



Crime Papers from AIG UK:

**Fraud and Occupational Crime
A Serious Global Threat: Understanding the Risk**

and

**Reasons to Buy Crime Insurance: Fraud and
Occupational Crime, Real Business Issues**

Dec 2007

AIG The power in business insurance



Fraud and Occupational Crime

A Serious Global Threat: Understanding the Risk

Contents

- Crimes—A Serious Threat to Corporations
- Why Is Fraud & Occupational Crime on the Rise?
- Types of Fraud
- Means of Concealment
- Where Does the Money Go?
- Minimizing Fraud & Occupational Crime
- Why Buy Insurance?
- What to Do When Fraud Is Discovered?
- A Final Note

"The man who is admired for the ingenuity of his larceny is almost always rediscovering some earlier form of fraud. The basic forms are all known, have all been practiced. The manners of capitalism improve. The morals may not."

John Kenneth Galbraith



Crime – A Serious Threat to Corporations

Despite all that has been and is being done by governments, financial institutions, commercial entities, crime prevention agencies, insurers, and other organisations to prevent crime, statistics show that crime is on the increase not only in terms of the numbers and size of individual cases, but also in the overall costs to victims, and in the degree of technical sophistication of the underlying modus operandi. In a recent survey of 3,600 companies in 50 countries, economic crime was shown to have markedly increased from 2001. In Europe alone, crime rose an average of nearly 8%¹. In the U.S., estimates peg fraud-related losses at 6% of an organisation's annual revenue, translating into approximately \$660 billion in total annual losses.²

Throughout the world, there is a widely held misconception that "white collar" crimes are not as serious as those involving physical violence as they are merely "economic" in character. Unfortunately, this prevailing attitude can diminish the desire of corporations to institute preventive measures designed to protect themselves, and also impedes the focus, scope and resources that law enforcement agencies dedicate to investigate such crimes.

More importantly, the rates of recovery of money or goods lost as a result of crime are generally poor even when the perpetrators are caught and brought to justice. When they are not, it is nearly impossible to secure any meaningful recovery.

It is common for frauds, particularly those involving senior members of staff, to remain undetected for a long time, sometimes years. In some cases, losses approach a magnitude that actually threatens the financial stability of a company and causes severe business disruption. Inevitably, a considerable amount of unproductive management time is required to mitigate such losses, to oversee and assist the investigations by law enforcement authorities, to handle the resultant insurance claim or claims, and in some circumstances, to support a criminal action. Unfortunately, the damage to the victimized company's reputation, brand image, and morale can be even more severe than the actual financial loss sustained.

Recoveries after fraud tend to be low. Over 60% of victims of crime said they had recovered less than 20% of their losses.³

This document focuses on the business impact of fraud and occupational crime. The issues raised are of immediate concern to those individuals charged with safekeeping the assets of their organisations. It is our intent to provide a better understanding of the problems associated with crime, their potential consequences, and the measures that can be undertaken to help mitigate their effect.



Why Is Fraud & Occupational Crime on the Rise?

Some commentators argue that the increase in white collar crime reflects a widening disparity in wealth distribution, declines in moral standards, and an overall complacency and acceptance of greed, which has manifested itself most recently in the breakdown of corporate governance. Others suggest that crimes of this nature are perceived as victimless, particularly in larger firms where the monetary cost of the fraud is not viewed as jeopardizing such entity's financial resources. Whatever the perception may be, the type of crimes discussed in this report continue to grow, at least partly due to the increasing complexity of organisations and transactions, a historic lack of focus, outdated and ineffective internal controls, overly aggressive accounting practices, increasingly transient employees and a general acceptance of some level of fraud as a "cost of doing business".⁴

Compounding the above problems is the fact that detection, arrest and conviction rates for such crimes are relatively low. Police and judicial authorities frequently lack the financial, technical and physical resources to match those of the perpetrators. In many of the less developed areas of the world, the police and judicial authorities are without the expertise necessary to investigate even relatively uncomplicated frauds. The ability of criminals to move swiftly between jurisdictions, the ineffectiveness of money laundering statutes, and the difficulty, expense and time involved in asset tracing are all other key factors which negatively influence loss recoveries.

In many frauds, the victims do not even suspect upon discovery of a loss that the perpetrator was actually part of their organisation. ***Eighty-five percent of fraudsters are on the payroll with 55% coming from the ranks of management.***⁵ Management is often ill prepared for the actions that should be taken. The legal costs to obtain injunctions, freezing orders, and arrest warrants, or to undertake extradition proceedings and other remedies are substantial. Even when a remedial action is taken as expeditiously as possible, it may not be soon enough to apprehend the perpetrators or to prevent the disappearance of the stolen funds or property.

