Financial Crime Investigation and Control

K.H. Spencer Pickett and Jennifer Pickett
Financial Crime
Investigation and Control
This book provides a general introduction to fraud investigation and control. However, each individual fraud is unique in terms of its features and context and therefore, legal counsel should always be sought whenever investigating fraud and designing specific controls to address financial crime.
This book is dedicated to
Lloyd and Frederica Livermore
ACKNOWLEDGMENTS

We would like to thank all those friends and colleagues who have contributed their stories and ideas. Special thanks to Professor Gerald Vinten, Professor Andrew Chambers, Neil Cowan, Richard Kusnierz, and Isabel Picornell for the personal comments they have supplied for the book. Thanks to Nigel Freeman and The Association of Certified Fraud Examiners for their continued support. And a very special thanks to our children, Dexter and Laurel-Jade. We hope, in a small way, to contribute to the drive to getting fraud prevention, detection, and investigation onto the agenda of managers, supervisors, and employees generally. In this way, everyone may be part of the solution to the growing threat from corporate white-collar crime.

SPENCER AND JENNIFER PICKETT
CONTENTS

One   Why Financial Crime?   1

Two   An Action Model   27

Three  Ethics at Work   51

Four    Whistleblowing and Detection   75

Five   The Fraud Response Plan   113

Six    Investigations   139

Seven  Integrated Fraud Risk Management   207

Appendix A  Forensic Statement Analysis   253

Appendix B  An Introduction to Data Mining as a Fraud Risk Management Tool   257

Index   267
Financial Crime
Investigation and
Control
CHAPTER 1

Why Financial Crime?

There is no little enemy.

WHAT IS FINANCIAL CRIME?

There is no precise legal definition of financial or white-collar crime that we can turn to, to start this book. The term is much like the associated concept of fraud, which again has no fixed legal definition. There are, however, various general definitions of white-collar crime that have evolved over the years. Black’s Law Dictionary defines fraud as:

An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. Bad faith—the conscious doing of wrong.

Webster’s New World Dictionary describes fraud as:

Intentional deception to cause a person to give up property or some lawful right.

Another useful definition comes from the Federal Bureau of Justice Statistics (Dictionary of Criminal Justice Data Terminology), which defines white-collar crime as:
Nonviolent crime for financial gain committed by means of deception by persons whose occupational status is entrepreneurial, professional or semi-professional and utilizing their special occupational skills and opportunities; also nonviolent crime for financial gain utilizing deception and committed by anyone having special technical and professional knowledge of business and government, irrespective of the person’s occupation.

In practice, there are numerous definitions of financial crime that can be used as a starting point. They tend to be similar and cover a number of key aspects of human behavior. It is the contrast between white-collar crime and other types of crime that is most interesting. Smash-and-grab robberies, rape, murder, muggings, and other such crimes are easier to describe and categorize. Violent crimes promote a clear response from citizens and law enforcement agencies in terms of various quick and effective countermeasures. In contrast, white-collar crime is, in the short term, perceived as being nontraumatic because it is generally nonviolent. It is in the longer term that deceitful behavior has a traumatic impact on business and communities. White-collar crime contains several clear components:

- **It is deceitful.** People involved in white-collar crime tend to cheat, lie, conceal, and manipulate the truth.
- **It is intentional.** Fraud does not result from simple error or neglect but involves purposeful attempts to illegally gain an advantage. As such, it induces a course of action that is predetermined in advance by the perpetrator.
- **It breaches trust.** Business is based primarily on trust. Individual relationships and commitments are geared toward the respective responsibilities of all parties involved. Mutual trust is the glue that binds these relationships together and it is this trust that is breached when someone tries to defraud another person or business.
- **It involves losses.** Financial crime is based on attempting to secure an illegal gain or advantage and for this to happen there must be a victim. There must also be a degree of loss or disadvantage. These losses may be written off or insured against or simply accepted. White-collar crime nonetheless constitutes a drain on national resources.
- **It may be concealed.** One feature of financial crime is that it may remain hidden indefinitely. Reality and appearance may not necessarily coincide. Therefore, every business transaction, contract, pay-
ment, or agreement may be altered or suppressed to give the appearance of regularity. Spreadsheets, statements, and sets of accounts cannot always be accepted at face value; this is how some frauds continue undetected for years.

