



HM TREASURY

FRAUD CASENOTES

Assurance, Control and Risk Team

CONTENTS

1. **Cash Handling Fraud**
2. **Bill Paying Fraud**
3. **Property Service Charges Fraud**
4. **Travel and Subsistence Fraud**
5. **Electronic Funds Transfer Fraud**
6. **Works Contract Fraud**
7. **Cheque Fraud**
8. **Payroll Fraud**
9. **Grant Fraud**
10. **Estates Management Fraud**
11. **Overtime Fraud**

The ACR team in the Treasury prepared these casenotes. The aim is to increase awareness of common fraud risks. Each casenote is based on actual frauds reported by department, sometimes drawing on more than one case to illustrate the lessons more effectively. If you have any questions about this or the other casenotes, contact ACR Admin on 0207 270 5174 (fax 0207 451 7567 and e-mail: gwin.trinh@hm-treasury.gov.uk).

1 Cash handling fraud

Case description

Transactions involving receipts of cash or cheques are high risk. Of the cases of staff fraud reported to the Treasury each year, a significant proportion involves misappropriation of cash. In this sample case, a member of staff committed a number of frauds over a period of five years, resulting in a loss of over £10,000.

The organisation's business included the **receipt of cheques** through the post and cash and cheques cover the counter. It was the responsibility of the member of staff to receive, record and **prepare the receipts for banking**. She had been in the job several years and her line managers, who trusted her implicitly, had given her **sole responsibility for these duties**. They were no longer carrying out checks or monitoring the process.

She would arrive early each morning, usually before her colleagues, **and open the post on her own**. Money handed in over the counters was also passed to her for banking. However, she **did not record or account for the cheques or money** prior to banking. She would, however, complete a daily cash balance record as part of the **banking reconciliation procedures**, but by this time she had already removed some of the cash and a number of cheques. There were **no independent cross-checks** between the documentation which came with the receipts and the amounts sent for banking. To make matters worse **written procedures were out of date** and had fallen into disuse.

The fraud came to light during the officer's **infrequent absences on leave**. A minor query by a member of the public regarding a previous payment led to an unexplained difference between the amount quoted in the documentation accompanying the payment and the amount recorded by the officer and banked.

Internal audit were brought in to carry out an initial investigation. They identified major discrepancies between records of receipts kept by counter staff, documentation accompanying payments from members of the public and the amounts being banked. The police were called in and under questioning the officer admitted the offences. She had opened a bank account with the initials of the organisation and had been paying in cash and cheques over a five year period. The case was taken to court and on conviction she was given a custodial sentence and had to repay the amounts stolen.

Control weaknesses

- š Lack of separation of duties between post opening, preparation of cash and cheques for banking and reconciliation of amounts banked
- š Inadequate supervision and monitoring by line management
- š Absence of management checks of accounting records, cash balances or bank reconciliations
- š Over-reliance on the honesty and integrity of one individual
- š Lack of adequate written instructions
- š Unawareness of implications of reluctance to use leave entitlement
- š The internal audit report also identified organisational factors which had contributed to the fraud. The main ones were:
 - Ø The organisation had not assessed the risk of fraud;
 - Ø There was no policy statement on fraud;
 - Ø Line managers were not clear about their responsibilities;
 - Ø Manuals and procedures were poorly structured and out of date.

Key control lessons

- š **Separate duties** at key stages of the process, e.g:
 - Ø Post opening and logging of receipts;
 - Ø Bringing receipts to account and preparation of cash and cheques for banking; and
 - Ø Daily cash balancing and bank reconciliations.
- š Ensure post-opening duties are carried out by **two people** and the daily log of receipts is signed by **both** officers.
- š Institute regular **and random** line management checks of source documentation, accounting records and bank reconciliations.
- š Ensure senior management also carry out regular and random checks, particularly they should monitor to ensure that the expected level of cash flow is achieved.
- š **Rotate officers** in sensitive posts such as cash handling.

- š Provide **clear instructions** about procedures.
- š Ensure management and staff clearly understand their responsibilities.
- š Introduce a **corporate fraud policy** and a strategy to counter fraud including risk assessments.
- š Be alert when staff in sensitive posts do not use their annual leave entitlement, or have working patterns which mean they are alone in the office.

Conclusion

For over-the-counter and postal income the most difficult problem, from the viewpoint of preventing fraud, is ensuring completeness of collection and recording. The organisation may not know of the timing of receipts and therefore two key controls are recurrent, supervision of activities (including management checks) and separation of duties. **In particular, no single officer should collect, record, bank and reconcile cash or other payments.** There should always be separation of duties in key areas of the cash receipting process.

2 Bill paying fraud

Case description

Situations involving payments for goods and services involve a high risk of fraud. The Treasury's 1996-97 fraud report identified that 41 per cent of the total value of reported frauds in central government (some £866,600) involved payments based on false claims or orders. The Audit Commission's statistics also show that, over a six year period, out of a total of £11 million worth of frauds nearly £3.5 million related to creditor payments. In this sample case, a junior member of staff over a period of two years was able to defraud a department of over £100,000 by exploiting weaknesses in purchasing and payments systems.

The junior clerk had been employed by the department for **six years in the purchasing directorate**. He showed an aptitude for computers and as well as the normal duties associated with his position he was also asked to carry out tasks such as **setting up and maintaining computer records**. He would also fill in for colleagues who were ill or on annual leave and so built up an extensive knowledge of how the purchasing directorate operated.

Two years after the junior clerk joined the department there was an upgrade to the computer system. As part of this process the purchasing directorate updated its supplier records and moved them onto a database. The junior clerk was involved in setting up the database and cleaning up individual records to be moved on to the database. He was given **a password** which enabled him to create and edit records. On completion of this task the junior clerk **moved to a purchasing team** where he was involved in the processing of purchase orders and the information needed to enable payments to be made to suppliers.

Security over the computer system was lax and the junior clerk realised that the password previously given to him to carry out specific tasks still allowed him access. In particular, he was able to **access the supplier database** and create **false supplier records**. He was aware that only **a minimal check of the database** was carried out by management and that generally there was **very little checking and monitoring** of the work of the procurement teams.

