THE ANATOMY OF A FRAUD INVESTIGATION

Follow the real-life case of a multimillion-dollar embezzlement at a high-profile nonprofit, from discovery through investigation and criminal referral. This session will walk you through how forensic investigators pieced together the evidence using a proven fraud investigation methodology and framework. Learn how investigators identified the alleged perpetrators, analyzed hundreds of falsified invoices, and earned their client the maximum insurance settlement possible as a result of their well-documented work product.

You will learn how to:

- Identify and apply elements of Cressey's fraud triangle.
- Adopt a methodology for conducting consistent fraud examinations.
- Apply tips and tricks to real-world fraud investigations.

LAWRENCE HOFFMAN, CFE, CPA, CGMA, CVA
Senior Partner
Raffa, PC
Washington, DC

Lawrence Hoffman has more than 35 years of forensic accounting, audit and accounting, and tax experience in public accounting and the private sector. He began his career with Coopers & Lybrand (now PWC) in Washington, DC. Hoffman founded his own firm in 1982 where he developed a nationally recognized practice in litigation support, fraud investigations, business valuation, and reorganization and insolvency services. He merged his practice with Raffa in 2008. He has been involved in numerous high-profile cases as a consulting and testifying expert, and has conducted and led teams of forensic accountants on fraud investigations ranging from small family-owned businesses to large governmental organizations with losses of more than $500 million.

THE ANATOMY OF A FRAUD INVESTIGATION

NOTES

Disclaimer

This presentation is based on an actual fraud investigation conducted by the presenter. The allegations against the individuals and entities involved in this case have not been proved in a court of law. Although the particulars of the case have been the subject of numerous media publications, the names of the individuals and entities have been changed for purposes of this presentation.

Introduction

On Sunday, October 27, 2013, I went outside and picked up my copy of the *Washington Post* off my doorstop, as I do every morning. I went inside and sat down to read it, only to be shocked by the front-page headline: "Millions lost by nonprofits, with little explanation."[1] The *Post*'s reporters had scoured the IRS Form 990 informational return filings for thousands of nonprofit organizations, looking for anyone who had checked the box in Part VI, Section A, Question 5—"Did the organization become aware during the year of a significant diversion of the organization's assets?" Then, they dug into the details of those diversions and reported more than 1,000 cases of embezzlement, theft, and other unauthorized uses of funds, accusing the charities of being dishonest in these public disclosures, including in particular, an organization I had investigated. I spent a considerable amount of time meeting and talking with both of the reporters who wrote the article to not only discuss the case I had investigated, but what I thought even more relevant to their article, the issue of fraud and abuse in the nonprofit sector. Based on my meetings with them, I was expecting a much different article, more of a general piece on fraud in the nonprofit sector. Instead, the article was an indictment of the nonprofit sector and the fraud perpetrated against the particular organization I investigated.

[1] For the full article, please visit http://tinyurl.com/lp6qmp7.

NOTES

I've spent more than three decades in the anti-fraud profession and helped found the *Raffa Nonprofit Fraud Prevention Institute* in 2013 with the mission of reducing the amount of fraud committed against nonprofits, and to help organizations preserve their time and resources in order to focus on their important work.[2] The *Washington Post* reporters had interviewed me, attended seminars I gave to the local nonprofit community, and we had talked at length about why nonprofits become victims of fraud. Instead of an article that lamented this victimhood, the *Washington Post* essentially ignored this complex issue of fraud and principally focused on the public disclosure piece.

The *Washington Post* certainly reminded the nonprofit community that someone is always watching, and the following months brought a slew of additional articles accusing the nonprofit community of failing to control its assets. Congressional investigators got involved, reviewing these public disclosures to see whether they were proper. Sadly, in the following months and years, I saw no reduction in the volume of fraud cases in the nonprofit community. Likewise, I saw no increase in law enforcement resources devoted to helping to prosecute fraud cases. But the entire saga helped to reemphasize the importance of strong fraud prevention and detection controls for the nonprofit community, since clearly, the public and lawmakers were on edge.

