

# Resist and Repel: The Experian Insider Fraud Dossier

An Experian white paper

---





# Introduction

Insider fraud is an issue that affects almost all organisations. While, for many, the problem may be isolated to an employee having exaggerated his qualifications to obtain a role, or infrequent cases of expenses fiddling, there are growing numbers of organisations whose assets increasingly make them a target for fraudsters.

This report, which examines the issues surrounding frauds committed by an organisation's employees and other 'insiders', provides a basis for understanding the nature of insider fraud, how it affects organisations and what they can do to discourage, prevent and detect it.

When discussing insider fraud, it is first important to understand what precisely is meant. Experian's definition is essentially theft of an organisation's assets by those the organisation has placed in a position of trust. Although most frequently this will be employees, the term also covers offences committed by other insiders, such as contractors, partners and suppliers. Assets include actual physical property, such as computers and stationary, but also money, data and intellectual property.

Collating meaningful data on the subject of insider fraud is a significant problem. There is no regulated body that collates insider fraud data or insists on cases being reported to the police, and many organisations decide not to instigate criminal proceedings given the heavier burden of proof required to

secure a conviction and a desire to avoid damage to its reputation, which could, in turn, affect trading and/or share price.

A study by KPMG in 2006 established a figure of more than £650 million stolen through fraud at British companies in the first six months of the year. However, it is very difficult to evaluate the losses associated with insider fraud, either that the organisations are aware of, or the likely majority that are still currently going undetected.

The evidence is largely anecdotal. A number of organisations have assisted Experian in compiling this report, by sharing their experiences, case studies and modus operandi, and we express our gratitude to them. They did not wish, or were unable, to provide statistics, and were not willing to be identified.

What can be said with absolute certainty is that insider fraud has the potential to be very damaging. In its February 2006 report entitled Firm's High-Level Management of Fraud Risk, the Financial Services Authority revealed that insider fraud,

whether arising from collusion, coercion, infiltration or existing employee action, was cited by financial institutions as one of the most serious threats they face today.

The City of London Police recently revealed that 35 per cent of its work now involved "some insider element", compared with about ten per cent in the late 1990s. While it is difficult to put a value on it, insider fraud represents a clear and present danger to UK organisations.

---

**it is very difficult to evaluate the losses associated with insider fraud, either that the organisations are aware of, or the likely majority that are still currently going undetected.**

---

# Nature of the beast

## Changing times

Over recent years, the UK has seen the demise of its manufacturing base as financial services and retail sectors have exploded. While, for some, this has brought tremendous wealth, for many people, potential 'jobs for life' have been replaced with less secure, low paid, transitory work. Employees, faced with organisations that continually aim to cut costs while increasing productivity, do not exhibit the same levels of trust and loyalty that once existed. While this, in and of itself, does not account for increasing levels of insider fraud, it does help to provide a motive for individuals looking to take back from their employers.

Linked to this, insider fraud is no longer limited to employees stealing money and goods from the workplace. Changes in technology are bringing new possibilities for fraudsters. With identity theft on the increase, data is worth money and, given the growth in contact and call centres, there exists in the UK a multitude of mass-data repositories, providing an array of targets for the organised fraudster.

## Who is responsible?

Insider fraud can originate in a number of areas from within an organisation, and from a range of different types of people. While many of those responsible are individual opportunists, improvements in anti-fraud measures designed to protect organisations from external threats

have pushed an organised criminal element to consider new options and approaches. These include convincing or coercing existing employees to act on their behalf, or infiltrating the organisation with an 'inside man'.

During 2003, CIFAS research with 127 organisations revealed only two that claimed not to have experienced insider fraud, and the largest organisations were typically dismissing over 100 employees a year for offences of this nature. Over 60 per cent of respondents reported that the frauds they had uncovered involved collusion with people outside the company.

