CHAPTER 1

Fraud Definitions, Models, and Taxonomies

INTRODUCTION

When bent on exploiting another person, a person's ingenuity in committing fraud may be unlimited. As P. T. Barnum is alleged to have said, "There's a sucker born every minute." He is also alleged to have said, "Trust everyone, but cut the deck."

It is important to understand the definitions, models, and taxonomies of fraud in order to further understand fraud and fraudsters. Therefore, the language of fraud and the antifraud business is a good starting point.

Definition: What Is Fraud?

One person can injure another either by force or through fraud. The use of force to cause bodily injury is frowned on by most organized societies; using fraud to cause financial injury to another does not carry the same degree of stigma. *Fraud* is a word that has many definitions. The more notable ones are:

- *Fraud as a crime. Fraud* is a generic term, and embraces all the multifarious means which human ingenuity can devise, which are resorted to by one individual, to get an advantage over another by false representations. No definite and invariable rule can be laid down as a general proposition in defining fraud, as it includes surprise, trick, cunning and unfair ways by which

another is cheated. The only boundaries defining it are those which limit human knavery.[1]

- *Fraud as a tort.* The U.S. Supreme Court in 1887 provided a definition of fraud in the civil sense as:

> *First: That the defendant has made a representation in regard to a* material *fact;*
>
> *Second: That such representation is* false;
>
> *Third: That such representation was not* actually believed by the defendant, *on reasonable grounds, to be true;*
>
> *Fourth: That it was made with* intent *that it should be acted on;*
>
> *Fifth: That it was acted on by complainant to* his damage; *and*
>
> *Sixth: That in so acting on it the complainant was ignorant of its falsity, and* reasonably believed it to be true.
>
> *The first of the foregoing requisites excludes such statements as consist merely in an expression of opinion of judgment, honestly entertained; and again excepting in peculiar cases, it excludes statements by the owner and vendor of property in respect of its value. [Emphasis added.]*[2]

Of the six, the fourth (*intent*) is usually the most difficult to establish in a court case. Guilty parties can use the excuse of an accident or carelessness as the cause of the incident rather than a deliberate intent to steal or commit the fraud, along with a plethora of other viable excuses.

- *Corporate fraud.* Corporate fraud is any fraud perpetrated by, for, or against a business corporation.
- *Management fraud.* Management fraud is the intentional misrepresentation of corporate or unit performance levels perpetrated by employees serving in management roles who seek to benefit from such frauds in terms of promotions, bonuses or other economic incentives, and status symbols.
- *Layperson's definition of* fraud. *Fraud,* as it is commonly understood today, means dishonesty in the form of an intentional deception or a willful misrepresentation of a material fact. Lying, the willful telling of an untruth, and cheating, the gaining of an unfair or unjust advantage over another, could be used to further define the word *fraud* because these two words denote intention or willingness to deceive.

In short, we might say that fraud, intentional deception, lying, and cheating are the opposites of truth, justice, fairness, and equity. Fraud consists of coercing people to act against their own best interests.

Although deception can be intended to coerce people to act against their own self-interest, deception can also be used for one's own defense or survival. Despite that rationale for deception, deception by current standards of behavior is considered mean and culpable. It is considered wrong and evil and can be excused only, if at all, if used for survival. But deception can be intended for a benevolent purpose, too. For example, a doctor might spare a patient from learning that a diagnostic test shows an advanced state of terminal disease. Benevolent deceivers in our society are not looked on as harshly as are those whose intentions and motives are impure. Those who act out of greed, jealousy, spite, and revenge are not so quickly excused or forgiven.

Synonyms: Fraud, Theft, and Embezzlement

Fraud, theft, defalcation, irregularities, white-collar crime, and *embezzlement* are terms that are often used interchangeably. Although they have some common elements, they are not identical in the criminal law sense. For example, in English common law, theft is referred to as *larceny*—the taking and carrying away of the property of another with the intention of permanently depriving the owners of its possession. In larceny, the perpetrator comes into possession of the stolen item illegally. In *embezzlement*, the perpetrator comes into initial possession lawfully, but then converts it to her own use. Embezzlers have a fiduciary duty to care for and to protect the property. In converting it to their own use, they breach that fiduciary duty.

Fraud Auditing, Forensic Auditing, and Financial Auditing

In the lexicon of accounting, terms such as *fraud auditing*, *forensic accounting*, *investigative accounting*, *litigation support*, and *valuation analysis* are not clearly defined. Some distinctions apply between fraud auditing and forensic accounting. Fraud auditing involves a specialized approach and methodology to discern fraud; that is, one

audits for evidence of fraud. The purpose is to prove or disprove a fraud exists. Historically, forensic accountants, however, have been called in after evidence or suspicion of fraud has surfaced through an allegation, complaint, or discovery.

Forensic accountants are experienced, trained, and knowledgeable in the different processes of fraud investigation: how to interview people (especially the suspect) effectively, how to write reports for court, how to provide expert testimony in court, how the legal system works. The Association of Certified Fraud Examiners (ACFE) refers to this definition of forensic accounting as "fraud examination." In recent years, the broadest of these terms in the antifraud professionals is *forensic accounting*, which typically refers to the incorporation of all the terms involved with investigation, including fraud auditing; that is, fraud auditing is a subset of forensic accounting.

Financial auditing is a wholly different term that needs to be distinguished from forensic and fraud auditing. Financial auditing typically refers to the process of evaluating compliance of financial information with regulatory standards, usually for public companies, by an external, independent entity. Financial audits performed under GAAS (generally accepted auditing standards), required for audits of public companies, must perform fraud-specific procedures. The well-publicized Sarbanes-Oxley Act of 2002 heavily incorporates concepts and procedures to deter and to catch fraud in audits of internal controls over financial reporting. However, the focus of financial audits and financial reporting ultimately is concerned with providing *reasonable* assurance that a *material* misstatement to financial statements has not occurred, regardless of the reason.