Having created bogus suppliers, he opened bank accounts in their names. Through his position in the purchasing team he was able to introduce **fictitious invoices** from these suppliers, designed on his computer at home, into the payment system. He easily obtained and signed the purchase orders and authorisation forms necessary to support the invoices for payment. The finance section **accepted his signature** as authorisation for payment. The finance section had in fact built up a practice of accepting any purchasing staff signature as payment authorisation. There was **no effective budgetary control** over purchases and little monitoring of actual expenditure against budgets. The junior clerk was in fact responsible for what little monitoring there was and he was able to satisfy his managers that where there had been an overspend this was a result of operational demands. No further checking was carried out by management.

The fictitious invoices were paid by payable orders in the normal manner. These were sent to **accommodation addresses** arranged by the junior clerk who visited these regularly and banked the orders.

The fraud came to light when a manager of one of the other purchasing teams became suspicious of the junior clerk's **lifestyle**. He had taken out a mortgage on a luxury flat to which his colleagues had been invited for parties. He had bought a sports car and booked an expensive holiday, telling his work friends that he had inherited money from a wealthy member of his family.

The suspicious manager had discussions with the purchasing director and it was decided to bring in a specialist fraud investigation firm to look at purchases over the last three years. The firm checked the supplier database to the employee records and found that the address of one supplier matched that of the junior clerk. They checked the VAT numbers of the suppliers and found that a number of these were false. They then checked the addresses of these suppliers and found that they were accommodation addresses which had been paid for by the junior clerk. The purchases made by the junior clerk were looked at in great detail and it was discovered that on numerous occasions he had re-used one particular invoice to initiate payments to false suppliers. The police were called in and the clerk admitted to offences totaling £100,000. He was given a custodial sentence and had to repay the money he had stolen.

Control weaknesses

- š Lack of password and other access controls over the computer system (particularly cancelling passwords of staff moving on from sensitive areas);
- š Lack of separation of duties in the purchasing process;
- š No rotation of staff after a set period of time;
- š No independent checks of the supplier database;
- š Lack of written guidance to staff defining the roles and responsibilities in purchasing, finance and computer areas;
- š No proper procedures for authorising payments;
- š Lack of effective management checks both in the purchasing directorate and the finance department;
- š No security for blank purchase orders and authorisation documents;
- š Lack of budgetary control - no effective monitoring of actual expenditure against budget;
- š No random checks by senior management over payments and supporting invoices.

Key control lessons

- š Develop effective **computer security**, particularly controls over access;
- š **Change passwords** on a regular basis and always when staff responsibilities change;
- š Set up a formal purchase order system which includes adequate **separation of duties** covering ordering, authorisation and receipt;
- š Institute a staffing strategy which includes **regular rotation of staff**;
- š Ensure new supplier records and changes to existing supplier records are approved by a senior manager, the computer system should identify all change for this manager;
- š Introduce written **desk instructions** detailing roles and responsibilities of purchasing, finance and computer staff;
- š Institute formal designation of staff at an appropriate level to authorise payments. An up to date list of the authorised signatories should be held in the finance department;
- š Ensure authorised signatories conduct checks of supporting documentation including order and invoices;
- š Ensure line and senior management conduct **independent checks** of payments and payments records on a random basis including purchase orders and authorisations documentation;
- š Be alert to significant changes in **lifestyle**.

Conclusion

Situations involving expenditure including purchasing, presents a number of risks. Most frauds occurring in this area are initially opportunistic and follow a breakdown in internal control. Over reliance on one person and poor physical control over computers and purchasing documents compound the risks.

The key is to design a system that effectively separates purchasing duties such as ordering, authorising and receiving. It should ensure security over access to computers and computer held information as well as key documents, such as purchase orders. Other safeguards should include rotation of staff, regular and random management checks and audits.

3 Property service charges fraud

Case description

A landlord defrauded a department of £100,000 over five years by submitting **inflated service charge bills** in respect of a leased office.

The lease included provision for some of the cost of the maintenance and servicing of the building to be shared amongst the tenants. The landlord had an agreement that payment was to be made quarterly, on an estimated annual spend, but that a **reconciliation against actual expenditure** would be undertaken at the end of the year.

It had been agreed with the landlord that he would submit the quarterly invoices to the department's local office for payment. The quarterly invoice was checked by the local manager who authorised it and passed it to the regional accounts section for payment. The accounts section checked the invoice for arithmetical accuracy and authorising signature and paid the landlord by payable order. The payment was recorded against the local office budget and the manager received a printout confirming expenditure against his cost codes.

However, it had been agreed at the lease negotiation, which had been carried out by the regional surveyor, that the yearly reconciliation would be **submitted direct to the surveyor for payment**. The surveyor met with the landlord each year to discuss the maintenance of the building and look through the receipts held by the property company for work carried out on the building. The surveyor reconciled the payments against the receipts provided by the landlord and authorised a balancing payment. This was made by the accounts section and in time filtered down to the local manager as part of his budget monitoring. However, as the reconciliation was agreed with the regional surveyor the manager **never queried the costs** or checked the work done against the terms of the lease. In fact, the landlord overcharged the department at the rate of £20,000 per year either for work where it was not entitled to recover the cost or which had not been done at all. This happened because the surveyor relied on the invoices provided by the landlord as evidence of work carried out on the property and **failed to seek local verification** that the work had actually been done.

Control weaknesses

- § Inadequate separation of duties, particularly between authorisation and verification of the annual reconciliations;
- § Absence of desk instructions setting out responsibilities for checking service charges to ensure coordination between the regional and local offices;
- § No checks by the regional surveyor or local management to validate the work carried out;

- § No checks by the regional surveyor or local management against the terms of the lease to ensure work carried out was a legitimate charge;
- § No systems in place to ensure that the checking of the reconciliation statement at financial year end was undertaken in a structured way.