Fraud in the Nonprofit Sector

The National Center for Charitable Statistics reports that there are more than 1.4 million nonprofit organizations in the United States, as of June 2014. Their estimated share of the GDP is a touch over 5 percent. The 966,000 public

[2] www.raffa.com/fraud

charities alone had more than $1.5 trillion in revenue, with more than $300 billion of that total coming from private charitable contributions. So, it is easy to see why the public has a vested interest in helping to deter fraud in the nonprofit sector—every dollar stolen through fraud is a dollar that doesn't go toward the organization's charitable purpose. If we use the ACFE's estimate of 5 percent losses due to fraud and apply it to the nonprofit sector, it would mean that nonprofits in the United States lose more than $80 billion to fraud each year!

The ACFE's reports don't suggest that fraud is any more prevalent in the nonprofit sector than in any other sector in the United States, but the public interest is certainly greater than in any other sector, other than perhaps the government and the mega public company frauds like Enron and Worldcom. The ACFE's *2014 Report to the Nations* notes with respect to "Victim Organization" that nonprofit organizations accounted for 10.8% of reported fraud cases, behind 37.9% for private companies, 28.5% for public companies, and 15.1% for government.[3] The report also notes that the "Median Loss" was $108,000 for nonprofits, versus $160,000 for private, $200,000 for public companies, and $90,000 for government.

It is true that there are a number of factors that are specific to the nonprofit community that can increase the risk of fraud:

- *Mission-driven vs. profit-driven*: Often, nonprofits do not make financial considerations a priority because their mission is overwhelmingly the greater priority. Without a profit motive, nonprofits may not pay careful attention to where every dollar is going, which means

NOTES

[3] www.acfe.com/rttn

some of those dollars may quietly be lining a fraudster's pockets.

- *Volunteers vs. owners*: Since nonprofits are so often reliant on volunteers, those volunteers may have a limited view of fiduciary responsibilities. They are there to shepherd the program more than the funds, and don't necessarily feel the same degree of personal investment that a private company's owner would.
- *Lack of internal controls/segregation of duties*: Managers who are very smart about the nonprofit's mission may not have a lot of experience with internal controls. Also, in the effort to devote the maximum amount of funds toward the mission instead of administrative expenses, often nonprofits have small finance departments, where staff are asked to wear many different hats, making it difficult or impossible to achieve proper segregation of duties.
- *Lack of hiring due diligence*: Basic prevention efforts related to hiring, like background checks, may be neglected because funds are not available. Also, sometimes nonprofits may get into the mindset that the passion about the mission means that an individual can be trusted, and hiring due diligence isn't seen as a necessity.
- *Lack of anti-fraud programs*: Anti-fraud programs are often seen by nonprofits as optional instead of necessary, particularly since it is very difficult for many nonprofits to spend scarce funds on preventive measures. Basic measures like anonymous hotlines and formal fraud policies are often not put in place until it's already too late. In addition, most organizations think that "it could never happen to them."
- *Reliance on external audits to catch fraud:* Many nonprofits suffer from the misconception that their external financial auditors are going to catch fraud if it exists. Sadly, the 2014 *Report to the Nations* estimated

NOTES

NOTES

that less than 5 percent of all fraud cases are caught by external auditors—or about half the amount caught "by accident."

- *Culture of trust:* Nonprofits can easily be caught in the trap of thinking that nobody could possibly be so dishonest as to steal charitable funds, and are therefore willing to put a good deal of trust in their employees and business partners. As I say time and time again, trust is not an internal control, so this simply puts them in a position where they are more likely to be defrauded.

Case Facts and Overview

A few years ago, I was called by a large high-profile nonprofit to help look into a whistleblower complaint. The nonprofit's new chief technology officer (CTO) had raised some concerns about a major vendor that had been used by his predecessor. He was concerned because he couldn't find much of the equipment ordered through the vendor, and when he tried to research and contact the vendor, it didn't seem like a legitimate company. Management told me that they couldn't imagine that the prior CTO was committing fraud, but they wanted me to check things out and see if there was anything that they should be worried about.

