JOURNAL OF ACCOUNTANCY

FRAUD

Criminal minds

What CPAs can learn from the way thieves think

BY JEFF DREW
AUGUST 2012

This is more than a story about six men, all of them admitted white-collar criminals. It is more than a story about their fraud schemes, which resulted in total combined losses of nearly $4 billion.

This is the story of what CPAs can learn from these men—from their motives and methods, from how they were caught and how they could have been stopped earlier. This is a story of fraud's impact and the role CPAs can play in spotting and preventing it.

The AICPA Fraud Task Force, a group sponsored and supervised by the Institute's Forensic and Litigation Services (FLS) Committee, provides fraud detection, investigation, and prevention information to AICPA members. As part of this mission, the task force located and interviewed a half-dozen perpetrators of significant accounting fraud. The task force summarizes the interview responses in a new report designed to help CPAs implement controls or other measures to prevent similar fraud.

The six individuals who agreed to talk to the task force did so with the understanding that their names would not be revealed. The information they provided paints a broad picture of who they were at the time each fraud took place—and how they have changed since then.

- All of the respondents hold college undergraduate degrees in fields including accounting, industrial engineering, and ancient history. Two of the men earned graduate degrees, including an MBA, and two were CPAs.
- All of the respondents held positions of trust in the organizations where their fraud schemes took place. The admitted thieves held the titles of chairman, CFO, tax partner, general partner, general manager, and senior manager.
- The perpetrators ranged in age from their 20s to their late 50s at the time they committed their crimes.
- All but one of the respondents spent time in prison for their white-collar crimes. Several of the perpetrators were behind bars for more than three years, with the longest sentence served lasting 60 months.
- All but one of the respondents said they had not defrauded other employers and said they would not commit their fraud again. The one exception said he was raised to be a criminal and that he "hasn't changed one bit." Asked if he would commit his fraud again, he answered, "You never know." Asked if he had defrauded any other companies, he said, "No, but are you going to believe a convicted criminal?"

A SUMMARY OF SCHEMES

The men interviewed by the fraud task force executed a variety of illegal schemes. Following is a brief description of each fraud; the dollar loss for the victim organization, investors, and others; what was done to conceal the fraud; how the scheme was discovered; and what CPAs, business leaders, and others could do differently to prevent or uncover these types of fraud.

Fraud No. 1: The Ponzi Scheme

Description: This scheme involved the embezzlement of money from a trust fund by the fund's sole trustee so he could make an urgent debt payment. The trustee, a CPA in a public accounting firm, rationalized the action as a loan, an idea that was reinforced when he set up the Ponzi scheme and paid back the money to the trust. He then continued the Ponzi scheme, using the money to upgrade his lifestyle.

Dollar loss: $250,000.

What was done to conceal the fraud: The perpetrator set up a fake bank account and false documentation to hide the fraud.

How the scheme was discovered: One of the perpetrator's investors had a sudden need for money. Determining that the fraud was unsustainable, the perpetrator reported the crime himself, admitting that he "was a liar and a thief." He later served time in prison and paid restitution with interest.

What could be done to prevent this type of fraud: The perpetrator said he took advantage of poor internal controls at his accounting firm. The requirement of two-signature checks would have stopped the first instance of embezzlement from the trust fund. He recommends that accounting firms evaluate internal controls and not allow CPAs to be trustees of clients' trusts. In addition, business leaders should take note of dramatic lifestyle upgrades among their employees and evaluate whether the person or people involved should have the financial means to maintain the higher standard of living.

Fraud No. 2: Resorting to Misappropriating Funds

Description: The perpetrator simultaneously served in general manager (GM) roles at two unrelated companies. A need for cash at one of the companies, a recreational resort, prompted the perpetrator to make unauthorized disbursements from the bank accounts of the victim company to the resort. The initial transfers were small, and the perpetrator intended to pay back the victim company once the resort's cash flow improved. But the resort continued to struggle, leading to continued shifting of money over a three-year period.

Dollar loss: $350,000.

What was done to conceal the fraud: As a GM at the victim company, the perpetrator had the authority to change the payees and amounts in accounting records. The GM was trusted by the board members, who failed to question monthly financial statement reports provided to them. To cover up the misappropriations, the perpetrator altered bank statements to ensure that the dollar amounts of individual checks used to transfer money to the resort were below the threshold at which the auditors would test them. The GM bought time to change the statements by delaying fieldwork by several months. He placated external auditors in part by giving them free passes to the resort.

