The CPA Journal

Print

The Fraud Diamond: Considering the Four Elements of Fraud

By David T. Wolfe and Dana R. Hermanson

Despite intense efforts to stamp out corruption, misappropriation of assets, and fraudulent financial reporting, it appears that fraud in its various forms is a problem that is increasing in frequency and severity. KPMG's *Fraud Survey 2003* documented a marked increase in overall fraud levels since its 1998 survey, with employee fraud by far the most common type of fraud. The 2003 survey also noted that fraudulent financial reporting had more than doubled from 1998. This trend is consistent with the unprecedented recent spate of large accounting frauds (Enron, WorldCom), as well as the increased number of accounting restatements and SEC enforcement actions in recent years. (See *2003 Annual Review of Financial Reporting Matters* by the Huron Consulting Group and the SEC's *Report Pursuant to Section 704 of the Sarbanes-Oxley Act of 2002*.)

In response to the fraud problem, Congress and regulatory authorities have enacted tougher laws and increased enforcement actions.

Organizations are implementing tighter controls and broader oversight. The auditing profession has adopted more rigorous auditing standards and procedures, and software developers are adding continuous monitoring features to back-office systems. It remains unclear whether these efforts are sufficient to mitigate the fraud problem.

Many studies suggest fraud is more likely to occur when someone has an *incentive* (pressure) to commit fraud, weak controls or oversight provide an *opportunity* for the person to commit fraud, and the person can *rationalize* the fraudulent behavior (attitude). This three-pronged framework, commonly known as the "fraud triangle," has long been a useful tool for CPAs seeking to understand and manage fraud risks. The framework has been formally adopted by the auditing profession as part of SAS 99.

A Different Way to Think About Fraud Risks

The authors believe that the fraud triangle could be enhanced to improve both fraud prevention and detection by considering a fourth element. In addition to addressing incentive, opportunity, and rationalization, the authors' four-sided "fraud diamond" also considers an individual's *capability*: personal traits and abilities that play a major role in whether fraud may actually occur even with the presence of the other three elements.

Many frauds, especially some of the multibillion-dollar ones, would not have occurred without the right person with the right capabilities in place. Opportunity opens the doorway to fraud, and incentive and rationalization can draw the person toward it. But the person must have the capability to recognize the open doorway as an opportunity and to take advantage of it by walking through, not just once, but time and time again. Accordingly, the critical question is, "Who could turn an opportunity for fraud into reality?"

Using the four-element fraud diamond, a fraudster's thought process might proceed as follows (Exhibit 1):

- Incentive: I want to, or have a need to, commit fraud.

- Opportunity: There is a weakness in the system that the right person could exploit. Fraud is possible.
- Rationalization: I have convinced myself that this fraudulent behavior is worth the risks.
- Capability: I have the necessary traits and abilities to be the right person to pull it off. I have recognized this particular fraud opportunity and can turn it into reality.

While these four elements certainly overlap, the primary contribution of the fraud diamond is that the capabilities to commit fraud are explicitly and separately considered in the assessment of fraud risk. By doing so, the fraud diamond moves beyond viewing fraud opportunity largely in terms of environmental or situational factors, as has been the practice under current and previous auditing standards.

For example, consider a company where the internal controls allow the possibility that revenues could be recorded prematurely by altering sales contract dates in the sales system. An opportunity for fraud exists, if the right person is in place to understand and exploit it. This opportunity for fraud becomes a much more serious problem if the company's CEO, who is under intense pressure to increase sales, has the technical skills to understand that the control weakness exists, can coerce the CFO and sales manager to manipulate the sales contract dates, and can consistently lie to analysts and board members about the company's growth. In the absence of such a CEO, the fraud possibility would never become reality, despite the presence of the elements of the fraud triangle. Thus, the CEO's capabilities are a major factor in determining whether this control weakness will ultimately lead to fraud.

The Person with Capability

Based on one author's experiences in investigating frauds for the past 15 years, there are several essential traits for committing fraud, especially for large sums or for a long period of time (Exhibit 2). First, the person's position or function within the organization may furnish the ability to create or exploit an opportunity for fraud not available to others. For example, a CEO or divisional president has the positional authority to influence when contracts or deals take effect, thus affecting the timing of revenue or expense recognition. *Fraudulent Financial Reporting: 1987–1997, An Analysis of U.S. Public Companies* (Beasley et al., 1999) found that corporate CEOs were implicated in over 70% of public-company accounting frauds, indicating that many organizations do not implement sufficient checks and balances to mitigate the CEO's capabilities to influence and perpetuate fraud. Additionally, when people perform a certain function repeatedly, such as bank reconciliations or setting up new vendor accounts, their capability to commit fraud increases as their knowledge of the function's processes and controls expands over time.

