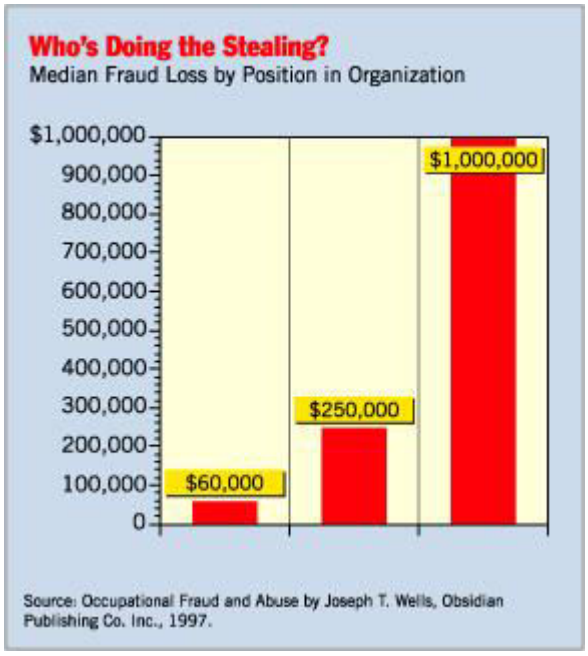
From the boardroom to the mailroom, all fraudsters think alike.

Let Them Know Someone's Watching

BY JOSEPH T. WELLS

The recent failure of Enron—even though fraud charges have yet to be proven—has renewed the hue and cry from Congress, regulators and the investing public: Why can't auditors catch these problems?



The answers run the gamut: Auditors lack independence from their clients, the audit process is not designed primarily to detect fraud, the number of audit failures is minuscule compared with the number of audits, it is not possible—because of collusion—to detect all material frauds.

While these explanations may be perfectly valid, the public isn't buying them. In a 1998 study, Bonner, Palmrose and Young determined that after a failed audit plaintiffs were more likely to sue auditors who didn't detect questionable transactions. And McEnroe and Martens' 2001 study found that only 41% of auditors—vs. 71% of

investors—said auditors should serve as "public watchdogs." The message seems clear: The public wants independent auditors to detect and deter fraud.

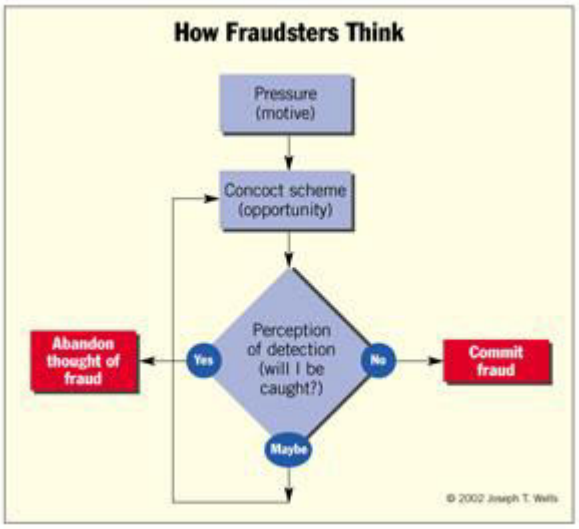
Unfortunately, there is no foolproof method for uncovering fraud. Unlike visible crimes—such as robbery or assault—fraud's hallmarks are deception and stealth. The company insiders who might be tempted to commit financial statement fraud constantly attempt to cover their tracks. And many of them are good at it—so good, in fact, that investigators will never catch them all.

Historically, CPAs have counted on internal controls as the main defense against fraud. Although there is no question that controls are a vital part of any organization's risk management program, their preventive effect on fraud is questionable for two reasons. First, internal controls provide only *reasonable* assurance against fraud. Second, if upper management is hell-bent on showing stronger earnings, it can find ways to override controls. Therefore, to catch offenders in the act, CPAs must start thinking like them.

THE POWER OF FEAR

English philosopher Jeremy Bentham originated classic criminological theory in the 18th century. It holds that a person's propensity to commit a crime is determined by his or her perception of related risks and rewards—the greater the risk of detection and apprehension, the less likely a person is to violate the law.

So what potential fraudsters are concerned about—from the CEO to the average rank-and-file employee (see "Pam's Parable," at the end of this article)—is getting caught; they're not thinking specifically about internal controls. Following classic criminology, their willingness to commit fraud is inversely proportional to their perceived risk of being discovered. This concept—the *perception of detection*—can be summarized as follows: *Those who perceive they will be caught engaging in fraud are less likely to commit it* (see "How Fraudsters Think," below). This graphic illustrates the potential fraudster's thought process. First, some sort of pressure creates a motive. For a CEO, it may be the need to create the appearance of greater corporate earnings. Next, the executive concocts a scheme—for instance, to add phony sales and receivables.



Since a CEO doesn't have access to the company's books and records, he or she then enlists the aid of someone in the accounting department—often the CFO. Finally, the fraudster weighs the risk of being caught. If he or she anticipates little or no risk, the fraud proceeds. But if the executive foresees the possibility of detection, he or she either develops another, less risky scenario or abandons the plan.

PREVENTION VS. DETERRENCE

Although many people use the terms "prevention" and "deterrence" interchangeably, they refer to different concepts. Prevention implies removing the root cause of a problem—principally the financial pressures that motivate a person to commit fraud. Deterrence, on the other hand, is the modification of behavior through the threat of sanctions. From the perpetrator's perspective, there is no sanction more negative than being caught. But note carefully that it is the *perception*—not necessarily the reality—that modifies the criminal's behavior.