I had some initial concerns, and the whistleblower allegation certainly had a lot of troubling pieces. I knew that the nonprofit had been in hyper-growth mode, since they had received significant upfront funding and were aggressively implementing numerous operational areas in pursuing their mission. This creates a high fraud risk environment. I also knew that the prior CTO, Evgeni, was a Russian national, who had left the organization several months ago to move back to Russia for "personal reasons." The vendor being questioned—PengCo—was introduced to

the nonprofit during Evgeni's seven-year tenure, and the nonprofit had purchased about $4.5 million in equipment and software over his employment. It seemed odd that the organization did not use the typical large IT equipment vendors for these purchases.

Conducting the Investigation

Since sufficient predication existed, management directed us to move ahead with a full-scale investigation. We employed our standard investigative framework and methodology that I developed over my years as a forensic accounting investigator. We use this framework on all forensic engagements as it is important to demonstrate that all investigations are done in a consistent and systematic manner with a proven framework and methodology. This is critical if the case ends up in court and the opposing side attempts to discredit your work or even exclude it under a *Daubert* challenge. The framework includes four phases consisting of:

1. *Pre-Investigation:* This phase includes examining the initial predication and various engagement considerations such as setting the scope of work, conducting conflicts checks, and receiving the signed engagement letter and retainer.
2. *Planning:* This phase includes preliminary assessment and formulation of a fraud hypothesis, team formation, determining location of data and potential evidence, establishment of communications protocols, legal analysis and other matters of law, formulation of a work plan, creating entity charts, and setting up case files.
3. *Execution*: This is the data and evidence gathering phase where we employ specific forensic investigative tools and strategies, including background investigations, interviews, imaging computer hard drives, reviewing documents, analyzing data, and conducting other forensic procedures.

NOTES

4. *Conclusion*: This phase includes conducting a "reverse proof," writing and producing our investigative report of findings, working with the client on remedies and recovery, and potentially judicial testimony.

Planning the Investigation

Since there was strong predication confirmed in our pre-investigative phase, it was time to properly plan the full scale investigation. First, we went about the business of forming the investigative team. Ultimately, it was decided on including:

- ❑ *Board member(s) and/or audit committee member(s)*: Since the case involved allegations against upper management, it was critical that we keep the Board fully informed of the investigation. The whistleblower seemed to think the CTO had worked alone, but we couldn't be sure at the outset.
- ❑ *Management representative*: A high-ranking official who helps coordinate interviews and data requests from the investigative team.
- ❑ *In-house counsel*: It was very important to make sure that work was privileged, considering its sensitivity.
- ❑ *Lead forensic accounting investigator:* This was my role.
- ❑ *Forensic accounting staff:* Various staff assisted in the investigation.
- ❑ *IT specialist*: Since the case was known to involve IT equipment, an independent IT specialist was brought in at the start to be able to provide subject matter expertise.

One of the first questions that the investigative team asked is what type of records were available, in terms of physical, documentary, and testimonial evidence.

- ❑ Available physical evidence:
  - IT equipment

NOTES

- Computer hard drives
- Offices and desks

❑ Available documentary evidence:
- Invoices from PengCo
- Depreciation schedules
- General ledger

❑ Available testimonial evidence
- Current CTO
- Current CFO (prior CTO's supervisor)
- Current CEO
- Current COO
- IT Staff
- Accounting Staff

Executing the Investigative Plan

The investigation consisted of five major components:

1. Interviews of cognizant individuals
2. Background checks on the entities involved
3. Physical inspection of IT equipment
4. Document review of invoices, emails, and ledgers
5. Analytical procedures, both quantitative and non-quantitative

We began by interviewing the whistleblower to find out what he knew. He told us that he had tried to contact PengCo without any success. He also said that the CTO is responsible for conducting IT inventories. When he tried to locate the inventory that had supposedly been purchased by Evgeni, he wasn't able to find a good deal of it. There had never been any problems with prior inventories, but they had all been conducted by Evgeni. Evgeni also had a long-standing policy of writing off and "junking" any IT equipment that was more than three years old as obsolete, which definitely wasn't industry standard for the types of equipment he was purchasing. This also allowed Evgeni to get the fraudulent transactions off the books.

NOTES

So, we asked the CFO what he knew about the situation, since he'd been Evgeni's supervisor. The CFO told us that, when they needed new IT equipment, Evgeni would present him with three price quotes from vendors, one of which was PengCo. Evgeni had told the CFO that he'd used PengCo in the past with his prior employer, and that he was able to negotiate better prices with them then other vendors. As an added benefit, PengCo took American Express, which meant the organization was earning rewards points. The CFO was emphatic that the Evgeni had been an exemplary employee, working hard even on weekends, and believed him to be very trustworthy.