Fraud Auditors, Forensic Accountants, and Financial Auditors

Fraud auditors are generally accountants or auditors who, by virtue of their attitudes, attributes, skills, knowledge, and experience, are experts at detecting and documenting frauds in books of account. Their particular attitudes include these beliefs:

- Fraud is possible even in accounting systems in which controls are tight.
- The visible part of a transaction fraud may involve a small amount of money, but the invisible portion can be substantial.
- Red flags of fraud are discernible if one looks long enough and deep enough.
- Fraud perpetrators can come from any level of management or society.

The personal attributes of fraud auditors include self-confidence, persistence, commitment to honesty and fair play, creativity, curiosity, an instinct for what is out of place or what is out of balance, independence, objectivity, good posture and grooming (for courtroom testimony), clear communication, sensitivity to human behavior, common sense, and an ability to fit pieces of a puzzle together without force or contrivance.

The skills fraud auditors require include all of those that are required of financial auditors, plus the knowledge of how to gather evidence of and document fraud losses for criminal, civil, contractual, and insurance purposes; how to interview third-party witnesses; and how to testify as an expert witness.

Fraud auditors must know what a fraud is from a legal and audit perspective, an environmental perspective, a perpetrator's perspective, and a cultural perspective. They also need both general and specific kinds of experience. They should have a fair amount of experience in general auditing and fraud auditing, but should have industry-specific experience as well: for example, banking industry fraud; insurance industry fraud; construction industry fraud; and manufacturing, distribution, and retailing frauds.

Forensic accountants may appear on the crime scene a little later than fraud auditors, but their major contribution is in translating complex financial transactions and numerical data into terms that ordinary laypersons can understand. That is necessary because if the fraud comes to trial, the jury will be made up of ordinary laypersons. Areas of expertise of forensic accountants are not only in accounting and auditing but in criminal investigation, interviewing, report writing, and testifying as expert witnesses. They must be excellent communicators, professional in demeanor, conservative in dress, and well groomed.

Financial auditors traditionally have been seen as, and to an extent have been, numbers-oriented, and their processes have been driven by the audit trail. The discipline of financial auditing has been thought to be almost a checklist of items to complete. In reality, judgment is crucial in financial auditing and has progressively increased in the direction of more dependence on auditor judgment. The Sarbanes-Oxley Act requirements involve auditor judgment to a large degree; auditors are to understand processes significant to financial reporting and to evaluate management's controls (in design and operating effectiveness) over those processes. Additionally, auditors are to consider environmental, including soft, intangible, factors in that evaluation.

Financial auditors have expertise in their knowledge of accounting and financial reporting (GAAP, or generally accepted accounting principles), auditing (GAAS), and how those apply to business transactions. As expressed in the GAAS literature, the most important financial auditing attributes are independence, objectivity, and professional skepticism.

The term *financial auditor* broadly applies to any auditor of financial information or the financial reporting process. The largest classification of financial auditors is those who work for public accounting firms and perform audits of financial statements for public companies. This classification is the most commonly used in this book when referring to financial auditors.

CLASSIC FRAUD RESEARCH

Fraud is a topic much in vogue today. Seminars, symposia, and conferences on that subject abound, sponsored by government agencies, universities, trade groups, professional organizations, chambers of commerce; and business, fraternal, and religious organizations. Most are well attended, particularly because the cost of such crimes to individual businesses and society is substantial, but also because few know much about fraud. Reviewing the literature creates an appreciation for the scope and nature of fraud and builds a foundation for understanding fraud topics.

The current term *fraud* was traditionally referred to as *white-collar crime,* and the two are used synonymously here. The classic works on

fraud are *White Collar Crime*, by Edwin H. Sutherland; *Other People's Money*, by Donald R. Cressey; *The Thief in the White Collar*, by Norman Jaspan and Hillel Black; and *Crime, Law, and Society*, by Frank E. Hartung.[3] These authorities essentially tell us:

> *White-collar crime has its genesis in the same general process as other criminal behavior; namely, differential association. The hypothesis of differential association is that criminal behavior is learned in association with those who define such behavior favorably and in isolation from those who define it unfavorably, and that a person in an appropriate situation engages in such criminal behavior if, and only if, the weight of the favorable definitions exceeds the weight of the unfavorable definitions.*[4]

In other words, birds of a feather flock together, or at least reinforce one another's rationalized views and values. But people make their own decisions and, even if subconsciously, in a cost-benefit manner. In order to commit fraud, a rationalization must exist for the individual to decide fraud is worth committing.

> *Trusted persons become trust violators when they conceive of themselves as having a financial problem which is nonshareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply their own conduct in that situation, verbalizations which enable them to adjust their conceptions of themselves as users of the entrusted funds or property.*[5]

Jaspan tried to derive antifraud measures in his research. His book, *The Thief in the White Collar,* is based on his many years of consulting experience on security-related matters, and contains a number of notable and often quoted generalizations. In a nutshell, Jaspan exhorts employers to (1) pay their employees fairly, (2) treat their employees decently, and (3) listen to their employees' problems, if they want to avoid employee fraud, theft, and embezzlement. But to temper that bit of humanism with a little reality, he also suggests that employers ought never to place full trust in either their employees or the security personnel they hire to check on employees.[6] Jaspan, like P. T. Barnum, would *always* cut the deck.

Hartung disagrees with Jaspan's generalizations and focuses on the individual. He argues:

> *It will be noticed that the criminal violator of financial trust and the career delinquent have one thing in common: Their criminality is learned in the process of symbolic communication, dependent upon cultural sources of patterns of thought and action, and for systems of values and vocabularies of motives.*[7]

In reality, both Jaspan and Hartung appear to have been correct. Hartung noted that individuals are inevitably affected by their environment. Although Jaspan might be considered too empathetic to the individual, his suggestions to deter fraud echo the same as modern efforts do: Create an environment with few reasons and with few opportunities to commit fraud.

FRAUD TRIANGLE

Why Is Fraud Committed?

Fraud or intentional deception is a strategy to achieve a personal or organizational goal or to satisfy a human need. However, a goal or need can be satisfied by honest means as well as by dishonest means. So what precipitates, inspires, or motivates one to select dishonest rather than honest means to satisfy goals and needs?

