

**H M Treasury**  
Brian Glicksman  
Treasury Officer of Accounts



**Room 507  
Allington Towers  
19 Allington Street  
London SW1E 5EB**

**Enquiries about distribution of DAO  
letters to:  
Mangai Rajasingham  
Tel: 020 7270 5362  
Fax: 020 7270 4311  
Mangai.rajasingham@hm-  
treasury.gsi.gov.uk**

**DAO(GEN)15/02**

30 May 2002

Dear Accounting Officer

## **REPORTING DETAILS OF THEFTS AND FRAUD TO THE TREASURY – NEW ARRANGEMENTS**

**The purpose of this letter is to make departments aware of revised procedures for reporting details of fraud and thefts to the Treasury. We will be seeking fraud data in the new format for the 2002-2003 annual fraud reporting exercise when we call for returns in May 2003.**

2. Over the past twelve months we have undertaken a number of consultation exercises with departments seeking views on a revision of the annual fraud reporting process. In the light of the comments and views expressed we believe that these new arrangements will meet the needs of most government bodies that report fraud to the Treasury.
3. We would like to thank those who contributed to the proposed new arrangements especially the members of a working group who volunteered to take this work forward.

### **Main Changes**

4. Departments should have systems for recording and reporting fraud cases for their own management purposes and for pursuing vigorously anti-fraud policies. Not all of this information needs to be reported to the Treasury.
5. We therefore require Departments to report, on behalf of themselves and their Agencies, details of cases of theft and fraud at the stage when preliminary investigations have demonstrated that fraud or theft has occurred (or that an attempt has been made to commit theft or fraud). We have made this change to improve consistency of reporting and to improve the quality of information currently provided to us.



INVESTOR IN PEOPLE

6. The **purpose and objectives** of the Report have been re-defined to indicate the various customers and stakeholders involved in the process.
7. The **definition of fraud** has been clarified.
8. Changes have been made to the **reporting categories** as we felt that the existing breakdown did not reflect a modern business environment and did not allow us to highlight specific areas of fraud risk in the Report. Some of the categories have been broken down into sub-categories to allow us to highlight specific control breakdowns or weaknesses that contributed to the perpetration of frauds or thefts. This will allow managers to target particular areas of fraud risk for review in their own systems.
9. Departments should report details of some fraud or thefts perpetrated against NDPBs. The cases to be reported are those that exceed £10,000 in value **and** that contain valuable lessons for other government bodies. These cases may highlight new areas of fraud risk and we hope that the benefits of supplying this extra information will outweigh any additional burden that this might place on departments.

### **Next Steps**

10. This letter should be copied to those responsible for reporting details of thefts and fraud to the Treasury in your department. Further copies of the new arrangements, both hard copy and electronic, are available from Doreen Barker (tel: 0207 270 1684; e-mail: [doreen.barker@hm-treasury.gov.uk](mailto:doreen.barker@hm-treasury.gov.uk)) or Richard Fennelly (tel: 0207 270 1686; e-mail: [richard.fennelly@hm-treasury.gov.uk](mailto:richard.fennelly@hm-treasury.gov.uk)) in the Audit Policy and Advice team.

*Yours sincerely*

*Brian Glicksman*

**Brian Glicksman**  
**Treasury Officer of Accounts**

# The Annual Fraud Reporting Process

## Definition of Fraud

There is currently no precise legal definition of fraud. Many of the offences referred to as fraud are covered by the Theft Acts of 1968 and 1978. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

“Fraud” is usually used to describe depriving someone of something **by deceit**, which might either be straight theft or misuse of funds or other resources, or more complicated crimes like false accounting and the supply of false information. In legal terms, all of these activities are the same crime – theft.

For the purposes of reporting fraud to the Treasury the following crimes fall within the context of the Fraud Report:

### *Theft*

Dishonestly appropriating the property of another with the intention of permanently depriving them of it (Theft Act 1968). This may include the removal or misuse of funds, assets or cash.

### *False Accounting*

Dishonestly destroying defacing concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive (Theft Act 1968)

### *Bribery*

Any circumstances where an inducement or reward is offered or given which may influence the actions of others (Audit Commission)

### *Corruption*

The offering, giving, soliciting or acceptance of an inducement or reward which may influence the actions taken by the authority, its members or officers (Prevention of Corrupt Practices Act 1896 and 1916)

### *Deception*

An act of hiding the truth, especially to get an advantage – Theft Act 1968.

### *Collusion*

Secret agreement or cooperation especially for an illegal or deceitful purpose (source: Merriam-Webster’s Collegiate Dictionary).