Key controls

- § Ensure proper **separation of duties** between authorisation, validation and payment;
- § Institute **guidance** for managers on their responsibilities for property and on checking and processing related payments, especially where these involve remote sites;
- § Ensure a copy of the lease is held and reviewed by the responsible local manager;
- § Submit all invoices, including any yearly reconciliation, via the local office;
- § Ensure the local manager in conjunction with the local accommodation officer **checks invoices** against work carried out and the lease and authorises payment. The landlord should provide copies of invoices for work carried out on the property each quarter;
- § Provide **specialist training** where necessary to interpret lease requirements or employ independent agent to advise.

Conclusion

Service charges are one of the risk elements of estates or facilities management. They may be perceived solely as the preserve, and therefore the responsibility, of the specialists. In fact, the specialists, such as surveyors who often look after a number of sites, rely heavily on close contact with local managers and staff for verification and validation of work carried out and service charges made.

It is essential that a sound system of control be put in place including formal authorisation, validation and payments processes. These should be backed up by appropriate separation of duties and clear guidance setting out key roles and responsibilities.

4 Travel and subsistence fraud

Case description

This fraud involved an employee who travelled regularly on official business. He **set his own programme** of visits which was **not checked** by his line manager. He then regularly **submitted fraudulent travel and subsistence claims** which included examples of:

- § Claiming subsistence allowances **in excess of entitlement**;
- § Claiming for overnight stays in hotels when in fact he had **stayed with friends or family**;
- § Claiming for **visits not made**;
- § **Forging** authorising signatures;
- § **Inflating claims** by altering details on claim forms **after authorisation** by countersigning officer.

These claims were paid by the finance team despite the **lack of receipts**, invoices or other supporting documents to verify his expenditure. Travel and subsistence **guidance was also out of date** and consequently had **fallen into disuse**.

The fraud came to light when his office tried to contact him at a hotel where he claimed to be staying. An investigation uncovered a large number of fraudulent claims spanning several years and the officer was eventually prosecuted.

Control weaknesses

- § Inadequate guidance on submitting, authorising and paying claims;
- § Inadequate supervision by line management;
- § Failure of countersigning officer to verify that journeys had been made;
- § Inadequate control exercised by countersigning officer in returning signed claim forms to the claimant rather than passing them directly to the finance team;
- § Inadequate checks by finance teams to query amendments to claims, verify countersignatures and ensure that receipts and invoices were included to substantiate claims;
- § Absence of spot checks on claims by the finance team management.

Key control lessons

- Š Establish a **comprehensive** set of travel and subsistence rules and ensure that they are **communicated to all** staff;
- Š Introduce **written procedures** and desk instructions detailing the roles and responsibilities of line managers, countersigning officers, staff who do not require a countersignature on their claims (often over a particular grade) and finance teams;
- Š Establish a formal process which involves line managers **approving and reviewing work plans** and programmes for visits, especially for staff where there is no countersigning requirement;
- Š Institute **checks by countersigning officers** of claims against approved work plans, standard mileages for regular destinations and primary evidence, such as rail tickets, hotel bills and taxi receipts;
- Š Ensure that countersigning officers pass approved claim forms **direct** to the finance team
- Š Instruct countersigning officers to **initial any amendments** to details on claim forms and finance teams to reject any claims where amendments have not been initialed;
- Š Instruct finance teams to ensure that **correct rates** are claimed, **substantiating documents** (e.g. hotel invoices) are included and to compare **countersignatures** on claims against **sample signature** cards provided by authorised countersignatories;
- Š Ensure that finance teams carry out **spot checks**, including random management checks, to verify details on claims (e.g. that claimants stayed in hotels specified, reasonableness of mileage claimed for car journeys);
- Š Ensure that finance team checks are rigorously applied to claims not requiring countersignatures (e.g. self-certification over a certain grade);
- Š Monitor travel & subsistence expenditure via the **budgetary control** process;
- Š Ensure claim forms spell out the responsibilities of claimants and countersigning officers and that the signature section includes a warning on the consequences if fraud is discovered.

Conclusion

Travel and subsistence expenses are a sensitive area due to the personal nature of the transactions. They are also an area **susceptible to fraud**. Most cases occur because of weak internal control or a failure to apply quite straightforward procedures. It is essential that a **sound system of control is put in place to cover line management approval of planned journeys and effective authorisation, validation and payment of claims**. Those involved in these processes should fully understand and apply the system.

It is particularly important that controls such as line manager's review of visits and finance team checks are strengthened for staff, often senior managers, able to sign-off their own claims.

Because of the personal nature of these type of claims the development of an overarching **anti-fraud environment** where fraud is not tolerated, perpetrators expect to be caught and punished and staff reporting fraud expect it to be properly dealt with, is as important as the control system itself. Any anti-fraud environment should be backed up with **clearly communicated fraud policies and response plans**.

5 Electronic funds transfer fraud

Case description

Fraudulent payments in excess of £500,000 were made to overseas bank accounts via the electronic fund transfer (EFT) system.

The basis of the fraud was simple. The perpetrators had no difficulty obtaining **blank payment vouchers** which were **not held securely**. They also set up bogus accounts in a number of overseas banks. The fraudulent payments were initiated using the vouchers which were supported by **photocopied** rather than original documents. The vouchers were then passed to the bank responsible for making the electronic transfers without being checked; in particular, there was no validation of the authorising signatures.

Because of delays in posting transaction details to the accounts system, the fraudulent payments were only discovered after the monies had been transferred to, and subsequently removed from, the overseas bank accounts.

A number of organisational factors also contributed to making the fraud possible. The organisation itself was going through a period of growth and structural change. This resulted in a **higher than usual turnover** of permanent staff and the employment of a number of **temporary, untrained staff**. One consequence of this was a **shortage of qualified or experienced personnel** to fill important finance posts.

The fraud was also perpetrated over a two-week Christmas holiday period when, because of annual leave and a general slowing down of business, routine controls, such as supervisory and management checks, were not operating with their normal frequency and regularity. **Holiday periods are often targeted for this type of fraud for these very reasons.**

Control weaknesses

- š Inadequate physical control over payment vouchers which were not viewed as accountable stationery and therefore not kept securely;
- š Inadequate checks over the validity of payment vouchers or supporting documentation;
- š Acceptance of photocopied rather than original supporting documentation;
- š Absence of checks of authorised signatures against the approved list;
- š Long delays between payment and posting transaction details to the general ledger;
- š Lack of regular monitoring and reconciliation of bank balances;

- § Lack of awareness by management of their responsibility to ensure compliance with financial monitoring controls;
- § Absence of contingency arrangements during holiday periods;
- § Use of temporary, unqualified, untrained or inexperienced staff in key financial posts.