Losses by managers and executives are 16 times greater than those caused by non-managerial employees.⁶

Unfortunately, fraud protection measures frequently lag behind other advances in business technology. Failure to implement, regularly review, and update security systems renders companies of every size vulnerable to attack. Although loss prevention techniques are constantly improving in an attempt to keep pace with criminals, it is easy for management to become complacent and underestimate the risks of being defrauded, and the subsequent detrimental effects this can have on a company.



Types of Fraud

A company can be defrauded by insiders (i.e., its own directors and/or employees), outsiders, or a combination of both through collusion. Although there are countless crime schemes, the principal categories are as follows:

- **Skimming:** Diversion of funds (either cash or cheques) belonging to a company, prior to the recording of such funds in the company's accounts (e.g., customer's payment directly into the hands of a company's employee).
- **Embezzlement:** Diversion of funds, assets or stock from the organisation coffers either in the form of cash or cheques or by raiding bank accounts.
- **Cheque/bank transfer tampering:** Perpetrated by persons having access to the organisation's cheque books or electronic banking systems and bank statements. Such frauds include forged signatures/transfer approvals, altered payees, or payments into a new account opened by the individual committing the fraud in the same name as the genuine payee.
- **False invoicing:** Perhaps the most common type of insider fraud is procurement operations consisting of an arrangement of excessive payments for goods or services purchased for the company in return for kickbacks (which can also be in the form of payments to complicit entities for phantom goods or services) from cooperative suppliers. An employee may deliberately make mistakes on legitimate payments (e.g. pay more than is due, pay twice, or pay the wrong entity) and request the recipients to rectify the error by means of a refund cheque, which is then diverted. The same modus operandi can be applied to companies with physical assets. The opportunities for this kind of abuse are extensive. Such frauds can vary enormously and are often schemes that are elaborate and accordingly difficult to detect.
- **Payroll fraud:** These are similar to procurement frauds inasmuch as the fraudster is instrumental in having the company pay for work that has not been performed. Examples of such fraud include "ghost pay-rolling", falsified time worked, and commission schemes involving fictitious sales or altered commission rates.
- **Expenses Schemes:** In these frauds, the culprit either misclassifies, overstates, duplicates or claims fictitious expenses.
- **Stock and Physical Assets:** Misuse or misappropriation of company property (e.g. premises, vehicles, supplies, equipment or computers and also theft of stock).



- **Bribery and Corruption:** Collusion between vendors and employees either by inflated invoicing by the vendor in return for kickbacks to the conspiring employee, or “bid-rigging” (i.e., the pre-arrangement of a bid to particular vendor instead of to the lowest bidder). Bribes may be disguised as “consultants’ fees” in which the consultants act as conduits for channelling the funds, less a nominal handling commission, back to the company official.

Means of Concealment

“Teeming and lading” or “lapping” are means to conceal earlier thefts with subsequent ones (e.g., stealing a customer’s payment and then using a subsequent payment to cover the previous customer’s account). The overlapping payments create a “float” of money that can be used as long as all payments are eventually posted. Usually the process builds like a pyramid until it falls apart when not enough payments are available to cover the amounts owed.

Where Does the Money Go?

The uses of the fraudulently secured funds are as varied as the individuals who perpetrate the underlying thefts. Gambling is probably the most common end-result of such ill-gotten gains. The range of gambling activity runs the gamut from simple horserace and casino betting to “playing” the financial markets and indices to investing in more elaborate, get-rich-quick schemes. The culprits almost invariably protest that their intention was only to “borrow” the money, with the stated intention to eventually repay such amounts. Not surprisingly, the only data available in respect of these losses occurs in circumstances in which the offender has not repaid the money. It is possible (albeit rare) that on some occasions, the “investments” have been lucrative, the original funds returned and the theft never detected.

Unfortunately, the guilty party can amass significant sums of money (initially hundreds of thousands which can rise into millions of pounds) undertaking the above-highlighted schemes within a short period of time. Several studies additionally support the premise that the individual undertaking the fraudulent activity is normally a first-time offender, making it difficult to rely on sound hiring practices to eliminate this threat. The Association of Certified Examiners’ 2004 Occupational Fraud Report supported this conclusion by stating that less than 12% of white-collar criminals possessed a previous conviction for a fraud-related offence.



