the public, were found to be claiming benefits to which they were not entitled. The frauds came to light following investigations into the activities of the individuals concerned, both officers were dismissed and action taken to recover losses.

## CENTRAL FRAUD REVIEW

---

**D.1** The final Fraud Review Report was published for consultation on 24 July 2006. The consultation period finished on 27 October 2006. An interim report was published on 22 March 2006. The Review's objectives were to define Government's role in dealing with fraud. Specifically, the Review set out to determine the scale of fraud in the UK, recommend an appropriate role for Government in dealing with fraud and determine how resources could be spent to maximise value for money across the system.

**D.2** The key messages and recommendations in the Report include:

- The lack of reliable data and the inconsistent measurement of fraud mean that we do not know the scale of the fraud problem. Without better information we cannot develop a sensible national strategy for dealing with fraud. The Review therefore recommends that fraud across the economy should be measured on a consistent basis.
- The Government must take an active role in protecting public money from fraudsters and must also do more to protect consumers and business against fraud. A national strategy for dealing with fraud which takes a holistic approach and deploys resources to where they will be most effective will ensure a more co-ordinated approach to combating fraud.
- The Review recommends that the Government should establish a National Fraud Strategic Authority to devise a national strategy for dealing with fraud, including the need for more public awareness and ensure that it is implemented.
- Fraud is massively unreported and is not a Police priority. Improving the reporting and recording of economic crime so that a better estimate of the scale of fraud can be gained is important for victims; business; prosecuting authorities and law enforcement agencies.
- The Review recommends the establishment of a National Fraud Reporting Centre for businesses and individuals to report fraud. To ensure a partnership approach to tackling fraud, the Centre should be jointly staffed and financed with public/private sector resources. The Review proposes the Government should seek legislative change where necessary to enable greater data sharing to prevent fraud.
- There are now barely 400 fraud squad officers in England and Wales investigating fraud and even these resources are under threat. The Review has made a number of recommendations to achieve better value for money from existing police resources and has also suggested areas for more civilian involvement.
- The Review also recommends that a National Lead Force should be established to act as a centre of excellence for other Fraud Squads and assist with or direct the most complex fraud investigations.
- The Review has considered specific measures to improve the effectiveness of fraud trials and has put forward a number of recommendations to ensure speedier and more cost effective justice for victims. Proposals include the establishment of a financial court; wider sentencing powers for the Crown court to provide for more

compensatory, regulatory and preventive orders; the introduction of plea-bargaining and the publication of sentencing guidelines for all fraud offences.

**D.3** The full Report can be found on the Legal Secretariat to the Law Officers website at: [http://www.lso.gov.uk/fraud\\_review.htm](http://www.lso.gov.uk/fraud_review.htm)

## **NEW POWERS AGAINST ORGANISED AND FINANCIAL CRIME**

---

**D.4** Organised crime causes social and economic costs of upwards of £20bn to the UK each year. In March 2004, the White Paper 'One Step Ahead: A 21st Century Strategy to Defeat Organised Crime - Cm 6167' set out plans for bringing a new approach to tackling organised crime. As a result, the intelligence-led Serious Organised Crime Agency (SOCA) came into being in April 2006. However, the 2004 White Paper noted that there was a significant gap in criminal law for catching those involved in organised crime.

**D.5** The report presented proposals which could be imposed on individuals or organisations in such a way as to prevent organised criminality continuing. The proposals encompass:

- Preventing identity fraud and money laundering
- Streamlining investigations and prosecutions
- The introduction of measures such as organised crime prevention orders
- Dealing with the proceeds of crime, including asset recovery

**D.6** The full report can be found at:  
[www.official-documents.co.uk/document/cm68/6875/6875.asp](http://www.official-documents.co.uk/document/cm68/6875/6875.asp)

## **THE SERIOUS ORGANISED CRIME AGENCY (SOCA)**

---

**D.7** The Serious Organised Crime Agency (SOCA) is a new law enforcement agency created to reduce the harm caused to people and communities in the UK by serious organised crime. It assumed its functions on 1 April 2006.

**D.8** SOCA is an Executive Non-Departmental Public Body sponsored by, but operationally independent from, the Home Office. The Agency takes over the functions of the National Crime Squad (NCS), National Criminal Intelligence Service (NCIS), that part of HM Revenue and Customs (HMRC) dealing with drug trafficking and associated criminal finance and a part of UK immigration dealing with organised immigration crime (UKIS).

**D.9** The SOCA Board has determined 5 generic priorities to guide SOCA's business as follows:

- To build knowledge and understanding of serious organised crime, the harm it causes, and the effectiveness of different responses.
- To increase the amount of criminal assets recovered and increase the proportion of cases in which the proceeds of crime are pursued.
- To increase the risk to serious organised criminals operating in the UK through proven investigation capabilities and in new ways.