Second, the right person for a fraud is smart enough to understand and exploit internal control weaknesses and to use position, function, or authorized access to the greatest advantage. Many of today's largest frauds are committed by intelligent, experienced, creative people, with a solid grasp of company controls and vulnerabilities. This knowledge is used to leverage the person's responsibility over or authorized access to systems or assets. According to the Association of Certified Fraud Examiners, 51% of the perpetrators of occupational fraud had at least a bachelor's degree, and 49% of the fraudsters were over 40 years old. In addition, 46% of the frauds the Association recently studied were committed by managers or executives.

Third, the right person has a strong ego and great confidence that he will not be detected, or the person believes that he could easily talk himself out of trouble if caught. Such confidence or arrogance can affect one's cost-benefit analysis of engaging in fraud; the more confident the person, the lower the estimated cost of fraud will be. In "The Human Face of Fraud" (*CA Magazine*, May 2003), R. Allan notes that one of the common personality types among fraudsters is the "egotist"—someone who is "driven to succeed at all costs, self-absorbed, self-confident and narcissistic." Similarly, Duffield and

Grabosky ("The Psychology of Fraud," *Trends & Issues in Crime and Criminal Justice*, March 2001) note that, in addition to financial strain, "Another aspect of motivation that may apply to some or all types of fraud is ego/power." The authors go on to quote Stotland ("White Collar Criminals," *Journal of Social Issues*, 1977) regarding ego: "As [fraudsters] found themselves successful at this crime, they began to gain some secondary delight in the knowledge that they are fooling the world, that they are showing their superiority to others."

Fourth, a successful fraudster can coerce others to commit or conceal fraud. A person with a very persuasive personality may be able to convince others to go along with a fraud or to simply look the other way. In addition, Allan notes that a common personality type among fraudsters is the "bully," who "makes unusual and significant demands of those who work for him or her, cultivates fear rather than respect … and consequently avoids being subject to the same rules and procedures as others." Many financial reporting frauds are committed by subordinates reacting to an edict from above to "make your numbers at all costs, or else."

Fifth, a successful fraudster lies effectively and consistently. To avoid detection, she must look auditors, investors, and others right in the eye and lie convincingly. She also possesses the skill to keep track of the lies, so that the overall story remains consistent. In the Phar-Mor fraud, the auditors claimed that Phar-Mor had formed a "fraud team" of executives and former auditors who "continually worked to hide evidence" about the fraud from them. The auditors claimed that the fraud team "lied, forged documents and 'scrubbed' everything the auditors saw to hide any indications of malfeasance." (See "Finding Auditors Liable for Fraud: What the Jury Heard in the Phar-Mor Case," Cottrell and Glover, *The CPA Journal*, July 1997.)

Finally, a successful fraudster deals very well with stress. Committing a fraud and managing the fraud over a long period of time can be extremely stressful. There is the risk of detection, with its personal ramifications, as well as the constant need to conceal the fraud on a daily basis. Former HealthSouth CEO Richard Scrushy now faces numerous criminal charges for allegedly masterminding a long-running scheme to inflate the company's earnings during the terms of several different CFOs. Despite the enormous pressure on him, Scrushy has remained resolute during the course of the investigation, even appearing on *60 Minutes* to proclaim his innocence. In contrast, during his sentencing, former HealthSouth Assistant Controller Emery Harris, who allegedly was coerced to participate in the fraud, told the judge how relieved he was after the company was raided by federal agents, thinking it provided him the opportunity to finally "get out of this mess."

Dealing with Capability

Appreciating the importance of capability as a fourth element of fraud is only part of the challenge. The next task is to address capability when assessing fraud risk, and to use knowledge about fraud capability to prevent or detect fraud. Beyond considering incentive, opportunity, and rationalization, the following steps could shed light on capability.

Explicitly assess the capabilities of top executives and key personnel. Focusing on capability requires organizations and their auditors to better understand employees' individual traits and abilities. The audit committee member, corporate accountant, or auditor should focus on the personality traits and skills of top executives and others responsible for high-risk areas when assessing fraud risk or seeking to prevent or detect fraud. Routine background checks on new employees can identify past criminal convictions.

