Finance and Resources Committee Meeting –23 June 2009

FRAUD REPORT 2007-08 – REPORTED FRAUD IN GOVERNMENT DEPARTMENTS

Executive summary and recommendations

Introduction
This is an online publication by H.M. Treasury, dated October 2008 and summarises significant reported fraud occurring in Government departments during the period 2007-08.

Decision
The Committee is asked to note the report.

Background information
The report is provided to the Committee as a background document, highlighting the types, frequency and magnitude of fraud as reported in Government departments during the year ending 31 March 2008. It is also being provided to the June Audit Committee as a paper to note.

In summary, twenty five central Government bodies reported 761 cases of internal fraud or theft, with a total value of £4.28M. This included 308 cases relating to theft of assets and 105 cases of personnel management-related fraud.

Although the number of reported cases dropped by 29% from the prior year, the total value of losses increased from £3.86M to £4.28M.

Payment fraud accounted for 85 cases and £2.95M of the reported fraud value. Such fraud involves falsely creating or diverting payments – see Appendix One, s1.6 for more details. One case involved payment fraud of £1M, involving a member of staff working with external parties.

At the HPC a variety of risk mitigations are in place to minimise the risk of internal fraud and there are annual audits of financial systems and processes. The audit findings for the annual Financial Systems and Processes audit is typically rated satisfactory by PKF, HPC's internal auditors and presented to the Audit Committee. Furthermore, the HPC Risk Register, including sections relating to Fraud risk is updated and reviewed twice yearly by the Audit Committee. Examples include;
Risk 4.11 Expense claim abuse by members
Risk 5.3 IT fraud or error

Risk 10.3 Inability to detect fraudulent applications
Risk 11.8 Employer/employee inappropriate behaviour
Risk 15.7 Registrant credit card record fraud/theft
Risk 15.10 Unauthorised payments to organisations
Risk 15.11 Unauthorised payments to personnel
Risk 15.12 Unauthorised removal of assets
Risk 15.13 Mis-signing of cheques (forgery)
Risk 17.1 Electronic record data security
Risk 17.2 Paper record data security,
Risk 17.3 Data held by third parties,
Risk 17.4 Data received from third parties

Resource implications
Nil

Financial implications
Nil

Appendices
Appendix One – Fraud Report 2007-08, by H.M.Treasury, Crown copyright.

Date of paper
11 June 2009

Fraud Report 2007-08:

an analysis of reported fraud in government departments

October 2008

HM TREASURY

HM TREASURY

Fraud Report 2007-08:

an analysis of reported fraud in government departments

October 2008

HM Treasury contacts

This document can be found in full on our website at:

hm-treasury.gov.uk

If you require this information in another language, format orhave 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

Printed on 100% recycled paper.
When you have finished with it please recycle it again.

ISBN 978-1-84532-501-5
PU663

Contents

Contents

Executive summary

25 departments reported 761 cases of internal fraud or theft with losses totalling some £4,278,000.The main observations are:

- There has been a decrease in the number of cases reported — from 1,067 cases last year to 761 this year. The main decreases occurred in the categories theft of assets (403 cases to 308) and personnel management related fraud (from 253 cases to 105);
- The biggest categories in terms of case numbers reported were theft of assets (308 cases) and personnel management related fraud (105 cases). 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 (over £2.9 million) and theft of assets (over £440k). The payment fraud category included one case with a loss of £1million and 6 further cases, each exceeding £100k, accounted for losses of over £1.6million;
- The number of cases involving GPC/credit card fraud misuse increased slightly with a significant rise in their overall value (from £27,800 to £123,700) due mainly to one case where misuse of a GPC card by a senior manager resulted in losses of nearly £78,000 over a 4 year period; and
- Eleven cases, each exceeding £100,000 in value, accounted for losses totalling £3,209,000 representing 75 per cent of the overall value of losses.

Control issues identified 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;
- Inadequate monitoring of GPC/Credit card usage; and
- Goods not always stored securely.

1 Main analyses

This section contains the main analyses of data relating to fraud and theft by staff reported by departments for the year 2007-08.

Introduction

1.1 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 2007-2008. 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.

1.2 The Report analyses data submitted 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 where losses of £20,000 or more were reported and containing generic lessons for others (see Annexes B and C). Annex D provides some useful information about fraud issues which might have an impact on anti-fraud activities in central government.