## Recruiting a mole

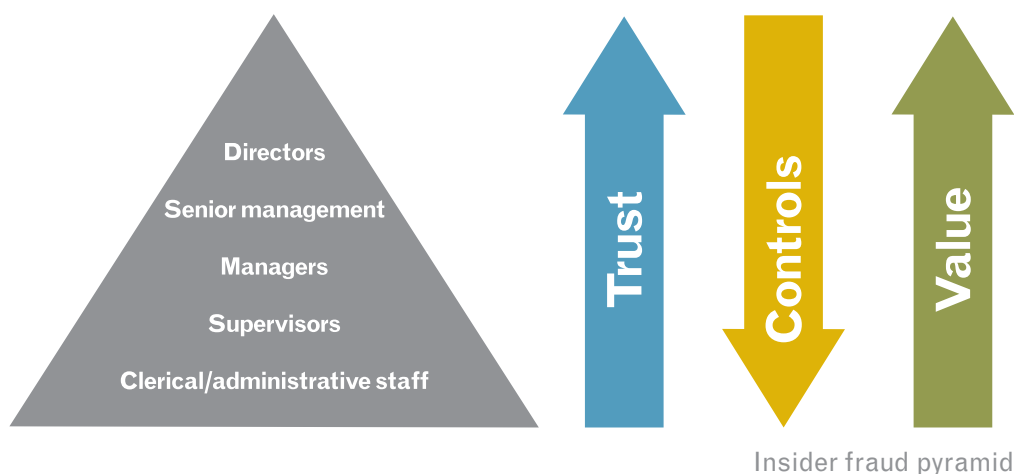
Despite the best company security systems, criminals will find the weakest link, which more often than not is a person. Criminals have been known to hang around pubs and cafes near target organisations seeking disgruntled employees, while 'smoke free' legislation has had the unfortunate effect of providing gangs with the opportunity to target staff taking cigarette breaks on the street.

Once targeted, the gangs will then attempt to bully or bribe employees to give up sensitive data that could be used to steal money. Threats of violence or blackmail may be extended to employees and their families if the orders of the gangs are not undertaken. Large operational centres, such as data processing and call centres, use a high

number of temporary and permanent staff. Often young, impressionable and low paid individuals, these are high risk personnel deemed most likely to turn 'staff fraudster'.

Valuable insight passed to Experian by a major UK bank sheds additional light on the types of person most likely to be detected and dismissed for committing insider fraud. The bank profiled the cases of insider fraud it discovered between January 2005 to April 2006 to identify high risk areas. Although there was little difference between the sexes, just over half of employees (51%) dismissed had been with the bank for less than a year and a quarter between one and two years. Almost four in every five employees (78%) dismissed were under the age of 30. 20% were under 20, 36% aged 21 - 25, and 22% aged 26 - 30. Only 4% of those dismissed were more than 41 years old.

Insight gained from another UK retail bank that had sought Experian's assistance revealed that the main type of insider fraud occurred at the branch level, where employees had been able to dip into customer accounts. The bank had a specialist department to investigate all employee fraud, irrespective of the value, and it was the policy of this particular bank to prosecute all frauds as a criminal offence where the evidence was sufficient to do so. The average loss per insider fraud case was £40,000, and the bank has insurance in place



for losses in excess of £5,000. Of the reported fraud in the six months from April 2006, 59 per cent of cases were branch related. 15 members of staff were dismissed, five resigned pending disciplinary action and five were given a warning. In four cases no further action was taken against the employees as no case could be proved. Four offers of employment were revoked.

When it comes to operational centres, there are many fraud detection controls in place. It is not unusual for telephone conversations to be recorded and computer logging systems show all accounts that have been reviewed and amended. CCTV often monitors employees at all times. Those new to the business world are often unaware of the controls in place and are easy to detect once frauds start to emerge. The criminal gangs know this and seek new employees in the first few months before they become aware of the audit controls in place. Subsequently, they also ensure they keep their distance in the eventuality that the frauds will be detected.

### Moving up the pyramid

However, it is not just those on low grades that commit frauds. The pyramid of an organisation, which puts management above and superior to other staff, leaves a business exposed to additional forms of insider fraud. This threat includes senior level employees, who fall outside the realms

of the controls in place to monitor 'high risk' personnel and, while data may be the target for fraudster operating at lower levels, there are sizable sums of money that can be obtained by the corrupt at management level.

Police have spoken of investigating a wide range of insider fraud, from instances of organised criminals planting temporary workers in low positions to steal account information, to high ranking executives like financial controllers stealing hundreds of thousands of pounds.

Senior personnel who deal with external suppliers, procurement and acquisitions have greater opportunities and a lower risk of detection as the focus in most organisations is elsewhere.

Frauds more commonly committed by more senior personnel within organisations include:

- Setting up false suppliers to purchase goods and services that are over-priced or never received
- Sanctioning contracts to companies for goods and services in exchange for kickbacks
- Embezzlement of company funds
- False cheque/electronic payments
- Placing fictitious staff on the payroll
- Falsifying sales figures to increase bonus payments
- Moving funds from dormant /clients' accounts

### Insider fraud in practice

Experian recently learned about a case that involved a senior accounts clerk who had been with his employer, the UK subsidiary of a large US corporation, since leaving school more than twenty years previously. Over a 15 year period, the employee forged invoices from genuine suppliers, for which payments were made directly to himself or his wife; used his company credit card to make unauthorised purchases for himself and his family; and made random payments to himself, coded as salary or expenses claims, to which he was not entitled. In a position of trust, the employee was able to hide his frauds as seemingly valid expenses on the company books. His crimes were only discovered when the company changed its auditors, and a detailed investigation into historic records revealed that the employee had stolen over £2 million over the 15 years. Although the employee was dismissed and company lawyers obtained a freezing order for over £1.78 million of his assets, the police were not called in.