Generally speaking, competitive survival can be a motive for both honest and dishonest behavior. A threat to survival may cause one to choose either dishonest or honest means. When competition is keen and predatory, dishonesty can be rationalized quickly. Deceit, therefore, can become a weapon in any contest for survival. Stated differently, the struggle to survive (economically, socially, or politically) often generates deceitful behavior. The same is true of fraud in business.

"Fraud Triangle"

Of the traditional fraud research, Donald Cressey's research in the 1950s provides the most valuable insight into the question why fraud

is committed. The result of this research is most commonly, and succinctly, presented in what is known as the fraud triangle.

Cressey decided to interview fraudsters who were convicted of embezzlement. He interviewed about 200 embezzlers in prison. One of the major conclusions of his efforts was that every fraud had three things in common: (1) pressure (sometimes referred to as motivation, and usually an "unshareable need"); (2) rationalization (of personal ethics); and (3) knowledge and opportunity to commit the crime. These three points are the corners of the fraud triangle (see Exhibit 1.1).

Pressure *Pressure* (or incentive, or motivation) refers to something that has happened in the fraudster's personal life that creates a stressful need for funds, and thus motivates him to steal. Usually that motivation centers on some financial strain, but it could be the symptom of other types of pressures. For example, a drug habit or gambling habit could create great financial need in order to sustain the habit and thus create the pressure associated with this aspect of the fraud triangle. Sometimes a fraudster finds motivation in some incentive. For instance, almost all financial statement frauds were motivated by some incentive, usually related to stock prices or performance bonuses or both. Sometimes an insatiable greed causes relatively wealthy people to commit frauds.

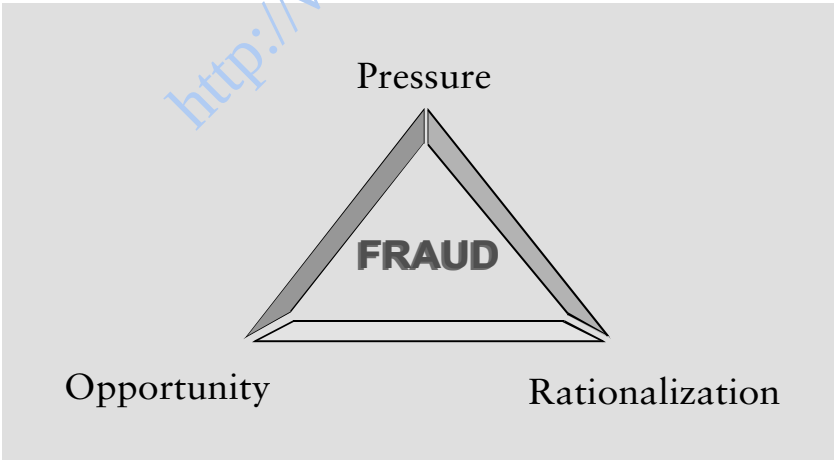

EXHIBIT 1.1 Fraud Triangle

Beyond the realm of competitive and economic survival, what other motives precipitate fraud? Social and political survival provide incentives, too, in the form of egocentric and ideological motives, especially in financial statement frauds. Sometimes people commit fraud (deception) to aggrandize their egos, put on airs, or assume false status. Sometimes they deceive to survive politically, or have a burning desire for power. They lie about their personal views or pretend to believe when they do not. Or they simply cheat or lie to their political opponents or intentionally misstate their opponents' positions on issues. They commit dirty tricks against opponents.

Motives to commit fraud in business usually are rationalized by the old saying that all is fair in love and war—and in business, which is amoral, anyway. There is one further category of motivation, however. We call it psychotic, because it cannot be explained in terms of rational behavior. In this category are the pathological liar, the professional confidence man, and the kleptomaniac.

Rationalization Most fraudsters do not have a criminal record. In the ACFE Report to the Nation (RTTN) 2004,[8] 88% of the reported fraudsters had no prior criminal record. In fact, white-collar criminals usually have a personal code of ethics. It is not uncommon for a fraudster to be religious. So how do fraudsters justify actions that are objectively criminal? They simply justify their crime under their circumstances. For instance, many will steal from employers but mentally convince themselves that they will repay it (i.e., "I am just borrowing the money"). Others believe no one is hurt so that makes the theft benign. Still others believe they deserve a raise or better treatment and are simply taking matters into their own hands to administer fair treatment. Many other excuses could serve as a rationalization, including some benevolent ones where the fraudster does not actually keep the stolen funds or assets but uses them for social purposes (e.g., to fund an animal clinic for strays).

Opportunity According to Cressey's research (i.e., the Fraud Tringle), fraudsters always had the knowledge and opportunity to commit the fraud. The former is reflected in known frauds, and in research studies such as the ACFE RTTNs, that show employees and managers tend to have a long tenure with a company when they commit the fraud. A simple explanation is that employees and managers who

have been around for years know quite well where the weaknesses are in the internal controls and have gained sufficient knowledge of how to commit the crime successfully.

But the main factor in opportunity is internal controls. A weakness in or absence of internal controls provides the opportunity for fraudsters to commit their crimes. It is noteworthy that the Treadway Commission (later known as the Committee of Sponsoring Organizations, or COSO) was formed to respond to the savings and loan frauds and scandals of the early 1980s. The committee's conclusion was that the best prevention was strong internal controls, and the result was the COSO model of internal controls, which was incorporated into financial auditing technical literature as SAS No. 78, *Consideration of Internal Control in a Financial Statement Audit*. Then the Sarbanes-Oxley Act (SOX) focused on an annual evaluation of the internal controls by management with an independent opinion of that evaluation by the financial auditors—Section 404 of the act. Again, if the purpose of SOX was to minimize fraud, internal control is the effective way to accomplish that goal. In fact, it could be argued that this aspect of the triangle is the only one that auditors can easily observe or control.

The opportunities to commit fraud are rampant in the presence of loose or lax management and (concomitant) inadequate attention to internal controls. When motivation is coupled with such opportunities, the potential for fraud is increased.

Motivation and Opportunities Fraud

On-the-job fraud, theft, and embezzlement are products of motivation and opportunity. The motivation may be economic need or greed, egocentricity, ideological conflicts, and psychosis. Most on-the-job frauds are committed for economic reasons and often are attributable to alcoholism, drug abuse, gambling, and high lifestyle. Loose or lax controls and a work environment that does not value honesty can provide the opportunity.