1.3 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

1.4 The analysis in this section is based on fraud data supplied by 47 central Government bodies, including all the main departments, covering the period 1 April 2007 to 31 March 2008. Overall the analysis shows:

- 22 bodies provided 'nil' returns (i.e. had no cases of theft or fraud to report);
- The remaining 25 bodies reported 761 cases of internal fraud or theft with a total value of £4,278,000;
- Overall there was a 29 per cent decrease (from 1067 to 761) in the number of cases reported. The largest decreases occurred in the categories theft of assets (from 403 last year to 308) and personnel management related fraud (from 253 last year to 105). The value of losses increased from £3,858,600 to £4,278,000;

- There were 18 large value cases (£20,000 or more) accounting for a total loss of £3,471,500 (81 per cent of total losses reported). Eleven of these cases each exceeded £100,000 in value with losses totalling £3,209,000 (75 per cent) and included 1 case with losses of around £1million; and
- The number of cases involving GPC/credit card fraud misuse increased from 36 cases last year to 42 this year. The overall value of losses also increased from £27,800 to £123,700 including 1 case where credit card misuse resulted in losses of nearly £78,000.

Fraud data

Table 1.A: Fraud Data Analysis

Fraud Category	No. of Cases		Value	
	Number	per cent	£	per cent
Payment fraud	85	11.17	2,948.300	68.92
Theft of assets	308	40.47	442,900	10.35
Procurement fraud	28	3.68	323,200	7.55
GPC/credit card fraud	42	5.52	123,700	2.89
Travel, subsistence and allowances paid via payroll	44	5.58	186,200	4.35
Pay or allowances paid via the payroll	44	5.78	191,300	4.47
Personnel management related fraud	105	13.80	18,100	0.42
Exploiting assets and information	50	6.57	23,200	0.54
Receipt fraud	28	3.68	15,200	0.36
Other	27	3.55	5,900	0.14
Total	761		4,278,000	

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

Payment fraud

1.6 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; and
- A member of staff authorising payments to himself.

1.7 This is the largest category in terms of value lost (£2,948,300 or 69 per cent) from 85 cases. Individual losses were sometimes significant with 7 cases, each exceeding £100,000 in value, accounting for losses totalling £2,678,000 (91 per cent of total losses in this category).

1.8 Many of the large value frauds arose because 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 pose a significant risk. It is not just payments to suppliers that are at risk. Central Government staff may be in a position to affect grant and benefit payments as well as collecting and administering taxes.

1.9 Segregation of duties, adequate 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 but 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 this risk. 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 on controlling cash handling, bill paying, electronic funds transfer and payment by cheque or Payable Order.

Theft of assets

1.10 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.

1.11 In total, departments reported 308 cases (40 per cent) of thefts with a total value of £442,900 (10 per cent). This year saw a reduction of 95 cases over last year's total of 403 and included PCs, laptops and palmtops which carried the additional risk of data loss.

1.12 This was the highest category in terms of number of cases reported and second highest in terms of value. Included were two large value cases with losses totalling £146,000 or 28 per cent of losses in this category. The highest value case (£116,000) involved the theft of bridge components which, because of their bulk, were stored in a non-secure area. One stolen mobile phone was used to make £12,000 worth of international phone calls.

1.13 It is important to focus on the basic physical controls that should prevent and detect these kinds of offences. These fundamental controls include 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. 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 (e.g. blocking phones to prevent their further use, closely checking bills and investigating high usage, placing credit limits on phones).

Procurement, fraud and GPC/credit card fraud

1.14 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 or irregular use of the Government Procurement Card (GPC) and payment claims for goods or services that were not delivered.

1.15 These two categories accounted for 70 (9 per cent) cases of fraud with a total value of £446,900 (10 per cent). This year's figures included 42 GPC/credit card frauds with losses totalling £123,700 (£27,800 last year). Two large-value cases (£20,000 or more) were reported

with losses of £182,000 (procurement) and £77,800 (misuse of Government Procurement Card) respectively.

1.16 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". Where credit cards are concerned, it is important that credit card statements are reconciled by budget holders (or on their behalf by somebody other than the cardholder) to receipts or vouchers supplied by the cardholder and that any unusual expenditure is properly investigated.