How the scheme was discovered: A secretary at the victim company became concerned about cash flow shortages and informed the board, which assigned a board member to watch over the GM. After several months, the board decided to hire a forensic accountant, who uncovered the scheme through an examination of bank and accounting records and canceled checks.

What could be done to prevent this type of fraud: External auditors should not accept gifts from clients they are auditing and should notify board members if one is offered. Also, auditors should notify the board of significant delays or lack of staff cooperation with the audit, such as company employees providing copies of bank statements when the auditors have requested originals. Boards of directors need to closely examine monthly financial statements and make sure effective controls are in place. The controls at the victim company had no teeth because there was no monitoring and the GM could easily override them. Finally, companies should not hire a GM or controller who serves in a controller position with another business.

Fraud No. 3: A Collections Job Gone Bad

Description: The perpetrator was a senior manager in the collections department of the victim company, which

established a $15 million bad debt ceiling and demanded that collections managers make budget. Members of the collections department, including the perpetrator, used a variety of fraudulent means to make the bad debt appear to be no more than $15 million, which was about one-tenth of the actual amount. The perpetrator then teamed with one of his most trusted customers to execute a side scheme that put millions of dollars in their pockets. The perpetrator would pressure delinquent customers of the victim company to pay their bills. The perpetrator's partner would then contact the delinquent customer and offer to pay the bill in return for an upfront commission and a note payable with established repayment terms. The commission and note payments to the partner were sent to a bank in the Caribbean.

Dollar loss: $6 million in the side scheme.

What was done to conceal the fraud: The perpetrator hid bad debt by having customers sign promissory notes, moving the account receivable to a note receivable; changing the date on invoices to adjust the account age; using placeholder credits to make it look as if payments had been made on accounts when they actually had not; and using unapplied cash to credit customer account balances.

How the scheme was discovered: A junior accountant from outside the collections department saw something that didn't look right and kept asking questions. That led to the discovery of misapplied payments in the account of one of the customers who was paying the perpetrator and his partner.

What could be done to prevent this type of fraud: The perpetrator credits the junior accountant with doing exactly what was needed to stop the fraud after six months. To prevent such a fraud from taking place, the perpetrator stressed the importance of the "tone at the top." The management at the perpetrator's company pressured the collections department to keep bad debt within budget by any means necessary. The perpetrator also emphasized the need for strong controls; the ones at the victim company were very loose. The first application of unapplied cash to customer accounts was an error. When the company failed to close that loophole, the perpetrator exploited it.

Also essential is teaching young auditors doing testing in the field the importance of following up on all discrepancies. Most will be mere errors, but sometimes they will be the first step in uncovering fraud.

Fraud No. 4: It All Started With a Loan Failure

Description: The perpetrator and his companies were the guarantors of several large loans related to entertainment contracts. The loans were participation loans with several foreign banks. The fraud began with the failure to record or disclose a liability caused by a failed loan. The perpetrator's internal accountants relayed that the bankers had requested that the loss be kept off the financial statements and that the external CPAs did not know about it. The fraud then grew to include the overstatement of assets and the understatement of liabilities to keep the businesses functioning.

Dollar loss: $236 million.

What was done to conceal the fraud: Extensive internal collusion helped to hide the fraud. "Audit evidence" provided to external CPAs included falsified contracts and invoices that presented certain assets as owned. In addition, assets that were sold were not removed from the books, assets that were borrowed were presented as owned, and certain guarantees of loans were not disclosed. To top it off, those involved in the collusion even borrowed physical assets to pass inspection and observation by external CPAs.

How the scheme was discovered: The perpetrator believes a whistleblower tipped off authorities to the fraud.

What could be done to prevent this type of fraud: The extent of the internal collusion would have made this scheme difficult for any external CPA to spot. It might have helped to have had a fraud hotline available. That might have encouraged a whistleblower to step forward sooner. As it was, the fraud took place for several years.

Fraud No. 5: Sales, Lies, and Stock Inflation

Description: This scheme had three phases and took place over nearly two decades. The first phase consisted

of the owners of a privately held family business skimming company revenue. The practice allowed the owners to pocket cash and to avoid paying income and sales taxes on the skimmed revenue. In the second phase, the company's owners reduced their revenue skimming while preparing the business for an initial public offering of stock. That created the illusion that the company's sales had increased. After the company went public, they shifted into the third phase of the fraud, overstating earnings to artificially boost the company's stock price. They then reaped profits by selling the stock at inflated prices.