Motivations and opportunities are interactive: The greater the economic need, the less weakness in internal controls is needed to accomplish the fraud. The greater the weakness in controls, the level of motivational need necessary to commit a fraud is less.

SCOPE OF FRAUD

How pervasive is business fraud? How likely is it to be discovered either by audit design or by accident? Research in the last 10 years has been able to reveal both the scope of fraud and the most effective means of detecting frauds.

The scope of fraud is such that almost all midsize to large businesses are certain to have a fraud currently being or soon to be perpetrated. Virtually no small business is safe. Nor are not-for-profits or other types of organizations. Research by the ACFE reveals that the estimated level of fraud detected from 1996 to 2004 has been consistent in the U.S. economy—approximately 6% of annual revenues.[9]

Regarding financial frauds, a major study by COSO provides valuable insights. In 1998, COSO released its *Landmark Study on Fraud in Financial Reporting*.[10] The report covered 10 years of the Securities and Exchange Commission (SEC) enforcement cases, analyzing 200 randomly selected cases of alleged financial fraud investigated by the SEC—about two-thirds of the 300 SEC probes into fraud between 1987 and 1997. COSO examined certain key company and management characteristics, and the key findings were interesting: Most fraud among public companies was committed by small firms (well below $100 million in assets), boards of directors were dominated by insiders and inexperienced people, executive officers were identified as associated with financial statement fraud in 83% of the cases, and the average fraud period extended over a period of 23.7 months. The report went on to say: "The relatively small size of fraud companies suggests that the inability or even unwillingness to implement cost-effective internal controls may be a factor affecting the likelihood of financial statement fraud." COSO suggested external auditors focus on the "tone at the top" in evaluating internal control structures.

In 2003, KPMG released its third *Fraud Survey*.[11] In it, KPMG surveyed 459 public companies and government agencies. The report found that fraud is increasing in the number of instances reported since its last survey. Of the respondents, 75% reported losses due to fraud in 2003, as compared to 62% in 1998. Employee fraud was most common category of fraud (60%). The category of financial

reporting frauds averaged $257.9 million in costs per organization for the previous year, and the category of medical/insurance frauds averaged $33.7 million. These were the most costly fraud categories in the survey. Of the frauds reported, 36% incurred $1 million or more in costs, up from 21% in 1998. The median loss per incident was $116,000 for all types of fraud (1998). Only 4% of the frauds were discovered during financial statement audits in the 1998 survey, up to 12% in 2003. The most frequent methods of detection were internal controls (77%), internal audit (66%), employee tip (63%), and accident (54%). Obviously, there was some overlap in multiple detection methods.

The ACFE tracks the trend in fraud and statistics on fraud regularly. It has been conducting surveys on occupational fraud and abuse since 1996 and communicating the results to the public via its Report to the Nation. In all three reports (1996, 2002, 2004), the ACFE surveyed hundreds of Certified Fraud Examiners (CFEs), who reported facts on a fraud from the previous year. The results show enormous amounts of fraud each survey. The reported losses due to fraud were about 6% of reported revenues for those entities for each of the three years. Thus one measure of the scope of fraud is about 6% of the U.S. economy, or about 6% of the average firm. According to the most recent ACFE RTTN (2004), that figure would be $660 billion total. Fraud losses have increased by 50% since the first survey in 1996. Financial frauds lasted an average of 25 months before being discovered.

The various ACFE RTTNs have also measured the common methods of detecting fraud. According to the reports, tips and complaints have consistently been the most effective means of detecting frauds, and are a much higher percentage than the second most effective means. Tips and complaints accounted for 39.6% of the initial detection of occupational fraud in the 2004 report. Internal audit was second (23.8%), accident was third (21.3%), internal controls was fourth (18.4%), and external audit was fifth (10.9%).[12]

These research studies and other similar research show that fraud, of various kinds, is widespread. The best detection methods include tips, internal controls, and internal audit. The first two are integral tenets of the Sarbanes-Oxley Act of 2002.

PROFILE OF FRAUDSTERS

Who Commits Fraud?

In view of the last section, one might conclude that fraud is caused mainly by factors external to the individual: economic, competitive, social, and political factors, and poor controls. But how about the individual? Are some people more prone to commit fraud than others? And if so, is that a more serious cause of fraud than the external and internal environmental factors we have talked about? Data from criminology and sociology seem to suggest so.

Let us begin by making a few generalizations about people.

- Some people are honest all of the time.
- Some people (fewer than the above) are dishonest all of the time.
- Most people are honest some of the time.
- Some people are honest most of the time.

Research has been conducted to ask employees whether they are honest at work or not. Forty percent say they would not steal, 30% said they would, and 30% said they might.

Beyond those generalizations about people, what can we say about fraud perpetrators? Gwynn Nettler, in *Lying, Cheating and Stealing*,[13] offers these insights on cheaters and deceivers:

- People who have experienced failure are more likely to cheat.
- People who are disliked and who dislike themselves tend to be more deceitful.
- People who are impulsive, distractible, and unable to postpone gratification are more likely to engage in deceitful crimes.
- People who have a conscience (fear of apprehension and punishment) are more resistant to the temptation to deceive.
- Intelligent people tend to be more honest than ignorant people. Middle- and upper-class people tend to be more honest than lower-class people.
- The easier it is to cheat and steal, the more people will do so.
- Individuals have different needs and therefore different levels at which they will be moved to lie, cheat, or steal.

- Lying, cheating, and stealing increase when people have great pressure to achieve important objectives.
- The struggle to survive generates deceit.

People lie, cheat, and steal on the job in a variety of personal and organizational situations. The ways that follow are but a few:

1. Personal variables
   - Aptitudes/abilities
   - Attitudes/preferences
   - Personal needs/wants
   - Values/beliefs
2. Organizational variables
   - Nature/scope of the job (meaningful work)
   - Tools/training provided
   - Reward/recognition system
   - Quality of management and supervision
   - Clarity of role responsibilities
   - Clarity of job-related goals
   - Interpersonal trust
   - Motivational and ethical climate (ethics and values of superiors and coworkers)
3. External variables
   - Degree of competition in the industry
   - General economic conditions
   - Societal values (ethics of competitors and of social and political role models)

Why Do Employees Lie, Cheat, and Steal on the Job?

