PRINT X CLOSE

Small Business FRAUD PREVENTION Manual

PART 1: INTERNAL FRAUD THREATS

I. INTRODUCTION TO EMPLOYEE FRAUD

The Shocking Cost of Employee Theft and Fraud

Occupational fraud is defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets.

Simply stated, occupational fraud and abuse occurs when an employee, manager, or executive commits fraud against his or her employer. Occupational fraud and abuse is roughly a synonym for terms like *employee fraud* or *embezzlement*, although technically, the term *occupational fraud and abuse* is more broad and better reflects the full range of employee misconduct through which organizations lose money.

The threat of occupational fraud looms over every business or public agency, regardless of its size, stature, or function. It is safe to say that if you have employees, at some point in time some form of occupational fraud will victimize you. These are not crimes that only happen to the company down the street; they occur in every organization (including yours) and employees at every level commit them — from top executives down to entry-level clerks. Research indicates that levels of occupational fraud and abuse are staggeringly high, both in their cost and in their rate of occurrence.

In 2003, KPMG released the results of its third *U.S. Fraud Survey*. The survey drew on interviews of more than 450 executives in medium-sized and large organizations across industries and in state and federal government agencies. According to the results of KPMG's 2003 Fraud Survey, organizations are reporting more experiences of fraud than in prior years and are taking concerted actions to deal with it. Seventy-five percent of companies surveyed reported that they experienced an instance of fraud — 13 percentage points more than in their 1998 survey.

Their survey showed that while employee fraud is the most prevalent type of fraud experienced by organizations, financial reporting fraud and medical/insurance fraud are the most costly. Their survey also showed that collectively, organizations are working hard to combat fraud. Three out of 4 organizations evaluated their compliance programs within the last 12 months. An equally large number plans to implement new programs or procedures to help combat fraud and misconduct in direct response to the Sarbanes-Oxley Act.

In March 2007, KPMG released its *2005-2006 Integrity Survey*. The results of the survey were based on responses from 4,056 U.S. employees, spanning all levels of job responsibility, 16 job functions, 11

industry sectors, and 4 thresholds of organizational size. According to the results of the survey, nearly three out of four employees reported that they have observed misconduct in the workplace in the prior 12-month period, with half of employees reporting that what they have observed was serious misconduct that could cause "a significant loss of public trust if discovered." Between 2000 (when the first *Integrity Survey* was conducted) and 2005, employees reported consistent levels of overall misconduct, with 74% reporting in 2005 that they had observed misconduct — compared with 76% in 2000, and consistent levels of serious misconduct — with 50% in 2005 characterizing the misconduct they observed as serious, compared with 49% in 2000. Although the level of observed misconduct has remained constant, employees reported that the conditions that facilitate management's ability to prevent, detect, and respond to fraud and misconduct within companies are improving. Employees who worked in companies with comprehensive ethics and compliance programs reported more favorable results across the board than did those who worked in companies without such programs. For instance, employees who worked in companies with such programs reported fewer observations of misconduct and higher levels of confidence in management's commitment to integrity.

In 2006, Ernst & Young conducted its ninth biennial global survey on fraud risk in emerging markets. They found that one in five respondents — regardless of region, industry, or size of business — said they had experienced a significant fraud in the past two years. E&Y found that robust internal controls remained the first line of defense against fraud for companies in all markets, but anti-fraud controls are not always integrated under an anti-fraud program or separately monitored for operating effectiveness. Over 90% of respondents believe that their internal controls are sufficient to identify and investigate fraud promptly. A heightened sensitivity to the effectiveness of internal controls is evidenced by the respondents' views on the reasons for investigating fraud. In the 2003 global fraud survey, investigating fraud was primarily driven by a desire to determine the extent of the fraud and to bring an end to it. In the 2006 survey, over 50% of respondents now investigate fraud with a clear desire to identify and improve internal control weaknesses, hence, preventing future frauds.

