

PART
I

**FRAUD AND CORRUPTION
TODAY**

COPYRIGHTED MATERIAL

CHAPTER 1

Can We Eliminate Fraud and Corruption?

Key points:

- Fraud itself cannot be eradicated, but fraud and corruption risks can be managed like other business risks.
- Fraud and corruption risk management strategies can help companies avoid some frauds and help them reduce the impact of frauds that occur.
- Resilient corporations focus more on strategies, not tactics, for managing fraud and corruption risks intelligently.
- In today's more brittle economy, fraud and corruption can more easily set off a chain of events resulting in significant loss for the companies affected.

Not a pretty picture

It is quite likely that fraud has existed in one form or another since the earliest days of organized societies. Despite the fact that it is illegal in most countries, despite the vigorous enforcement of anti-fraud laws in many countries, despite corporate self-policing, and despite significant attempts in many companies to create more ethical cultures, fraud continues to be an inevitable and unpleasant component of modern life.

4 Corporate Resiliency

Duleep Thomas, former senior vice president and general auditor at Wyndham Worldwide Corporation, describes this harsh reality this way, “Senior management needs to acknowledge that fraud can occur anywhere, at any time, and at any company. It is not okay to say, ‘We operate in an environment of trust.’ Once you accept this reality, then you need to understand where fraud could be perpetrated—both internally and externally—with respect to the business.”

In general, fraud means taking financial advantage of another party through deception. Frauds affecting companies, the subject of this book, take a variety of forms. They can be threats from outside and carried out by members of the public. For example, they can be false claims made to a medical insurer, in which claims are made for injuries or ailments that the claimant does not suffer. They can also be threats from within and carried out by employees. An example of this would be procurement or vendor fraud, in which an employee sets up a false vendor in the company’s accounts payable, then submits bills for goods or services, and collects payments in an account controlled by the employee.

One of the most dangerous form of fraud for a company occurs when the fraud is committed in the name of the company. Examples are misleading claims about products, offering returns on investment that can never be realized, or false financial statements designed to mislead analysts and investors.

Fraud prevention remains an imperfect art for most companies, with less than perfect results. Fraud in the corporate world, therefore, seems an inevitable fact. This is the result of several factors. First, we need to accept the reality that some people will resort to deception if they see an opening. Second, and building on this psychological fact, we need to recognize the lag in time between when schemes are invented and applied, and when they are detected and placed into the knowledge base that fraud prevention techniques rest on.

Third, there is also the difference between what is generally known about fraud schemes and prevention techniques, on the one hand, and what is known and practiced by a particular company, on the other. To stop the fraud schemes that are generally known requires that companies learn about them, evaluate the risks they pose, and diligently apply lessons learned.

The creativity of those who commit fraud seems inexhaustible. As a result, fraud itself can seem more like a disease than a simple

criminal phenomenon. Its tendency to mutate suggests a cancer-like quality. Its ability to mask or change its appearance suggests some sort of predatory virus.

However, as we learn about fraud schemes and their characteristics, we *can* act to prevent them. A significant part of this book is devoted to strategies for applying knowledge about fraud in order to try to prevent it, and certainly to detect and limit the effects of schemes.

“It is unlikely that we will ever be able to eliminate fraud and corruption completely. In some societies, it is systemic,” says our colleague Mary Jane Schirber. “The more we trade globally, the more likely we are to conduct business in countries with different social norms. It is natural for different cultures to have different customs, and it is important for us to remember that many of the rules we are accustomed to following are not followed everywhere.”

That said, it is also important to remember that fraud often accompanies corruption (usually as a way of compensating for the money paid out as bribes) and that the true victims of fraud and corruption are usually innocent people.

“Instead of receiving fair value in a business transaction or exchange of goods, they are getting less than fair value in the form of shoddy products, inferior services, or substandard food,” says Schirber. “So they are being hurt by a system they do not have the power to change.”