These 25 reasons for employee crimes are those most often advanced by authorities in white-collar crime (criminologists, psychologists, sociologists, risk managers, auditors, police, and security professionals):

1. The employee believes he can get away with it.
2. The employee thinks she desperately needs or desires the money or articles stolen.
3. The employee feels frustrated or dissatisfied about some aspect of the job.
4. The employee feels frustrated or dissatisfied about some aspect of his personal life that is not job related.
5. The employee feels abused by the employer and wants to get even.
6. The employee fails to consider the consequences of being caught.
7. The employee thinks: "Everybody else steals, so why not me?"
8. The employee thinks: "They're so big, stealing a little bit won't hurt them."
9. The employee doesn't know how to manage her own money, so is always broke and ready to steal.
10. The employee feels that beating the organization is a challenge and not a matter of economic gain alone.
11. The employee was economically, socially, or culturally deprived during childhood.
12. The employee is compensating for a void felt in his personal life and needs love, affection, and friendship.
13. The employee has no self-control and steals out of compulsion.
14. The employee believes a friend at work has been subjected to humiliation or abuse or has been treated unfairly.
15. The employee is just plain lazy and will not work hard to earn enough to buy what she wants or needs.
16. The organization's internal controls are so lax that everyone is tempted to steal.
17. No one has ever been prosecuted for stealing from the organization.
18. Most employee thieves are caught by accident rather than by audit or design. Therefore, fear of being caught is not a deterrent to theft.
19. Employees are not encouraged to discuss personal or financial problems at work or to seek management's advice and counsel on such matters.
20. Employee theft is a situational phenomenon. Each theft has its own preceding conditions, and each thief has her own motives.
21. Employees steal for any reason the human mind and imagination can conjure up.
22. Employees never go to jail or get harsh prison sentences for stealing, defrauding, or embezzling from their employers.

23. Human beings are weak and prone to sin.
24. Employees today are morally, ethically, and spiritually bankrupt.
25. Employees tend to imitate their bosses. If their bosses steal or cheat, then they are likely to do it also.

To be respected and thus complied with, laws must be rational, fair in application, and enforced quickly and efficiently. Company policies that relate to employee honesty, like criminal laws in general, must be rational, fair, and intended to serve the company's best economic interests. The test of rationality for any company security policy is whether its terms are understandable, whether its punishments or prohibitions are applicable to a real and serious matter, and whether its enforcement is possible in an efficient and legally effective way.

But what specific employee acts are serious enough to be prohibited and/or punished? Any act that could or does result in substantial loss, damage, or destruction of company assets should be prohibited.

The greatest deterrent to criminal behavior is sure and even-handed justice; that means swift detection and apprehension, a speedy and impartial trial, and punishment that fits the crime: loss of civil rights, privileges, property, personal freedom, or social approval. Having said all that, why is it that, despite the dire consequences of criminal behavior, we still see so much of it? Apparently because the rewards gained often exceed the risk of apprehension and punishment; or, stated another way, because the pains inflicted as punishment are not as severe as the pleasures of criminal behavior. The latter seems to be particularly true in cases of economic or white-collar crimes. Many times, if not most, when a fraud is detected, the extent of punishment regarding the perpetrator is to be fired, sometimes without even paying back the fraud losses. So while potential white-collar criminals might believe they might get caught, the ramifications are below some acceptable threshold.

Are white-collar criminals more rational than their blue-collar counterparts? If so, they probably weigh the potential costs (arrest, incarceration, embarrassment, loss of income) against the economic benefit—the monetary gain from their crime. If the benefit outweighs the cost, they opt to commit the crime—not just any crime, but crimes against employers, stockholders, creditors, bankers, customers, insurance carriers, and government regulators.

High-Level and Low-Level Thieves

All thieves steal as a matter of greed or need and as a matter of ease of opportunity. At high levels of organizational life, it is easy to steal because controls can be bypassed or overridden. The sums high-level managers steal, therefore, tend to be greater than the sums low-level personnel steal. For instance, according to the 2004 ACFE RTTN, executives average about $900,000 per fraud, managers about $150,000, and employees about $63,000. The number of incidents of theft, however, is greater at low levels of organizations because of the sheer number of employees found there.

The ACFE RTTN[14] has assessed the profile of fraudsters from the information provided by CFEs in its 2004 survey. The more expensive frauds, in terms of cost/losses, are done by fraudsters who tend to have these traits: (a) have been with the firm a longer time, (b) earn a higher income, (c) are male, (d) are over 60 years of age, (e) well educated {the higher the education, the higher the losses}, (f) operate in collusion rather than alone, and (g) have never been charged with anything criminal. These factors are probably correlated. That is, executives steal larger amounts and they fit this profile. The most frequent frauds, however, tend to point to a slightly different profile: (a) length of service—about the same, (b) income—earns much less, (c) gender—about even between male and female, (d) age—41 to 50, (e) education—high school, (f) operate—alone, (f) criminal record—about the same.

Another source[15] provides a similar profile for a typical fraudster: (a) position—low position, higher up, (b) gender—usually male, (c) age—over 50, (d) marital status—married, and (e) education—highly educated. This profile is similar to the one from the ACFE RTTN, and leads us to this overall conclusion: A white-collar criminal *does not look like a criminal*!

WHO IS VICTIMIZED BY FRAUD MOST OFTEN?

One might think that the most trusting people are also the most gullible and therefore most often the victims of fraud. Using that rationale, we could postulate that organizations with the highest levels of control would be least susceptible to fraud. But organizations

that go overboard on controls do not necessarily experience less fraud; and they have the added burden of higher costs.