- To collaborate with partners in the UK and internationally to maximise efforts to reduce harm.
- To provide agreed levels of high quality support to SOCA's operational partners and, as appropriate, seek their support in return.

**D.10** More information can be found on SOCA's website: <http://www.soca.gov.uk>

## IDENTITY MANAGEMENT

**D.11** On 11 July 2006, the Chancellor of the Exchequer appointed Sir James Crosby to chair the Public Private Forum on Identity Management. The Forum will examine the evolving technologies used for identity management and consider how the public and private sectors can work together to maximise efficiency and effectiveness. The Forum will be a key part of the identity management architecture across Government and will build on the work underway across Whitehall.

**D.12** The Forum's terms of reference are to:

- Review the current and emerging use of identity management in the private and public sectors and identify best practice.
- Consider how private and public sectors can work together, harnessing the best identity technology to maximise efficiency and effectiveness.
- Produce a preliminary report for the Chancellor of the Exchequer and the Ministerial Committee on Identity Management by Easter 2007.

## PAC AND NAO REPORTS

**D.13** The following PAC and NAO reports which were published in the period covered by this Report (i.e. 1 April 2005 to 31 March 2006) relate to or contain information about fraud:

- Financial Management of the European Union (HC 498 – 4 April 2005);
- Inland Revenue: Tax Credits and Deleted Tax Cases (HC412 – 8 September 2005);
- Fraud and Error in Benefit Expenditure (HC411 – 11 October 2005);
- HM Customs and Excise Standard Report 2003-04 (HC695 – 6 December 2005);
- Financial Management in the European Union (HC999, 29 March 2006, ISBN: 0102937419).

**D.14** The reports are available on the following websites:

- <http://www.publications.parliament.uk/pa/cm/cmpubacc.htm>
- <http://www.nao.org.uk/publications/index.htm>

## USEFUL WEBSITES

---

**D.15** The following websites offer advice about reducing the risk of fraud in a number of areas including identity fraud:

- <http://www.hm-treasury.gov.uk/fraud> - contains anti-fraud advice produced by the Treasury.
- <http://hefce.ac.uk/finance/assurance/fraud/> - contains a number of interesting fraud case studies in the education sector.
- <http://www.ipf.co.uk/governance/counterfraud/> - CIPFA's counter fraud website.
- <http://www.iaa.org.uk/knowledgecentre/keyissues/fraud.cfm> - Institute of Internal Auditors UK and Ireland.
- <http://fraudadvisorypanel.org> - the Fraud Advisory Panel.
- <http://www.cfsms.nhs.uk/> - NHS Counter Fraud Security and Management Services.
- <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/fraud/> - provides links to a number of useful websites offering anti-fraud advice.
- <http://www.soca.gov.uk> - Serious Organised Crime Agency
- <http://www.cifas.org.uk> - the UK Consumer Credit Industry's Fraud Prevention Service.
- <http://www.met.police.uk/fraudalert> - fraud advice from the Met Police.
- <http://www.banksafeonline.org.uk> - advice about reducing the risk of conducting business transactions online.

## CFSMS FORENSIC COMPUTING SERVICES

---

**D.16** The NHS CFSMS's Forensic Computing Unit (FCU) provides a comprehensive and professional service to recover digital evidence for use in criminal, civil and disciplinary proceedings. It also provides a data recovery service for lost documents, password-cracking capability and an auditing service to help ensure compliance with corporate policies.

**D.17** The FCU has achieved BS7799, the British Standard governing information security and management, showing that the processes and procedures operated in all departments are designed and implemented professionally. The FCU has qualified and experienced forensic computing staff from a range of backgrounds including fraud investigation, statistical analysis and criminal investigation. All Accredited Counter Fraud Specialists, they receive extensive ongoing training on the latest forensic computing tools. They ideally placed to investigate fraud and any inappropriate computer use. They will also ensure that any evidence they uncover is suitable for use in a court of law.

**D.18** The FCU can carry out audits of computer use and undertake covert computer acquisitions and analysis. With the ability to recover data on-site or even across a network while a computer is in use, staff can perform a full investigation while allowing an organisation to maintain business continuity. The unit operates to the highest

forensic standards and adheres to the guidelines set out in the Good Practice Guide for Computer based Electronic Evidence issued by the National High-Tech Crime Unit (NHTCU) and agreed by the Association of Chief Police Officers (ACPO). Importantly, by adhering to ACPO guidelines, the FCU safeguards the integrity of the evidence for court proceedings.

**D.19** For more information about the work of the FCU and how it can be applied to both NHS and non-NHS organisations, please contact the FCU on 020 7895 4999 or email [forensics@cfsms.nhs.uk](mailto:forensics@cfsms.nhs.uk) or look on their website [www.cfsms.nhs.uk](http://www.cfsms.nhs.uk) and follow the link to the FCU.