Travel and subsistence, pay and other allowances

1.17 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

1.18 In total there were 88 (44 travel & subsistence, 44 payroll frauds) with losses totalling £377,500 (9 per cent). There was a small decrease in the value of fraud and the number of cases reported in these categories over last year's total value of £407,300 and 122 cases. Two cases exceeded £100,000 in value accounting for total losses of £233,000. One case with losses totalling £113,000 involved new staff being paid allowances they were not entitled to claim, the other (£120,000 loss) involved false documentation to support false claims over a 3 year period.

1.19 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, 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

1.20 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); and
- Deceit or misrepresentation for advantage (e.g. false references or false qualifications used to secure employment).

1.21 The second highest number of cases (105, 14 per cent) was reported under this category but most involved little or no financial loss to the departments concerned. In most cases action had been taken against perpetrators that included dismissals, demotions, and loss of spine points and/or bars on promotion.

1.22 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 flexible working hours records and

independent monitoring of staff accesses to official data are all examples of controls designed to detect these types of frauds.

Exploiting assets and information

1.23 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).

1.24 This year departments reported 50 cases (7 per cent) in this category with losses totalling £23,200. This is potentially a high risk area and fraud could involve government employees providing details of departmental records to external accomplices. There were no high-value cases (£20,000 or more) reported this year.

1.25 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 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 also be effective.

Receipt fraud

1.26 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.

1.27 The overall value of fraud in this category was £15,200 involving 28 cases. This is a big decrease over last year's figures of 74 cases with losses totalling £281,000. There were no large value cases (£20,000 or more) reported.

1.28 The scale of income collected by the Government is vast and individual frauds can potentially be very significant. There is a need for fraud-risk assessment and effective anti-fraud measures (e.g. accurate debtor records, regular management and independent checks to ensure that income is collected and brought to account, supervision of officers with responsibility for pursuing large value debts). 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.

Other fraud

1.29 This category accounted for 27 cases (4 per cent of the total) and a total value of £5,900.

External and contractor frauds

1.30 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 above.

1.31 In all, 11 external fraud cases were reported with losses totalling nearly £1.6million. Summaries of individual cases can be found in Annex C. This annex does not represent 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 for this exercise because they contain lessons for those departments only, and may be covered in other reports and publications.

1.32 Seven contractor cases were reported with losses totalling nearly £1.4million. All of these were contractors engaged to deliver services on behalf of departments to the public and in most cases losses had been, or were likely to be, recovered. In some cases the frauds arose because of weak controls such as insufficient checking of evidence to support claims for payment by the contractors. One external case involved the misuse of a corporate procurement card resulting in losses of £70,000.

1.33 Advice on managing external fraud risk effectively can be found in the joint Treasury and NAO publication "Good Practice in Tackling External Fraud"[1].

[1] http://www.hm-treasury.gov.uk/media/E/2/tackling_external_fraud.pdf

A 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

£1,000,000

Enquiries to locate misallocated payments led to the discovery of a fraud involving a member of staff working in collusion with external parties. The member of staff was suspended and a full criminal investigation is being carried out with a view to prosecuting all parties to the fraud. An immediate internal audit review resulted in the strengthening of internal procedures.

£516,000

The fraud involved a member of staff using a variety of methods to divert payments for the benefit of others (e.g. creating false repayments). The fraud was identified as a result of internal control procedures. The staff member was suspended from work and legal proceedings were being taken at the time of reporting. Additional security and monitoring controls were introduced to prevent any future recurrence.

£400,000

An investigation revealed that a staff member used information about claimants to create false payments. Internal control procedures identified an unusual pattern of activity by the member of staff who processed payment claims. The officer was suspended during the investigation which was ongoing at the time of reporting. Internal audit continues to run monthly checks to identify evidence of similar fraudulent activity.

£390,000

Three members of staff colluded with external accomplices to perpetrate frauds against a department's payments system. The fraud involved the staff supplying information about some of the department's customers to the external parties who used the information to make false claims. One officer has been dismissed, prosecuted and sentenced. The remaining two are currently suspended from duty and further action may be taken when the investigation is completed. Internal control procedures led to the discovery of the fraud. Additional security and monitoring controls have been introduced to prevent any future recurrence.

£153,000

A fraud was under investigation where three false invoices were submitted to a department and paid. Internal involvement was suspected but those involved were not identified. The fraud came to light when one of the perpetrators contacted the department to query non-payment of one of the invoices. This payment (£90,000) was stopped by the department. The police are investigating the fraud and payment controls have been strengthened.

