

## Fighting Internal Fraud in Financial Services and Retailing



### Staff Theft: A Growing Problem to Be Managed and Controlled

Businesses of all kinds suffer from thefts by staff. The retail industry has probably been the most highly-researched sector in terms of business crime, but it does not actually suffer most crime and fraud.

Financial services, telecoms, and IT are all more vulnerable to staff fraud than retailing.

If you would like to receive a copy of our Staff Theft Briefing please get in touch (details at the end of the article).

### Greatest Losses from Staff Fraud

1. Banking
2. Insurance
3. Telecommunications (including mobile phone networks)
4. Information Technology and software
5. Retailing and services

The latest figures from PwC show that in 2005 the Banking and Financial Services sector provided 38.2% by value of all fraud cases heard in court.

### How much internal fraud?

Estimates of the amount of fraud in the UK vary wildly. KPMG estimates a little under £1 billion whilst the UK Government estimates it to be £20-£22 billion.

These estimates are not comparing like with like. The KPMG figures relate to court cases. Yet most fraud cases do not come to court, either because they are undiscovered or because the company tries to avoid bad publicity. The Government figures are estimates of fraud, including frauds committed against the state such as tax fraud, housing, and benefits fraud.

**The Centre's own estimate of internal fraud for 2006 is £10-£12 billion.**

This includes theft and fraud:

- **Theft** of employer property, goods, cash and financial assets
- **Fraud**, corruption, false accounting, bribery, collusion, fictitious employees, non-existent suppliers, and the sale of company or customer details to others.

**Internal fraud of between £10-£12 billion represents  
£183 per head for every person in the UK**

### Emerging trends in fraud

Most staff theft and fraud consists of thefts of cash, goods and conventional business assets. These remain the most likely areas of loss.

The most disturbing new influences relate to organised crime, the penetration of call centres, and identity theft.

### Emergent Threats of Staff Fraud

1. Organised crime placing thieves in organisations
2. Corruption of existing employees or threats to induce cooperation
3. Fraud via call centres including CNP (card-not-present) fraud
4. Large-scale theft of personal consumer data and bank and card data

Crime depends on opportunities. When companies put up stronger barriers to fraud, criminals may look elsewhere. Call centres set up by financial and service-oriented businesses are seen as the latest opportunity, particularly with the growth of card-not-present fraud as a result of the success of Chip and PIN in reducing traditional plastic card fraud. Cases have been brought against call-centre employees by HSB, Tesco, Norwich Union and at several financial call centres in India.

Strathclyde Police claim that 10% of Glasgow call centres have been infiltrated by gangs. Whilst this may be an overestimate, it has dramatised a potential problem for businesses that use or own call centres (ie everyone).

***"We know of organised crime groups who are placing people within the call centres so that they can steal customers' data and carry out fraud and money laundering."***

Detective Chief Inspector Derek Robertson, Strathclyde Police

**Perceived anonymity in call or contact centres helps otherwise honest people feel they can cheat and steal without being found out.**



### Perceptions and reality

A majority of people who think they can enrich themselves with little risk will give in to temptations.

The retail sector, which apprehends more staff fraudsters than any other single business sector (26,000 in 2005), knows that anybody and everybody will steal, given an opportunity.

Whilst burglars, robbers, muggers and shoplifters may conform to certain low-life

'types', the person committing staff fraud is often white, male and better educated. He or she may often be the most committed and high-achieving person, with a good knowledge of company procedures and IT systems, and may work long hours often with little supervision. He or she may adopt a better lifestyle than one might expect (a 'small lottery win' or 'inheritance'), a better car ('why has the junior accountant got the best car in the car park?'), holidays to exotic destinations and generosity to friends and family. Alternatively there may be a costly divorce or an expensive drugs or gambling habit which soaks up the cash.

### **The hole in the middle of the staff fraud doughnut**

If one or several thieves steal £40,000 in a complex way they may find that nothing much happens to them. The case is too small for the Fraud Squad, which only deals with £¼ million or more. It may be too difficult to understand for the DC or a jury (particularly if several possible crooks are involved) so the Crown may well decide not to prosecute. So if your business has lost something like £100,000 that can just be tough luck.

### **Closing the fraud loopholes**

Fraud control is not simply about buying the latest technology and having an active policy of informing the police.

It has to be based on:

- Identifying the key problem areas
- Spotting discrepancies early and taking remedial action
- Loss prevention marketing
- Loss-prevention policies and procedures
- Focused security products

### **Watch the managers**

Our own study of retailing found that one-quarter of frauds are committed by supervisors, managers or security staff. The most trusted staff, the people having access to keys, accounts files and IT systems have the greatest opportunity to steal. When they do steal they can rapidly become prolific offenders.

### **Types of Staff Thief**

The Chancer	Many use their computer skills to test the system - or they may simply press the wrong key. If nothing happens and no one checks up, then they have found a new way to steal from the company.
The Collaborator	Within a month of joining, the right sort of new staff member may be inducted in several ways of stealing or invited to join a theft group
The Rolling Stone	The recidivist changes jobs frequently and has left before his frauds are discovered
The Insider	A criminal gang may recruit an existing member of staff or place one of their own within the business to find out how the systems work, get access codes and passwords.

### **Support from The Centre for Retail Research**

The Centre produces quarterly Staff Theft Briefings. If you would like to receive one

free of charge please get in touch (as follows) giving your name and address.

- [research@retailresearch.org](mailto:research@retailresearch.org)
- Centre for Retail Research, 20 Fletcher Gate, Nottingham NG1 2FZ
- Telephone 0115 983 8752

The Centre has considerable experience in analysing and dealing with internal fraud problems. If you would like to meet for an outline discussion, please get in touch at [research@retailresearch.org](mailto:research@retailresearch.org) or 0115 983 8752