## The Purpose of the Report

The Annual Report on theft and fraud forms part of a government wide deterrence culture. It exists to provide, within defined categories, summarised details, as defined below, of the reported extent, nature and value (estimated or actual) of fraud and theft within central government bodies. It also provides an assessment of trends in fraudulent activity and is an aid to departments in assessing the risks applying to their own procedures.

The objectives of the Report are to:

- contribute to a fraud deterrence culture by illustrating control weaknesses contributing to cases of actual or attempted fraud or theft as an aid to government bodies in assessing the risks in their internal procedures;
- promote a wider fraud deterrence culture by offering advice about combating fraud and theft generally;
- act as a warning to potential perpetrators that fraud is unacceptable and not tolerated within central government and that appropriate action will be taken in respect of all suspected cases;
- provide information on reported fraud and theft, analysed by the **reporting categories** detailed below, to Parliament, public bodies, and the wider public domain.

## Report Coverage

The Report will contain information on reported incidents of theft and fraud supplied by departments and their agencies. Departmental returns should include cases of theft or fraud perpetrated against their agencies.

The Report will also capture some cases of fraud from other organisations that departments are responsible for (e.g. NDPBs), cases that will help to raise fraud awareness in central government and help management strengthen their own anti-fraud strategies.

Departments should report, on behalf of themselves and their Agencies, details of thefts or fraud as in Annex 1 where preliminary investigations during the reporting period have demonstrated that a fraud or theft has occurred or been attempted. Updates on cases reported in previous reporting periods where the final outcomes were not known should also be provided (by completing a fraud return for each case and providing a narrative summary for cases with an estimated or actual value of £10,000 or more) - updated returns should be provided every year up to and including the year in which the final outcomes are known.

## Narrative descriptions

Narrative descriptions are required for certain cases of reported fraud perpetrated against departments and agencies as follows:

- all cases of fraud perpetrated by staff or involving collusion with staff with a value of £10,000 or more;
- all cases where perpetrators are “unknown” with a value of £10,000 or more;
- all cases of contractor or supplier fraud;
- cases of fraud committed by the public with a value of £10,000 or more **and** that contain possible lessons for a wider audience.

In order to learn from frauds perpetrated against other central government bodies (e.g. NDPBs) it would be useful for us to know about large value cases that contain lessons that might benefit a wider audience. Reporting bodies should provide narrative descriptions for cases which exceed £10,000 in value **AND** which contain lessons that might benefit a wider audience.

Narrative descriptions should briefly cover the main elements of the case including the main weaknesses that allowed the fraud to occur, how the fraud was discovered, its value, action taken against the perpetrator and action taken to reduce the risk of similar frauds occurring again. It is important to ensure that the descriptions are in a form suitable for publication in the Annual Fraud Report.

## Exclusions

Departments should have systems for recording and reporting fraud cases for their own management purposes and for pursuing vigorously anti-fraud policies. Not all of this information needs to be reported to the Treasury. The following need **not** be reported:

- Minor disciplinary cases that fall within the main reporting categories (Annex 1) (e.g. abuses of: flexitime, the Internet, sick leave; staff exceeding the level of their authorised access to data or who access information for non-business reasons etc) where disciplinary action taken has **not** gone beyond the oral/written warning stage. However, where information is supplied to an external party for profit, these cases should be reported.
- Cases involving breaches of computer security that do not lead to, or are unlikely to lead to, a financial loss (e.g. hacking) as this information is captured under separate arrangements.
- Frauds committed by members of the public where the cases are peculiar to the business of the reporting body (e.g. benefit fraud, tax fraud, agricultural grants, educational grants). However, where such cases involve collusion with departmental staff, these cases **should** be reported.

## The Annual Fraud Return - Reporting Categories

Below is the suggested model for fraud returns. This will be completed in the form of an electronic spreadsheet. Explanations about the categories can be found in **Annex 2**.

### A. Perpetrator of Fraud

1. Internal;
2. External – public;
3. External – contractor/supplier;
4. Unknown.

[Reporting bodies will be asked to indicate on the spreadsheet whether the fraud involved collusion]

### B. Collusion

1. With a member of staff.
2. With a contractor/supplier.
3. With a member of the public.

### C. Value

1. Value of loss (actual or estimated);
2. Amount recovered through recovery action.

### D. Type of Fraud

The categories are arranged on a systems basis so as to allow us to highlight areas where most frauds occurred and help managers focus their attention on areas of potential fraud risk.

1. Travelling, subsistence and allowances;
2. Pay related frauds;
3. Theft of assets and information (including IT equipment);
4. Exploiting assets and information;
5. Procurement fraud:
  - 5.1 tendering;
  - 5.2 Government Procurement Card/credit cards;
  - 5.3 goods/services not delivered as claimed;
  - 5.4 Other (please specify).
6. Personnel Management related fraud;
7. Fraud related to payment processes;
8. Income related fraud;
9. Other (please specify)

**E. Fraud Risk Areas**

1. Absence of control.
2. Control system by-passed or controls not properly applied due to:
  - 2.1 inadequate supervision;
  - 2.2 poor separation of duties;
  - 2.3 management checks not applied/lack of management checks;
  - 2.4 collusion;
  - 2.5 other reasons(please specify);
3. Other (please specify).