Key control lessons

- § Ensure that accountable stationery, particularly documents used to authorise transfers, is **held securely**, forms are pre-numbered and only issued to **authorised** personnel, records are kept of issues and **regular** stock reconciliations are undertaken;
- § Ensure pre-payment checks, including random supervisory and management checks, include **confirmation of authorising signatures** against approved list, payment vouchers are fully supported by **original documents**, and that payments are reasonable in terms of amounts, payees and destinations;
- § Establish **segregation of duties** between those who can prepare, authorise and process transfers;
- § Post transaction details to ledger **immediately** after transfers have been made and ensure **frequent monitoring** and **reconciliation** of bank balances;
- § Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. Transfer codes and passwords should be **changed frequently**, and always when staff leave;
- § Provide **adequate supervision** of all staff particularly new, inexperienced or temporary staff;
- § **Issue guidance** to staff and managers on their responsibilities, provide formal guidance on processing payments through the EFT system and provide specialised training where necessary;
- § Set up **contingency arrangements** to provide adequate cover for key staff during periods of absence (e.g. during holiday periods);
- § Set up procedures to ensure the organisation making the electronic transfers **refer back suspicious payment instructions** before the transaction takes place.

Conclusion

Potentially very large sums are at risk from this type of fraud, and recovery can be extremely difficult. They usually involve the forgery of documents authorising the transfers and/or the misuse of passwords and authorisation codes. It is therefore vital that **strong control is exercised** over the forms used to authorise transfers, **that transfers are properly authorised**, that **appropriate checks are built into the system**, both before and after payments are completed, and that access to any computer terminals from which payment instructions are communicated to the organisations making the transfer (e.g. banks) is restricted to authorised personnel.

6 Works contract fraud

Case description

A department decided to rationalise the management of its HQ building and its five satellite sites. A new facilities management contract worth some £1.5 million was to be let for a three-year period with possible extensions for a further two years.

The contract was advertised in the European Journal and let under EC procurement rules. A short list of four contractors who expressed an interest was drawn up which included one firm which had carried out maintenance work previously at the sites. The contractors were vetted to ensure that they were financially viable and capable of carrying out the work to the standards specified, **except the firm which had been used before**. This firm went on to win the contract.

The contract was managed centrally by HQ accommodation staff who **initially checked the firm's work closely**, regularly carrying out visits to the satellite sites. After the first year of the contract however the **monitoring declined** until eventually **no site visits were undertaken** and no provision was made to fill the gap with feedback from staff at these locations.

The contract itself included maintenance charges covering work for gutter and drain clearance, minor roof repairs and general minor building works. The contractor submitted his bills on a quarterly basis using the agreed rates. As the bills were in line with the previous year's spend they were **automatically authorised** for payment by the accommodation staff. It was only when a major flood took place in a secure storeroom that the actual quality of the work was checked. It was found that pipes were blocked and gutters were full of debris.

A team, which included a specialist investigator and quantity surveyor, was set up to investigate other payments made to the contractor. They found several examples where work had been **paid for but not carried out**. The team estimated that the department had been defrauded by some £100,000 over two years.

The team also checked into the company and discovered financial problems which would have come to light if it had been **properly vetted** at the time it was selected to bid for the contract. Another department had reported similar problems with this contractor and as a result the firm had, in fact, been removed from the then Department of the Environment's register of works contractors.

The investigation team also concluded that the staff responsible for managing the contract did not have the necessary expertise and **had received no training**. They relied on the contractor to provide explanations to queries raised on their invoices.

Control weaknesses

- § Inadequate vetting procedures during the selection process, in particular in checking previously used contractors;
- § Lack of appropriate training for departmental staff responsible for contract management;
- § Over-reliance by contract management staff on the contractor in substantiating the quality of work carried out;
- § Lack of checks by HQ accommodation staff on the quality of the contractor's work;
- § Inadequate use of the department's site-based staff to monitor the contractor's work and confirm quality;
- § Lack of regular management checks on contractor's work and associated invoices.

Key control lessons

- § Issue **clear written instructions** and guidance particularly setting out the responsibilities of staff letting, managing and monitoring contracts and those responsible for checking invoices before passing for payment;
- § Use **trained procurement staff** to negotiate and let contracts, particularly where EC regulations apply. Procurement Guidance is available from the Treasury's Public Enquiries Unit on 0171 270 4558 and on the Treasury website at <http://www.hm-treasury.gov.uk>;
- § Provide **suitable specialist training** in contract management where necessary and involve contract managers in the preparation of specifications to ensure awareness of contract terms;
- § Ensure **adequate supervision** of staff letting, managing and monitoring contracts;
- § Ensure **all** firms invited to tender are **fully evaluated** against the relevant selection and award criteria;
- § Ensure staff responsible for monitoring contracts **carry out regular checks** of contractors' work, where necessary involving specialist staff, such as surveyors;
- § Carry out **random management checks** of work against specification and where necessary involve specialist staff;
- § Use **locally based staff to monitor work** where necessary and reasonable;
- § Keep **records of work inspected** and results;
- § Ensure certification of invoices is based on a **proper validation** of the work carried out;

§ Instigate sample management **checks on invoices** prior to payment.

Conclusion

Works services projects are traditionally seen as carrying a **higher risk of fraud and corruption** than other forms of procurement. Contributory factors include the complexity of projects, the difficulties of measuring the quality of the product and opportunities for contractors to exaggerate the amount of work carried out. These frauds can take a number of forms and **may involve collusion with departmental staff**.

Fraud in this area arises because of **basic failings in letting and monitoring works contracts**, including unclearly specified services, insufficient checking of the suitability of potential contractors, weak contractual arrangements, lack of control over contractor performance and inadequate checking of invoices.

