1
What Do We Mean by Fraud?

Fraud can involve mundane activities such as employees regularly taking home small items of office equipment, right through to complex schemes established by executive directors for manipulating the financial statements to pump up the share price of their failing company. In this book we are mainly concerned with employee fraud, which affects small businesses, larger companies, public-sector organizations and the many types of not-for-profit entities that exist in developed and developing countries across the world. Our goal is to help raise awareness among non-specialists to help get everyone involved in the fight against fraud. Organizations that succeed in fighting fraud will benefit, while those that do not may well see their reputations suffer as they become targets of their own employees and even of outsiders, who launch attacks either alone or by colluding with these employees.

One argument suggests that fraud against businesses and government agencies is growing at an alarming rate and we now need to take a firm stance or suffer the consequences. This book is based around the Fraud Smart cycle, which covers five key aspects of helping non-specialists get to grips with fraud at work, as set out in Figure 1.1.

This chapter sits within the first part of the Fraud Smart cycle, Understanding the Threat, and provides an outline of some of the more common types of fraud.

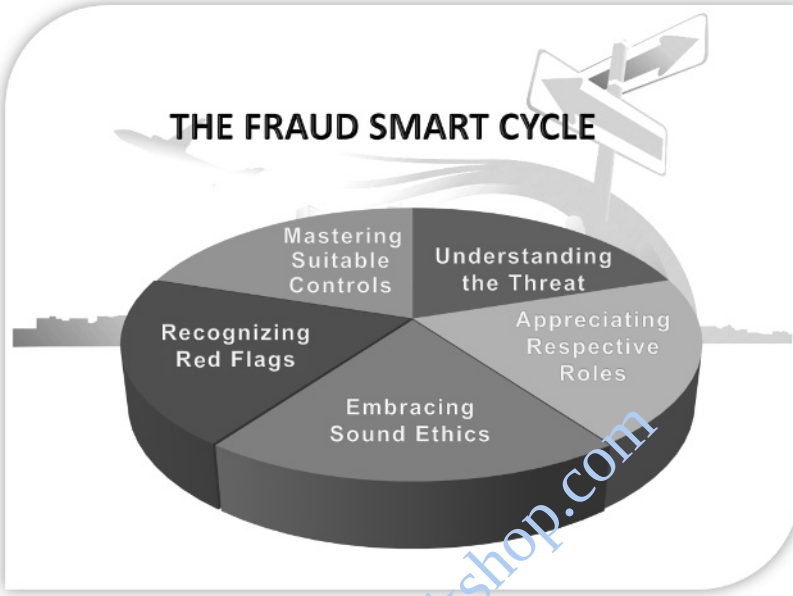

Figure 1.1 The Fraud Smart cycle.

WHAT CAN GO WRONG?

If we fail to get a handle on fraud, there is much that could go wrong. In the past, on discovering that one of their employees was acting in a dishonest manner many organizations would seek out the easiest way to get rid of the problem. This often involved a secretive meeting with the employee, the manager and someone from human resources to force the culprit's resignation, so that he or she would simply go away, as would the problem. A successful outcome would mean that some kind of repayment might be secured and the whole affair would be hushed up. This 'old-style' solution meant that there was no need to ensure that employees were aware of the potential for fraud, or indeed to design any fraud-management process. Bad apples would be quietly removed and it was business as usual, with any losses simply written off, while the culprit would often seek out a new victim.

We can consider the way in which problems can arise by looking at two brief illustrative case studies taken from the UK and the USA. To set the scene, we can turn to the *Times* newspaper for inspiration:

> Frauds, like economies go in cycles. As boom turns to bust, frauds emerge with the inevitability of a hangover after a party. During the

> celebrations, there are more opportunities to pick pockets and less chance of getting caught. In the cold light of day, people check their wallets and call the police. With the economic boom coming to a crashing end, the wave of frauds has arrived right on cue.
>
> *David Wighton, Business and City Editor, The Times, December 20 2008, News, page 3*

High-powered people can get together and plan to defraud a funding body:

CASE STUDY

Three company directors of a training company were given prison sentences for rigging trainee course attendance numbers to gain Learning Skills Council funds. Two people operating a training consultancy as shadow directors admitted a conspiracy to defraud another organization which made funds available to firms in the region, on behalf of the Learning Skills Council. Another registered director admitted a failure to keep accurate accounting records in breach of companies legislation.

A manager who has a responsible position can abuse this position and, along with others, commit fraud:

CASE STUDY

A hospital manager and four other people were sentenced for conspiring to defraud a hospital trust of £580 000. The manager pleaded guilty to conspiracy to defraud and was jailed for three years. Two other defendants were sentenced for conspiracy to defraud, and a further two for money laundering offences. All were given prison sentences. The fraud was uncovered by finance staff and the police discovered that over half a million pounds had been defrauded from the payroll system. The manager was found to have used her position of responsibility to create 'ghost' employees who she pretended had worked shifts as administrative and clerical staff. After the wages for these false shifts had been paid to the other defendants, the manager attempted to cover this up by deleting the phantom shifts from the payroll list. Her actions left an electronic 'footprint' in the system which could be traced back to her.