- **There may be an appearance of outward respectability.** Fraud may be perpetrated by persons who appear to be respectable and professional members of society, and may even be employed by the victim.

For the purposes of this book, financial crime involves the use of deception for illegal gain, normally involving breach of trust, and some concealment of the true nature of the activities. We now have a working definition, but it covers a whole array of activities that fall under the general banner of financial crime. In this book, we will use the terms *financial crime*, *white-collar crime*, and *fraud* interchangeably.

A lot of illegal activity can occur in both the commercial and public sectors. In one sense, so long as there are weaknesses that can be exploited for gain, companies, organizations, and private individuals will always be taken advantage of. Some of these illegal activities include:

- **Consumer fraud**—attempts to coerce consumers into paying for goods not received or goods that are substandard, not as specified, or at inflated prices or fees. The growing use of attractive Internet Web sites, as an alternative to unsolicited phone calls or visits to potential customers, compounds this problem.

- **Credit card fraud**—use of stolen credit card details to secure goods or services in the name of the cardholder. Sometimes a brand new credit card is forged using known details. Cards can be stolen or details obtained from files that are not properly secured; credit card details may also be purchased from people who are able to access this information. This is another growth area.

- **Kickbacks**—generally involve an employee with influence over who gets a particular contract, who is able to obtain something for assisting the prospective contractor. Likewise, bribes may be paid to inspectors to turn a blind eye to substandard goods coming into a loading dock. If bribes do not work, the dedicated fraudster may well turn to blackmail and threats.

- **Bid rigging**—When a vendor is given an unfair advantage to defeat an open competition for a given contract. A vendor may be provided with extra information to bid low but then raise more income
through many variations to the set contract. This may be linked to the receipt of kickbacks. Election rigging is a similar but more sinister type of fraud.

• **Inflated invoices**—when a company inflates its bills without agreement from the bill payer, who may be a customer. Conversely, an employee may arrange to pay a vendor more than is due in return for an unauthorized payment or some other gain. An employee could also pay an amount to an entirely fictitious supplier, and divert the check to a personal bank account.

• **External fraud**—schemes by people who do not work for an organization but seek to defraud it. Advance-fee fraudsters attempt to secure a prepaid commission for an arrangement that is never actually fulfilled or work that is never done. Many international frauds committed via the Internet require advance payments for fictitious or substandard goods or services. Billions of dollars worth of health care fraud has resulted from several parties in the health industry conspiring with individuals to submit fraudulent medical bills for services not provided. Insurance companies suffer multitudes of fraudulent claims, often from sophisticated parties who conspire to commit a series of well-planned scams. In short, any organization or public body that provides something of value (for example, food stamps, cash grants, compensation payments, claims, refunds, loans, and equipment) may be subject to efforts by external parties to defraud it. In Europe, the European Commission has found that fraudsters can obtain millions of dollars from irregular claims if there are not adequate controls over the process, including physical verifications.

• **Inventory theft**—straightforward stealing of stock from an employer. It can also involve stealing scrap and goods that are returned by customers, as there may be less control over these items. A bigger problem is shoplifting: customers rather than staff steal billions of dollars worth of goods from retail outlets each year.

• **Theft of cash**—misappropriation arises when cash comes into a company and is diverted. **Skimming** occurs when cash is taken before it enters the books; for example, by a cashier. **Embezzlement** involves a direct breach of trust, when someone entrusted with the cash diverts it for personal use. **Lapping** is a technique whereby the theft of cash or checks is covered up by using later receipts so that the gap in funds is not noticed, sometimes for many years. Some argue that the
reported figure for these types of frauds is only around 10 percent of the actual losses.

