Expen$ive Indifference

by John Nemo

In the time it took her to drive to the computer store and back, Debra Thompson had the tools to commit a fraud that could potentially net thousands of dollars.

(continued on page 18)

(continued from page 17)
"I bought a computer program that has watermarked checks. I could print the bank number on them. I could get the company's logo by just going to the Internet and copying it from their Web site," says Thompson, director of forensic accounting and fraud investigations at LarsonAllen. "All I need is a photocopy of a check, and I could reproduce it. It used to be it would take somebody a long time and you would have to wash the signature off the check. Not anymore."

Thompson shares a simple example of how complicated the problem of fraud has become. Consider evidence from the Association of Certified Fraud Examiners' (ACFE) 2002 *Report To The Nation on Occupational Fraud And Abuse*:

- An estimated six percent of revenue was lost in 2002 as a result of fraud, translating to a total cost of $600 billion, or about $4,500 per employee, up from $400 billion in 1996.
- Over half the frauds reported in the ACFE survey caused losses of at least $100,000, while nearly one in six caused losses in excess of $1 million.
- The average fraud scheme lasted 18 months before it was detected.
- The typical perpetrator was a first-time offender.
- The most common method of detecting fraud was by employee, vendor, customer or anonymous tips. The second most common method was by accident.

"The scale of fraud is growing because it continues to be under-managed as a risk and cost for businesses," says Toby Bishop, president and CEO of the ACFE. "Business owners and managers tend not to focus on the cost of fraud because in most organizations it is hidden within other line items on the financial statement. There is no line on the income statement saying, 'Fraud Expense.' If there was, their eyes would pop out of their heads and they would do something about it."

"Fraud should not be a new concern, because fraud is not a new thing," says Craig Arends, LarsonAllen's principal-in-charge of corporate governance and Sarbanes-Oxley compliance services.

With high-profile cases like the Enron scandal dominating headlines in recent years, fraud has become a hot topic. The accounting industry and federal government have responded with new safeguards that put more responsibility on companies and auditors alike to detect fraud.

It use
take a lo
Not an

The smaller, the better

Small companies are often the easiest targets for fraud, experts say, largely because of a lack of basic control points.

For example, Arends points to gaps in background checks for new hires.

"Quite honestly, if you don't do background checks, it's a material weakness, especially in financial areas or with people who have access to liquid assets," he says.

Too much trust can actually be a bad thing for business owners, Bishop says.

"In small businesses, owners tend to trust their bookkeepers with a lot,"

Three most common types of fraud:

Fraud Q&A

Craig Arends and Debra Thompson are two of LarsonAllen's experienced professionals when it comes to detecting and investigating fraud. Here are some of the most common questions they face when dealing with clients and companies that suspect fraud.

Craig Arends

Debra Thompson

What's the difference between how an auditor handles a fraud investigation versus a Certified Fraud Examiner?

Thompson: "The difference between a fraud investigation and an audit is that an investigation focuses on a particular aspect of the processes occurring within a company. Auditors are giving an opinion on the financial statements so they need to look at all different areas—from cash to accounts receivable to sales and liability. The whole financial statement is taken into consideration."

What should an employer do when learning a fraud might be taking place?

Thompson: "When fraud or a potential fraud is brought to a company's attention, there are basic steps every employer must take. First is to contact your legal counsel, typically your general counsel, though they might not be well-versed in fraud and all of its ramifications. Second, you have to try he says. "But unfortunately the damage from doing it can be devastating. In a small business, an embezzlement of $400,000 or $500,000 could mean bankruptcy, and that's not an unusual amount for an embezzlement where a bookkeeper is helping himself or herself over a few years."

ed to
ong time.
ymore.

Bishop says another problem is that many small business owners become so involved in running their business that they don't want to spend time looking at things like bank statements or financial reports. They'd rather hand all of that responsibility over to a bookkeeper.

"Some business owners are their own worst enemy by refusing to get involved and do the minimum due diligence to protect themselves," he says.

The ACFE study showed that companies with less than 100 employees consistently suffered higher median losses than larger companies with more than 10,000 employees. Frequently, many small companies do not have enough staff to keep detailed accounting records or effectively manage internal controls. In some small firms, one employee may be in charge of writing and signing checks, handling bank statements and keeping the books.

Common frauds

The three most common types of fraud are asset misappropriations, corruption and fraudulent statements, according to the ACFE study. It found that 80 percent of frauds were asset misappropriations, with cash being the targeted asset 90 percent of the time. Corruption accounted for 13 percent of all fraud, causing over $500,000 in losses on the average. Fraudulent statements were the most costly form of fraud, ringing up median losses of $4.25 million per scheme.