Controls to protect against fraud by either organization insiders or outside vendors, suppliers, and contractors must be adequate; that is, they must accomplish the goal of control—cost-feasible protection of assets against loss, damage, or destruction. *Cost-feasible protection* means minimal expenditures for maximum protection. Creating an organizational police state would be control overkill. A balanced perspective on controls and security measures is the ideal, and that may require involving employees in creating control policies, plans, and procedures. A balanced perspective weighs the costs and benefits of proposed new controls and security measures. It means that a measure of trust must exist among employees at all levels. Trust breeds loyalty and honesty; distrust can breed disloyalty and perhaps even dishonesty.

Fraud is therefore most prevalent in organizations that have no controls, no trust, no ethical standards, no profits, and no future. Likewise, the more these circumstances exist, the higher the risk of fraud.

FRAUD TAXONOMIES

Most technical books have a glossary at the end. This one provides a taxonomy at the beginning to lay a simple but expanded foundation for what follows in the text. Another benefit of the taxonomy is that it provides a periodic quick review and thus reinforces the lessons learned at the first reading. In essence, the taxonomy summarizes the major principles of fraud auditing and forensic accounting.

General Dichotomies of Frauds

Consumer and Investor Frauds *Fraud,* in a nutshell, is intentional deception, commonly described as lying, cheating, and stealing. Fraud can be perpetrated against customers, creditors, investors, suppliers, bankers, insurers, or government authorities (e.g., tax fraud), stock fraud, and short weights and counts. For our purposes, we will limit

coverage to frauds in financial statements and commercial transactions. Consumer fraud has a literature of its own. Our aim is, therefore, to assist accountants and investigators in their efforts to detect and document fraud in books of account.

Criminal and Civil Fraud A specific act of fraud may be a criminal offense, a civil wrong, or grounds for the rescission of a contract. *Criminal fraud* requires proof of an intentional deception. *Civil fraud* requires that the victim suffer damages. Fraud in the inducement of a contract may vitiate consent and render a contract voidable.

The definition of a criminal fraud according to the ACFE is the one used in this book:

> Criminal fraud *denotes a false representation of a material fact made by one party to another party with the intent to deceive and induce the other party to justifiably rely on the fact to his/her detriment (i.e., his injury or loss).*

Fraud for and against the Company Fraud can be viewed from yet another perspective. When we think of fraud in a corporate or management context, we can perhaps develop a more meaningful and relevant taxonomy as a framework for fraud auditing.

Corporate frauds can be classified into two broad categories: (1) frauds directed against the company, and (2) frauds that benefit the company. In the former, the company is the victim; in the latter, the company, through the fraudulent actions of its officers, is the intended beneficiary. In that context, we can distinguish between organizational frauds that are intended to benefit the organizational entity and those that are intended to harm the entity.

For example, price fixing, corporate tax evasion, violations of environmental laws, false advertising, and short counts and weights are generally intended to aid the organization's financial performance. Manipulating accounting records to overstate profits is another illustration of a fraud intended to benefit the company but that may benefit management through bonuses based on profitability or stock prices in the market. In frauds *for* the organization, management may be involved in a conspiracy to deceive. Only one person may be involved in a fraud against the organization, such as an

accounts payable clerk who fabricates invoices from a nonexistent vendor, has checks issued to that vendor, and converts the checks to his own use.

Frauds for the company are committed mainly by senior managers who wish to enhance the financial position or condition of the company by such ploys as overstating income, sales, or assets or by understating expenses and liabilities. In essence, an intentional misstatement of a financial fact is made, and that can constitute a civil or criminal fraud. But income, for example, may also be intentionally understated to evade taxes, and expenses can be overstated for a similar reason. Frauds for the company by top managers are usually to deceive shareholders, creditors, and regulatory authorities. Similar frauds by lower-level profit-center managers may be to deceive their superiors in the organization, to make them believe the unit is more profitable or productive than it is, and thereby perhaps to earn a higher bonus award or a promotion. In the latter event, despite the fact that the subordinate's overstatement of income, sales, or productivity ostensibly helps the company look better, it is really a fraud *against* the company.

Frauds *against* the company are intended to benefit only the perpetrator, as in the case of theft of corporate assets or embezzlement. The latter specific category of fraud is often referred to as misappropriation of assets. Frauds against the company may also include vendors, suppliers, contractors, and competitors bribing employees. Cases of employee bribery are difficult to discern or discover by audit, because the corporation's accounting records generally are not manipulated, altered, or destroyed. Bribe payments are made under the table or, as lawyers say, "sub rosa." The first hint of bribery may come from an irate vendor whose product is consistently rejected despite its quality, price, and performance. Bribery may also become apparent if the employee begins to live beyond her means, far in excess of salary and family resources.

Several other financial crimes do not fit conveniently into our schema here but also are noteworthy: for example, arson for profit, planned bankruptcy, and fraudulent insurance claims.

Internal and External Fraud Frauds referred to as corporate or management frauds can be categorized as *internal frauds* to distinguish them from *external fraud* (a category that includes frauds committed by

vendors, suppliers, and contractors who might overbill, double bill, or substitute inferior goods). Customers may also play that game by feigning damage or destruction of goods in order to gain credits and allowances.

Corruption in the corporate sense may be practiced by outsiders against insiders, such as purchasing agents, for example. Corruption can also be committed by insiders against buyers from customer firms. Commercial bribery often is accompanied by manipulation of accounting records to cover up its payment and protect the recipients from the tax burden.

Management and Nonmanagement Fraud Corporate or organizational fraud is not restricted to high-level executives. Organizational fraud touches senior, middle, and first-line management as well as nonmanagement employees. There may be some notable distinctions between the means used and the motivations and opportunities the work environment provides, but fraud is found at all levels of an organization—if one bothers to look for it. Even if internal controls are adequate by professional standards, we should not forget that top managers can override controls with impunity, and often do so. In addition, even the best of internal controls suffers from atrophy, to the degree they depend on human intervention. This effect is measured by "effectiveness" of internal controls, to ensure they are functioning at the level designed and intended, and not at some subordinate level due to slackness on the part of employees responsible for elements of the controls.