According to the E&Y survey, on a global basis, over 40% of companies do not have a formal anti-fraud policy. This demonstrates that the implementation of corporate governance guidelines and the focus on internal controls has not automatically extended to the adoption of a formal anti-fraud policy. Less than half of the companies with anti-fraud policies communicate those policies to their suppliers and customers, while even fewer communicate them to agents/intermediaries and joint venture partners. Of the companies surveyed, alarmingly 72% do not provide their employees with training to understand and implement the organization's anti-fraud policy.

In September 2007, the *2006 National Retail Security Survey* was released which reported that retailers attributed 47% of their company's losses to employee theft in 2006. Assuming a total inventory shrinkage dollar amount of approximately $40.5 billion, this translates into an annual employee theft

price tag of $19 billion. This is a staggering monetary loss to come from a single crime type. In fact, there is no other form of larceny that annually costs American citizens more money than employee theft.

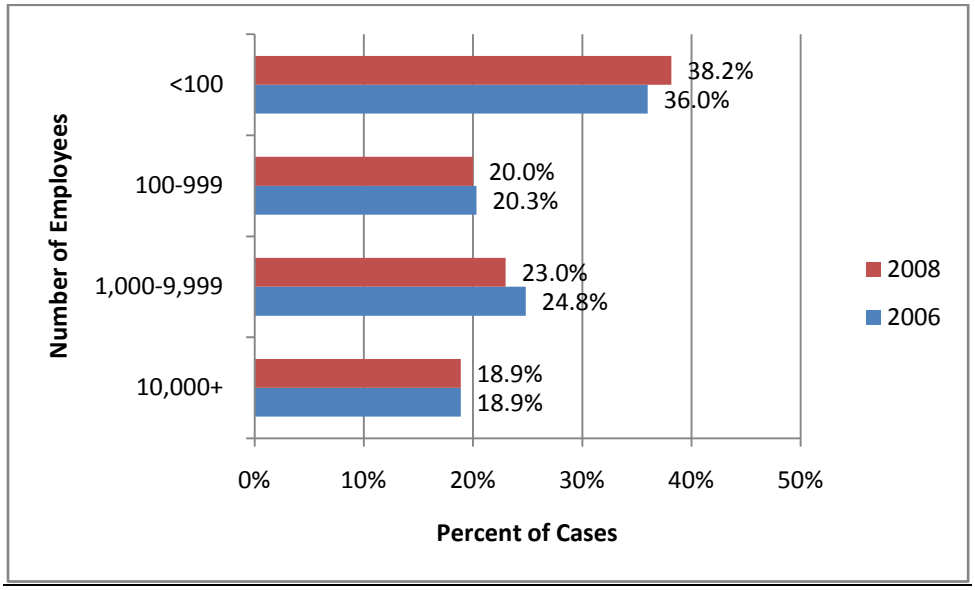
In 2008, the Association of Certified Fraud Examiners published the fifth *Report to the Nation on Occupational Fraud and Abuse*, which was based on a survey of 959 Certified Fraud Examiners throughout the United States. Those CFEs estimated that, within their own companies, losses due to fraud and abuse accounted for approximately 7% of annual revenues. If this figure is applied to the U.S. Gross Domestic Product — which is estimated to be $14,196 trillion in 2008 — this translates to losses of about $994 billion annually. This finding differs from the first, second, third and fourth *Report to the Nation,* conducted in 1996, 2002, 2004 and 2006 respectively, in which CFEs estimated that their organizations lost 5-6% of revenues to fraud.

Unfortunately, any estimate of the total cost fraud imposes on our economy is just that — an estimate. The 7% figure reflected by the *Report to the Nation* is simply the collective opinions of those who work in the anti-fraud field. The figure provides a best-guess point of reference based on the opinions of 959 anti-fraud experts with a median of 15 years' experience in the prevention and detection of occupational fraud. Finding the actual cost may not be possible by any method. Many organizations are reluctant to report fraud when it occurs for fear that it will make them look vulnerable to consumers or hurt their stock price. Some feel embarrassment at having been victimized and prefer closure to the ongoing process of discovery that comes with an investigation and prosecution. Even those who do report fraud cases frequently are unable to determine the true cost sustained by the crime. And, of course, there are the frauds that are not caught, that go on day after day, silently draining organizational resources. All these factors make it virtually impossible to determine how big a factor fraud is in the business world. But whatever the actual costs, it is clear that they are high, and organizations are unwittingly paying them already as a part of their total operating expenses.