Minimizing Fraud & Occupational Crime

Fraud and economic crime is a serious problem that cannot be eradicated. As such, the most prudent and cost effective manner to address this issue involves taking such measures necessary to mitigate its potential effect on your business. These measures include: (i) recognizing that fraud is endemic in business, (ii) dedicating the time and resources necessary to deal with this increasing problem; and (iii) remaining pro-active in your approach to evaluating and implementing those processes and systems which minimise temptation and highlight early detection (i.e. removing opportunity is the best defence).

“He who does not prevent a crime when he can, encourages it...”

Lucius Annæus Seneca

Prudent management will also develop and promote, throughout the organisation, a culture of awareness concerning this threat and reiterate the constant need to be watchful and focused of the associated risks. Many frauds perpetrated over an extended period of time, and resulting in some of the largest losses, are committed by trusted senior executives. Remaining mindful of this fact when creating effective controls and procedures is a key element in implementing a successful strategy to minimize fraud and occupational crime.

- **Create a Code of Conduct** that covers such areas as conflicts of interest, third-party gifts and disclosure of confidential information, and which requires all members of staff irrespective of seniority to sign and abide by such Code of Conduct. On a similar note, that describes the duties of each grade of employee and the accompanying requirements draft and implement a Procedures Manual to comply with such procedures. Ensure that prevention of insider fraud is a topic for regular discussion and review by senior management.

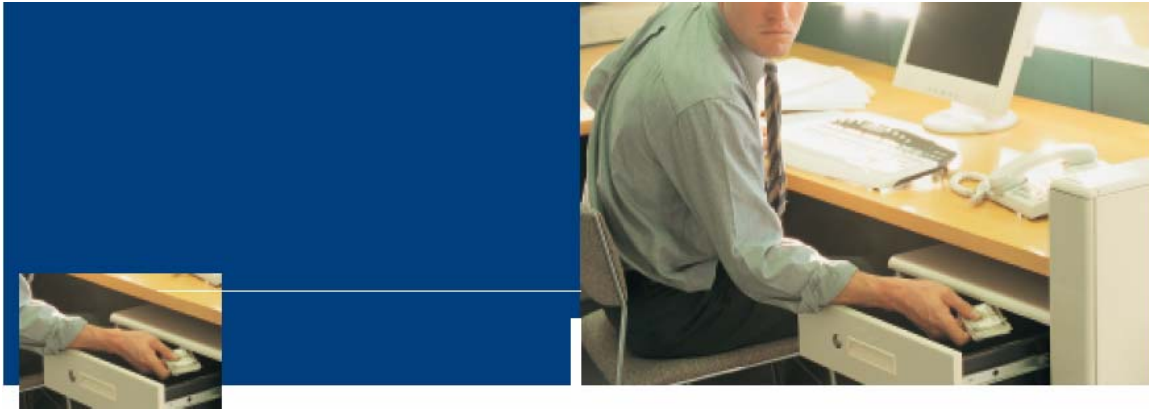
- **Appoint a senior official** to be responsible for insider fraud prevention. This individual should have experience in the field of fraud prevention or receive fraud prevention training. Membership of anti-fraud organisations should also be encouraged as well as regular cooperation and liaison with officials in other companies in the same lines of business. Ensure that the Head of Internal Audit reports directly to the Board to avoid filtering of information that could potentially conceal a fraud.

- **Implement a program of fraud-awareness training** in order to highlight common trends in fraud and to inform staff of losses that other companies have suffered. The dissemination of information describing the



potential cost of fraud to the company, how it manifests itself and how such fraud can be prevented and detected is instrumental in promoting a corporate "anti-fraud culture". If implemented successfully, fewer people will be tempted to commit fraud if only because they will be aware that their colleagues are alert to the dangers that insider crimes present to the company and possibly to their own livelihoods. Staff should also be encouraged to question and discuss any irregularities they perceive or concerns they may have and have clearly defined access to the audit and compliance department