As seen in casenote 3 on property service charges, **the basic elements of a sound control system are relatively simple to set up and operate**, particularly if set out in **clear guidance, backed up by relevant training and a knowledge of when to call in the experts**. It is management's responsibility to ensure their staff fully understand and apply these controls.

7 Cheque fraud

Case description

A supplier contacted a government body to ask why an invoice had not been paid. The finance records of the body showed that a cheque had been produced as payment and despatched to the supplier.

The bank was asked to trace the cheque and it was discovered that the **cheque had been intercepted, payee details had been expertly altered** and the **cheque cashed** at a building society. The alteration had been skilfully carried out by **removing the original print** and printing the new name in the **same style and font**. It was not clear whether the cheque was **intercepted** in the government body's premises or after posting.

The government body, after consulting their bank, made amendments to improve the security of their printed cheques, specifically by using a heavier print which left an indentation on the paper.

This event prompted the government body to commission a review of its own procedures relating to payments generally and to the production and **issue of cheques** specifically. This revealed that **signed cheques were usually returned to those who prepared them in the first place** for despatch, that **cheques awaiting some action** (e.g. authorising signature) were **not always held securely**, that cheques were **posted in window envelopes** and that envelopes containing payments were simply **left in out-trays** for collection by messengers to be taken to an internal post room to await collection by the Post Office. Cheques were therefore **vulnerable at a number of stages** in the process.

Control weaknesses

- š The cheque was printed using a quality of print which was easy to remove.
- š Cheques awaiting action were not held securely.
- š Signed cheques were returned to originators for despatch.
- š Cheques awaiting despatch were not held securely.
- š Postal arrangements were inadequate.
- š Cheques were despatched in envelopes that allowed the contents to be easily identified.
- š The bank reconciliation process failed to identify incorrect payee details.

Key control lessons

- § Reconcile **high value** cheques presented for payment against **the authority's** records to ensure that **amounts**, and **payee details** have **not** been altered.
- § Treat completed and used **cheques** as **securely as cash**.
- § Discourage the fraudulent **amendment of cheque details** by the careful choice of inks and printers used to print details on cheques so that the print produced is as indelible as possible. If necessary, get advice from “the experts” (e.g. banks).
- § Print the **amount** in figures as close to the £ sign as possible.
- § Write **payee details in full** rather than use **abbreviations** or **acronyms**.
- § Use **restrictive crossings** such as “not transferrable” and “a/c payee”.
- § Fill up **blank spaces** with insignificant characters such as asterisks.
- § Use envelopes which make it **less obvious** that they **contain a cheque** for mailing purposes.
- § Consider incorporating **security measures** into cheques such as multi-coloured cheque backgrounds, special inks which run if a cheque is tampered with, special cheque paper on which the word “void” appears if the cheque is photocopied, watermarks, etc.
- § Ensure that cheques are **authorised** only after payment details are added.
- § Ensure that **signed cheques are not** returned to payment staff.
- § Ensure that cheques are despatched **independently** of certifying officers and payment staff.
- § Despatch payments by taking them to a **post box or post office** rather than have them despatched via an **internal postage** collection service.
- § Carry out **regular independent** checks on a sample basis to ensure that amounts and payee details accord with organisational records and that the internal control system operated effectively.
- § Reconcile bank statements with the authority's cheque listings **frequently**.

Conclusion

Where cheque frauds occur they are often due to basic weaknesses in their handling. These frauds usually involve theft of a cheque, altering the amount and/or payee details, paying the cheque into an alternative bank account and withdrawing the proceeds. There are opportunities for fraudsters at every stage of the cheque handling process. It is therefore vital that strong control is exercised over supplies of blank cheques, the preparation of cheques, cheques awaiting authorisation (for instance they should not be left lying about in in-trays), post handling arrangements and the bank reconciliation process. Organisations should also ensure that their response to fraud is established, well planned and well publicised as a further deterrent to would be fraudsters. Departments should consider whether the use of electronic payment methods may be more secure.

Note: many of the weaknesses and controls referred to above also relate to payments via Payable Order. Government Accounting, chapters 28.4.15 to 28.4.20, includes guidance on the use of cheques and payable orders.

8 Payroll fraud

Case description

A cleaning supervisor working for a government body had **sole responsibility for recruiting employees**. Her manager delegated this role and carried out **no meaningful authorising or checking** activities. She used her position to set up several **fictitious casual and part-time** employees with **inflated pay rates** on the payroll.

The fraud involved the supervisor **completing “starter” forms** which provided the fictitious employee details. These were forwarded to the payroll section who accepted the **supervisor’s signature** as authorisation and input details to the payroll system **without checking their validity**. Casual and part-time staff were **not subject** to the same rigorous **recruitment checks** as full-time permanent staff.

The supervisor then created **bogus timesheets** for these employees which she authorised along with timesheets for legitimate employees. Because they were casual and part-time it was easier to conceal that the employees did not actually exist. The manager **did not approve or check** the timesheets. The timesheets were passed to the payroll section, together with timesheets for legitimate employees, who generated paycheques **based solely** on the supervisor’s authorisation and **without carrying out any appropriate checks**. These paycheques were then collected by the supervisor for issue to employees. The supervisor kept the cheques for the non-existent employees and paid them into **bank accounts** which she had opened in the names of the fictitious employees.

The fraud was found when a payroll clerk questioned the **high hourly rate** being paid to the fictitious employees. **Internal audit** were asked to carry out an investigation and established that the employees did not exist. The police were informed; the cleaning supervisor was arrested, prosecuted and dismissed. Internal audit went on to make a number of recommendations to improve control over appointing new staff.

Control weaknesses

- š The manager did not authorise additions to the payroll or carry out any associated checks.
- š There was no segregation of duties in the functions of completing and authorising starter forms.
- š The manager did not approve or check the timesheets.
- š No checks were carried out by the payroll department to verify the existence of starters before inputting details to the payroll system.

- § Periodic checks were not carried out by the personnel department to confirm that the correct persons were shown in post, that appointments were properly authorised and that basic salary and allowances were correct.
- § The supervisor was allowed to collect paycheques on behalf of employees.
- § No signatures were required on the issue of paycheques.
- § Standard exception reports (e.g. no NI numbers, emergency tax codes for more than 6 months) were not produced and investigated.