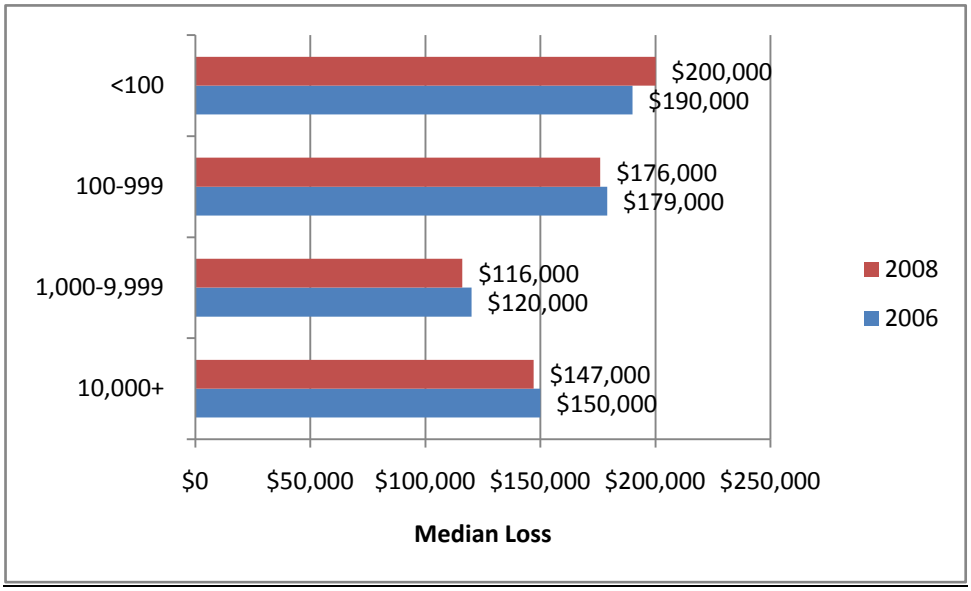
The Cost of Fraud to Small Businesses

The *2008 Report to the Nation* was designed in part to help measure the effects fraud has on businesses of various sizes. The fraud schemes that we studied were classified according to size of the victim companies (based on number of employees). We then sought to determine the median cost of occupational fraud schemes based on the size of the organization that is victimized. Continuing the trend we have seen in our previous studies, small businesses — defined as those with less than 100 employees — suffered both a greater percentage of frauds (38%) and a higher median loss ($200,00) than their larger counterparts. These findings accentuate the unique problems in combating fraud — primarily the limited amount of fiscal and human resources available for anti-fraud efforts — frequently faced by small organizations.

Size of Victim Organization — Frequency



Size of Victim Organization — Median Loss



There appear to be two key factors that contribute to the large losses suffered by small companies. First, organizations with small staffs often lack basic accounting controls. Many small businesses have a one-person accounting department — a single employee writes checks, reconciles the accounts, and posts the books. Whenever control of a company's finances is consolidated in a single individual, occupational fraud is easy to commit and conceal.