## Case Study 1

A credit card issuer had 60 cards stolen, with losses of around £450,000. Cards destined for overseas had been despatched but returned to the card issuer. The wrong coding on the envelopes had resulted in insufficient postage being paid. The investigation identified a junior member of staff dealing with the returned mail, keeping the cards and passing them on externally. Secondary ID was obtained to support cards presented for large value transactions, mostly for use at foreign currency/exchange bureaux. The employee was identified, arrested and charged.

It later transpired that the employee had been recruited from a London nightclub. Six further individuals were arrested. Three custodial sentences and three community service orders were imposed. Two family homes were identified and subjected to a confiscation order under the proceeds of crime. In addition to prison sentences, court orders were made for two defendants to pay around £45,000 within six months or face a further six months in jail.

# Solving the problem

As we have already discussed, insider fraud is a growing concern for organisations of all sizes and in all sectors. However, it is large companies operating in key industries such as finance and insurance that are the prime targets for organised criminals. Companies with significant data assets are more at risk from insider fraud than ever before, and when you consider that such organisations often run large contact centres employing predominantly young and low paid workers, it should not come as too much of a surprise where organised criminals look to find their next insider.

Although financial losses from fraud are damaging, the potential harm that an internal data compromise can do to any organisation's reputation is significant, especially when that data is of a personal or financial nature.

## Don't wait to protect yourself

Experian believes that organisations should not wait for legislation or a security breach to take action; this is shutting the stable door after the horse has bolted. Companies must take it upon themselves to protect their assets and reputation by assessing the risks to their business and putting in place robust anti-fraud policies and protection that cover every eventuality.

The best place to stop insider fraud is at the recruitment stage. The process

should start right at the outset, and continue through ongoing monitoring and the ability to share information when something does go wrong in order to prevent the same person re-offending elsewhere.

## Policies and procedures

Key to effective anti-insider fraud deterrents is having in place robust policies and procedures to minimise their exposure. Organisations should identify the key roles and highest risk areas for the most intense scrutiny; enhance recruitment processes; strengthen security controls; and put in place trusted whistle-blowing procedures.

Having said this, organisations should take a very public stance on the tools they have available to them to monitor and detect inappropriate activities. It is often argued that the point of a speed camera is to slow the traffic rather than to catch the offenders. Using this principle, and given that in many environments, it is the young and naïve who are most likely to commit insider fraud, it is wise to use the systems as a deterrent.

Thorough checks are absolutely vital, not only to verify that the person is able to perform the role they have applied for, but also to ensure they are actually who they say they are. When taking on a new employee, the authentication of the individual's

identity using electronic data sources can provide a more robust measure than forgeable paper-based proofs of identity. If you do not establish the true identity and any alias names used, then further checks to other sources such as the Criminal Records bureau may return a negative return as no fuzzy logic is applied.

Discrepancies and falsehoods on CVs and job applications need to be uncovered to ensure that only the right people gain employment. If a person is willing to deceive on a CV, then they do not possess the integrity that most employers would expect as standard.

## Catching the CV cheats

As best practice, the right questions need to be asked at this early stage so the information gathered is sufficient for the highest level of checks to be carried out. Most CVs contain the same basic data – personal details, educational information and qualifications, employment history and references.

Signed authority should be sought from the candidate for financial checks and criminal records disclosures. In addition, there should be a question relating to unspent convictions; if the question is not asked at the outset, it is difficult to deal with the issue should it later be found that there are outstanding convictions.

All information on the applicant's CV should be thoroughly checked to verify its accuracy. Employment history, including dates, should be confirmed to identify any gaps. Qualifications should be checked with educational bodies, where possible, to avoid the reliance on documents as these cannot always be confirmed as genuine.

Backgroundchecking.com, which is part of the Experian Group, offers a range of background checking services to organisations. It checks thousands of CV every week. From its analysis it has found that 28 per cent of CVs contain inaccuracies, and two per cent are pure fiction.

Most companies are reliant on criminal records alone to check for unsuitable employee. The main problem here is that relying on criminal record checks alone can still result in fraudsters being employed as it fails to pick up on discrepancies and inconsistencies in other areas on the CV. The overwhelming majority of individuals picked up for committing insider fraud do not have previous criminal records, and many organisations do not pursue a criminal conviction of fraudsters they have dismissed due to the greater burden of proof required.