## FRAUD BILL

---

**D.20** The Fraud Act is currently working its way through Parliament having had a second reading in the House of Commons on 12 June 2006. The Act creates a new offence of fraud that can be committed in three ways:

- By false representation;
- By failing to disclose information; or
- By abuse of position.

**D.21** The Bill creates two other offences:

- Obtaining services dishonestly; and
- Possessing articles for use in fraud (e.g. machines for copying personal data from credit cards).

**D.22** The new Act should make it easier for organisations to prosecute fraud cases and relies on the proof of dishonest intent on the part of the defendant. Those convicted face a maximum penalty of 10 years imprisonment. Organisations can receive unlimited fines.



# E

## ANTI-FRAUD INITIATIVES

### DEPARTMENT FOR WORK AND PENSIONS

#### Background

**E.1** In 2001, machinery of Government changes resulted in the merger of the former Department of Social Security and the Employment Service (an executive agency of the then Department of Employment and Skills), into a new Department for Work and Pensions (DWP). This change also enabled the creation of two new large agencies, Jobcentre Plus and The Pension Service, and more recently the Disability and Carers Service. The creation of the new Department resulted in an organisation of 125,000 staff, with responsibility for the administration of over £100bn annual expenditure of social security benefits, and the arrangements for assisting job seekers to find work.

**E.2** These changes provided a catalyst to review, and subsequently inspire a change in the way in which the DWP responded to the threats posed by internal employee fraud and related abuse.

**E.3** Up until 2003, the arrangements for dealing with this threat were largely left to local arrangements organised on a regional basis within the respective Departments. Small groups of locally managed staff investigated individual incidents or suspicions which had been raised. Apart from centralised reporting, so as to fulfil HM Treasury requirements, there was no significant or co-ordinated response at a corporate level, and because of inevitable local variations, a lack of consistency, and much fragmentation of activity.

**E.4** Apart from the obvious attendant major financial risks, the DWP is also one of Europe's largest data controllers, responsible for the processing and safeguarding of personal information for virtually the entire UK population. The risk of data theft or misuse by staff is especially significant.

#### New arrangements

**E.5** In 2003, a new organisation was formed under a single senior manager (a Head of Investigations) reporting to the Department's Director of Internal Assurance. All the former separately managed units were then brigaded together to form an independent organisation within the now 'Risk Assurance Division', the primary focus of the unit being to investigate suspicions of internal fraud or related impropriety across the Department. Since 2003, the new unit has assumed direct responsibility for the following areas:

- Conducting 'Internal Investigations' across the main areas of the Department's business, in a co-ordinated manner, and reporting findings to management;
- Developing and providing internal fraud and related policies for the Department, linking these in with existing and related Discipline and other employee policies;
- Developing and supporting a locally-based internal security infrastructure (which in turn improved staff awareness, and encourages incident reporting), in conjunction with the Department's Head of Security;

- Providing routine quarterly reports to senior management across the Department, on a corporate and agency-specific basis. These new arrangements have been successful in shaping management awareness of internal fraud, and prompting management to take action to address specific risks;
- Developing a professional and specialist cadre of investigation staff equipped with the right blend of skills and methodologies to deal with staff fraud in a large public sector organisation in the 21st century;
- Setting up in the last year, a new intelligence-based approach which will look at a proactive way at particular risk areas. In addition this team has acted as a tactical group to deal with major incidents. For example since December 2005, this resource has been used to investigate the loss of staff data which was subsequently used for fraudulent tax credit claims;
- During 2005, the group formerly within Jobcentre Plus that investigated cases of contractor-fraud was also successfully integrated into the investigations organisation.

**E.6** The new Departmental approach has undoubtedly improved the quality and consistency of internal investigations which are conducted in the DWP, and has also laid the foundations for a more targeted use of resources through the development of intelligence led work, which in time is expected to help focus investigative resources on perceived risks, rather than simply reacting to specific incidents.

**E.7** Although the larger independent statutory bodies in the Department manage their own internal fraud risks (which are generally lower than in the wider Department), they separately have a good range of measures in place, such as Fraud Response strategies and plans, standards of behaviour policies, which are overseen by both internal audit and the relevant audit committees.

## HMRC

---

**E.8** In 2005/06 HMRC encountered a number of cases involving the postal interception of payable orders. This is where the payable order does not reach its destination and is encashed through either an account in the payee name, (whereby the bank account has been opened with other stolen post), or where there is an alteration on the name only. All cases are reported to the Police for action and if there are funds in the fraudulent bank account, this is recovered.