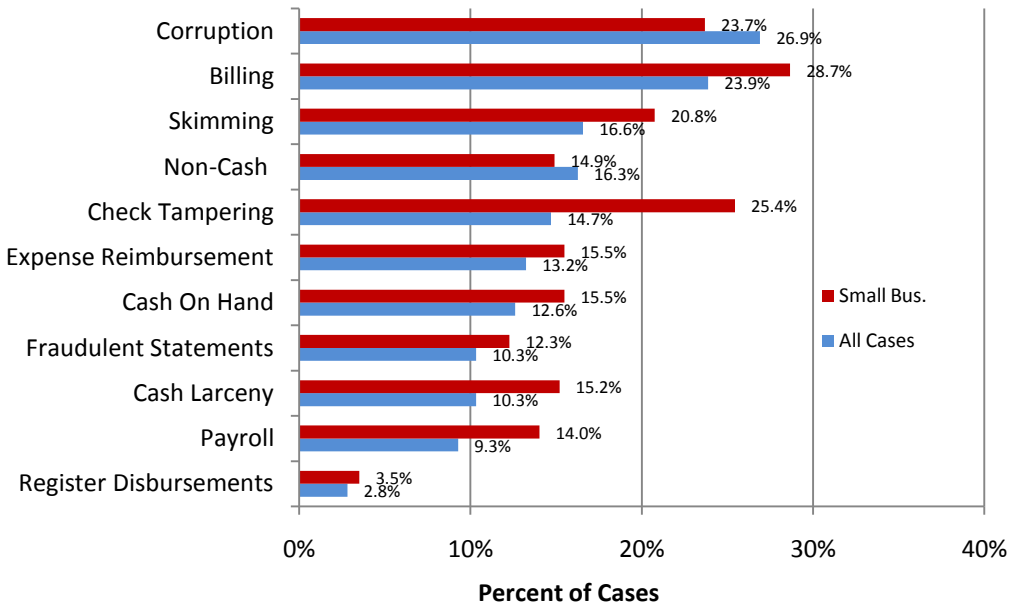
The second reason losses are so high in small organizations is that there tends to be a greater degree of trust among co-workers in small businesses. In an atmosphere where employees and management know each other well on a personal basis they tend to be less alert to the possibility of fraud.

Methods of Fraud in Small Businesses

Because of persistent evidence suggesting that fraud operates on small businesses differently than on larger organizations, the ACFE felt it was important to identify the most common schemes in small organizations. This may provide some guidance to small business owners on where to focus anti-fraud efforts. To better understand the fraud issues faced by small businesses, the ACFE measured the frequency with which different fraud schemes occurred in these organizations. As the chart below illustrates, check tampering was much more common in small businesses than in other organizations. Over one-fourth of all small business frauds involved this form of fraud, which commonly occurs in situations where duties over the cash disbursement function are not segregated. Anecdotal evidence suggests this control weakness is often present in small organizations. Billing schemes, skimming, cash larceny, and payroll fraud were also noticeably more common in small businesses.

SMALL BUSINESS — <100 EMPLOYEES (342 CASES)		
Scheme	**Cases**	**Pct**
Billing	98	28.7%
Check Tampering	87	25.4%
Corruption	81	23.7%
Skimming	71	20.8%
Expense Reimbursement	53	15.5%
Cash on Hand	53	15.5%
Larceny	52	15.2%
Non-Cash	51	14.9%
Payroll	48	14.0%
Fraudulent Financial Statements	42	12.3%
Register Disbursements	12	3.5%

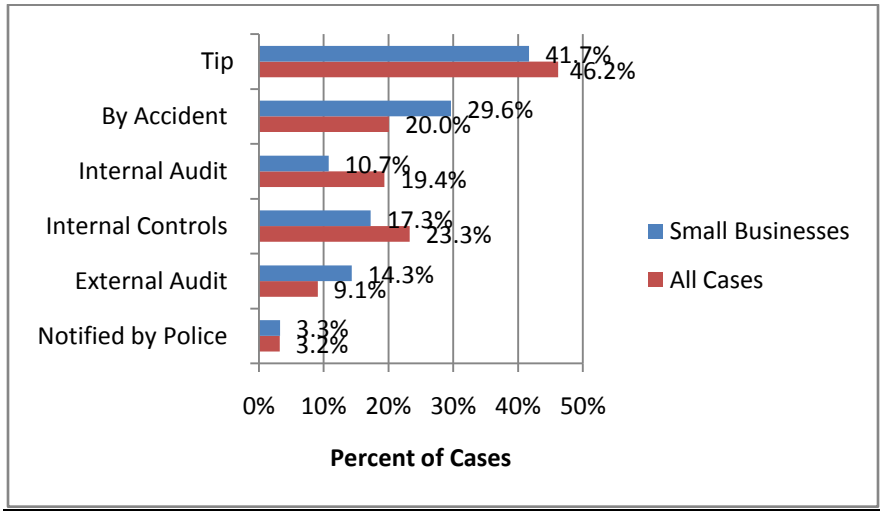
Methods of Fraud—Small Business Cases vs. All Cases