Key control lessons

- § Provide clear **written instructions** and **procedures** to **all** staff involved in recruiting new staff, adding details to the payroll and making payments.
- § Ensure that wherever possible **all appointments** and **other payroll changes** are made by a **personnel function** which is organisationally separate from the **payroll function**. Only personnel should be able to authorise changes to the payroll.
- § Ensure that **all new appointments** not subject to recruitment by a separate personnel function (including **part-time and casual staff**) and changes to standing data (e.g. new pay rates) are approved and separately authorised by the employing department (in this case the supervisor and manager) and by Personnel who should also independently **confirm** the existence of starters and that the rates of pay to be paid to starters are correct.
- § Produce listings of all **starters, leavers and changes to standing data** as part of every payroll run. At least a sample should be checked by payroll section and a further random sample **checked independently** by management.
- § Ensure that those who process payroll data reject any timesheets, where they are produced, which **are not signed** by valid employees and/or are not **approved** and **separately** countersigned by **authorised signatories**. The accuracy of **all** signatures should be confirmed by reference to **copy signatures** held.
- § Ensure that timesheets which have been checked and authorised by relevant line managers are **forwarded to the payroll section** and are **not returned** or otherwise made available to **relevant employees**.
- § Ensure that **paycheques** are **collected** and signed for by employees (signatures to be checked against specimens held by the payroll section), **posted** to them or, ideally, **paid direct into a valid bank account**. Where pay is collected on behalf of an employee a clear **written authority** should be provided by the **employee** and retained for audit trail purposes.
- § Produce regular **exception reports** (e.g. emergency tax code for more than 6 months, no NI numbers) for **investigation** by management.

- § Subject the **payroll masterfile** to periodic checks **by Personnel** to ensure that **each post** is **authorised**, that the **correct person** is in post, that the person **exists** and that **basic salaries** and **allowances** are correct.
- § Carry out **periodic management checks** to confirm that the correct procedures are being applied (e.g. that timesheets are properly completed, checked and authorised).

Conclusion

Payroll frauds are quite common and usually take the form of payments to non-existent employees (e.g. 'ghosts', 'echoes'), employees on more than one payroll or employees claiming amounts not due (e.g. overstating hours worked, applying incorrect rates of pay, over claiming allowances). It is therefore vital that **strong control is exercised** over starters (particularly over the employment of part-time or casual staff), leavers, changes to standing data and access to computer systems. Good **segregation of duties** is also critical, particularly between the employing (e.g. operational or personnel sections) and payroll functions. The payroll and personnel functions should be **managed independently** of one another.

9 Grant fraud

Case description

Grant claims frauds are vulnerable to a number of deceptions including fictitious applicants, false claims or overstatement of amounts. In addition there may be collusion between staff and claimants. The following case, concerning an individual who obtained £200,000 of a government grant dishonestly, is typical and involves the invention of bogus companies and forgery.

The fraudster claimed that he had formed **three companies** which created **80 new jobs** qualifying for certain government grants. In fact, the companies **never operated** and 80 names, together with **National Insurance numbers** were obtained from a number of different sources. Additionally, **leases were forged** for the premises of the three alleged companies and thousands of pounds worth of electronic equipment **was borrowed** to show an accountant who was validating the claim before the application for the grant was accepted.

The fraud was **discovered** when a member of staff at the grants office recognised one of the names of the bogus employees. The perpetrator was prosecuted and given to a custodial sentence.

An internal audit review was instigated which made a number of telling observations:

- § The fraud was made easier because staff at the grant office were **under pressure** to turn cases around quickly as the requirements for funding by applicants were often time critical.
- § Cases were often **processed** and **authorised** by the **same officer**.
- § Authorisation limits and **delegated authorities were ignored**.
- § Junior or inexperienced personnel sometimes processed **complex** cases.
- § Claims were **not checked** and validated as thoroughly as they should have been.
- § A clear **audit trail** was not always evident. **Case papers** were often **incomplete, badly filed**, not always **cross referenced** to other relevant papers or simply **missing**.
- § Few **management checks** (e.g. random checks to ensure that cases were processed properly) were carried out.

Control weaknesses

- § No risk assessment carried out to identify high risk claims so as to allocate them to experienced staff.
- § Lack of written internal control procedures.
- § Insufficient checks to ensure that the companies were real.
- § Inadequate checking to ensure that the new jobs had in fact been created.
- § Delegated authorities and authorisations not communicated clearly to staff or enforced.
- § Lack of supervision to ensure that claims were being processed correctly.
- § Incomplete audit trail.
- § Expectations of claimants not managed resulting in pressure to attain a high turnaround of case load resulting in poor quality case paper and controls not being operated effectively.
- § Staff not receiving appropriate training or coaching.

Key control lessons

As grant fraud is such a wide-ranging subject with many different types of payment, these key control lessons have been divided into those that relate directly to the case and those that are applicable to grant payment systems generally. The second list covers controls to guard against the risk of collusion.

Key control lessons relevant to the case

- § Set down strict **guidelines** on the claim procedures and communicate them to **all staff**, particularly **new recruits**.
- § Ensure that **all claims** and, in particular, **supporting evidence** are **checked** for accuracy, completeness and timeliness. These checks should be in **proportion** to the **level of risk**.
- § Carry out regular management checks on a **random selection** of cases to ensure that guidance is adhered to. Any supervisor or management checks should be clearly **evidenced**.
- § Assess claims to determine their complexity and level of risk and allocate accordingly to officers with the **relevant experience** and **expertise**.

- Š Ensure that **delegated authorities** and **levels of authorisation** are applied at an appropriate level.
- Š Ensure that no **single** officer is involved in processing and authorising a **complete** claim and that appropriate **segregation** is achieved throughout the process.
- Š Maintain **good quality** case papers as these may be needed later at **court** or **tribunal** hearings.
- Š Maintain adequate **resources** and **staff to supervisor** ratios based on the risk assessment and any independent organisational reviews carried out.
- Š Carry out **training** needs assessments **periodically** and ensure that appropriate training plans are drawn up and acted upon.