Focusing on the larger picture

It is worth noting that there are accelerating factors involved in the prevalence of fraud and corruption in the contemporary world. These include changing social norms, the democratization of finance, and the unintended consequences of two decades, worth of market deregulation. It also seems clear that our collective ability to fight fraud, on a company-by-company basis, has been hampered by a lack of appreciation for what can happen when vigilance is inconsistent and urgency is lacking.

As a society, we have tended to focus more on anti-fraud tactics than on anti-fraud strategies. In this book, we will argue that the companies that are successful in avoiding the consequences of fraud employ strategies that allow them to be resilient. Such companies focus on developing practical strategies, workable frameworks

6 Corporate Resiliency

and robust processes for preventing fraud, detecting fraud when it occurs, and responding appropriately to minimize the impact of fraud after it has occurred.

During one of our many conversations while writing this book, we realized that the fight against fraud and corruption is in many ways similar to the quest for good health. Our dieting, exercising, and annual physicals won't prevent us from dying one day—but they will help us to live longer, healthier, and more fulfilling lives.

Just because a company has a great risk management program in place does not guarantee that it will never experience an incident of fraud or corruption—but it does mean that when it occurs, the company is likely to recover more quickly and suffer less damage than a company that has been getting by with minimum efforts.

We suggested that fraud and corruption share some similarities with disease. Some diseases we learn to cure; some we learn to treat. We have not yet discovered a “cure” for fraud and corruption, but we can do a lot to make companies resilient and to mitigate their effects.

Potential for catastrophe

Make no mistake—fraud is a problem that drains hundreds of billions of dollars from the economy each year. In addition to directly reducing corporate profits, fraud can lead to a host of other negative consequences down the road. This includes losses of brand power, reputation, market position, competitive advantage, momentum, innovation, revenue, and equity.

In today's highly leveraged global economy, any one of those losses can set off a chain reaction leading to catastrophic results for a company.

Worse, fraud and corruption have a corrosive and damaging effect on a key driver of progress—the competitive spirit. Fraud dampens the human urge to compete because it creates uneven playing fields and rewards behaviors that are fundamentally uncompetitive.

It is no exaggeration to say that the qualities associated with fraud—secrecy, deception and the destruction of value—are the polar opposites of the qualities we now consider essential for success in today's markets—transparency, candor, and the creation of value.

Why now?

Ongoing legal and regulatory requirements, board pressure, and increased media coverage have created a new sense of urgency and have raised legitimate questions about whether companies are prepared to deal effectively with the complexities of fraud in a global economy.

For example, despite the fact that the Foreign Corrupt Practices Act (FCPA) has been around for years, it has only recently become an issue for many companies. Prosecutions of FCPA violations have increased rapidly over the past several years, due to increased focus by U.S. and other authorities on anti-corruption. Several years ago, bribery violations would not have been on the horizon as major risk concerns. Today, for companies dealing with officials in other countries, they can be paramount, thanks to recent international fines and penalties as high as \$1.6 billion for a single company.

The unnerving speed at which new fraud risks appear and grow seems to argue for a new kind of corporate agility based on risk management processes supported by advanced analytical technologies. These newer technologies enable companies to develop forward-looking capabilities for anticipating and responding quickly to new risks as they emerge.

Ed Rosenberg, vice president, corporate security for financial institution CIBC, says, “The nature of the threat has expanded. The level of complexity or sophistication of the threat has changed. You need to be responsive to these changes and recognize that sometimes your controls need to be enhanced, need to be altered. The ability to use information from monitoring systems to predict patterns or to identify something that has gone wrong has been very valuable.”

What we hope to show in this book is that part of the answer to “Why now?” lies in the knowledge and tools that are currently available to blunt the risk of fraud. In other words, aligning with the sense of urgency is an expanding body of knowledge, techniques, and strategies that can help companies today.

At the head of the list of such techniques and strategies are ways to tackle the diversity of fraud, as well as its changing face, and visualize the relationship between the likelihood of a fraud event in a particular company and its impact on the company. Equally important, there is today a sound set of strategies for deflecting the threats identified and, after the fact, dealing with those not yet understood.