Dollar loss: Between $500 million and $600 million, in a combination of investor losses plus the money skimmed from the company.

What was done to conceal the fraud: Poor internal financial controls allowed the fraud to take place. The family members running the business, including the perpetrator interviewed by the Fraud Task Force, all had a vested interest in hiding the fraud. The respondent, who used to work at an audit firm that did business with the company, purposely hired accounting firms that he knew would send inexperienced auditors, usually young men, to conduct audits. The respondent said the company took advantage of the auditors' inexperience and youth, in part by assigning an attractive female employee to assist them with getting information. The female employee was instructed to flirt with the auditors and use her beauty and charm to gain their trust. She also was told to stay in the room where the audit was being conducted and consistently interrupt the auditors to keep them off track. The respondent said the ploy worked "like magic," with the auditors being led to believe the books contained items that actually didn't exist. People are naturally good natured and gullible, with most not understanding the art of lying, he said.

How the scheme was discovered: Ex-lovers, former business associates, and former employees reported it to the authorities.

What could be done to prevent this type of fraud: The respondent said that he took advantage of accounting firms that sent out inexperienced auditors to do fieldwork. The auditors were as young as 22 or 23 years old and often had between six months' and two years' experience. In addition, most auditors the respondent dealt with did not have a background in fraud. These auditors were not prepared to objectively question his company's audit process, with its added distractions and deception, or to stand up to company management if they did believe something was wrong. To better combat fraud, firms should send out more seasoned auditors who have had enough fraud education to understand the reasons people perpetrate fraud and the ways they execute those crimes. The problem is that firms that send out more experienced auditors most likely will have to charge more, and that could put them at a competitive disadvantage.

Fraud No. 6: A Scheme That Cost Billions

Description: The fraud started when the perpetrator and his co-conspirators made a small but fictitious accounting entry to create bogus revenue that would allow their large public company to meet quarterly earnings expectations. The original plan was to correct the entry the next quarter, but that didn't happen and the fraud grew. The co-conspirators, who were members of the senior management team, altered the financial statements to include fictitious cash, nonexistent fixed assets, and bogus goodwill from acquisitions. The goal of the fraud was to keep the company in business. The fraud always took place during the same quarter each year. The co-conspirators would determine the company's revenue shortfall and divide up responsibility for creating the bogus entries. In addition, a low-level accounting clerk was responsible for creating hundreds of entries related to the fixed-asset account. The perpetrator believed until the end that the company could still turn itself around and that the fraud eventually could be removed from the financial statements. The scheme lasted 16 years.

Dollar loss: $2.9 billion, incurred by shareholders.

What was done to conceal the fraud: Only a small number of people in the company knew about the fraud, and they never discussed it in email. The perpetrator had worked at the accounting firm that conducted the company's audits, and he used his knowledge of the firm's audit procedures, techniques, and thresholds for materiality to design the fraud in a way that would escape the auditors' attention. The co-conspirators paid the accounting clerk an exorbitant salary to ensure complicity and silence. The company also kept the general ledger away from the external CPAs.

How the scheme was discovered: An executive's large stock sale shortly before the company issued

disappointing quarterly results prompted the FBI to launch a probe into insider trading at the company. The investigation eventually led to the perpetrator telling authorities of the larger fraud scheme.

What could be done to prevent this type of fraud: One red flag is if a company executive, especially the CEO, CFO, or controller, previously was employed by the accounting firm conducting the company's external audit. The perpetrator also suggested that the following actions could have caught his company's fraud scheme earlier:

1. Verify cash in bank accounts.
2. Insist on accurate and timely inventories of fixed assets.
3. Research and verify goodwill calculations.
4. Compare salaries to levels of experience.
5. Keep an eye out for suspicious patterns. For example, in this scheme, the bogus entries were always entered in the third quarter of each fiscal year.

CONCLUSION

The fraud schemes described in this article resulted in losses much greater than the nearly $4 billion taken from corporate and investor coffers. Companies were forced into bankruptcy, costing hundreds of jobs. Reputations were ruined. Nest eggs were shattered. Families were torn apart.

CPAs play a crucial role in preventing, spotting, and stopping fraud. Insights into the mindset of criminals such as those interviewed by the Fraud Task Force can provide ideas for better structuring internal controls and knowing which questions to ask about a financial statement. Success in fighting fraud can save untold numbers of people from the toil and trouble such criminal activities can inflict. That's the CPA's opportunity and challenge.