£112,000

An allegation that a member of staff was receiving benefit for himself and his family which he was not entitled to receive was investigated and resulted in the dismissal and prosecution of the staff member. Action is also being taken to recover the losses. Data matching has been introduced to detect similar fraud in future.

£107,000

An officer used his position and detailed knowledge of his department's payment and procurement system in order to create and process false invoices over a period of 18 months. The case also involved false accounting. The officer was arrested by the police and the case is due to go to court.

£63,900

An anonymous complaint of unauthorised access into customer records led to an investigation which discovered that customer payments were being diverted to a staff member's bank account. The individual was dismissed, is being prosecuted and action planned for the recovery of losses. Details of the case were publicised within the Department to deter others from attempting similar frauds.

£20,600

As a result of a department's scans of high-value payments it was discovered that a member of staff had altered bank account details in order to divert a payment to their own and third party bank accounts. The individual was dismissed and is being prosecuted. Action to recover the loss is also being taken.

£20,500

A data matching exercise led to the discovery that a member of staff was claiming benefit to which he or she was not entitled. Disciplinary action was in progress at the time of reporting.

£20,500

A department's internal checking process identified a fraud involving the re-opening of dormant payment accounts and amending bank details so that payments were diverted to the perpetrator's own bank account. The individual was dismissed and prosecuted. Action to recover losses is also being taken.

Procurement and GPC/credit card fraud

£182,000

A management review of project activities identified anomalies in the procurement process and accounting records. An internal audit investigation confirmed that fraud had taken place involving:

- Widespread collusion resulting in the defrauding of money, goods and materials;
- Thefts of fuel; and

- Manipulation of accounting records.

The principal contributing factor that allowed the fraud to occur was lack of management oversight. A number of staff were dismissed, stronger controls put in place to prevent similar frauds occurring in future and action taken to recover losses.

£78,000

This case involved the misuse of a Government Procurement Card by a senior manager over a 4 year period. Irregularities were noticed by a staff member who reported them to management. The perpetrator was dismissed and the police are considering a criminal prosecution. An internal audit investigation into the weaknesses that allowed the fraud to be perpetrated resulted in a number of recommendations to improve control which were all implemented.

Theft of assets

£116,000

A department reported the suspected theft of bridge components by persons unknown. The size of the items prevented secure internal storage and they were left on hard standing in a non-secure area. A police investigation failed to identify the perpetrators or recover the goods. The case was closed.

£30,000

A department reported the suspected theft of two Land Rovers. A police investigation failed to identify the perpetrators or recover the goods.

No loss

This attempted fraud involved the theft of a blank HMPG payable order which was recorded as having been destroyed. The account to which it referred had been previously closed. The stolen payable order was subsequently presented for payment for £45,000 but was not honoured as the account had been closed and therefore no cash loss occurred. A police investigation failed to identify the perpetrator. New guidance was issued to prevent this happening again.

Pay or allowance paid via payroll

£113,000

An anonymous allegation led to the discovery that a number of staff appointed to fill several vacancies had claimed expenses they were not entitled to claim. The frauds arose because HR guidance had not been followed. Recommendations were made to prevent similar fraud from occurring in future and disciplinary action was taken against the managers who approved the claims.

£29,000

A part-time employee was set up on the payroll as a full-time employee in error and was paid as a full-time employee for several years. The employee failed to report the mistake which not was identified at the time the record was set up because local checking of new employee details was not carried out then. These checks were introduced later but were applied to new employees only. A functional manager's check of pay costs identified the overpayment. The staff member was dismissed and action taken to recover the overpayments.

Travel and subsistence

£120,000

Routine internal checks into staff with high mileage claims led to an investigation into an alleged fraud which appeared to involve the submission of false overtime, mileage, subsistence and travel claims over a 3 year period. The alleged fraud arose because the authorisation process did not function effectively (e.g. poor segregation of duties in the authorisation process, roles not clearly defined and a lack of challenge function). The fraud was under investigation at the time of reporting. New measures put in place to reduce the risk of similar frauds arising in future included: the appointment of a dedicated manager to oversee the processing of claims; a clarification of roles in the authorisation process; and the introduction of more sample checking of claims.