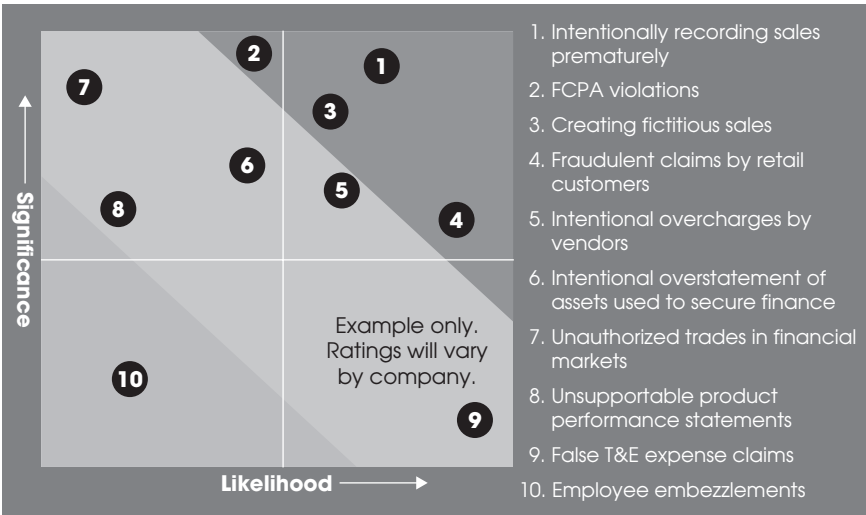


Figure 1.1 Sample “Heat Map”

The start of any fraud and corruption risk management strategy is an assessment of the risks facing a company. The details are commonly assembled in a spreadsheet or database, which can be great for control purposes but may not be easy for senior executives or directors to interpret quickly. A “heat map,” which illustrates cold to hot risk scenarios, can be a great way to communicate the key results. A sample heat map of fraud and corruption risks shows the likelihood of specific risks and the potential significance of each item’s impact, as shown in Figure 1.1.

This sample “heat map” depicts the hypothetical results of a fraud risk assessment for one company with ten risks identified. The map is simplified since in reality there would often be many more risks identified that would be grouped together, or not considered significant and omitted entirely. Fraud and corruption risks, and the resulting heat map, would vary by industry and by company based on the entity’s facts and circumstances. Your company’s fraud and corruption risk heat map might look quite different.

If we placed heat maps representing different time periods over the course of two or three years next to each other, we would see the fraud risks evolving over time. Think for example, about stock option administration. A chart looking ahead to the year 2006 could likely be very different from the chart looking ahead to