- **Basic company frauds**—when an employee fakes sickness to obtain paid sick leave, submits inflated overtime claims, or uses company equipment for an unauthorized purpose which may be to operate a private business. When this private business competes with the employer’s business, the fraud may also involve theft of ideas and company information such as a client database. A more dangerous development is the sale of information and ideas that the employee has access to. Pilferage relates to small items taken home by staff. Fabricated time sheets can constitute a theft of time (and therefore pay) from businesses. What used to be a basic deception, but is now a major problem, is falsified information on résumés from persons seeking employment. In some cases, the person being employed is very different from the person on paper, who appeared to have the skills, competencies, and credentials needed. Some argue that more than half of the material that appears in a typical résumé is misleading. Someone who lies to a prospective employer from day one may be the type of person who will engage in deception as he or she settles down with the company. Many organizations have some staff who engage in basic company deceptions.

- **Travel and entertainment (subsistence) claims**—when claims are falsified, inflated, or there is basic abuse of the scheme. Small-scale abuse occurs when people simply overstate their claims. It gets more serious when the claimants put in fabricated sums and even forge the line manager’s signature. Fraud by an accounts clerk who operates a payments scheme can be substantial, as the aggregate amount grows over time.

- **Check fraud**—when a company check is stolen, altered, or forged, it may be diverted to an unauthorized person who accesses the funds and then closes the account or simply disappears. Company secretaries and accounts personnel may also slip additional checks into a signing routine to effect significant levels of fraud against a company. An extension of check fraud is bank fraud, whereby individuals (and businesses) seek to defraud banks of funds, normally in the form of unsecured loans.

- **Identity fraud**—this is now a major issue in society. There are many reported cases where people have had to defend themselves against claims, because others have stolen their identity, using personal data
such social security number, address, date of birth, and so on. The costs of reestablishing a reputation that has been impaired through credit card fraud and other fraudulently incurred debt can be tremendous in terms of both money and time.

- **Ghost employees**—getting extra names onto a company payroll and diverting the funds to a bank account specially set up for this scam. If an employee can stay on the payroll after having left the company, again extra funds can be obtained for a while. Unauthorized changes to payroll times, rates, and claims can also result in money being diverted for illegal gain.

- **Misappropriation schemes**—come in many forms and guises; detection is made more difficult by efforts to conceal the nature of the funds lost to the company. Writing off income that was actually received is one concealment technique. Altering sales figures, obtaining blank purchase orders, amending documentation, diverting vendor discounts, and writing off balances that are thrown out from account reconciliations are all ways that an employee can misappropriate funds and balance the books at the same time.

- **Computer-related crimes**—computer hacking can be a stepping-stone to securing data, accessing rights, and providing a means to commit fraud. Therefore, fraudsters may be involved in sabotage, software piracy, stealing personal data, and amending or damaging records held on computer systems. Younger people brought up in a computerized environment can run rings around their senior managers, who may not appreciate the opportunities for unauthorized transactions that are inherent in automated information systems. In some organizations staff have more access rights than they need to have to do their jobs. Computers have great facilities to hide irregular transactions, but at the same time can capture lots of information on the trail of each transaction.

- **Financial statement fraud**—this can be very serious and can be used to encourage investment and loans through fabricated or falsified financial figures. Inaccurate earnings figures may also be used as a basis for performance bonuses. Popular frauds involve people buying stock and then “talking up” the price and selling before the market spots the distortion and falls back in line. Some credit card frauds link into share frauds, in that the stolen cards are used to buy stock in the name of the rightful card owner to help boost share prices.
Alternatively, a company may be entirely fabricated to attract funding; once the money is obtained, it and the bogus company disappear from the face of the earth.