B Large value frauds - external cases

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

£297,600

This case concerns suspected over-claiming of payments for services provided by a contractor over a period of up to 6 years. The suspected fraud was discovered when a newly appointed Senior Quantity Surveyor carried out a sample check of invoices against contract terms. The investigation identified poor control over the checking of invoices and payment authorisation. At the time of reporting the case was under investigation. A project was launched to review the internal control arrangements over contractor payments. In the interim more rigorous control over the processing of invoices was introduced (e.g. invoices are checked against contract details and contractor activity verified).

£367,500

Following an allegation from an ex-employee of an organisation contracted to provide certain services on behalf of a department, it was discovered that contractor staff regularly submitted invoices for payment that were supported by false paperwork (e.g. timesheets). Weak controls (e.g. lack of segregation of duties, inadequate checking of timesheets) within the contractor's system allowed the frauds to arise. The contractor has dismissed the staff involved and agreed to repay all losses to the department. A joint internal audit review by the department's and contractor auditors resulted in stronger controls being implemented.

£328,700

A contractor employed to deliver services on behalf of a department submitted false paperwork to support payment claims. The fraud was discovered as a result of a complaint by a customer and arose because of weak controls within the contractor's checking processes. The department carried out a review of contractor processes and made a number of recommendations about improving the level of control. Negotiations were underway regarding repayment at the time of reporting.

£130,400

Following checks carried out by a department into claims by a contractor for payment, it was discovered a number of overpayments had been made. The contractor agreed to repay most of the losses and to improve control over payment processing.

£93,000

Following an inspection of a contractor's activities by a department, it was discovered that the contractor failed to maintain adequate records of services provided to support payment claims. This resulted in a number inflated claims which the department paid. The contractor agreed to repay all losses.

£42,000

A member of staff queried an authorising signature on a payment claim form which led to an investigation by a department into the activities of a contractor employed to deliver a service to the public on behalf of the department. The investigation identified a number of false records submitted by contractor staff to support their claims for payment. The contractor disciplined the staff involved, repaid the losses to the department and agreed to implement closer monitoring.

£22,800

Complaints by participants on training courses organised by a contractor on behalf of a department led to the discovery that some contractor staff had submitted false paperwork to support their claims for payment. The individuals responsible were dismissed by the contractor who agreed to implement better checking of staff claims for payment.

Other external fraud

£70,000

An internal review of financial procedures identified misuse of a corporate procurement card by a senior manager. The fraud involved the following elements:

- Misleading descriptions of the items purchased;
- Missing, fake or altered receipts; and
- Purchase of items for personal use.

The fraud arose because the budget holder failed to carry out any checks of the manager's procurement activities. The perpetrator was dismissed, prosecuted, was jailed for 14 months and ordered to repay the value of the goods obtained. The budget holder was also disciplined (final written warning) and details of the case were sent to all staff by e-mail.

£59,300

A department's internal checks led to the discovery that a customer had received payments over several years which he was not entitled to receive. The customer was prosecuted, pleaded guilty and received a 10 month prison sentence suspended for 2 years. An application has been made by the department for a confiscation order to recover the losses in full.

£48,500

Allegations made by a whistleblower that a customer was receiving payment of benefits to which they were no longer entitled resulted in an investigation by the department which led to the prosecution of the customer and action to recover the losses. At the time of reporting the department had plans to carry out an audit of controls to see whether additional measures were required.

£25,000

An investigation by the police into possible fraudulent claims for compensation by members of the public for damage caused to property and livestock through the activities of departmental staff resulted in the prosecution of individuals who pleaded guilty to obtaining money by deception and were ordered to complete 180 hours community service.

C Fraud update

This section covers fraud-related issues including an update on progress towards implementing the recommendations of the Government Fraud Review; extending the National Fraud Initiative; some novel or interesting frauds; and fraud-related PAC or NAO Reports.

Government fraud review update

National fraud strategic authority

C.1 The National Fraud Strategic Authority (NFSA) will be launched on 1 October. An Executive Agency of the Attorney General's Office, the NFSA aims to reduce the harm caused by fraud to the UK by building a more hostile environment for fraudsters at home and abroad.

C.2 National Fraud Strategic Authority's key priorities will include the delivery of:

- A victim-focused criminal justice system that brings fraudsters to swifter justice, efficiently and effectively;
- Stronger deterrence by tough, multi-agency law enforcement; and
- Greater public confidence and capability through close working with private and voluntary sector stakeholders.