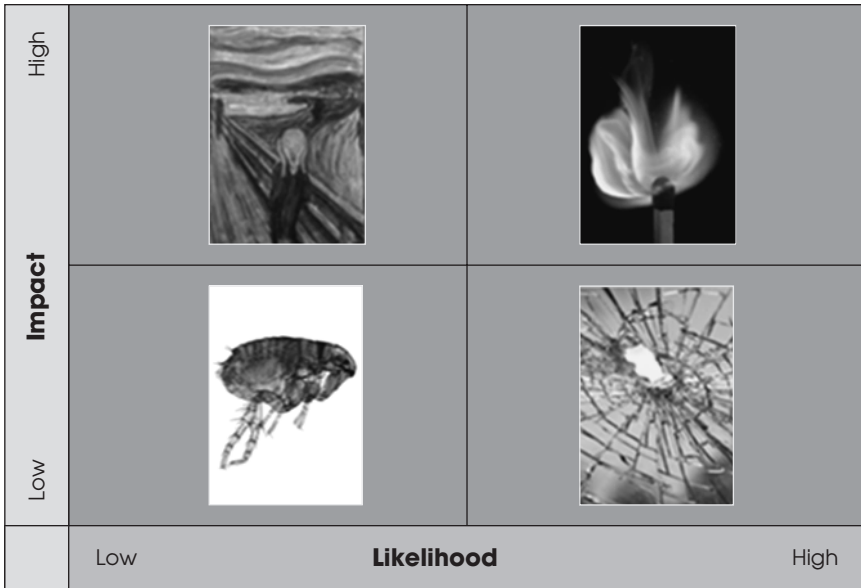


Figure 1.2 Fears, Fires, Fleas, and Flaw

Fears (“The Scream”) image: ©2008 The Munch Museum/The Munch-Ellingsen Group/Artists Rights Society (ARS), NY; Fleas image: ©iStockphoto.com/Oliver Sun Kim; Fires (match flame) image: ©iStockphoto.com/Sille Van Landschoot; Flaws (broken window) image: ©iStockphoto.com/David H. Lewis.

2007 and later years, when stock option backdating risks became prominent.

The next step in devising a strategy is to consider the fraud and corruption risks in their four quadrants representing both the likelihood of their occurrence and the significance of their impact on a company-by-company basis.

The “Fears, Fires, Fleas, and Flaws” chart in Figure 1.2 represents the four quadrants of the fraud and corruption risk heat map, characterized by the nature of the risks in each.

This type of chart helps us visualize existing and emerging fraud risks more clearly *from a strategic point of view*. We will discuss this chart in much more detail in Chapter 5, but we wanted to introduce it to you now because the concept it represents is central to one of our basic premises, which can be stated simply:

Fraud risks can be categorized in a way that makes it clear that different fraud risk management strategies may be employed for each.

Resiliency as a corporate goal

The title of this book begins with the words “Corporate Resiliency.” Why did we choose the word “resiliency” as a way to describe a corporate goal? Partly because we understand that fighting fraud is always a catchup game. More importantly, we know that companies that genuinely prepare themselves to deal with fraud, meaning the frauds they can prevent and those that they will have to react to and contain, are generally successful and are a more appropriate model for corporate success.

We will suggest that, broadly, there are four basic elements to the strategies to be deployed by industry and by company, for managing the categories of risks identified in heat maps and other risk visualization devices. We maintain that these four elements can collectively lead companies toward resiliency. Roughly speaking, the elements of fraud and corruption risk management are *assessment, prevention, detection, and response*.

We will define the connection between these four elements and the goal of resiliency and corporate success in the remainder of this book. For now we provide a brief overview.

Performing a competent fraud and corruption risk assessment is the key first step to fraud risk management. Before putting preventive or detection strategies in place, it is necessary to identify, categorize, and assess risks, on the one hand, and to determine which risks require mitigation and what mitigation strategies to use, on the other.

Second, and based on the fraud and corruption risk assessment, is putting in place preventive strategies. There are a number of them, ranging from enterprise-wide, non-fraud-specific strategies, such as corporate ethics policies, to highly targeted controls designed to prevent specific fraud schemes. Preventive strategies prefigure actual frauds by focusing on elements of enterprise-wide measures, such as avowals by corporate leaders that misrepresentations are off-limits, and other measures designed to discourage or prevent the occurrence of specific frauds.

Third, detection strategies, which vary from periodic auditing to continuous monitoring of transactions and relationships, can selectively be put in place depending on the fraud risks identified by the company. For most companies, detection strategies will fall along a spectrum between after-the-fact sampling of selected transactions and the continuous examination of all transactions in real time.

It is worth noting that detection strategies are meant both to deter frauds, due to employees knowing they are in place, and to uncover those that occur. Clearly, the limiting factor of detection strategies lies in the fact that we can test only for schemes we know about in detail.

Finally, companies can develop response strategies designed to minimize the impact of frauds that occur, are discovered, and come to the attention of the company, authorities, and other interested parties. The response strategies include the capability to conduct sound investigations.

Response strategies occupy a wide range, varying from feedback loop techniques for updating risk analyses and detection programs, on the one hand. Then to the ability to quickly respond to discovery requests from regulators and others, and to policies relating to corporate self-investigation and disclosure to the Board, shareholders, and regulators and law enforcement officials, on the other.

We maintain that deploying these strategies collectively will put companies on the path of resiliency in regard to the threat of fraud and corruption.