- **Sundry frauds**—there are many types of fraud that have not yet been mentioned, such as illegal price-fixing cartels; pyramid investment schemes; environmental abuse, such as waste pollution; money laundering, where illicit money is turned into legitimate usable funds; mail fraud; counterfeiting; and racketeering, where someone operates an illegal business for personal profit.

A lot can and does go wrong for both organizations and private individuals when fraud is allowed to prosper. Note that, for the purposes of this book, we will be primarily concerned with employee fraud. The Association of Certified Fraud Examiners (ACFE) has tried to put this into context: in its *Report to the Nation on Occupational Fraud Abuse* (Case Study 2389), the ACFE argued that employee fraud is big business. Smaller businesses were found to be most vulnerable because they tended to have less sophisticated financial controls, and to place more trust in managers. According to the ACFE, employee fraud is costing the nation some $400 billion a year, which is around $9 per employee and 6 percent of turnover. Losses caused by fraud among executives and managers were found to be some six and four times greater, respectively, than losses caused by other employees. Typical frauds found were asset misappropriation (cash, supplies, information, and equipment), fraudulent statements, illegal gratuities, bribery, and corruption. Typical perpetrators were college-educated, white males; the frauds examined ranged from a $22 misappropriation through to a $2.5 billion investment swindle. The ACFE quite rightly feels that fraud is an important issue in society and that the rate of its occurrence is rising.

**MODELS OF FINANCIAL CRIME**

Only some of the myriad of frauds that exist were discussed in the preceding section. In practice, there are hundreds of methods by which an employee may defraud an employer. Likewise, there are many ways that outsiders can deceive an organization into parting with something of value. Private individuals, particularly the elderly and more vulnerable members of society, can fall prey to con artists in a variety of ways. To help put these
issues into focus, we need to develop some basic models of financial crime. The first one distinguishes between fraud by members of an organization and fraud by external third parties, as shown in Figure 1.1.

An organization may be attacked from all sides. Employees may engage in both minor and more serious fraud; outsiders may also seek to obtain something for nothing, if given the chance. The other side of the coin is misleading the public through distorted information on the business (i.e., financial misreporting). Pump-and-sell schemes occur when company shares are acquired, the price is artificially inflated (say, through false Internet reports), and then quickly sold. Figure 1.2 looks at the potential layers of fraud affecting larger organizations.

Here the type of fraud varies with the position of the potential fraudster, although there is scope at all levels throughout and outside an organization. The more senior the employee, the greater the opportunity for committing more material fraudulent activity. Fraud can entail small amounts of regular

<table>
<thead>
<tr>
<th>Criminal</th>
<th>The CEO</th>
<th>Unethical Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gangs</strong></td>
<td>check fraud</td>
<td>Medicare fraud</td>
</tr>
<tr>
<td></td>
<td>fabricated invoices</td>
<td>shoplifting</td>
</tr>
<tr>
<td><strong>Directors</strong></td>
<td>financial accounts</td>
<td>government claims fraud</td>
</tr>
<tr>
<td></td>
<td>misreporting</td>
<td>food stamp fraud</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>share-price scams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>conflict of interests</td>
<td></td>
</tr>
<tr>
<td><strong>Employees</strong></td>
<td>concealed debts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bribes, kickbacks, travel and expense misreporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>petty cash, misappropriation, pilferage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>false overtime, use of company equipment</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1.2 Layers of Fraud
items that are misapplied or misappropriated, or it can involve huge sums in a scheme to artificially inflate profits. Scams can be custom and practice, when everyone adds a few hours to their overtime claims as a matter of course. Other frauds can be one-time hits, where funds are transferred to an overseas bank account and then quickly disappear from the system—along with the perpetrator. It could consist of a security guard who fails to turn up with thousands of dollars that he was conveying for the company. Fraud happens in thousands of health care claims that are regularly overstated by fairly small amounts. An entire company could embark on a scheme to rip off investors with promises of huge returns that fail to materialize. The point is that there is a risk of up to $400 billion of fraud in the U.S. economy from all aspects of business, and if there are no real safeguards against white-collar crime, the consequences could be devastating. Professor Andrew Chambers sets out the real impact of financial crime on society:

With breathtaking cynicism we build the cost of fraud into the price of our products and are often prepared to require our customers to pay 5 or 10% more to subsidize the defrauder. Of course, this area of debate is shot through with moral tones. In particular, there is the immorality of the defrauder, notwithstanding that many defrauders find it hard to see that any individuals are hurt as a consequence of their frauds. But there is also the issue as to whether it is moral to launch new products and services which are prone to fraud. Do not enterprises have a moral obligation to minimize the temptation of fraud? Might this not also be in their enlightened self interest? We suggest that the situation has now become so acute that it calls for urgent action at senior levels of government, by regulators and in the boardrooms of companies and other entities.

**REAL-LIFE EXAMPLES**

The press is full of stories of fraud and some cases go into extreme levels of detail. This book does not seek to reproduce the various stories, or embarrass named organizations and individuals, but it is appropriate to briefly mention some past cases that can help us understand and appreciate the problem:

- *An insurance claims settler stole $1 million, to support a gambling habit, by sending 417 checks to his friends in payment of bogus claims. He was jailed for eight years.*
The key factor was an addiction to gambling and the huge losses that this entailed. The solution for our friend, the claims settler, was to conspire with his friends to defraud his employer. A jail term concluded this story of greed and abuse.

- A Post Office worker falsified travel expenses by $4,500 to improve family finances. He forged claims and his manager's signature and was convicted of false accounting. Instead of helping the family, he is now in jail.

In this case, the fraudster felt that crime would be the solution to financial problems. There was a worthwhile motive—to provide for his family—but the net result of these endeavors had the opposite effect.

- A company director gave a friend a corporate credit card. The friend racked up $17 million over 2.5 years, which was discovered when the director went on leave and a box of receipts was found in his desk.

The director was someone in a powerful position, such that his actions were not questioned at all. In fact, the fraud was uncovered by accident; the extent of the losses is astounding.

- An attorney who was mild, unassuming, and of good character stole from his clients' accounts. He went to Monte Carlo to bet on roulette in an attempt to pay it back. He was subsequently convicted of theft.

Many fraudsters excuse their actions by maintaining their intention to repair any damage done. Their need is great and once they settle their problems, they will pay back the sums taken. In most cases this intention is simply an attempt to soothe a guilty conscience.

- A promising young law student was attacked during a road-rage incident. She had to take sick leave and fell behind in her studies, although she still attempted to take her exams. She subsequently broke into the university at night and altered her exam results, but was found out. She could not face the shame of a court hearing and committed suicide at a nearby beach.

People of high social standing face the prospect of irreparable damage to that standing if they get caught committing fraud. This sad case shows the emotional extremes that drive a person to commit an act of deceit and the impact of this dishonesty being uncovered.
A security guard stole £1.5 million in gems and cash from Versace in London. A person who is given a position of trust is able to do much more damage than someone who is kept away from valuable resources. When breach of trust occurs, it can be disastrous. What’s more, if the same person is fairly junior and is presented with an opportunity to divert a large sum, there will always be some temptation.

**UNDERLYING COMPONENTS**

There are many and varied types of fraud that threaten all organizations. These attacks can come from a variety of sources, and can be directed toward government, public bodies, and commercial enterprises. At this stage, we need to extract the essential components of financial crime to complete the initial analysis of this problem. There has been a great deal of detailed research on why people commit fraud and what circumstances are required for fraud to arise. One of the founding fathers of fraud theory is Edwin H. Sutherland, who felt that opportunity, means, and motive together provide the impetus for white-collar crime. Donald R. Cressey, in *Other Peoples’ Money* (Patterson Smith 1973), developed three key factors in fraud, shown in Figure 1.3.