A further drawback is that organisations relying on this method alone often run criminal record

checks on applicants for positions that don't necessarily need them. For many, a simple verification that the CV is a true and accurate indication of their backgrounds would suffice. Monitoring and assessment of individuals should not finish once they have been accepted into an organisation. Further assessments and checks can be performed when staff are promoted or moved to more sensitive areas.

### Early warning signs

There are a number of early warning signs that may be indicators of staff fraud. These should be considered as part of an effective monitoring system:

- Employees living beyond their means. Are there clear signs of wealth not in line with salary?
- Employees under financial pressure. Drug, alcohol and gambling addictions can put people in financial difficulty and in touch with the wrong crowd?
- Employees continually working late and not wanting time off. This could be an indication that they do not want anything to be exposed.
- Employees not wanting to change jobs. This could be a sign of kickbacks, fiddling or exposure to illegal activity if the position is vacated.

The most recent development in the fight against insider fraud is the ability to compare and contrast

CVs and applications against a database of other CVs, employment records and previous known frauds. Data mining for falsehoods and inconsistencies is more likely to show up the potential fraudster than any other means.

### Summary

Organisations should take a risk based approach to vetting potential employees. Putting best working practice in place right at the point of application ensures that they will continue to recruit quality employees who are who they say they are and are suitably qualified for the job. Approaching this stage in the appropriate manner aids operational risk compliance and minimises internal and external liabilities.

## Case Study 2

A high street bank received a number of customer accounts on unauthorised bill payments. The investigation identified a number of accounts being compromised, with fraudulent transfers to student accounts. The students had been recruited to accept bill payments into their accounts, by fraudsters who used a number of reasons for needing to do this, the favourite being they had no bank account to receive their student grants. On receipt of the funds into their accounts, they would be taken shopping to obtain goods/cash.

A common link on the accounts, the point of compromise, was identified by the bank as a major insurance company. The insurance company was holding personal bank details to

collect payment and to send insurance credits and payouts.

The initial police investigation highlighted problems in the insurance company's audit trails – in particular, no system was in place to see who had viewed accounts. The decision had been made that this slowed down response time and the benefits outweighed the risk. Subsequently, the switch was placed on and a staff member identified and arrested. Evidence found suggested that data from a number of high street banks had been compromised. The students who had been duped into assisting the fraudsters themselves became victims, as the payments were subsequently reversed from their accounts, leaving them with the debt.

# Insider Fraud Typologies

## CV manipulation

Misrepresentation on job applications. This could include undisclosed addresses, previous jobs held, criminal convictions, exam results or even an inflated salary. Recent consumer research by Backgroundchecking.com, an Experian company, revealed that more than 20 per cent of respondents would consider falsifying the salary level on their CV

## Accounts payable/procurement

Payments made for goods from bogus companies that are then not received. Paying inflated prices for goods, with the staff member getting a 'kick back' in the form of cash, free lunches, holidays, etc.

## Expenses

Fiddling of time sheets, mileage and expense claims

## Bonus payments

Inflated sales or performance statistics to ensure a cash bonus. One contract may be double charged in conjunction with other staff member

## Bribery & corruption

Corrupt practices to win sales orders, promotions to engage in unfair competition, acquisitions in return for cash payback

## Blackmail

Using information held on individuals to force them to undertake orders

## Data compromise

Personnel or company data (with or without a monetary value) stolen and given away

## Infiltration / moles

People working within organisations to learn company policies and procedures, products and designs

## Theft

Stealing of goods, money or any asset with a monetary value

## Overriding systems / decisions

Sanctioning of new accounts or credit limits which would otherwise have been declined

# Experian Fraud & Identity Solutions

## An end-to-end approach to combating fraud

Experian provides a suite of services to help prevent organisations suffering the damaging effects of insider fraud throughout the entire employee life cycle:

- To assess the identity of new applicants / employees
- To identify potential 'high risk' applicants'
- To enable periodic assessment of employees
- To enable sharing of 'suffered' fraud in order to prevent re-occurrence
- Background check, pre employment, Criminal Records Checks

Experian's leading Authentication solutions – which harness the power of our vast consumer data assets – can provide a simple and cost effective way of conducting electronic identity checks.

Our BackgroundChecking.com service offers a comprehensive range of bespoke background checking solutions which can be infinitely tailored to meet the unique needs of any business in any industry.

Experian can also record and make available the outcome of known insider fraud. This will ensure that dismissed staff are not unknowingly employed in similar positions elsewhere. This capability can be provided through the sharing of insider fraud data by organisations within closed user groups.

---

**To find out more about Experian's fraud solutions, please speak to your Experian Account Manager or call the Fraud Consultancy team on 0115 992 2962.**

---

Talbot House  
Talbot Street  
Nottingham  
NG80 1TH  
[www.experian.co.uk](http://www.experian.co.uk)