Detecting Fraud in Small Businesses

Small businesses are typically thought to have fewer or weaker controls in place than their larger counterparts, primarily due to a lack of personnel or financial resources. The results of our survey bear this out, as a lower percentage of frauds in small businesses were caught by internal controls. Additionally, internal audits and tips were cited as the detection method in fewer small business cases than among all cases, while small business frauds were also more likely to be detected by accident. These findings indicate that small organizations have room for improvement in their proactive fraud detection efforts.

Initial Detection of Frauds in Small Businesses



Why Employees Commit Fraud

Donald R. Cressey and the Fraud Triangle

When asked why employees commit fraud, most people would say it is because the perpetrators are "greedy" or "con artists" or something of the like. These terms imply that the offenders possess some defect of character that separates them from normal, law-abiding citizens. By using these terms; we are able to view occupational fraud as an aberration, something far outside the norm, and as misdeeds committed by "bad" people. To extend the implication, as long as we employ "good" people, we would be safe from falling victim to an occupational fraud scheme.

The truth, however, is that even "good" people commit occupational fraud. To be sure, fraud constitutes aberrational conduct and it necessarily involves both greed and deception. Furthermore, there are some predatory employees who move from job to job with the sole intent of robbing whoever is unlucky enough to hire them. But most fraudsters are not career criminals. Most employees who embezzle do not take their jobs with the intention of stealing from their company. Typically, the employee who steals from his or her company is an otherwise law-abiding citizen who, for a variety of reasons, crosses the line into illegal conduct. In fact, when fraud occurs in a small business, it is usually committed by a long-term, trusted employee. If your company is victimized by employee fraud, the new employee who keeps to himself, the one who seems a little shady, probably won't commit it. Chances are the one who steals from you will be the highly trusted employee, the hardest-working person in your company, the one who's been with you ten years and knows your children's' names. After small businesses have been attacked by an employee fraud scheme, the most commonly repeated sentiment is, "I never would have thought it would be him/her." The biggest hurdle for most people to get over in terms of understanding occupational fraud is to realize that *anyone* can commit fraud.

Once we understand that fraud can be committed by anyone, the obvious question is, why do they do it? What causes certain employees to commit fraud? When trying to understand what motivates this form of criminal behavior, we must first understand that there is no single factor that causes employees to commit fraud. Instead, there is a complex set of motivators that, when combined in the right environment, produce the impetus for an employee to begin committing fraud.

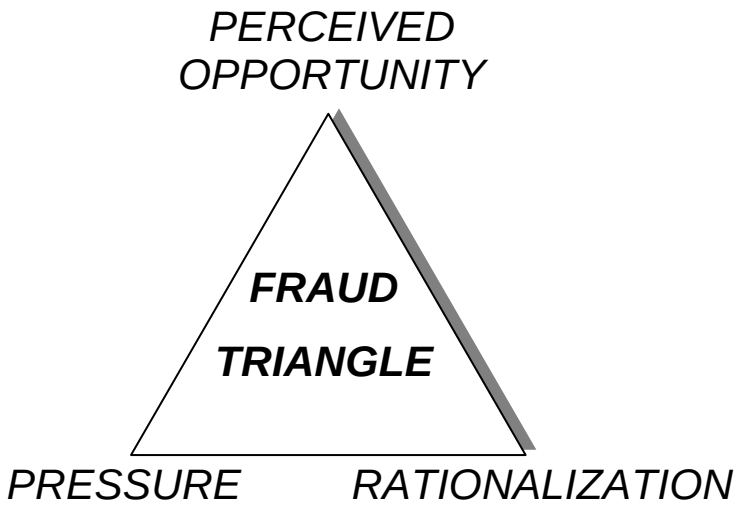
The most widely accepted theory for explaining why people embezzle was postulated by Dr. Donald R. Cressey (1919-1987). Cressey was intrigued by embezzlers, whom he called "trust violators." In 1953, while working on his doctorate at Indiana University, Cressey decided to focus his dissertation on the factors that lead people to embezzle. He was especially interested in the circumstances that led otherwise honest people to be overcome by temptation. For that reason, he excluded from his research those employees who took their jobs for the purpose of stealing — a relatively minor number of offenders at that time.