Specific Frauds and Categories

As stated earlier, fraud is intentional deception. Its forms are generally referred to as lying and cheating. But theft by guile (larceny by trick, false pretenses, and false tokens) and embezzlement sometimes are included as fraudulent acts. The element of deception is the common ground they all share. But *fraud* and *deception* are abstract terms. They go by many other names as well. For example, in alphabetical order:

Accounts payable fabrication
Accounts receivable lapping
Arson for profit
Bank fraud
Bankruptcy fraud
Benefit claims fraud
Bid rigging
Breach of trust
Breach of fiduciary duty
Business opportunity fraud
Bust out
Cash lapping
Check forgery
Check kiting
Check raising
Collateral forgery
Commercial bribery
Computer fraud
Concealment
Consumer fraud
Conversion
Corporate fraud
Corruption
Counterfeiting
Credit card fraud
Defalcation
Distortion of fact
Double dealing
Duplicity
Electronic Funds Transfer fraud
Embezzlement
Expense account fraud
False advertising
False and misleading statement
False claim
False collateral
False count
False data
False identity
False information
False ownership
False pretenses
False report
False representation
False suggestion
False valuation
False weights and measures
Fictitious person
Fictitious customer
Fictitious employees
Fictitious vendors
Financial fraud
Financial misrepresentation
Forged documents
Forged signatures
Forgery
Franchising fraud
Fraud in execution
Fraud in inducement
Fraudulent concealment
Fraudulent financial statement
Fraudulent representation
Industrial espionage
Infringement of patents
Infringement of copyrights
Infringement of trademarks
Input scam
Insider trading
Insurance fraud
Inventory overstatement
Inventory reclassification fraud
Investor fraud

Kickback
Land fraud
Lapping
Larceny by trick
Loan fraud
Lying
Mail fraud
Management fraud
Material misstatement
Material omission
Misapplication
Misappropriation
Misfeasance
Misrepresentation
Oil and gas scams
Output scams
Over billing
Overstatement of revenue
Padding expenses
Padding government contracts
Payables fraud
Payroll fraud
Performance fraud
Price fixing
Pricing and extension fraud
Procurement fraud
Quality substitution
Restraint of trade
Sales overstatements
Securities fraud
Software piracy
Stock fraud
Subterfuge
Swindling
Tax fraud
Tax shelter scam
Technology theft
Theft of computer time
Theft of proprietary information
Throughput scam
Trade secret theft
Undue influence
Understatement of costs
Understatement of liabilities
Unjust enrichment
Vendor short shipment
Watered stock
Wire fraud
Wire transfer fraud

There are several models for categorizing the numerous possible typologies of fraud schemes. Those models are discussed later and are presented together in Exhibit 1.2.

One way to view the pervasiveness and complexity of fraud might be to design a fraud typology by various groups involved, as in Exhibits 1.2, 1.3, 1.4, and 1.5. An array of fraud characteristics may provide such insight. These lists of fraud perpetrators, victims, and fraud types summarize most frauds, but are far from exhaustive.

To summarize these typologies, our rough guide to classification appears as:

Insider Fraud against the Company

- Cash diversions, conversions, and thefts (front-end frauds)
- Check raising and signature or endorsement forgeries
- Receivables manipulations, such as lapping and fake credit memos
- Payables manipulations, such as raising or fabricating vendor invoices, benefit claims, and expense vouchers, and allowing vendors, suppliers, and contractors to overcharge
- Payroll manipulations, such as adding nonexistent employees or altering time cards
- Inventory manipulations and diversions, such as specious reclassifications of inventories to obsolete, damaged, or sample status, to create a cache from which thefts can be made more easily
- Favors and payments to employees by vendors, suppliers, and contractors

Outsider Fraud against the Company

- Vendor, supplier, and contractor frauds, such as short shipping goods, substituting goods of inferior quality, overbilling, double billing, billing but not delivering or delivering elsewhere
- Vendor, supplier, and contractor corruption of employees
- Customer corruption of employees

EXHIBIT 1.2 Fraud by Corporate Owners and Managers

Victim	Fraud Type
Customers	False advertising
	False weights
	False measures
	False labeling/branding
	Price fixing
	Quality substitution
	Cheap imitations
	Defective products
Stockholders	False financial statements
	False financial forecasts
	False representations
Creditors	False financial statements
	False financial forecasts
	False representations
Competitors	Predatory pricing
	Selling below cost
	Information piracy
	Infringement of patents/copyrights
	Commercial slander
	Libel
	Theft of trade secrets
	Corruption of employees
Bankers	Check kiting
	False application for credit
	False financial statements
Company/Employer	Expense account padding
	Performance fakery
	Overstating revenue
	Overstating assets
	Overstating profits
	Understating expenses
	Understating liabilities
	Theft of assets
	Embezzlement
	Conversion of assets
	Commercial bribery
	Insider trading
	Related party transactions
	Alteration/destruction of records
Insurance Carriers	Fraudulent loss claims
	Arson for profit
	False application for insurance
Government Agencies	False claims
	Contract padding
	Willful failure to file reports/returns

EXHIBIT 1.3 Fraud by Corporate Vendors, Suppliers, and Contractors

Victim	Fraud Type
Customers	Short shipment
Customers	Overbilling
Customers	Double billing
Customers	Substitution of inferior goods
Customers	Corruption of employees

Source: Adapted from Jack Bologna, *Forensic Accounting Review* (1984).

Frauds for the Company

- Smoothing profits (cooking the books) through practices such as inflating sales, profits, and assets; understating expenses, losses, and liabilities; not recording or delaying recording of sales returns; early booking of sales; and inflating ending inventory
- Check kiting
- Price fixing
- Cheating customers by using devices such as short weights, counts, and measures; substituting cheaper materials; and false advertising
- Violating governmental regulations (e.g., Equal Employment Opportunity Act [EEO], Occupation Safety and Health Administration [OSHA], environmental securities, or tax violations standards)
- Corrupting customer personnel
- Political corruption
- Padding costs on government contracts

EXHIBIT 1.4 Fraud by Corporate Customers

Victim	Fraud Type
Vendors	Tag switching
Vendors	Shoplifting
Vendors	Fraudulent checks
Vendors	Fraudulent claims for refunds
Vendors	Fraudulent credit cards
Vendors	Fraudulent credit applications

Source: Adapted from Jack Bologna, *Forensic Accounting Review* (1984).

