

Courant.com

The CPA Goes CSI

Accountants Hone Their Detective Skills to Crack Fraud Cases

STORY BY JANICE PODSADA ILLUSTRATION BY WES RANDTHE HARTFORD COURANT

October 7, 2007

Jeffrey Rossi, a certified public accountant, was doing a routine audit of a West Hartford company's finances when he found a \$1,169 canceled check for "bagels and kitchen supplies."

It was a lot of dough for bagels, but it wasn't the dollar amount that struck Rossi as odd - it was the appearance of the two "ones" in front of the dollar sign.

"The thickness of the pen strokes was different," Rossi said. "It jumped out at me." The check, originally written for \$69, had been altered.

"We ended up following a little trail of bread crumbs that led to the discovery of a quarter-million-dollar embezzlement scheme," Rossi said.

A forensic audit revealed that the firm's bookkeeper, a 67-year-old grandmother whom company officials described as a trusted 14-year employee, had embezzled more than \$250,000 over three years by altering checks.

That was Rossi's first encounter with business fraud. A certified fraud examiner, Rossi is now a partner at Haggett Longobardi, a Glastonbury accounting firm where he specializes in forensic accounting.

Like many accounting firms, Haggett Longobardi, a division of J.H. Cohn, offers forensic accounting services. Those services range from business valuations to reconstructing lost records to working with law enforcement authorities in cases of suspected fraud to determine culpability, the loss amount and how it was accomplished.

Forensic means "related to the law," said agent Thomas Martin with the South Windsor Police Department's investigations division.

"Forensic accounting is a brand new term - it's only 4 or 5 years old. People may have been doing forensic accounting before, but now there's a name for it," Martin said.

Each year, U.S. organizations lose about 5 percent of their annual revenue to crimes such as antitrust fraud, bankruptcy fraud, bribery, kickbacks, counterfeiting, embezzlement or price-fixing. Last year, losses totaled an estimated \$650 billion.

By comparison, the annual financial loss resulting from robbery, burglary, larceny and auto theft was about \$20 billion, according to the FBI.

"Most embezzlement cases are generally successful because the perpetrator has a position of trust," Martin said.

If you suspect fraud, you need a forensic accountant who is specially trained to gather evidence and interview

suspects, Rossi said.

As a result, the demand for forensic accountants is rising. More colleges and universities are offering classes geared toward uncovering fraud as part of their accounting programs, including the University of Connecticut.

The ability to sift "the books" is critical, but so is the ability to interview people - to read body language, Rossi said. During an investigation, it's often the responsibility of the fraud examiner to interview suspects and gather evidence on behalf of the company or police. That said, not all forensic accountants end up in court.

Many businesses choose not to involve the police. Some don't want media coverage; that's particularly true of nonprofit organizations that might see donations decline if a fraud were made public. Others want the money returned or are hesitant to prosecute longtime employees.

The West Hartford company that Rossi investigated fired its check-altering bookkeeper, who claimed she had stolen the money on behalf of a sick grandchild, but didn't press charges.

"They let it go," Rossi said.

Fraud On The Rise

In the last three to five years, accounting firms and law enforcement officials say that they've seen an increase in the number of fraud schemes.

"As a firm, we're getting more of this work, but it could be due to an increased awareness," Rossi said.

In 2005, nearly half of the nation's organizations reported being victims of economic crime in the previous two years. Worldwide, the incidence of fraud rose from 37 percent to 45 percent, according to the PricewaterhouseCoopers' 2005 Global Economic Crime Survey.

In spite of the reported increase, a significant percentage of victimized organizations never report a crime. In a 2006 study of 1,200 cases of occupational fraud, almost 30 percent of organizations chose not to contact authorities, according to the Association of Certified Fraud Examiners.

"When a fraud is discovered, everybody wants to rush out and get the cuffs put on somebody and get them arrested - but they have to think about it. If someone is in jail, they can't make restitution," said Stephen Pedneault, founder of Forensic Accounting Services in Glastonbury and a certified fraud examiner.

Pedneault's tools of the trade include his "response bag," which he uses to secure a crime scene. If someone suspects that they're being investigated they'll often "steal the computer, steal documents - evidence disappears overnight," Pedneault said.

His black leather bag contains a calculator, latex gloves, evidence tape, cameras, a jump drive and tweezers - to avoid adding his fingerprints to a document - and a small pack of tissues.

"People get emotional. If a suspect starts to cry, I can at least offer them a tissue," he said.

Pedneault's motto is "follow the money." If there are several suspects, look for the one who would benefit the most financially from the scheme, he said.

But forget elaborate scams. When it comes to fraud, the run-of-the-mill schemes that have been around for decades predominate, Pedneault said. Those include stealing from the cash drawer, setting up a sham company

and creating fake invoices, or simply writing a check to yourself.

That was the case with the greedy comptroller who wrote himself \$15,000 and \$20,000 checks drawn on a Connecticut company's bank account several times a month, beginning the first month he was hired. Four years into his check-writing activities, a bank official called the owner and told him that bank tellers had noticed a series of "even-dollar-amount checks payable to the comptroller," Pedneault said.

The firm's owner never looked at the canceled checks. By the time the suspect was caught, he had stolen \$1.3 million and was driving a Corvette to work.

"Every business owner should get the bank statement unopened every month and review it - they might discover checks payable to the bookkeeper, payable to employees, or vendors you've never heard of," said Pedneault, who is developing an online forensic accounting course in collaboration with Larry Gramling, an assistant professor of accounting at the University of Connecticut.