The 'sweep it under the carpet' approach no longer works, as this simply encourages dishonesty if the only sanction when caught is enforced resignation. The threat of fraud has grown not only due to the economic downturn but also because management layers have been removed, and low-paid junior staff now have much more responsibility, including instant access to customer information as online commerce becomes the norm. We can mix into this potent cocktail the fact that people frequently move jobs and often have no time to bond with their employer and create strong ties of loyalty. Meanwhile, organized crime gangs have replaced their guns with virtual but much more lethal weapons in the form of online access to try to defraud large organizations.

There is no way to combat these developments other than by making sure that the workforce throws itself into fraud control and by installing a robust anti-fraud strategy. Any failure to do so may result in a vulnerable business being subject to continual fraud and abuse, and staff as well as customers becoming demoralized by a poor corporate reputation. It does not stop there, however, as a further trend is for companies to be fined if they fail to control fraud in an appropriate manner.

WHAT DO THE EXPERTS SAY?

As explained in the Preface, we have drawn from two main sources of expertise to help explain Fraud Smart management, as follows:

- *Managing the Business Risk of Fraud: A Practical Guide*, sponsored in 2008 by the Institute of Internal Auditors, The American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners. We will refer to this guide as the 'MBRF'.
- *Report to the Nations (On Occupational Fraud and Abuse) 2010 Global Fraud Study*, published by the Association of Certified Fraud Examiners. We will refer to this extensive survey of fraud across the world as the 'ACFE Report'.

These two publications contain extremely useful guidance and some of the extracts that are relevant to this chapter are noted. We start with a definition of fraud taken from *Managing the Business Risk of Fraud: A Practical Guide*:

> Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain. (MBRF, page 5)

The guide goes on to warn about the menace from uncontrolled fraud:

> All organizations are subject to fraud risks. Large frauds have led to the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets. Publicized fraudulent behavior by key executives has negatively impacted the reputations, brands, and images of many organizations around the globe. (MBRF, page 5)

We can turn now to the *Report to the Nations* for a frightening estimate of the scope of fraud internationally:

> Survey participants estimated that the typical organization loses 5% of its annual revenue to fraud. Applied to the estimated 2009 Gross World Product, this figure translates to a potential total fraud loss of more than $2.9 trillion. (ACFE Report, page 4)

This sky-high figure of a $2.9 trillion potential loss sets the scene for the rest of the book. We return to this report for more information on the quoted figure:

> Asset misappropriation schemes were the most common form of fraud in our study by a wide margin, representing 90% of cases – though they were also the least costly, causing a median loss of $135,000. Financial statement fraud schemes were on the opposite end of the spectrum in both regards: These cases made up less than 5% of the frauds in our study, but caused a median loss of more than $4 million – by far the most costly category. Corruption schemes fell in the middle, comprising just under one-third of cases and causing a median loss of $250,000. (ACFE Report, page 4)

You can see from these statistics that fraud is not harmless, victimless and therefore of low concern. It is unfair, since it diverts funds from the people and entities that have a legal right to those funds. Moreover, it has been found that fraud can be used by organized crime to fund other serious offences such as drug dealing and people trafficking. In

some cases an entire business can collapse if it has been defrauded by an employee. There is good reason for employees, partners, associates and customers at all levels to help combat fraud as far as possible.

OUR MODEL EXPLAINED

We have developed a simple model, shown in Figure 1.2, to illustrate one way of dealing with the issues raised in this chapter.

Our model suggests that we can view fraud as affecting at least four main aspects of an organization: its income received, its spending, its data (or information) and its assets. We can explore these issues by briefly considering each separate part of our model in turn.

Income

Income is an obvious target for fraudsters, in the sense that if it can be diverted into someone else's bank account then it becomes the income

Figure 1.2 Types of fraud.

of the beneficiary. In one case cheques due to the company were intercepted by postroom staff and given to a criminal gang, whose members altered the payee and paid them into a specially established bank account. An even better fraud involved the gang setting up bank accounts in the same name as the company so that stolen cheques could be banked unaltered.

Income is thus due to the company but diverted to the fraudster. One problem for the fraudster can occur when the company continues to chase the debtor and the fraud eventually comes to light.

There are several questions that can be asked to assess how far income could be at risk, including:

- Do we have processes that involve receiving cash in such a way that it could be misappropriated?
- Is there a source of income for which records could be falsified?
- Is there a source of income such as donations or refunds that are not expected by the company and that could be diverted?
- Could an employee arrange to write off debt so that if it is later received, it can be fraudulently diverted without any obvious gaps in the account?

All income belongs to the organization and it is at risk if it is not carefully controlled. The issue is whether the controls are sound enough to protect all sources of revenue. The key question to ask is: Can funds due to the organization be intercepted and diverted?