Jeff Drew *is a* JofA *senior editor. To comment on this article or to suggest an idea for another article, contact him at jdrew@aicpa.org or 919-402-4056.*

Signs of the crimes

The six white-collar criminals interviewed by the Fraud Task Force recommend the following policies, practices, and procedures as weapons in the fight against fraud:

1. Organizations need to implement and enforce strong financial controls. Management and boards of directors need to emphasize the importance of testing the controls and closing all loopholes.
2. Board members, executives, and accountants need to closely scrutinize monthly financial statements and other documents, keeping an eye out for signs of suspicious activity.
3. Management should establish a "tone at the top" that encourages ethical conduct and prohibits policies that pressure staff to meet unrealistic financial goals.
4. Organizations should provide a fraud hotline for employees, making it easier for them to act as whistleblowers.
5. Businesses should prohibit CFOs and controllers from simultaneously holding a similar position in another business.
6. Organizations should be wary of entering into an external-audit agreement with an accounting firm that once employed a member of their management team, especially the CEO, CFO, or controller. Knowledge of the accounting firm's audit practice and testing thresholds can be invaluable in designing a fraud scheme to avoid auditors' detection.
7. Organizations should require the use of two-signature checks.
8. Accounting firms should assign auditing fieldwork to seasoned auditors who have received formal education into how to prevent and uncover fraud schemes.
9. CPA firms should teach auditors the value of questioning any discrepancies in client financials. While most occurrences are honest mistakes, a handful point the finger at illicit activities.
10. Accounting firms should prohibit CPAs from serving as trustees for clients' trusts.
11. External auditors should decline any offers of gifts from clients and should notify board members immediately if such an offer is made.
12. Management should take note of any unexpected lifestyle upgrades among staff. If an employee suddenly

shows up driving a $100,000 sports car or wearing a $2,500 Italian suit, the employer should determine whether the employee's compensation would allow for such purchases.
13. Organizations and auditors should question any unexpectedly high compensation levels for employees and take a closer look at any particularly close relationships between employees, including management and vendors.
14. External auditors should notify the organization's board if any employees, including managers, are delaying or denying the delivery of documents or acting in any other way to impede the auditors.
15. Auditors should verify cash in bank accounts, insist on accurate and timely inventories of fixed assets, research and verify goodwill calculations, and keep an eye out for suspicious patterns.

Antifraud initiative seeks to educate

The Center for Audit Quality (CAQ), an AICPA-affiliated nonprofit dedicated to promoting high-quality public company audits, is on the front line of an education offensive in the war on fraud.

The campaign dates to the October 2010 publication of the CAQ report *Deterring and Detecting Financial Reporting Fraud: A Platform for Action*. Shortly after that, the CAQ embarked on several collaborative projects in partnership with Financial Executives International (FEI), The Institute of Internal Auditors (the IIA), and the National Association of Corporate Directors (NACD).

Each organization in the partnership represents a segment of the financial reporting supply chain. The CAQ, for example, represents a membership of more than 600 public company auditing firms.

The partnership is in the midst of rolling out an arsenal of products and programs designed to equip internal and external auditors, executives, board members, and others with the knowledge and skills to fight fraud. The first of the partnership's tools, FEI's Fraud Literacy Quiz, was introduced in November 2011.

In June, FEI presented "Interview With a Fraudster," a program giving members of the partnership an opportunity to learn about fraud deterrence and detection from convicted felon Sam Antar.

Beginning in September, the NACD will host a series of five webinars focusing on what skepticism means for each member of the financial reporting supply chain.

For its part, the CAQ is developing a number of fraud scenarios customized to various industries. The Washington-based group expects to begin releasing the scenarios in October.

In December, the IIA will host a round-table event on the topic of "Closing the Expectation Gap."

To learn more about the antifraud initiative, visit thecaq.org/Anti-FraudInitiative.

AICPA RESOURCES

***JofA* articles**

- "What's Your Fraud IQ?" Aug. 2012, page 32
- "Small Businesses, Big Risk," Aug. 2012, page 38
- "Corporate Governance Best Practices 10 Years After SOX," July 2012, page 24
- "What's Your Fraud IQ?" May 2012, page 44
- "What CPAs Need to Know About Organized Crime," April 2012, page 38

Publications