Key control lessons relevant to grant claims generally

- Š Ensure that a **senior manager gives final approval for a claim** or panel of adjudicators or some other person(s) **separate** from those who receive it.
- Š Ensure that **all** claims relating to a single individual or organisation are **identified** and **cross referenced** to avoid duplicating payments. All **evidence supporting** claims should be **retained** on file (e.g. rent books, leases, bank statements, wage slips, deeds etc).
- Š Ensure that all claims, including notifications of changes in circumstances, are on standard official **pre-numbered** forms and that claim **reference numbers** are issued in sequence as soon as a claim is received. Any delay in the allocation of a number while the claim is being handled adds to the risk of loss, misfiling, suppression or false amendment.
- Š Perform **periodic reassessments** of circumstances where **on-going** claims are concerned. **Officers not previously involved in the case should carry out follow up visits periodically.**
- Š Clearly set out any manually performed calculations which should be **checked** by a second officer.
- Š Make sure that officers who perform calculations or who input data to a computer system can be **easily identified**. Copies of all outgoing correspondence should be **traceable** to the originating officer.
- Š Send **guidance** to potential claimants explaining the systems, their **responsibilities**, what they can expect from the system and the **penalties** for trying to abuse it.
- Š Ensure **appropriate levels** of liaison with other **public** and **private sector** organisations (particularly to check application data and avoid making payments where the payment of other grants mean that claimants are not entitled to them).

Conclusion

A wide range of grants, benefits, allowances and subsidy payments are made to individuals and organisations through a variety of government agencies. The paying of grants is a **difficult area to control** as most frauds of this type involve claimant dishonesty. Part of the reason many frauds succeed is because the systems involved are not managed and controlled in an appropriate manner. The large number of conditions relating to some grants, frequent changes in legislation and the introduction of new grants add pressure to staff responsible for processing claims. However, it is possible to put into operation a number of **key controls** which are both **detective and preventive** including clear guidance to both claimants and staff, segregation of duties, appropriate delegation of authorities, close supervision, management checks, auditable documentation and liaison with other relevant agencies.

10 Estates management fraud

Introduction

Estates management is an area where a number of significant frauds have occurred in the past and organisations with large property portfolios are particularly vulnerable to the risk of this type of fraud. This casenote is not based on a specific fraud but on the lessons learnt from the NAO's review of "the Risk of Fraud in Property Management"¹ in the MOD. The control weaknesses below are based on those noted in the NAO report; the key control lessons are based on MOD's response to it.

Control weaknesses

The following control weaknesses were noted by NAO during their investigation of property management systems in the MOD.

- Ø The department's anti-fraud policy had not been communicated formally to contractors. They were not always aware of their responsibilities for compliance with the policy.
- Ø There was no coherent strategy for communicating and implementing the department's anti-fraud policy.
- Ø Complicated organisation responsibilities for fraud reporting and investigation made it difficult to discern the roles of the various fraud units and to share experience in this specialised area.
- Ø Small teams in the department had attempted to counter fraud but the fragmented approach had not achieved a high degree of success.
- Ø Contractual arrangements did not make clear the responsibilities of contractors who carried out, managed and monitored property management work to protect the department from fraud.
- Ø Guidance had not been provided in the way important controls (such as inspections of work) should have been operated.
- Ø Sample checks by property management staff were applied less frequently than required.
- Ø Standard checks, such as checking work invoiced under term contracts to standard rates, were not being applied.
- Ø Check results were not always followed up (e.g. significant differences between works estimates and values tendered).
- Ø Not all property management staff understood the purpose of the various controls or how controls should be operated to provide the necessary assurance.

¹ http://www.nao.org.uk/publications/nao_reports/9900469.pdf

- Ø The department's arrangements for reporting suspicions of fraud were not clear, as there were a number of potential avenues for reporting fraud.
- Ø The department had not started to explore the data they possessed to identify patterns and relationships in property management expenditure. Also, there were gaps in the data held and difficulties in extracting and analysing relevant data and in making comparisons between establishments.
- Ø The department did not hold information on the total losses they were pursuing nor on the cost and nature of the various investigations.
- Ø Central information on suspected fraud was weak. Also, because there was no defined strategy and associated targets, there were no performance indicators either.
- Ø Lack of information also hindered the networking of experiences between various stakeholders within and outside the department.
- Ø A high proportion (about 20%) of property managers had not attended any fraud awareness training. About 50% of property managers had not received any fraud awareness training in the two years prior to NAO's review.

Key control lessons

- Ø Establish a **High Level Fraud Prevention Steering Group**, chaired by the Chief Executive, Defence Estates, with members from all Top Level Budget Holders (TLBs) to develop and agree Fraud Prevention Policy implementation across MOD.
- Ø Establish a central database for storing data about suspected or actual fraud, which can be used for reporting to management, details about the level of fraud or progress on major investigations.
- Ø Create a **central focus for fraud** (e.g. a team of experts) with responsibilities that include:
 - § Developing a fraud deterrence and detection strategy;
 - § Promoting an on-going fraud awareness programme;
 - § Coordinating the departmental anti-fraud policy;
 - § Investigating fraud;
 - § Collecting and analysing fraud data;
 - § Providing advice to the department on all aspects of fraud.
- Ø Develop a **Fraud Policy** statement which covers:
 - § Recruitment of personnel;
 - § Deterrence and detection;
 - § Developing an anti-fraud culture;
 - § Zero tolerance;
 - § Management responsibilities;
 - § A commitment to prosecute and recover losses;
 - § Encouraging staff to report fraud;
 - § Requires a Fraud Prevention Risk register.
- Ø Communicate the **Fraud Policy** statement to **all staff** and **contractors/suppliers**.

- Ø Introduce a **fraud response plan** that:
 - § Defines line management responsibilities;
 - § Stresses the importance of line management responsibilities;
 - § Defines the responsibilities of individuals;
 - § Creates separation of duties; and
 - § Defines reporting routes;
 - § Contains a Fraud Prevention Risk register (this register can be obtained via Workshops involving all parties to identify Fraud risks).

- Ø Communicate the **Fraud Response Plan** to all **appropriate** staff.