The organization's IT staff told us a slightly different story. They thought that PengCo was owned by some of Evgeni's friends or family, and they thought it was a little strange that Evgeni would always receive orders directly and handle the equipment himself, instead of letting the staff handle it. Sometimes, they said the equipment would be sent directly to Evgeni's house, not even to the organization. They thought that PengCo was just reselling equipment from a larger vendor.

So, we started digging into PengCo's background. The company had two directors, Sergei and Ilya, and both of them were also Russian nationals. Sergei and Ilya's home addresses were what PengCo used on its corporate filings and invoices. Sure enough, PengCo and its employees had links to Evgeni. First, we noticed that Ilya had sold a condominium to Evgeni. Also, from reviewing some of the records related to PengCo, we knew they had an employee named Maria. She shared a prior address with Evgeni, and had a number of convictions for fraud and theft. We developed an extensive entity chart showing all the various connections between the parties. When we presented this chart to the client, they were now convinced that a

NOTES

NOTES

significant fraud may have been perpetrated against them by this former employee. They were devastated and could not believe that such a highly regarded and trusted employee could betray them, a typical response I find with many fraud investigations.

At this point, we were confident that Evgeni was definitely linked to PengCo. So, the best case scenario for the nonprofit is that the company was legitimate and the prices were fair, but that Evgeni hadn't disclosed a conflict of interest. The worst case scenario is that all of the $4.5 million that had been paid to PengCo were fraudulent, and there had never been any equipment received. So, we started to work on determining which payments, if any, were fraudulent.

We spent a considerable amount of time reviewing and analyzing the PengCo invoices. This resulted in a very large data file where we could employ further forensic tests and analysis. Many of the invoices were incomplete, and the format was always changing. We saw shipping charges that had no logical relationship with the products being shipped. Dozens of duplicate products had been ordered, including the quantity and price details—which was highly unexpected, given that prices for IT equipment virtually always decline over time. Often, the invoices hadn't been properly approved for payment, since the CTO and CFO should have both signed to show they had reviewed and approved. And in a number of instances, organizational policy was violated because payment had been made by credit card before the CFO had formally authorized the use of the credit card. Evgeni had authority to use the credit to place the orders once approved by the CFO.

Things didn't look good for the nonprofit, but we still hadn't conducted our own inventory of equipment. So, we

went out to the various sites where the IT equipment was supposedly being employed in the operations, and we couldn't find much of the equipment. Evgeni had loved to buy one piece of IT equipment in particular—Hewlett-Packard blade servers. That's not a small piece of equipment that could easily go missing, and we couldn't find dozens and dozens of them, all ordered from PengCo.

So, we put all the pieces together and performed additional nonfinancial reasonableness analysis. What we found was that the nonprofit was purchasing more equipment from PengCo then they could ever possibly use! They had more server power than Google's Chicago office, if they had actually received and used all of it. Not only that, they had purchased multiple enterprise-level copies of the same software from PengCo, when there was no way that they could ever have needed more than one copy. Evgeni had definitely also been lying about the "great prices" that PengCo was charging. We found that they were charging amounts well in excess of industry average, so the organization was overpaying for all this equipment that they weren't even receiving!

Concluding the Investigation

In the end, based on the evidence we estimated that at least $3 million of the PengCo purchases were completely fraudulent, and the equipment had never been received. In addition, for any equipment and software that was received, the organization significantly overpaid. Evgeni had launched his scheme almost immediately after he was hired, continuing it for seven years! When we presented our findings to the organization, they were shocked and in disbelief. They had trusted Evgeni, and he had betrayed that trust completely. They took their case to the U.S. District Attorney, but unfortunately for them, since Evgeni had already left the country, it was going to be difficult to

NOTES

NOTES

pursue him. But, we did track down some of his spoils—he's the proud owner and operator of a children's amusement park back home in Russia.