To serve as a basis for his work, Cressey conducted extensive interviews with about 200 inmates at Midwest prisons who had been incarcerated for embezzlement. Upon completion of his interviews, he developed what still remains the classic model for the occupational offender. His research was published in *Other People's Money: A Study in the Social Psychology of Embezzlement*.

Cressey's final hypothesis was:

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

Over the years, the hypothesis has become better known as the *Fraud Triangle*. According to the Fraud Triangle Theory, there are three factors (each represented by a leg of the triangle) that when combined, lead people to commit occupational fraud. One leg represents a *perceived nonsharable financial need*. The second leg represents a *perceived opportunity* to secretly resolve the financial need. The third leg represents the perpetrator's ability to *rationalize* the illegal conduct, to justify crime in their mind. One of the most fundamental observations of the Cressey study was that it took all three elements — perceived motive, perceived opportunity, and the ability to rationalize — for the trust violation (fraud) to occur.



Nonsharable Financial Need

The role of the nonsharable financial problem is crucial. An otherwise honest employee usually only starts committing fraud when faced with some great financial pressure. The extreme need for money leads the person to engage in illegal acts, something the person probably would not do under normal circumstances. In his study, Cressey asked his subjects why they had embezzled in one instance, but had refrained from doing the same thing in previous jobs or positions of trust when they had had the chance. Their responses usually fell into one of the following categories: "(a) 'There was no need for it like there was this time.' (b) 'The idea never entered my head.' (c) 'I thought it was dishonest then, but this time it did not seem dishonest at first.'"

Keep in mind that the first leg of the triangle is not simply financial pressure. We all have financial pressure. The common element in the subjects Cressey studied was a *perceived, nonsharable* financial pressure. Cressey wrote, "*In all cases of trust violation encountered, the violator considered that a financial problem which confronted him could not be shared with persons who, from a more objective point of view, probably could have aided in the solution of the problem.*" In general, nonsharable financial problems are those that carry, in the subject's mind, some sort of shame or stigma. As a result, the subject feels unable to discuss the problem or seek help from others.

That which is considered "nonsharable" is wholly in the eyes of the potential occupational offender, Cressey said. One person might lose $1,000 gambling at the racetrack, but not consider this to be a nonsharable problem. Another man who loses the same $1,000 might feel a sense of shame attached to the loss and therefore feel the need to keep his loss secret. Although both men have experienced the same loss in terms of dollars, only the second man has experienced a perceived nonsharable financial problem. It is the second man who is more likely to resort to secret, illegal means to rectify his problem.

Cressey divided "nonsharable" problems into six basic subtypes:

- **Violation of ascribed obligations**: the subject faces the prospect of being unable to pay his debts.
- **Problems resulting from personal failure**: the subject experiences problems such as drug addiction that result from poor personal judgment.
- **Business reversals**: the subject faces the prospect of a failing business.
- **Physical isolation**: the subject is isolated from people who could help him with his problem.
- **Status gaining**: the subject seeks to maintain a certain status level but does not have the financial means to do so.
- **Employer-employee relations**: the subject feels he has been mistreated by his employer and needs to "get even."