C.3 The National Fraud Strategic Authority has identified five key priority areas:

- Tackling the key threats of fraud that pose greatest harm to the UK;
- Acting effectively to pursue fraudsters, hold them to account, and improve the support available to victims;
- Reducing the UK's exposure to fraud by building the nation's capability to prevent it;
- Targeting action against fraud more effectively by building, sharing and acting on knowledge; and
- Securing the international collaboration necessary to protect the UK from fraud.

C.4 The NFSA has been working with partners from across the anti fraud community, ranging from banks, building societies, insurance companies, trade association bodies, regulatory authorities, Ministry of Justice, Serious Fraud Office, Department of Work and Pensions, HM Treasury, Home Office and Business Enterprise Regulatory Reform departments to identify the areas of most concern that need to be addressed as a priority and how to tackle them. The outcome of this work will be the National Fraud Strategy, to be published at the end of the year.

Measurement Unit

C.5 With the true scale of fraud currently largely unknown, the NFSA is setting up a measurement & analysis function which will combine the use of existing fraud measurement data and extend measurement activity into sectors where it is not being currently undertaken. It is anticipated that this will uncover a far greater loss to the economy than is currently estimated.

National Fraud Reporting Centre

C.6 Managed by the City Of London Police, the National Fraud Reporting Centre (NFRC) will address the underreporting of fraud and the lack of consolidation in managing intelligence. Through a call centre, or via the Internet, it is planned that both individuals and businesses will be able to report fraudulent activity.

National Fraud Intelligence Bureau (NFIB)

C.7 The National Fraud Intelligence Bureau (NFIB) will receive fraud intelligence from partner agencies, combining this information, much of which is likely to be previously unconnected fraud intelligence, with that already collated by the NFRC. It is envisaged that this will provide new information about emerging fraud risks to the National Fraud Strategic Authority and to business and law enforcement agencies to inform their activities and contribute to the fight against fraud.

Policing

C.8 Government funding has been secured to develop and operate a National Fraud Reporting Centre and a new National Fraud Lead Police Force. The City of London Police have been given responsibility for developing and delivering these, building on their role and expertise in policing economic crime in the South East of England.

C.9 The City of London Police National Fraud Lead Force will provide:

- Specialist training for public/private sector investigators;
- Best practice;
- Prevention advice;
- Advice on complex enquiries in other regions; and
- Assistance with, or direction on, complex investigations.

National fraud initiative extended to central government and private sector

C.10 In 2007 the Audit Commission gained new data-matching powers that extends to central government and the private sector the National Fraud Initiative (NFI) – the country's largest public sector fraud detection programme.

Increasing fraud detection

C.11 The NFI detected a record £140 million of potential fraud against the public sector in 2006-07 – a 26 per cent increase on 2004-05. This rise does not necessarily indicate increasing fraud levels, but may be a result of greater success in detection. A total of around £450 million of fraud has been detected since 1996.

C.12 The NFI is a data-matching technique that identifies potential fraud and overpayments in the public sector. It matches information such as housing benefit claims, payrolls and social housing records from local councils, police authorities, local probation boards and fire and rescue authorities across England, Scotland and Wales. Northern Ireland will also be participating in the next cycle (2008-09).

C.13 The process enables public bodies to share and compare information through a secure, encrypted website, and identify those taking services or money they aren't entitled to. Examples include council tenants with a council property in two different authorities, fraudulent claims for housing benefit and pensions being claimed for deceased people.

C.14 Successes include:

- sixty-nine council properties recovered by detecting tenancy fraud;
- overpayments revealed in 46 per cent of student loans and 31 per cent of occupational pensions, by passing matches directly to Jobcentre Plus and The Pension Service;
- a new data match to detect council tax single person discount fraud, that could increase the tax base of local authorities by as much as £200 million; and
- detection of payments of more than £650,000 for the care of deceased residents, following matches of care home payments to the records of the Department of Work and Pensions.

C.15 Data security has been strengthened and a series of software enhancements have been made. A new web-based application allows data matches to be hosted on a secure website, offering full fraud case management facilities for investigators.

C.16 The Serious Crime Act 2007 amends the Audit Commission Act 1998 to include new powers enabling the NFI formula to be extended to central government bodies and the private sector. A new Code of Data Matching Practice, drawn up by the Commission and laid before both Houses of Parliament and closely scrutinised by the Office of the Information Commissioner, will ensure that data protection will be given top priority alongside protecting the public purse.