**E.9** To combat postal interception the following processes were introduced in 2006:

- Reporting monthly statistics to the Bank of England (our Clearing agent) on volumes, values and collecting bank. This information is then fed back to all Banks during the monthly meetings held by Bank of England and is particularly useful for the banks to identify repeated problems in geographical areas or perhaps errors in account opening processes.
- Reporting monthly statistics to Royal Mail on volumes, values and post code where the item was encashed. (Both ex- IR and ex-C&E payable orders). This information is collated by Royal Mail with data from other large cheques issuers e.g. Dept. of Work and Pensions to identify 'post code' hotspots. Again it is used by Royal Mail to target internal/external problems.

- Where a particular problem is identified with one collecting bank sort code, a manual search of the cleared items is initiated each day, targeting that sort code. It is not possible to do this with all cleared items as the volumes, some 30,000 per day, and loss of funds currently experienced do not justify the staff resource needed to do this.
- Lastly, where possible positive action is taken to discourage the use of issuing paper payments by examining the Intranet for new projects that may impact on the team. One example is the Modernisation of PAYE Processes for Customers (MPPC) program. The original proposal to hold taxpayer bank details was side lined on a cost basis. HMRC has ensured that the Program is fully aware of the costs involved in processing payable orders to enable them to make an accurate cost benefit analysis. A sort of 'spend to save' proposal!

## HOME OFFICE

**E.10** The main initiatives over the past three years have included:

- Developing and implementing a fraud strategy for the Home Office in 2003.
- Establishing a dedicated team (of three staff) to:
  - Provide and maintain a central point of contact where staff can confidentially report potential fraud;
  - Ensure that potential frauds reported are followed up and investigated as appropriate;
  - Provide fraud awareness training;
  - Undertake limited proactive investigation of areas exposed to risk of fraud;
  - Keep under review the department's fraud strategy and response plan.
- In the past year, the focus has also been on developing appropriate whistleblowing policies, developing an intranet site, undertaking targeted publicity campaigns to raise awareness amongst staff and management, facilitating self assessments of exposure to risks of fraud and impropriety by all teams within the Home Office (via a detailed briefing on potential areas of risk and anti-fraud measures), regular articles in the in-house magazine (e.g. a Team of the Month feature on the work of the anti-fraud and Investigation team), and publicising the draft and final versions of the new Civil Service Code.
- Home Office has also been assisting NAO in their review of governance at the Department. NAO's report includes recommendations to enhance activity in the areas covered in bullet points 5 and 6 above. These are under consideration.

## DEPARTMENT OF TRANSPORT

### Main Department

**E.11** New fraud guidance placed on Intranet covering policy statement and procedures for reporting suspicions of fraud (whistleblowing). Updated fraud response plan sent to line managers.

### Vehicle and Operator Services Agency

**E.12** Fraud Policy statement and response plan developed and published. Whistleblowing guidance developed and published. Fraud Risk stewardship passed to Director Testing & Inspection. Developing with DVO partners an approach to Identity Fraud. Standard approach to investigating the Internet for sites that promulgate forged documents. Have an agreed process with the High Tech Crime Unit to shut such sites down and use the police to monitor activity for potential follow up.

### Driver and Vehicle Licensing Agency (DVLA)

**E.13** The DVLA fraud policy has been re-written and re-launched. A fraud response plan has been written with the specific aim of ensuring that internal frauds are dealt with in the same consistent manner throughout the Agency. The establishment of fraud case panels in each case goes some way to ensuring this. The establishment of a DVLA Fraud Forum, with some independence inasmuch that the chair is a non-executive director, oversees fraud policies and responses to fraud in the Agency. All cases of fraud are discussed within the Forum and it ensures that lessons learned and best practice is shared throughout the various groups within the Agency. The Fraud Forum reports through the Head of Risk to the Audit Committee.

### Driving Standards Agency (DSA)

**E.14** Wherever new systems have been introduced DSA looks for the opportunity to reduce fraud from the implementation of those systems. An example of this will be the interface between the Shared Services Time and Attendance module with the business delivery system (DTCS) which includes examiners' time and attendance details.

**E.15** However there are some areas with an increased risk of loss, for example the rollout of PCs to test centres, which has increased the risk of theft of PCs.

**E.16** In addition to the internal and external frauds reported, in the last few years DSA has been dealing increasingly with impersonation, involving fraudulently obtaining driving licences. DSA has invested in an Integrity Team with a view to investigating and prosecuting individuals and recovering licences. The budget for this team was £800,535 in 2005/06. The table below details the number of projects and prosecutions made over the last 3 years:

YEAR	OPERATIONS	ARRESTS	CHARGED	CAUTION	NO ACTION	BAIL	CONVICTED
04	158	111	7	35	12	14	42
05	303	66	12	19	6	23	6
06	136	6	0	0	1	2	0

NB. The figures for 2006 are not yet complete.

**E.17** Investigations can often identify no MOT, no VED, no insurance, illegal immigration, etc, and DSA work increasingly with the police, HRMC and DWP to bring criminal prosecutions.

ISBN 1-84532-208-8



9 781845 322083 >