Asset misappropriation schemes involve things like embezzlement and skimming, along with payroll, billing and reimbursement scams, check tampering and register disbursements based on false refunds or voids. Corruption can go the route of bribery and kickbacks, illegal gratuities, economic extortion and conflicts of interest like sales or purchase schemes. Fraudulent statements can be financial, involving asset and revenue overstatements, or non-financial, which may involve falsifying resumes or company documents.

Fraud investigation

"When I am investigating a fraud, it is because one is either strongly suspected or one is known to have occurred," Thompson says. "If you have a suspected fraud, you typically have a specific situation that you call me in to examine."

Thompson gives an example: "Say you think you have an accounts receivable clerk who is not putting all the receipts against the customers' accounts. Instead, the clerk is actually helping himself or herself to some of the funds. We would determine what access the clerk has to records, mail and computer files. I would look at those areas that he or she has control over.

"On a fraud investigation, I am more focused on a particular individual or particular department. If the

(continued on page 20)

1 2 3 asset misappropriations, corruption and fraudulent statements

and gather documentation to show there is a reason why you believe a person is committing fraud.

"Finally, when it comes to confronting an employee suspected of fraud, it is very important to handle things appropriately. In a fraud investigation, you interview the most peripheral employee first. The last person you want to interview is the person you suspect of committing anything."

What kind of emotional impact does fraud have on a company and its employees?

Thompson: "There is an emotional toll on people. When I'm working with them, they are either totally revengeful and want to get the person no matter what, or they can't believe it because the person is like family. A lot of the cases you don't read about in the paper involve people's retirement plans or other large chunks of money. And that's money they don't have now for their business, retirement or other things."

What role can a company's insurance play in helping with recovery from fraud?

Thompson: "Even if you're a small company, review your policy if you even suspect fraud or some sort of impropriety and report it to your insurance company. Many times you can recover some portion of the loss and, possibly, some of the costs associated with the investigation."

Arends: "There's usually a time limitation involved. You have a duty as the insured to report suspected fraud or actual fraud, and it's a relatively short amount of time on a lot of these policies, like 60 or 90 days."

What can companies do to head off fraud before it happens?

Arends: "Set the tone at the top. If you're an owner or a manager in a business, do you ever ask your employees to lie for you? Even if it's for small things such as, 'I don't want to take that call, tell them I'm not here?' That's how you set the tone at the top. It's what you do in your everyday business that determines if you really value honesty and integrity.

—John Nemo

(continued from page 19)

suspected person is a manager or somebody in a high-level position, I look at whether they are intimidating people, or if they are making journal entries that aren't appropriate."

Adds Thompson: "The first thing we look at is the internal controls. Because the place that you first identify the weaknesses and what that person could potentially have control over is through your review of the internal controls."

> "The scale of fraud is growing because it continues to be under-managed as a risk and cost for businesses today."
>
> *—Toby Bishop, president and CEO of the ACFE*

Playing by new rules

When the American Institute of Certified Public Accountants (AICPA) issued SAS 99, *Consideration of Fraud in a Financial Statement Audit,* two years ago, the goal was to put greater emphasis on professional skepticism and help auditors be more effective in addressing fraud in a financial statement audit.

"As an auditor, I am a referee," Arends says. "On one side you have the companies. Companies need capital. And on the other side are investors, and investors have money on which they want to see a return. In between is the auditor."

Arends says the Generally Accepted Auditing Standards (GAAS) and Generally Accepted Accounting Principles (GAAP) provide guidance to auditors on how to make the tough calls.

"That tells me how, as a referee, I'm supposed to describe what the playing field looks like," he says. "SAS 99 was developed to address an expectation gap where auditors, as a profession, were always trying to say, 'We're not responsible for detecting fraud.' Finally, the investors said, 'No, you are responsible for detecting material fraud because you're saying those financial statements are materially correct.' "

An additional safeguard—the Sarbanes-Oxley Act of 2002—defines management's responsibility for internal control over financial reporting in public companies, Arends says.

"The expectations of investors are that management will prevent and detect fraud," he says. "Investors are also saying that auditors are clearly responsible for finding and preventing fraud."

Arends says the new legislation has put more pressure on auditors.

"The auditor's role as we know it has changed significantly," he says. "Prior to Sarbanes-Oxley and SAS 99, the auditing profession was a self-regulated industry. Now, it is regulated for a majority of the profession."

Future fears

As fraud continues to evolve, experts like Arends and Thompson will continue to evolve with it. And whether it's bad checks, phony Web sites or other high tech schemes, companies and fraud examiners have to be prepared.

"What they can do today, they couldn't do yesterday," Thompson says of fraud perpetrators. "And what they can do tomorrow, they couldn't do today."

John Nemo is a freelance writer, author and syndicated columnist. Contact John at johnnemo@comcast.net.