**F. Means of Discovery**

1. Operation of control procedures;
2. Reported via hotlines;
3. Reported via other internal arrangements;
4. Confession;
5. Other (please specify).

**G. Action Taken Against Perpetrator (if identified)**

1. Prosecuted;
2. Contract terminated
3. Dismissed or resigned without prosecution;
4. Downgraded;
5. Loss of spine points and /or promotion;
6. Written or oral warnings;
7. Insufficient evidence to sustain further action;
8. Awaiting the outcome of internal or legal proceedings;
9. No action taken on the grounds of mental or physical health;
10. Other action taken (please specify).

**H. Has action taken to recover losses?**

1. Yes.
2. No.

**I. Action Taken to Improve Control/Reduce Risk**

Short narrative description (see Annex 2 for examples).

**J. Update on case reported in a previous reporting period**

1. Yes.
2. No.

**K. Number of other perpetrators (if appropriate)**

**L. Other comments**

## Guidance on Completion of Annual Fraud Returns

### A. Perpetrator of Fraud

#### Internal

Frauds perpetrated within a department by members of its own staff, referred to collectively as Crown Servants. This category should include any cases where members of staff have acted in collusion with people outside the department. Temporary staff such as those supplied by an Agency should be treated as employees of the organisation for the purposes of the Fraud Report.

#### External – public

Thefts or frauds perpetrated by members of the public, which contain useful lessons for other government bodies, **and** where the value of the incident is more than £10,000. Reports should exclude cases involving income or expenditure that is **peculiar** to the business an organisation (e.g. benefit payments, tax fraud, agricultural grants, educational grants).

#### External – Contractor/Supplier

All frauds or thefts perpetrated by suppliers or contractors or contractors' staff in connection with contracts or orders placed by departments for the supply of goods and/or services. This involves fraud carried out exclusively by contractors/suppliers. Cases involving collusion with staff members should be recorded under **“Internal”**. Cases involving sub-contractors where losses were incurred by the department should be reported. Cases involving sub-contractors where the main contractor was defrauded should **not** be reported unless the main contractor tries to recoup losses by defrauding the department.

### B. Collusion

Frauds perpetrated by external parties (e.g. contractors, suppliers, members of the public) that involve collusion with a member of staff should be described as “Internal” under category A.

### C. Value

The estimated or actual value of the loss and the amount recovered through action taken to recover assets should be supplied. In the case of attempted fraud or theft, where there has been no loss of funds, a zero value should be shown on the return. In those cases information should be given in the comment box to indicate the potential size of the loss/risk involved.

## **D. Type of Fraud**

### **1. Travelling, Subsistence and Personal Allowances**

Relates to frauds involving travel and subsistence claims and personal allowances that involve the completion of a claim for payment. Examples of fraudulent activity in this area include:

- Claims for journeys that were not made;
- Claims for overnight subsistence but staying with relatives rent free;
- Overstated claims;
- Forged signatures on claim forms;
- Claims for allowances for which there was no entitlement (e.g. warm and cold weather clothing allowances);
- Claims relating to circumstances no longer applying such as education needs, marital status, excess fares etc.
- Forged receipts (e.g. fuel bills, hotel bills, taxi receipts).

### **2. Pay Related Frauds**

Covers all frauds that involve payment via the payroll process. Examples include:

- The creation of “ghosts”, “echoes” and other fictitious employees on the payroll.
- False claims such as claims for overtime and other taxable allowances.
- Altered performance markings or false documentation leading to bonus payments.
- Unauthorised changes to payroll data.
- Deliberate failure to repay advances of salary.
- The retention of credits, supplements or allowances beyond the period of entitlement.
- Misuse of pay advances or loans (e.g. season ticket advance used for a purpose other than that intended).

### **3. Theft of Assets**

Thefts of assets that are recorded on Asset Registers for Resource Accounting purposes.

### **4. Exploitation of Assets and Information**

This type of fraud involves using the assets of the organisation for other than official purposes and/or supplying information to outside organisations for personal gain. Examples of this type of fraud include:

- Using official vehicles for personal use;
- Running own business using the organisation’s assets (e.g. IT system);
- Selling information to mail shot companies;
- Downloading pornography for sale.

Putting a value on this type of fraud is not always easy and we would suggest that no value be recorded for these unless one is easy to establish (e.g. having to hire equipment, fuel used etc).