Consider an example. When attempting to control street crime, the authorities usually increase police visibility in crime-prone neighborhoods. Officers' mere presence—a proactive deterrent—is the most effective way to discourage offenders.

But punishing criminals once they've acted—a necessity in a civilized society—is reactive deterrence. While many organizations use this tactic as their principle weapon against fraud, experience shows it is the least effective method of all—fully three-quarters of incarcerated criminals are subsequently arrested again, usually for increasingly serious offenses. Criminologists have found it difficult to determine whether the threat of punishment deters other members of an organization from committing crimes.

If we accept, however, that increasing the perception of detection is the best deterrent, the profession has alternatives to consider including in its antifraud efforts. We can start at the logical place: the top of the organization, where most financial statement fraud schemes begin.

UPPER MANAGEMENT AND FRAUD

A 1999 Committee on Sponsoring Organizations of the Treadway Commission (COSO) study found the CEO and/or CFO directed the fraud in at least 82% of the cases examined. Given that, CPAs must increase management's perception that auditors will catch on to their misdeeds. Consider three practical ways to achieve this:

Closer examination of management's compensation. Empirical studies by Jensen and Warner (1988), Jensen and Murphy (1990) and Beasley (1994) showed a connection between the finances of top executives and their likelihood of committing financial statement fraud. The researchers found the more stock an executive owned, the less likely he or she was to commit financial statement fraud. The reason? Those who own stock want to see it grow and increase in value.

Conversely, other executives—with little equity in their company but receiving compensation through various arrangements based on predetermined financial goals—had little disincentive to commit fraud: The results of their fraudulent acts would have hurt investors, not themselves. Therefore, a detailed examination of the finances of key insiders could reveal conflicts of interest, related-party transactions, sales and purchases of stock and even evidence of high-stakes embezzlements.

Frequently auditors can uncover these schemes by examining insiders' personal financial statements, tax returns and bank statements. If executives were aware of the

possibility that auditors might scrutinize their finances, it would—as increasing police visibility on the street does—proactively deter them from committing a crime.

Diligent inquiry. A good way of increasing the perception of detection is for the auditor—as part of his or her routine duties—to diligently inquire about the existence of fraud within the organization. (See "'Why Ask?' You Ask," *JofA*, Sep.01, page 88, www.aicpa.org/pubs/jofa/sept2001/wells.htm). Since, in financial statement fraud, the CEO nearly always has one or more accomplices, there is always the possibility that someone else involved will reveal the truth.

Human nature being what it is, we look down on "squealers." It's one thing to expect someone to voluntarily come forward and quite another to ask a potential informer point-blank questions: *Are you aware of any fraud within this organization? Has anyone asked you to do something you thought was illegal or unethical?*

Toward that end, the Auditing Standards Board (ASB) in February issued an exposure draft, *Consideration of Fraud in a Financial Statement Audit,* which proposes requiring auditors to gather from management and others within the audited entity information necessary to identify the risks of material misstatement due to fraud.

Surprise audits. In today's complex business environments, conducting a complete audit by surprise would be a practical impossibility. In CPAs' natural zeal to serve their clients and cause them minimal disruptions, they've gradually gotten away from unannounced audit work. But historically, large financial statement frauds usually showed up in one or more of three accounts: inventory, sales and accounts receivable. If auditors periodically examined certain accounts without warning, it might help deter upper management from attempting to artificially inflate assets or revenue.

Perhaps the best proof of the value of surprise is the disastrous result its complete absence can produce. In one of the most striking examples, auditors for the Phar-Mor drugstore chain advised management months in advance which of their stores would be selected for audit. Not surprisingly, this gave management enough time to ensure that auditors would find nothing wrong in those stores. As a result, auditors failed to detect a financial statement fraud of some half a billion dollars. (See "Ghost Goods: How to Spot Phantom Inventory," *JofA*, June01, page 33, www.aicpa.org/pubs/jofa/jun2001/wells.htm.)

In the wake of Enron and beyond, members of the profession must effectively address these difficult issues because every instance of fraud hurts the victim, the perpetrator, the auditor and the criminal justice system. Fortunately, with the aid of the ASB's proposed auditing guidance and by thinking like the thieves they're trying to catch, CPAs can start winning the struggle against fraud. ■

Pam's Parable

Pam, a recent high school graduate, got a job at a photo kiosk in the parking lot of a mall. With little training, Pam began work. After two weeks of sitting alone in her small booth, it occurred to Pam that no one was watching. Since she was a little short on money, she snitched $10. The next day, she took $20 more. Several

weeks went by with Pam continuing to filch small amounts of money.

Then one day an auditor showed up at the kiosk unannounced. By counting her cash, the auditor quickly found Pam had stolen more than $500. When he confronted her, she confessed she had "borrowed" the money without authorization. She was fired. When he spoke with Pam, the auditor asked whether she knew someone would audit her work. "No," she replied. "Until you walked in here, I didn't even know what an audit was."

This parable teaches us two important lessons. First, Pam didn't actually have an opportunity to commit and conceal her thefts; she only thought she did—because management didn't tell her it was planning to conduct a surprise audit. So, managers must continually reinforce employees' awareness of the risks facing anyone who commits fraud. This process also works in reverse: People who *do* have the opportunity but perceive that they *do not* are less likely to take the chance. The perception—not the actual likelihood—of detection determines whether or not a person will commit fraud.

Second, Pam's thinking is not unique. CEOs considering a major financial statement fraud also expect their misdeeds to go undetected.