Opportunity exists where there are poor controls over organizational resources. Severe pressure in the form of financial problems can occur in any family at any time. When the problem is not shared at all, feasible solutions like asking family members for temporary assistance may not be considered. Likewise, help may not be obtained for problems such as

![Figure 1.3 Fraud Triangle](image-url)
alcoholism or an addiction to gambling. Rationalization is a really interesting concept, because perpetrators are able to justify their actions, at least to themselves. Excuses may be simple—say, that most staff engage in similar or worse behavior—so pilferage or taking kickbacks is seen as the norm. Other excuses may be less obvious, such as when an employee feels that the company “owes” him for many hours of unpaid overtime, so he recoups it through regular kickbacks. Society values both business success and personal integrity. When these two concepts conflict, the individual has a clear decision to make. Which is more important?

- To obtain a high standing in society?
- To alleviate a financial crisis, such as college fees, medical bills, or a divorce settlement?
- To acquire a better car, vacation, property, school education?
- To assist a friend or family member with a major financial commitment?
- To fuel an addictive lifestyle that involves vices such as gambling or drugs?
- To observe, above all, the highest standards of personal integrity?

There may be great pressure to lower one’s standards of personal integrity and choose between loyalty to one’s employer or solving a major financial problem. Rationalization may allow someone to forgo integrity because of the compelling weight of the financial problem. Moreover, perpetrators may argue that they:

Will pay it all back later on.
Take what’s only their fair share.
Just do like all the rest of them.
Don’t worry because no one really cares about this anyway.
Must bow to a greater and more pressing need.
Are getting their own back on a corrupt employer.
Take what won’t be noticed from a wealthy company.

The point is that professional, respected, and trusted members of an organization may commit fraud against the organization for a variety of reasons that make sense to them. They are not members of violent criminal gangs and they do not walk around armed with guns and wearing heavy scowls on their faces. They may appear and act like honest, law-abiding citizens, even while breaching their fiduciary duty to their employer.
Trusting your co-workers and bosses and staff is part of organizational life. It is difficult to know how to work together without this mutual trust and understanding. The new world of staff empowerment makes this reliance on trust even more of an issue. Researchers have found that there are many reasons people may turn to fraud and in many cases both the fraud and the precipitating factors for it come as a shock to their colleagues.

The position is not simple. The world does not consist of criminals and honest people—it is more complicated than this. The world is full of people acting under tremendous, and in many cases conflicting, pressures which can lead to behavior that, although wrong, can be explained and even excused. Often a fraudster, if discovered, risks only his or her reputation. It depends on the value the person places on reputation and whether this is a risk worth taking. One thing that most organizations now accept is that people are, if anything, unpredictable.

The chances of getting caught also come into the equation: fraudsters will want to secure the desired gain, but also retain their freedom and perceived status in society as honest and upright. Where controls are poor, ethical standards are nonexistent, and real oversight in the organization is lacking, substantial employee fraud and concealment become much more likely. This lethal combination of forces—components of what some now call economic crime—make this a major growth area in business, public services, and society generally. Professor Gerald Vinten has described the real dangers of white-collar crime in today’s society:

White collar crime seems like the nice end of criminal activity, since it does not usually involve violence, and the perpetrators are just like the people next door. However, its economic consequences can be devastating, and in the wider scheme of things it can be even more lethal than crimes of physical violence. White collar and other types of crime tend to operate hand-in-glove and even be symbiotic. Money laundering is another illegal activity that makes the crosswalk between the ‘nasty’ end of crime and the ‘nice’ end. What is clear is that ‘white’ collar crime is not the preserve of the angels although policing agencies tend to treat it as a low priority compared with other types of crime. It is a difficult balancing act between civil liberty and minimizing crime, but a system which plays into the hands of the organized white collar criminals has a mushrooming impact on crimes generally. It is already expensive economically, and is a price that the law abiding are forced to pay, a redistributive tax which has all to do with human rapacity and nothing to do with the public good. It has to be time to confiscate the ill gotten gains of such activity, and to place the burden of proof for once back on the suspected perpetrators. The huge excitement
and promise which greeted the onset of the 21st century is in danger of being undermined if the white collar crime threat is allowed to perpetuate itself unchecked.