In fraud cases, small and medium-sized businesses are often the biggest losers, experts say.

Last year, the median dollar loss per fraud scheme suffered by companies with more than 1,000 employees was \$120,000, while those with fewer than 100 employees was almost \$200,000, according to the Association of Certified Fraud Examiners.

Internal controls at smaller businesses are typically less stringent than larger organizations. Although fraud insurance is available, very few businesses carry the coverage. And only a tiny percentage ever recover lost money.

Recent technological innovations have made it easier to steal, in some cases. Accounting software programs have replaced hard-bound ledger books, but some programs allow entries to be changed or deleted at any time. Automated deposits and the advent of the electronic check reader have made it more difficult to detect fraud. "If the check isn't retained, that trail is gone," Rossi said.

In recent years, fraud prevention software programs have been developed to statistically analyze company records for suspicious transactions. But internal audits catch only about 30 percent of fraud schemes.

In a few cases, company officials will sense that something is wrong.

"I'll get a call from a business owner who'll say, 'I feel like I'm making a lot of money, but I don't have any cash,'" said Joseph Centofanti, director of the fraud services group at Kostin, Ruffkess & Co. in Farmington. "When things are good, you may not miss a lot. You're making a lot of money, you don't even know you should be making more."

The majority of schemes - more than 60 percent - are discovered by accident.

"Sheer luck reveals a lot of cases," Pedneault said: A suspect leaves an incriminating document on the copy machine. Or in the case of a local health care provider who was the victim of fraud, the suspect forgot to change one billing statement back to its original amount.

The Slip Up

Four years ago, a New Britain health-care provider was the victim of embezzlement. The provider asked not to be named because of a legal settlement he negotiated with the suspect. The provider initially became suspicious when a patient came to the office after receiving a bill she believed was erroneous. As it turned out, "the billing

statement did not match what the computer said," the health-care provider said.

"I thought it was something wrong with my software. I called the software company and they said it's not the program - you're getting embezzled."

The provider called a forensic accountant, who discovered that patients' bills had been changed to make it look as though the suspect was doing more work than the suspect had actually performed. The changes resulted in higher paychecks for the suspect.

"When my associate knew something was up, they disappeared," he said. They didn't show up for work."

The suspect had been the provider's associate for several years. "It was an awful feeling. It felt like a divorce," he said.

"All I wanted was my money back," the provider said. Police were called, but the suspect was never prosecuted and never admitted wrongdoing. Eventually, the suspect agreed to make restitution of more than \$75,000.

Looking back, the health-care provider can recall a series of red flags. The person used to carry a little notebook in a lab coat, he said. "This was a very tricky scheme, and there were a lot of details they must have had to keep track of."

The forensic accountant who investigated the case estimated that the suspect had altered more than 4,300 transactions.

"I'd walk into the office and my associate would X-out of the software program," the provider said. His staff also noticed these little quirks they thought were in the computer system. "They made no sense," he said.

But the thought that his associate was stealing from him never crossed his mind.

At a recent health care conference, the New Britain provider learned that he wasn't alone. "They told us that 35 to 40 percent of us would be embezzled from."

"I still trust people," he said, "but I changed my computer habits. I had made it too easy for things to be changed. I would log in, but wouldn't log out. My associate was careful never to log in under their user name when they changed records."

Some experts say a lust for material goods is the most frequent motive in fraud cases.

"In the last couple years, what's coming up more and more is entitlement," Pedneault said. "I just wrapped up a case involving a woman who took between \$50,000 and \$80,000 just because she said she wanted her kids to have a big TV and an Xbox in their bedrooms. I've seen more and more people who feel they want to live beyond their means."

Last week, a Simsbury man, Jeffrey M. Bourke, 32, pleaded guilty to charges that stemmed from his scheme to embezzle nearly \$2 million from his employer, Anthem Blue Cross and Blue Shield. Bourke formed a phony company and created fictitious invoices, which he billed to his employer. He spent the money to buy expensive watches, artwork and vacations and to purchase and remodel a home.

Others, including the U.S. attorney's office in Connecticut, say that in the past five years a growing number of defendants cite gambling addiction as a motive.

In May, a 50-year-old Simsbury man was convicted in U.S. District Court of stealing more than \$5 million from 225 investment clients. Investigators said that David M. Faubert spent the money on lavish vacations, expensive cars and gambling.

Last year, a 56-year-old Middletown attorney was sentenced to 30 months in prison after embezzling more than \$850,000 from clients. Stephen T. Gionfriddo, a Middletown city councilman for 14 years and a former mayor, testified that he took the money to cover gambling losses at local casinos. And in June 2003, a 54-year-old Hartford woman was sentenced to 80 months in prison for defrauding American Commercial Finance Corp. of West Hartford of more than \$4.7 million. Mildred Miller testified that she used most of the money she obtained for gambling.

"Southeast Connecticut appears to have a disproportionate number of problems. Gambling is such a lure," Centofanti said. "Their rationale is that they're borrowing the money - when they hit, they'll put it back."

That said, "you can't always believe the reasons people give for their behavior," Pedneault said.

"I had this woman who stole \$250,000 from a physicians' group. She said it was because she was raising all these kids and grandkids in her house, trying to feed all these people."

The doctors agreed that if that were the case, they didn't want to prosecute.

"But once we got her bank account - we saw the trips, the shopping sprees, the tattoos they got. I said we could have gotten her those tattoos for free if she'd gone to prison."

Contact Janice Podsada at jpod sada@courant.com.

Copyright © 2007, The Hartford Courant