EXHIBIT 1.5 Fraud by Corporate Employees

Victim	Fraud Type
Employers	False employment applications
Employers	False benefit claims
Employers	False expense claims
Employers	Theft and pilferage
Employers	Performance fakery
Employers	Embezzlement
Employers	Corruption

Source: Adapted from Jack Bologna, *Forensic Accounting Review* (1984).

The ACFE has developed a model for categorizing known frauds that it calls the "fraud tree," which lists about 51 different individual fraud schemes grouped by categories and subcategories. The three main categories are (1) fraudulent statements, (2) asset misappropriation, and (3) corruption. Fraudulent statement fraud schemes typically are done by executives. They are the most expensive frauds but the least frequent ones. They are often driven by motives related to stock prices in the market (e.g., stock bonuses, pressure to keep stock prices trading high or higher, etc.). Asset misappropriation schemes typically are done by employees and include a large number of different schemes. They are the most common by occurrence (frequency) but the least costly per incident. Because they tend to be immaterial, especially individual transactions, they are difficult for financial or internal auditors to discover doing traditional financial and internal audits. Corruption involves a number of schemes, such as bribery and extortion, that usually involve more than one person, even though one might be an unwilling party.

Other notable fraud taxonomies exist. KPMG used a different taxonomy in its fraud surveys. Dr. Steve Albrecht uses another one in his book on fraud.[16] Exhibit 1.6 summarizes these major taxonomies.

EVOLUTION OF A TYPICAL FRAUD

Most frauds follow a similar pattern in the life cycle of the processes or steps. There are differences to consider depending on the fraud. For example, a skimming fraud scheme is "off the books" and therefore

EXHIBIT 1.6 Summary of Models/Typologies/Taxonomies

Source	Fraud Taxonomy
Bologna – Lindquist [2e]	Insider fraud against the company Outsider fraud against the company Frauds for the company
KPMG	Employee fraud Consumer fraud Vendor-related fraud Computer crime Misconduct Medical/insurance fraud Financial reporting fraud
Steve Albrecht	Employee embezzlement Management fraud Investment scams Vendor fraud Customer fraud Miscellaneous fraud
ACFE	Fraudulent statement fraud Asset misappropriation Corruption

requires no real concealment of the fraud. Likewise, the motivation for financial statement frauds is usually very different from that of asset misappropriation frauds. A general evolution of a typical fraud follows.

1. **Motivation/Pressure**
   - Need
   - Greed
   - Revenge
2. **Opportunity (control weaknesses)**
   - Access to assets, records, and/or documents that control assets
   - No audit trails or separation of duties
   - No rotation of duties
   - No internal audit function
   - No control policies
   - No code of ethics

3. **Rationalization (formulation of intent)**	Rationalization of the crime as borrowing, etc., not stealing
4. **Commit the Fraud**	Execute the particular fraud scheme; fraud, theft, embezzlement, etc.
5. **Convert to Cash**	If it is not a cash theft, the fraudster must convert the theft to cash (e.g., theft of inventory, financial fraud to stock to cash, or cashing a check made out to a bogus or real payee)
6. **Conceal the Fraud**	Alter documents and/or records Forgery Destruction of records *(For skimming and other off-the-books frauds, no concealment is necessary.)*
7. **Red Flags**	Variances detected Allegations made Behavior pattern change noted in the fraudster *(If it is an on-the-books scheme, red flags are likely to occur in the accounting records and data. But even off-the-books schemes exhibit the behavioral red flags.)*
8. **Audit Initiated**	Detection of fraud or discrepancies detected by some method (tips most common; also internal controls, accident, and internal audit are common methods) Anomalies identified and determined to be fraudulent in nature

9. Investigation Initiated	Evidence gathered Loss of assets confirmed and documented Interrogation of third parties, employees with knowledge, and suspect conducted
10a. Disposition: Fraudster Terminated	Employee terminated for cause (often management does not desire to pursue legal disposition for various reasons) Insurance claim filed
10b. Disposition: Prosecution Recommended	Criminal prosecution sought Civil recovery sought Insurance claim filed
11. Trial	Presentation of facts and testimony

Some of these items are covered in this chapter, at least by way of introduction to basic concepts. The remainder of the book focuses on this list, usually in the sequence listed.

ENDNOTES

1. Michigan Criminal Law, Chapter 86, Sec. 1529.
2. *Southern Development Co. v. Silva,* 125 U.S. 247, 8 S.C. Rep. 881, 31 L. Ed. (1887).
3. Edwin H. Sutherland, *White-Collar Crime* (New York: Dryden Press, 1949), p. 234; Donald L. Cressey, *Other People's Money* (New York: Free Press, 1949), p. 30; Norman Jaspan and Hillel Black, *The Thief in the White Collar* (Philadelphia: Lippincott, 1960), p. 37; and Frank E. Hartung, *Crime, Law, and Society* (Detroit: Wayne State University Press, 1965), pp. 125–136.
4. Sutherland, *White-Collar Crime.*
5. Cressey, *Other People's Money.*
6. Jaspan, and Black, *The Thief in the White Collar.*
7. Hartung, *Crime, Law, and Society.*

8. Association of Certified Fraud Examiners (ACFE), *Report to the Nation* (RTTN), 2004.
9. Association of Certified Fraud Examiners (ACFE), *Report to the Nation,* 1996, 2002, and 2004
10. Committee of Sponsoring Organizations (COSO), *Landmark Study on Fraud in Financial Reporting,* 1998.
11. KPMG, *Fraud Survey,* 1994, 1998, and 2003.
12. ACFE, *Report to the Nation:* 1996, 2002, and 2004.
13. Gwynn Nettler, *Lying, Cheating and Stealing* (Cincinnati: Anderson Publishing, 1982).
14. ACFE, *Report to the Nation,* 2004.
15. James A. Hall and Tommie Singleton, *IT Auditing & Assurance* (New York: Southwestern, 2004).
16. W. S. Albrecht and C. Albrecht, *Fraud Examination and Prevention* (New York: Thomson/Southwestern, 2004).