Perceived Opportunity

Having a perceived nonsharable financial need is only one element of the fraud tree. In order for the employee to take the next step towards committing fraud that employee must believe he will be able to resolve his financial situation in secret. In other words, he must *perceive* that there is an *opportunity* to fix the problem without being caught. Cressey wrote:

> *"Although the clear conception of a financial problem as nonsharable does not invariably result in trust violation, it does establish in trusted persons a desire for a specific kind of solution to their problems. The results desired in the cases encountered were uniform: the solution or partial solution of the problem by the use of funds which can be obtained in an independent, relatively secret, safe, and sure method in keeping with the 'rationalizations' available to the person at the time."*

The *perceived opportunity* leg of the fraud triangle is very important because it goes right to the heart of what companies do to prevent fraud. Generally, employee's only commit fraud when they perceive that there is a way to commit the crime in such a way that the company will not realize a fraud has occurred. After all, if the fraud is discovered, the employee will face punishment, humiliation, and loss of job. Unlike the typical street criminal, the employee who commits fraud is not in a position to steal money and flee the scene. On the contrary, the employee-fraudster has to keep coming back to the scene of the crime every day.

If an employee knows, for instance, that he is the only person who writes checks, posts entries, and reconciles the checking account, then he may perceive that there is an opportunity to solve his financial problem by writing a check to himself, a creditor, etc. If no one ever looks at the checkbook, the fraud will never be discovered. The employee will see an opportunity to solve his personal crisis without getting caught. On the other hand, if the employee knows that someone always reviews the monthly bank statement or that authorized check signers will question any suspicious checks, then he will perceive that if he tries to write a fraudulent check, the crime will be detected.

This illustrates the key to preventing fraud: *perception of detection*. Employees are less likely to commit fraud when they believe that the company will detect it. Therefore, by establishing strong controls and by letting employees know that management is looking out for fraud, a company can deter its employees from attempting to steal.

Rationalization

The third leg of Cressey's fraud triangle deals with *rationalization* — how are offenders able to convince themselves that stealing is okay? Cressey found they were able to excuse their actions to themselves by

viewing their crimes as (1) noncriminal, (2) justified, or (3) part of a situation, which the offender does not control.

Recall that most employees who commit fraud are not career criminals at least they don't start out that way. These are generally people who consider themselves to be upright, law-abiding citizens. Therefore, in order for them to begin stealing, it is critical for them to be able to develop some excuse to rationalize their conduct and help them maintain their image of themselves as moral people. Also, by developing a rationalization they feel that their conduct will be explainable if it is discovered. One of the simplest ways to justify unacceptable conduct and avoid feelings of guilt is to invent a good reason for embezzling — one sanctioned in the social group as a greater good.

There are several rationalizations that are common to embezzlers and are repeated over and over by those who are caught committing occupational fraud. They include:

- "I was only borrowing. I was going to pay everything back."
- "I only did it because of unusual circumstances. Normally, I'd never have taken the money."
- "I did it to provide for my family (pay bills, keep up the mortgage, etc.)."
- "My employer had been cheating me/treating me unfairly. I only did it to get even."
- "My employer is dishonest. They rip off their customers; so they deserve to be ripped off."
- "I had to have the money. I only did it out of necessity."
- "Everybody does it."
- "After all I've done for the company, I was entitled to it."

Conclusions

Cressey's classic fraud triangle helps explain the nature of many — but not al l— occupational offenders. It is obvious that one model will not fit all situations. In addition, Cressey's study is nearly half a century old. There has been considerable social change in the interim. And now, many anti-fraud professionals believe there is a new breed of occupational offender — one who simply lacks a conscience sufficient to overcome temptation.

Cressey's model also does not fit the predatory employee who takes a job with the intent of stealing. But for the majority of occupational fraudsters, the fraud triangle provides a framework to explain why they commit their crimes. Companies can use Cressey's model to help them prevent employee fraud. For instance, because we know that most employees start stealing when faced with a *nonsharable financial problem*, companies can be alert for employees who exhibit signs of stress or who indicate that they are in a bad financial situation. By establishing open door policies, companies can provide these employees with a place to air their problems, to seek help, and to hopefully find solutions before they turn to fraud.

With regard to the second leg of the fraud triangle, companies can attempt to limit *perceived opportunities* to commit fraud. This can be accomplished in a variety of ways: establish strong internal controls; separate duties; conduct random audits or cash counts (let employees know random tests will be conducted, but not when); establish a management presence wherever cash or merchandise is handled; and terminate and refer for prosecution anyone who is caught committing fraud; etc.