In assessing individuals' traits and abilities, several methods of gathering information may be helpful. First, there is no substitute for spending time with a person. Frequent interaction under a variety of circumstances, both business and social, can provide a meaningful picture of the person's capabilities.

Second, look for signals in the "little things." If the person cuts corners on small issues or consistently displays an absolute refusal to lose or fail, no matter what the issue or the cost, this may suggest similar behavior on larger issues. For example, many have said that an executive who cheats in golf will cheat in business. Finally, pay attention to what others say about a person. If there are consistent statements about certain traits or tendencies, this information can supplement more direct observations. For example, if people in the organization are consistently in awe of someone's technical or creative ability, this provides additional insight into the person's capabilities.

If there are concerns about capability, respond accordingly. If someone's capabilities present a significant risk factor, respond with stronger controls or enhanced audit testing. For example, if the sales vice president is overly aggressive, competitive, and obsessed with hitting monthly sales quotas, there may be a need for extra-tight controls over revenue recognition or expanded testing of sales during the annual audit. In addition, implementing a periodic rotation of routine, but key, functions among staff can minimize the opportunities for fraud gained from long-term knowledge of the function and its controls.

In this response phase, a key to mitigating fraud is to focus particular attention on situations offering, in addition to incentive and rationalization, the combination of opportunity and capability. In other words, "Do we have any doorways to fraud that can be opened by people with the right set of keys?" If so, these areas are especially high risk, because all the elements are in place for a fraud opportunity to become reality.

For example, when designing detection systems, it is important to consider who within the organization has the capability to quash a red flag, or to cause a potential inquiry by internal auditors to be redirected. Cynthia Cooper, the internal auditor at WorldCom credited with discovering the massive fraud, has described in *Time* magazine how CFO Scott Sullivan had exercised his position and seniority to dissuade her team from looking into certain areas that later proved to have been infested with massive fraud. But believing they were on to something, her teams worked behind Sullivan's back, on many occasions at night or from home, to avoid detection and retribution. Although it appears he tried, according to Cooper, in this instance Sullivan was not capable of completely thwarting the persistent efforts of the auditors to uncover the apparent fraud.

Reassess the capabilities of top executives and key personnel. Assessing capability and responding to concerns should not be viewed as one-time exercises. Continuous updating of the capability assessment and response is warranted for two reasons. First, people can develop new capabilities over time, especially if they are climbing the corporate ladder and growing professionally. Just because someone did not have enough power or knowledge of an area to commit fraud in the past, there is no guarantee that the person will not develop such power or knowledge in the future. Their capability to commit fraud may increase, and additional controls or scrutiny may be warranted.

Second, organizational processes, controls, and circumstances change over time. As a result, some people may be better suited to commit fraud in the new environment, even though they were not capable under previous conditions. For example, consider a company that has recently implemented a complex new IT system. The new system may render those less digitally sophisticated employees incapable of exploiting its controls. On the other hand, for those with strong IT skills, the change might increase their capability of committing fraud. This new capability should be considered, and appropriate responses implemented.

Beyond Standards

In the final analysis, recent legislation, increased enforcement, regulatory oversight, broader controls, improved auditing standards, and sophisticated monitoring technology are all steps in the right direction

and will contribute to preventing and detecting fraud. Limiting this effort to current standards and practices may not be enough, however, especially for auditors. Consistent with this view, the *2004 Miller GAAS Guide* describes the fraud triangle elements presented in SAS 99 and notes that "it is obvious that the Auditing Standards Board is struggling with the broad topic of how to detect fraud … auditors should be careful about following relevant professional standards and then having a sense of security about the likelihood that fraud does not exist in a particular engagement."

Accordingly, if capability could play a role in influencing or magnifying the other fraud elements, other checks and balances or detection systems should be implemented, or an auditor should expand audit scope, procedures, and testing for potential fraud.

David T. Wolfe, CPA*, is the founder of Glasgow Forensic Group, a forensic accounting firm in Atlanta, Ga., and has served a variety of clients, including top-tier law firms, government agencies, privately held small to mid-sized businesses, and Fortune 500 companies.*
Dana R. Hermanson, PhD*, is a professor of accounting in the Coles College of Business at Kennesaw State University and currently serves as a research fellow of the Corporate Governance Center at the University of Tennessee.*

Close