How did the organization respond? They took strong actions to strengthen their internal controls and procedures for asset handling, and took the time to train their staff thoroughly on fraud prevention and detection. And, fortunately, as a result of the strong and thorough report we produced, they were able to recover a good portion of their financial losses from their insurance company. But, they can never really fully recover, since this event destroyed their ability to feel like they could trust their employees, and it was a tremendous blow to their operations and reputation. This fraud will also most likely go down in history as a landmark case in nonprofit fraud since it garnered so much attention through the press and lawmakers. I would not be surprised to see lawmakers push for regulation similar to Sarbanes-Oxley in the nonprofit sector in the future. Nonprofits with "significant diversions," as defined by the IRS, can no longer sweep the matter under the rug to avoid unwanted publicity and reputational damage. Since nonprofits have a high fiduciary duty to the public, much like publicly-held companies do, they will always be held to a high standard in their oversight of their financial affairs and proper safeguarding of funds.

Lessons Learned and Takeaways

I say it over and over—trust is not an internal control. It's a tragedy when I see a nonprofit learn that the hard way. Fraud is always committed by someone you know and trust, and that's what makes it so painful when it happens. In this case, the nonprofit had failed to segregate duties sufficiently, meaning that Evgeni had the authority to purchase equipment, receive it, and maintain the related

inventory records. In addition, the internal controls lacked in what I term the "three-way match." When procuring goods, payment should not be made without the proper matching of a purchase order, invoice, and most importantly the receiving report including the packing slip. In this case, none of the fraudulent invoices were supported by a receiving report and packing slip. The perpetrator was too trusted, and given too much control, which he took advantage. Proper internal controls, like proper segregation of duties, job rotation, or greater management analysis of overall purchasing patterns, might have prevented Evgeni from perpetrating this scheme, or at the very least, caught it much earlier.

So, what should an organization tell its employees to do if they suspect fraud? I always recommend that an organization instruct employees to:

- *Follow the organization's fraud policy*: An organization's fraud policy should outline, in detail, the employee's responsibilities to report and respond to fraud, and the organization's plan for response. This needs to be in place before any instances of expected fraud arise, so that the incident can be handled smoothly by all parties involved.
- *Report through the official whistleblower channels*: Organizations should have formal, and preferably anonymous, processes in places for whistleblowers to report suspect fraud. Hotlines are certainly the most popular method, and often the easiest to implement.
- *Share your concern with your immediate supervisor, appropriate management, or the audit committee*: If employees are willing to put their name behind an allegation, it can be a tremendous boon for the investigator. Since the employee's immediate supervisor may be the problem, it is important for organizations to have alternative reporting chains so

NOTES

that the appropriate level of management can handle the investigation.

- *Document observations and discussions promptly*: It is easy for us to forget specific details which may be critical in an investigation—documenting the details immediately after an event can save valuable investigative resources.
- *Do not confront the suspected perpetrator:* We often find that whistleblowers want desperately to confront the suspected perpetrator so that their concerns can be assuaged and they can go back to "normal" operations. But, confronting the perpetrator may tip them off to a potential investigation and give them an opportunity to destroy valuable evidence.
- *Do not investigate the matter on your own:* The whistleblower has not been trained in investigative techniques, and are just as likely to hinder an investigation as they are to help it. But they are often severely tempted to do so, and must be reminded to leave the matter to those that are professionally trained to handle it.
- *Do not discuss the matter with others:* The more people that know about an alleged fraud, the more likely it is that the perpetrator will find out about the investigation and destroy evidence. Also, discussing an alleged crime before it has been fully investigated can open individuals to liability for defamation of character.

And the next step—how should the organization react when they receive a credible allegation of fraud?

- Remember, you have a duty to investigate promptly and thoroughly!
- Retain counsel to preserve attorney-client privilege.
- Retain a forensic expert to assist in the investigation, working through counsel.

NOTES

- ❑ If appropriate, suspend the alleged perpetrator with or without pay.
- ❑ Identify and suspend the alleged perpetrator's access rights to physical and digital assets.
- ❑ Inform your insurance carriers, regulators, or any other parties to whom you owe a duty to disclose.

Your employees are your eyes and ears, so make sure they're empowered to report potential fraud to you, and make sure that you are equipped to investigate those allegations.

NOTES