- ***Install a free-to-call fraud "hotline"*** for all employees to use on an anonymous and confidential basis to report suspicious activity they observe or to voice concerns they wish to raise.
- ***Implement segregation of duties (i.e., dual control procedures)*** so that no one person is permitted to control a transaction from beginning to end. The Procedures Manual should be drafted so as to ensure that this principle is prescribed for all procedures.
- ***Ensure that reconciliation of bank statements is conducted regularly*** and by persons other than those responsible for effecting banking transactions. Surprise checks and internal audits of those departments responsible for the management of the company's assets should be performed on a periodic basis.
- ***In critical areas, implement a practice of short term job rotation and ensure that employees take vacations of at least one full week*** (preferably two consecutive weeks) once a year during which time their duties are carried out by someone else.
- ***Install software systems that require users to change their passwords at regular intervals.***
Allowing employees access to another employee's password should be a disciplinary offence, as should the actual use of other persons' passwords. Implement procedures to ensure that passwords are withdrawn automatically when an employee's service is terminated or when password access is no longer required for an individual.
- ***Fraud procedures should specify a process for vetting vendors and suppliers*** to include the invitation of prospective suppliers to tender in order to promote competition and avoid improper relationships with third parties. All payments to vendors and suppliers should be supported by original invoices that are marked "paid" at the time of payment.
- ***Avoid placing too much trust in individuals during times of administrative upheavals***, such as those that occur in the start-up phase and both during and after mergers and acquisitions. Extra vigilance is required for those businesses as they are especially susceptible to fraud during these times.



Why Buy Insurance?

Crime insurance with adequate limits from an experienced and financially sound entity is one of the best means of protecting a company against a catastrophic crime loss. Fraud pervades all entities and crime insurance is as essential as any other policy purchased to protect a company's physical assets. Purchasing crime coverage should form part of a comprehensive risk management strategy. The benefit of such insurance coverage is well substantiated.

- Research indicated that responding companies who reported having crime insurance policies were three times better placed to recover their losses compared with non-insured companies.⁷
- Insurers work closely with specialists that can review a company's processes, procedures and systems of control. These services can be extremely valuable in helping to uncover vulnerabilities, promote awareness and reduce the potential effects of crime-related loss.
- Corporate governance related legislation puts companies under pressure to demonstrate the implementation of measures to reduce exposures that could impact the company's value to shareholders. Fraud represents a breakdown in internal controls, and companies need to mitigate its impact before sizeable losses result.

Maintaining adequate levels of crime coverage helps to offset the financial burden from such loss and demonstrates management's awareness and recognition of a real and pervasive threat.

What to Do When Fraud Is Discovered?

- ***Notify the police.*** This is not a problem that should be overlooked, rationalized or "swept under the rug". It is important to act quickly in order to put the company in the best position possible to prevent additional loss, mitigate the impact of the event and pursue recovery.
- ***Notify insurers.*** It is a condition of most insurance policies that timely notice is given of any circumstance that could lead to a claim being made under the policy.
- ***Take all reasonable measures to mitigate the loss.*** These steps may include overcoming negative media, reassuring business partners, and addressing employee morale issues.
- ***Take all reasonable measures to recover stolen funds or property.***
- ***Evaluate internal controls and make the necessary changes in order to prevent such activity from recurring.***



The Power In Business Insurance

The member companies of American International Group, Inc. are leading providers of a wide range of innovative insurance products to protect corporate entities from commercial crime losses. This document is intended to raise awareness of the issues and concerns that commercial crime presents to individual businesses, as well as suggest strategies that can form part of a comprehensive approach to mitigate the risk of loss from this peril.

Editors and Contributors

We would like to thank Edward Davies, principal of Verus Adjusters, for his significant contribution, cooperation, and assistance in creating this report. Mr. Davies has been involved in the field of reviewing and investigating fraud and economic crime for over 15 years.

This summary is for general informational purposes only. It should not be construed as legal or other advice of any nature. Should further analysis or explanation of the subject of this summary be required, please seek qualified legal advice. We compiled this summary from sources believed to be reliable. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any summary, representation or comment herein, ©2005 American International Group, Inc. (AIG). All rights reserved.

End Notes

- ¹ PricewaterhouseCoopers – Economic Crime Survey 2003
- ² Association of Certified Fraud Examiners – 2004 Report to the Nation on Occupational Fraud and Abuse
- ³ PricewaterhouseCoopers – Economic Crime Survey 2003
- ⁴ Ernst & Young: Fraud – The Unmanaged Risk (8th Global Survey)
- ⁵ Association of Certified Fraud Examiners – 2004 Report to the Nation on Occupational Fraud and Abuse
- ⁶ Ernst & Young: Fraud – The Unmanaged Risk (8th Global Survey)
- ⁷ Ernst & Young: Fraud – The Unmanaged Risk (8th Global Survey)

AIG UK Limited

The AIG Building, 58 Fenchurch Street, London EC3M 4AB. Telephone: 020 7954 7000 Fax: 020 7954 7001

This insurance is underwritten by AIG UK Limited which is authorised and regulated by the Financial Services Authority (FSA number 202628). This information can be checked by visiting the FSA website (www.fsa.gov.uk/register). AIG UK Limited is a member of the Association of British Insurers and a member company of American International Group, Inc. Registered in England: company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London, EC3M 4AB.