C.17 For more information about the NFI or to arrange a workshop contact Peter Yetzes Head of NFI via nfiqueries@audit-commission.gov.uk or voicemail 0844 798 2222 (local rate call).

PAC and NAO reports

C.18 The following PAC Or NAO reports published in the period covered by this report (i.e. 1 Apr 2007 to 31 March 2008) contain information on fraud:

- HC401 (18 Apr 07): Financial Management in the European Union
- HC487 (9 May 07): Tax Credits
- HC227 (22 Jan 08): Evasion of Vehicle Excise Duty
- HC102 (23 Jan 08): DWP – Progress in Tackling Benefit Fraud
- HC300 (5 Feb 08):Tax Credits and PAYE
- HC250 (26 July 07): Standard Report on the Accounts of HMRC: VAT Missing Trader Fraud

Tackling external fraud

C.19 A new version of the NAO/HM treasury guide "Tackling External Fraud" was launched at the "Taking Forward the Fight Against Fraud" conference in London on 25 June 2008. The guide demonstrates and explains some of the good practices used by organisations in managing external fraud risk and includes a number of useful checklists to help them assess their anti-fraud practices. The guide can be found on Treasury's public website[1].

Novel or interesting fraud cases

C.20 A number of novel or interesting cases were reported to us this year which are summarised below:

- An organisation reported an on-going problem involving job advertising with various companies copying genuine job adverts from well known publications and then approaching the contact in the job advert seeking approval to republish in other publications. Such approaches are often of an extremely pushy nature (e.g. "we are about to go to press and I need confirmation faxed back right away") with the person approached believing that they are approving the design or placing of the original advert. If the person approached responds, this is usually followed up with an invoice and aggressive debt chasing tactics if payment is refused. There is no certainty that the adverts were placed elsewhere.
- An organisation placed an advert in a medical journal and the person who placed the advert received a telephone call from somebody claiming to work for the journal saying that the advert would be sent by fax and asking that it be proof read, signed and faxed back. When the advert was faxed through, it was noted that a price and a date were recorded above the space for the approving signature. A telephone call to the medical journal confirmed that the telephone call had not come from them. Fortunately no loss occurred, the fraud relying on a member of staff blindly accepting the person on the phone as genuine and signing the fax without question.
- An individual was dismissed from his job and an agreement was drawn up by HR setting out any benefits (e.g. payment of school fees) that the individual would continue to receive for a limited period. A Word version of the agreement was sent to the ex-employee who rewrote part of the agreement before printing it off and signing it. Fortunately the changes were noticed and the organisation suffered no loss. Procedures have been changed (e.g. send PDF versions of agreements that cannot be altered) to prevent any further attempts of this nature.

Identity Fraud

C.21 The latest estimate of the cost of identity fraud to the wider UK economy is £1.2bn (source: the Identity Fraud Steering Committee). There is a great deal of advice about reducing the risk of becoming a victim of identity fraud on a number of websites including:

- A website produced by several bodies including CIFAS, Home Office, APACS, HMRC, Met Police, FSA and the British Bankers Association. This can be found at: http://www.identity-theft.org.uk/ and offers the following simple advice:

  1 Keep you personal information secure;

[1] http://www.hm-treasury.gov.uk/media/E/2/tackling_external_fraud.pdf

2 Keep all your plastic cards safe;

3 Keep your documents safe; and

4 Keep you passwords and PINS safe.

- The CIFAS fraud protection service website at: http://www.cifas.org.uk/default.asp?edit_id=561-56
- The Metropolitan Police website at: http://www.met.police.uk/fraudalert/section/identity_fraud.htm

C.22 Government departments hold a great deal of personal data which could, if it fell into the wrong hands, be used to perpetrate identity fraud. A great deal of advice and guidance has been produced by the Cabinet Office to help government departments reduce the risk of losing personal data. The advice can be found on the CSIA website at: http://www.cabinetoffice.gov.uk/csia.aspx and includes the following publications:

- Data Handling Procedures in Government: Final Report; and
- The "Cross Government Actions: Mandatory Minimum Measures". This is a core set of measures to protect information which will be updated from time to time to accommodate lessons and new developments.

ISBN 978-1-84532-501-5