- Ø Introduce improved procedures for dealing with suppliers that:
 - § Commit suppliers to ethical business practices;
 - § Set minimum standards;
 - § Require suppliers to have a fraud prevention statement;
 - § Require suppliers to have a fraud response plan;
 - § Include better performance monitoring;
 - § Clearly define reporting responsibilities;
 - § Establish evaluation thresholds for future business.

- Ø Develop a fraud awareness training programme for all staff and suppliers.

- Ø Produce and circulate **best practice guidance** to **all** staff and suppliers.

- Ø Improve IT fraud investigation techniques and data mining.

- Ø Establish **hotlines** for reporting suspected fraud.

- Ø Introduce risk based works review regimes.

- Ø Carry out **no-notice inspections** (“Blue Sky Inspections”) on a regular basis.

- Ø Develop a property management **risk model** to:
 - § Provide an annual indication of how fraud prevention measures are working;
 - § Identify the key risks in property management;
 - § Assess measures in place to prevent or detect fraud;
 - § Identify actions that can be taken to reduce the risk of fraud.
 - § Allow MOD to target resources effectively;
 - § Identify performance indicators;
 - § Allow MOD to benchmark with others; and
 - § Allow MOD to manage the risk of fraud more effectively.

- Ø Produce risk models for Prime Contracting and other methods of procuring services to ensure Fraud Prevention measures are in place and working.

Conclusion

As a result of the NAO review the MOD took a clear corporate approach to the deterrence and detection of fraud. Hard lessons have been learned but the **published policy** and the overarching **strategy** are in place. The strategy is based on defined responsibilities, the central focus provided by the Defence Fraud Analysis Unit (DFAU) assisted by Defence Estates Fraud Prevention Unit (DE(FPU) and closer working relationships at all levels. It is a basic tenet that **line management at all levels has to have the prime responsibility for deterring and detecting fraud**, but the initiatives of recent years have provided the structure, emphasis, support and change in culture that underpins this responsibility.

11 Overtime fraud

Case description

A routine internal audit highlighted unusually high levels of overtime being paid to a particular group of workers. Three members of the group accounted for over 50% of the total amount of overtime paid and one individual accounted for nearly a quarter of the total. An in-depth investigation into the activities of this one individual identified fraudulent claims totalling more than £15,000, resulted in his dismissal and the recovery of most of the money. A combination of **weak control** and a **failure by management to apply what controls existed** allowed the fraud to be perpetrated. The individual was employed on a team involved in publishing and overtime was sometimes necessary in order to meet publishing deadlines on important Government publications. The overtime was usually worked at publishers' premises and workers were also entitled to claim travelling time.

Other aspects of the case included:

- § The individual recorded the start time of the overtime period as the time he left the office and the time he returned to it. He additionally submitted a separate claim for travelling time so he was, in effect, receiving **double payments** for travel time.
- § Overtime, expense claims and timesheets were submitted to a line manager for approval who **did not scrutinise the data too closely** because the way in which time-sheet data was recorded made it **difficult to reconcile** claims and time –sheets.
- § **Approval to work overtime** was usually given **orally** by line managers in response to oral requests by the perpetrator. The manager simply **trusted the individual's judgement** that overtime was justified. Line managers did not always **know enough about individual jobs** to be able to question whether overtime was necessary or not.
- § Investigations also revealed that overtime was not always recorded against the job on which it was worked. Production officers had performance targets to achieve breakeven on individual jobs so overtime was often recorded against jobs which were under budget.
- § Enquiries with suppliers revealed the perpetrator had not been present on their premises during many of the periods when overtime was claimed.

Control weaknesses

- § Inadequate arrangements for **justifying** the need to work overtime and for seeking **approval** to work it.

- § **Over reliance** on the honesty and integrity of overtime claimants.
- § Lack of adequate **written instructions** relating to overtime working.
- § Badly completed time sheets made **meaningful reconciliations** to overtime claim forms difficult to perform.
- § Lack of effective **management checks** of overtime claim forms when they were submitted for approval.
- § Absence of **management reports** to allow regular monitoring by managers and budget holders of total overtime worked by individuals and teams against individual jobs.

Key Control Lessons

- § Establish a comprehensive set of overtime **rules** and ensure that they are **communicated** to staff.
- § Establish a formal process that involves line managers **approving** and reviewing **work plans** including the need to work overtime.
- § Ensure that overtime claims forms and **supporting documentation** (e.g. time sheets, written authorisation to work overtime etc) are submitted to an appropriate line manager for **authorisation** (e.g. production manager or budget holder).
- § Ensure that line managers only authorise overtime claims when they are **satisfied** that claims properly reflect approved overtime worked, that overtime is recorded correctly against the correct jobs and that overtime claimed is supported by **properly completed timesheets**.
- § Ensure that line managers forward the authorised claim forms and all supporting documentation **direct to accounts payable** for processing and payment.
- § Instruct accounts payable to **check** that overtime claims have been properly authorised and that claims are properly supported.
- § Introduce **random management checks** to verify details on claims and ensure that line manager and accounts payable checks are carried out.
- § Establish **clear budgets** for individual jobs.
- § Provide budget holders with sufficient **information** to enable them to **monitor costs** on individual jobs including overtime costs.
- § Produce **regular** reports that analyse the amount of overtime worked by individuals and teams and require line managers to **review** them.

- š Ensure that claim forms spell out the **responsibilities** of claimants and counter signing officers and that a warning about the **consequences** if fraud is discovered is clearly visible.

Conclusion

Overtime is an area that can, if not properly controlled, contribute significantly to **overspending** on budgets. It is also an area that is very **susceptible to fraud**. Most cases occur because of a **lack of proper control** or because **controls are not applied effectively**.

It is essential that **clear rules** are established and communicated to all staff, that appropriate management **approve** the need to work overtime, that overtime claims are **checked** by managers to meaningful supporting documentation before **authorisation** to pay is given and that budgetary information is **monitored** by managers and budget holders.

An overarching **anti-fraud environment** where fraud is not tolerated and where perpetrators expect to be caught and punished is an important **deterrent**. Any anti-fraud environment should be backed up with a clearly communicated **anti-fraud policy** and **response plan**.