Fraud and Occupational Crime: Real Business Issues

Crime Losses are increasing. In a survey of 3,600 companies in 50 countries, economic crime markedly increased compared to those reported in 2001. In Europe fraud and occupational crime rose an average of nearly 8%.¹ In the United States: fraud-related losses were estimated at 6% of an organisation's annual revenue, translating into approximately \$660 billion in total annual losses.²

Crime Losses Cost Real Money. As it is not uncommon for frauds to remain undetected for extended periods of time, the end result can be a significant loss. The average corporate fraud-related loss is £1.2 million.³

No Industry or Company Is Immune. A recent survey indicated that over 30% of respondents in each industry interviewed suffered a fraud loss. Both large and small entities are affected: 37% of companies with less than 1,000 employees, and 52% of companies with more than 1,000 employees reported such losses.⁴

Losses Can Be Devastating. The discovery of an uninsured or underinsured loss can be material and significantly impact earnings as well as damage reputation, shareholder confidence, brand image and morale.

Insiders Are The Biggest Culprits. Eighty-five percent of fraudsters are on the payroll, with 55% of them coming from the ranks of management—the size of loss attributed to managers is 16 times greater than those caused by non-managerial employees.⁵

Organised Crime is Big Business. The fast moving criminal fraternity continues to devise refined methods of sophisticated fraud and make it their priority to stay ahead of the security industry.

Management Is Vulnerable: Increasing focus on sound corporate governance means that directors and officers are under increasing scrutiny to implement all measures necessary to protect shareholder value. A director or officer can't afford to be in the precarious position of having to explain why corporate assets were not better protected through the use of available, cost-effective risk transfer protection via crime insurance coverage.

Business Complexity Is Driving Losses: The increasing complexity of organisations and transactions combined with geographically diverse operations, increasing mergers and acquisitions, downsizing, restructuring and outsourcing greatly increases the risk, size and extent of crime loss to a company.

Globalisation Creates Greater Vulnerability: Increasing numbers of transient employees, distant overseas locations, greater reliance on limited management with varying levels of segregation and control significantly increases the risk of fraud-related loss.

Reliance on Internal Controls May Not Be Enough. Even the most careful and ethical companies are exposed to white collar crime as it remains very difficult to monitor individual behaviour and controls can be overridden. Collusion among employees (including managers) and third parties contributed to 48% of reported fraud cases.⁶

Insurance Provides Real Financial Protection: Companies with crime coverage are reported to be three times better placed to recover their losses than non-insured entities.⁷

*The risks are real.
Can you afford not to be protected?*

The Power In Business Insurance

The member companies of American International Group, Inc. are leading providers of a wide range of innovative insurance products to protect corporate entities from commercial crime losses. This document is intended to raise awareness of the issues and concerns that commercial crime presents to individual businesses, as well as suggest strategies that can form part of a comprehensive approach to mitigate the risk of loss from this peril.

This summary is for general informational purposes only. It should not be construed as legal or other advice of any nature. Should further analysis or explanation of the subject of this summary be required, please seek qualified legal advice. We compiled this summary from sources believed to be reliable. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any summary, representation or comment herein, ©2005 American International Group, Inc. (AIG). All rights reserved.

End Notes

- ¹ PricewaterhouseCoopers—Economic Crime Survey 2003
- ² Association of Certified Fraud Examiners—2004 Report to the Nation on Occupational Fraud and Abuse
- ³ PricewaterhouseCoopers—Economic Crime Survey 2003
- ⁴ PricewaterhouseCoopers—Economic Crime Survey 2003
- ⁵ Association of Certified Fraud Examiners—2004 Report to the Nation on Occupational Fraud and Abuse
- ⁶ 2003 KPMG Fraud Survey
- ⁷ PricewaterhouseCoopers—Economic Crime Survey 2003

AIG UK Limited

The AIG Building, 58 Fenchurch Street, London EC3M 4AB. Telephone: 020 7954 7000 Fax: 020 7954 7001
This insurance is underwritten by AIG UK Limited which is authorised and regulated by the Financial Services Authority (FSA number 202628).
This information can be checked by visiting the FSA website (www.fsa.gov.uk/register). AIG UK Limited is a member of the Association of British Insurers and a member company of American International Group, Inc. Registered in England: company number 1486260. Registered address:
The AIG Building, 58 Fenchurch Street, London, EC3M 4AB.