Regarding the third leg of the fraud triangle, companies can look for signs of *rationalization* among employees, particularly those who are already at-risk fraud candidates. Be aware of employees who seem disgruntled, who feel they have been treated unfairly or passed over for promotions. Also look for signs of extreme financial stress that could lead an employee to justify misconduct. Finally, review compensation policies to make sure employees receive adequate pay based on their jobs and the labor market. Simply stated, happy employees are less likely to steal.

Continuing Conduct

Cressey's model is a great tool for explaining why employees *begin* to commit fraud, but experience shows that once an employee starts stealing, they will tend to continue. The thefts usually get larger or more frequent (or both) until the perpetrator gets caught or leaves the company, or until the company is driven out of business. As fraud schemes progress, the importance of the elements that make up the fraud tree begin to diminish. For instance, suppose Anne, a bookkeeper, begins writing company checks to pay off a personal debt. Once Anne sees that she can write bad checks without getting caught, she will become hooked on the source of extra income that she has found. Though the scheme may have begun because of a nonsharable financial problem, she will tend to continue with it, even after the immediate problem has been solved. She may start writing checks to pay for luxury items, vacations, and other non-essential purchases. Likewise, she might begin the scheme by rationalizing that she is only borrowing the money from the company. But as the scheme progresses, there will be less and less need for her to keep rationalizing her misconduct. The theft will become the norm for her, to the point where she will not have to justify it to herself at all, until she finally gets caught.

The preceding example illustrates what some anti-fraud professionals have dubbed "The Potato Chip Theory of Fraud." As the theory goes, a perpetrator cannot stop at just one fraud. They keep nibbling and nibbling. Frequently, these employees will continue their schemes even after they leave one company and start working for another. At this point, they have become what are known as predatory employees. These people fall outside the fraud triangle model; they steal not because of a defined set of circumstances, but as a matter of course. Small businesses can best protect themselves against these persons by conducting thorough background checks before hiring any employee, particularly anyone who will have access to the company's cash or merchandise.

The importance of screening out bad applicants or preventing existing employees from stealing cannot be overstated. Many small businesses resist measures like internal controls because they are costly and time consuming. But we must remember that the average fraud scheme in a small business costs $200,000, according to *The Report to the Nation*. Just because this cost doesn't show up on the balance sheet, does not mean it is not there. How much would you pay to save $200,000 in payroll or inventory expense? When we realize how much is to be lost by ignoring the threat of fraud, we see that measures like internal controls and background checks are actually a bargain.

Working Conditions and Fraud

The Hollinger - Clark Study: The Effect of Workplace Conditions

In 1983, Richard C. Hollinger of Purdue University and John P. Clark of the University of Minnesota published federally funded research involving surveys of over 9,000 American workers. In their book, *Theft by Employees*, they reached a different conclusion than Cressey. They concluded that employees steal primarily as a result of *workplace conditions*; specifically, Hollinger and Clark found that job dissatisfaction is the primary cause of employee theft. They also concluded that the true costs of employee misconduct are vastly understated: "In sum, when we take into consideration the incalculable social costs... the grand total paid for theft in the workplace is no doubt grossly underestimated by the available financial estimates."

Employee Deviance

Employee deviance can be defined as conduct detrimental to the organization and to the employee. Hollinger and Clark broke down employee deviance into two basic categories of deviant behavior: (1) acts by employees against property (such as theft or embezzlement); and (2) violations of the norms regulating acceptable levels of production (counterproductive behavior such as goldbricking). Hollinger and Clark developed a written questionnaire, which was sent to employees in three different sectors: retail, hospital, and manufacturing. Over the three-year duration of the study, they received 9,175 valid employee questionnaires, representing about 54% of those sampled. The following table represents the first category of employee deviance: acts against property. As we can see, in all three sectors approximately one-third of employees surveyed admitted to some form of property crime.