Expenditure

Expenditure is also a target, in that fraudsters will try to achieve payment to themselves (or an associate) by diverting funds so that they fall under their control. A clever accounts staffer may be able to invent false supplier accounts as well as their own special bank account and arrange one or more payments from the company. Bid rigging, where contractors conspire to set the rates for projects that a company is letting, means that the company in question will not achieve value for money and will end up spending more on its contracts. One reprographics manager set up a printing company and then sent out subcontracted jobs to this same company. Meanwhile, he did the jobs himself by using his employer's printing facilities at weekends, which he also claimed as overtime.

There are several questions that can be asked to assess how far expenditure could be at risk, including:

- Could someone falsify their qualifications and thereby earn more money than they otherwise should have?
- Could someone falsify their timesheet, overtime claim, expenses or performance figures to earn extra income?
- Could a fabricated order be placed that leads to a fraudulent payment being generated?
- Could duplicate payments be scheduled and one of the duplicates then diverted?

Authorized spending can end up in a fraudster's account if it is diverted there, while unauthorized spending can be generated by circumventing disbursement controls. The key question to ask is: Can payments be activated so that they end up in a fraudster's account or be misapplied in any way?

Assets

The theft of corporate assets can be widespread in companies that hold equipment, inventory and stocks of finished goods. This is an age-old problem. The theft of cash bags is a further problem if the organization has cash receipting and movement systems in place. Misuse of company resources is a different type of problem, where in extreme cases an employee may run their own business using company facilities. One manager of a children's home over-ordered food supplies and his deputy and caretaker would help him take home the excess food once or twice a week. Meanwhile, the manager's wife ran a catering firm and used this food to reduce her outgoings.

There are several questions that can be asked to assess how far assets could be at risk, including:

- Could equipment be removed from office premises without authorization?
- Could stationery be removed on a regular basis?
- Could office resources be used to support a private business?
- Could corporate information systems be breached and the underlying data stolen?

- Could corporate assets be over-stated on the balance sheet to give a misleading impression to users?

Many organizations have an edge over their competition through the information they hold on markets, financial products, partners and customers. Together with other assets, this information can be at risk.

The key question to ask is: What assets are at risk and could they be accessed in an inappropriate manner?

Data

Data, information and company intelligence present a growing problem in terms of the fraud angle. Straight data loss is an issue that is compounded where these data can be used to perpetrate fraud. In fact, there is a black market in personal data that can be used by opportunist fraudsters, who access the files and pass on relevant data relating to personal and financial details to criminal gangs who can take advantage of the facility.

Banking details, national insurance numbers, addresses, credit details and other personal data are being hoovered up by large organizations to power their customer information systems, but nonetheless pose a threat whenever there is a breach of security. It has been known for customer service employees to photograph customer screens on their mobile phones and pass this information on to outsiders, who create false accounts or address changes to divert funds to their control. Victims of identity theft then face an uphill battle to reinstate their identity and they rightly blame the organization for allowing their details to be stolen.

There are several questions that can be asked to assess how far data could be at risk, including:

- Could personal details be accessed to facilitate identity fraud?
- Could customers' financial details be stolen to commit banking or credit card fraud?
- Could sensitive company knowledge be applied to share dealing based on insider trading?
- Could confidential details of new product designs be stolen?
- Have official-looking emails been received that request user ID and password details, possibly appearing to be from the corporate IT security team?

Data and the more common store of information that 'knowledge-based' companies now harvest are at risk as the increasingly most sought-after aspect of organizational resources. The key question to ask is: How can we protect the vast amount of information held on our corporate and local systems?

There are obvious parts of the organization that are at risk of fraud in all but the smallest of organizations. The sad fact of human nature is that if something can go wrong then at some point in the future it probably will go wrong. One view is that frauds do not just happen, they are *allowed* to happen because no one thought to ask key questions about areas that are at risk.

OUR THREE KEY CONCLUSIONS

There are three main conclusions that we can draw from our discussions and suggestions. These conclusions will be used to drive your Fraud Smart toolkit, which you will be designing at the end of this part of the book:

1.1 Fraud is ever present and is growing in most developed and emerging economies, so that it must be seen as representing a major threat to most organizations in most sectors.
1.2 It is no longer possible to sweep fraud under the carpet, hoping that any incidents can be dealt with by simply asking the culprit to resign.
1.3 Organizations own income, expenditure, assets and data and these are all at risk if there are no effective measures in place to ensure that everyone is Fraud Smart and is operating as a full-time custodian of the corporate resource.

In the end, protecting income, expenditure, assets and data is about protecting the organization's reputation. We said in the Preface that everyone who works for or is associated with a larger organization should appreciate what fraud is and its ramifications. What we need to add now is that this stance is not a *nice-to-have* but more of a *must-have* approach, which means that ideally the entire workforce should possess the basic knowledge conveyed by this book.