**REASONS FOR NOT BOTHERING**

So far, we have outlined the great potential for financial crime to undermine our economy. The statistics are shocking, but fraudulent activity is both wide in scope and difficult to detect. The growth in fraud depends in part on the financial pressures placed on normal working people and the value placed on ethical behavior. There are always tensions resulting from these two factors; the third factor that completes the cycle of damage is the way organizations respond to the perceived risk of fraud. When fraud is not seen as a priority business risk, there is little incentive to tackle it head on. When directors and managers are not bothered about fraud as a corporate issue, their response contributes to the forces that are driving fraud further and deeper into all organizations. In this section we address some of the reasons why people, companies, directors, nonexecutives, and others do not always hold fraud as a key concern.

**General Lack of Awareness**

Many managers and staff members do not have a particular interest in white-collar crime. It is generally seen as an unfortunate occurrence that occasionally happens to other organizations and when it arises, specialist investigators are brought in to deal with it. There is no real appreciation of the power of greed, nor the pressures that lead individuals to become deceitful. The typical manager may fail to think through why a staff member who has a small workload is always very busy. Managers do not follow through the implications of the accountants asking for more deductions in certain areas to get profits down. Some feel that men and women in suits rushing around the office indicates that all is well, as people in suits are by definition perceived as respectable.

**Not Seen as a Personal Threat**

Fraud tends to be nonviolent and therefore does not have an immediate physical impact on the victim. Not bothering about fraud at times simply reflects society’s priorities; people respond first to issues that threaten their physical safety and comfort. White-collar crime is not “in your face,” as are
other crimes. It is not something that will necessarily be on the tip of the tongue of police officers and security staff. As such, it may be seen as unfortunate or bothersome rather than criminal.

No Real Victims—Write It off

Industries such as retail and distribution recognize that a degree of fraud is inherent in the nature of operations that possess, display, or move around valuable and portable goods. Some see crimes against such organizations as victimless because the losses are built into profit margins. The aim is not so much about removing fraud as it is about ensuring that the company does not exceed industry norms. Losses are written off, insured against, and lived with. This high-level policy sets the tone for the entire organization.

Business before Security and Not Vice Versa

Linked to the preceding point is the view that securing company resources, if taken to the extreme, will mean little or no business gets done. A phone inquirer may hang up if asked dozens of questions to verify identity. Likewise, a grocery store owner may spend an hour making goods readily accessible to street thieves, just to get them to the eyes of potential customers. New information systems tend to be installed with the security and audit trail facilities set to zero, to be activated in a manner that suits the client. The point is that the more secure the system, the more resources it uses and the slower it becomes. Entrepreneurs have a keen eye on the business but less thought about the potential for abuse. This is also true in the sales arena: businesses love to supply large quantities of goods even when most of it is on credit. Turning customers away because of poor credit ratings has caused pain to many a dynamic salesperson.

Not Understanding the Link between Fraud and Controls

*Controls* are mechanisms that guard against unacceptable risk. Most people accept that fire alarms are in place to detect and warn against fire. Plans are prepared and put into action to help counter the risk of not meeting strategic objectives. Performance appraisal systems may likewise counter the risk of failing to set and meet personal and group targets. Fraud is an invisible risk, in that it is potentially everpresent but may actually never materialize. Many people see fraud as something that happens if the company is unlucky and has taken on the occasional “bad apple.” Not everyone links control standards to safeguards against fraud. When you spot your boss signing dozens of blank check request forms and handing them over to an assistant...