## **5. Procurement Fraud**

Procurement is the whole process of acquisition from third parties and covers goods, services and construction projects. For the purposes of the Fraud Report the process begins at the initial concept and definition of business needs and ends when the goods or services are delivered successfully or, in the case of assets, when they are recorded in the asset register.

Procurement fraud can involve a contractor, a sub-contractor, Crown Servants or any combination of these colluding to perpetrate a fraud or act of corruption. Examples of this fraud type include:

- Manipulating tenders/collusive tendering (including rings and cartels);
- Rigging specifications in favour of one supplier;
- Product substitution or sub-standard work or service not meeting contract specifications;
- Theft of new assets before delivery to end user and before being recorded in the asset register;
- Fraudulent (false or duplicate) invoicing for goods and services not supplied or for interim payments in advance of entitlement;
- Improper or unauthorised use of Government furnished equipment or information;
- False accounting and cost misallocation or cost migration between contracts;
- Goods ordered for personal use, including misuse of the Government Procurement Cards/credit cards and e-procurement facilities;
- Provision of fraudulent test or quality assurance certificates;
- Corruption or attempted corruption of Crown Servants.

## **6. Personnel Management Related Fraud**

Cases reported under this category should only include those where the action taken against the perpetrator is beyond the oral/written warning stage. Examples of fraudulent activities in this area include:

- Staff on sick leave but working elsewhere;
- Abuses of flexible working time systems;
- Annual leave abuses;
- Misuse of official time (e.g. Internet abuse, operating a personal business in official time);
- Deceit and misrepresentation for advantage (e.g. false references or false qualifications used to secure employment).

## 7. Payment Processes

These are frauds that involve expenditure systems relating to payments for resources acquired by the department for official use and consumption. Payments involving claims by an employee will normally be covered under “travel, subsistence and allowances” or “pay related frauds”. Included in this category are:

- Creating false payments;
- Theft of completed payable orders;
- Theft of letters containing payable orders prior to posting;
- Providing confidential information to outsiders allowing them to make fraudulent claims;
- False accounting;
- Theft of cash (i.e. from petty cash floats, safes etc);
- Creating false BACS payments (e.g. by adding records to a BACS file before it is sent to the bank).

## 8. Income Related Fraud

Fraud in this area will include:

- Theft of income (e.g. income received that has not yet been recorded in the accounting system such as income received by post, cash from a safe, income awaiting banking);
- Understating or failing to record income so that “surplus” income can be stolen (i.e. false accounting);
- Manipulation of fees/charges/sales records;
- Manipulation of debtors records and write-off provisions;
- Theft of income received via the post after it has been recorded in the accounting system.

## E. Fraud Risk Areas

These are weaknesses in laid down controls and procedures exploited in the perpetration or attempted perpetration of a theft or fraud.

## F. Means of Discovery

These are the ways in which frauds or thefts came to light in the first place. Many thefts are discovered by staff simply noticing that assets have disappeared (e.g. PC missing from desk). These cases should be described under **operation of control procedures**. Cases described as having been discovered in some **other** way should be supported by a narrative description of the means of discovery.

## G. Action taken against perpetrator

There are a number of possible actions that can be taken against perpetrators and an analysis of this information is a very useful way to demonstrate that central government bodies always take appropriate action against known perpetrators.

“Action taken to recover losses” has been added which may be used in addition to other actions taken.

#### **H. Has action been taken to recover losses?**

If action has been taken in an attempt to recover assets, enter a 1 in this field. If no action was taken, enter 2. Where recovery action was not necessary, leave the field blank.

#### **I. Action taken to improve control/reduce risk**

Examples of short narrative descriptions include:

- Better segregation of duties;
- More frequent management checks introduced;
- Improved management information;
- Regular independent checks introduced;
- Responsibilities allocated to named individuals;
- Delegated financial authorities introduced;
- Physical access to buildings, storerooms etc improved;
- Restricted access to computer data improved;
- More comprehensive checking of potential new employees;
- Complete overhaul of internal control system that includes the introduction of the following controls (list the key controls introduced).

#### **J. Update on Cases Reported in Previous Reporting Periods**

This field should be used to indicate whether the record is an update of a case reported in a previous reporting period. Updated information should be provided for cases previously reported where the final outcome was not known at the time of reporting. Updates should be provided annually until the final outcome is known.

#### **K. Number of other perpetrators (if appropriate)**

If more than one perpetrator was involved in the fraud, enter the number of other perpetrators involved. Otherwise leave the field blank.

#### **L. Other Comments**

This field can be used to provide more information where any of “other” categories have been used. It can also be used to supply any additional information that might be useful when analysing the fraud data.

# Completing Annual Fraud Returns

