CHAPTER 1

FIRST INDICATIONS
(THEY'RE DOING WHAT?)

It was a bit after 5:00 P.M. on a Friday afternoon. The sun was out and still strong, and I was looking forward to ending my busy week by relaxing outside in my reclining lawn chair, soaking up the warm evening air. I had just pulled into my driveway and started to unload my client files and briefcase from the trunk of my car when I heard my cell phone ringing. As it rang, I fumbled through my pockets trying to find it, only to realize I had left it on the front seat of the car. Of course, by then the fourth ring had finished, and the caller went into my voicemail. I carried the files into the house and returned back out to retrieve my phone and see if the caller left a message. Although the missed call number looked familiar, I couldn't place it.

I retrieved the message and recognized the voice immediately. It was the chief financial officer of a well-known non-profit organization called Crestview that I had done work for in the past. I knew right then before I concentrated on his message that if he was calling me on a Friday night after 5:00, something big was happening or about to happen. His message went like this:

''Steve, Tim Hill. How are you? Sorry to bother you on a weekend, but I need to talk with you, the sooner the better. Any chance you can call me back tonight when you receive this message, I would appreciate it. I will be here late tonight, and you can reach me anytime on my cell phone. My number is 806-510-1234. I would really like to talk with you as soon as possible.''

I took out a pen and pad from my car and listened to his message a second time, this time writing down his cell number. I

walked into the house, checked in with my wife and kids, and let them know I needed to return a very important call to a client that I just received. Then I walked back outside, straight over to my front steps, and sat down, knowing the call might take a while and that the sun lasted the longest in that area of my yard. I knew once I returned Tim's call that my plans for a restful night and weekend were going to change.

• • •

I dialed his number and he answered immediately. After asking each other what was new and how things were going, I asked Tim how I could help. He asked me if I had a few minutes, or did I want to call him back later in the evening when he could spend a few minutes with me on the phone. I told him now would be fine. Tim provided me with the following details:

''I received information this week that a controller in one of our divisions could be stealing money from the organization. While the person who provided me with this information wished to remain anonymous and provided little to no details, I told them there was little I could do unless they provided me with more details and possibly examples of how the controller was stealing the funds. Reluctantly, they managed to get a copy of a credit card statement used by the controller that is paid through their division's checking account. Once I saw the statement, I realized I had a big problem due to the high volume of personal charges made on the card in the one month alone that was paid using the division's funds. The controller does not know I am aware of this information, or that I have a copy of his credit card statement. The person who provided me with the information works in the same division and cannot become known in this matter as the source of the information, nor can we acknowledge that we have a copy of the credit card statement. The controller will be able to identify who provided it to me immediately if it ever becomes known that we have it. The division has five employees at their location, and they manage their own finances. They collect their own revenues and pay their own bills. The controller keeps all the records for their division out at their location, and he has an office manager who helps keep things filed and organized. I need your help this weekend to think about what I just shared with you, and to come up with a plan to address this issue.

I want to deal with it as quickly as possible, and will be available all weekend if needed to react to this by Monday morning. What are your thoughts?''

FRAUD FACTS

Anonymous tips and complaints are the leading method of detection of fraud. According to the Association of Certified Fraud Examiners' 2008 Report to the Nation on Occupational Fraud & Abuse, tips accounted for 46 percent of all frauds detected, followed by 20 percent discovered by accident.[1] Tips included employee, customer, and vendor complaints, and were the leading detection method in their 2006 survey as well. The high percentage of detection by anonymous tips emphasizes an organization's need to educate employees regarding their fiduciary duty to provide information, as well as implement a means or process for individuals to provide such information. On the receiving end, the organization must implement a system to collect, screen, and process complaints and information when it is received.

I simply sat in the sun in silence, listening to Tim provide me with the details, and watching the sun set on my weekend plans. For an instant, I thought about how virtually every fraud embezzlement case had come to me on a Friday afternoon typically around 4:00, just in time to ruin a perfectly good weekend.

I told Tim I understood the gravity of the situation, and would be available to help him as much as needed throughout the weekend. I then started in with my standard host of questions, a process I call ''triage.''

I asked Tim these questions, and have included his responses.

''Other than the informant who provided the card statement, is there anyone else at the division aware that you know the controller may be stealing funds?'' Tim indicated he was certain the controller and the other staff did not know that the information was brought to his attention.

''Is there any reason to believe the controller knows his situation has been compromised, and would be destroying the evidence as we speak?'' Tim stated the informant called him to let him know the controller had left for the weekend as usual, and that nothing unusual or suspicious was noted with his behavior throughout the day. Tim indicated there would be no risk of loss of evidence by waiting and working on a plan over the weekend versus going to the division immediately and securing any evidence.

LEARNING POINT

Why would it be important to know if anyone was aware that the scheme had become known? Timing in these cases is everything. In virtually every fraud matter, the perpetrators maintained evidence of their crime, in the form of documents in a drawer, tracking the details in a notebook, or keeping files electronically on their computers. Once they feel their circumstance has been compromised by someone learning about their misdeeds, the evidence is almost immediately destroyed or removed offsite. If they have left the building for the day, they come back after-hours and steal or destroy the evidence. They also call co-workers and ask favors of them. Such favors could include deleting files and bringing physical files and information home with them. Fraud perpetrators have been known to break into their employer's buildings or even burn the building down in acts of desperation to ensure the evidence is never found and used against them. I had one case involving an employee embezzlement where the suspect burglarized the office, stole the receipts ledgers, and corrupted the computer files so no one could access the computerized accounting system the next morning. A week or so later the same office was burglarized a second time, only this time some of the accounting records were actually returned in a poor attempt to show they were there the entire time, buried below other papers and information. Desperate people do desperate things.

Knowing that, timing is of the essence in these cases. Typically, I like to deal with searching for evidence immediately after receiving a call such as Tim's. In my experience, too much happens if you wait until tomorrow morning. I drive right to their location regardless of the time of day, and secure any and all information possible, removing any possibility of it being lost, stolen, or destroyed. If I find any actual or potential evidence, it all leaves with me so I can be assured nothing will happen to it. If there are computers involved, they come with me as well.

''Do they have computers at their location, and are they backed up in a reliable fashion in the event the controller or anyone else potentially involved gets nervous and deletes the hard drives?'' Tim indicated there were computers on each desk and a local area network, and that they performed their own backups on a regular basis. Tim was not aware of how the backup tapes were maintained.

''Is the organization's legal counsel involved and up to speed on this matter?'' Tim stated he had been speaking with counsel

throughout the week awaiting the credit card statement, and that as recent as late afternoon he had spoken to counsel about the status of the matter. Counsel was aware that Tim would be reaching out to me to solicit my involvement in resolving the matter.

LEARNING POINT

Why would you want to know about any computers, as well as if and how they were backed up? Just as with physical evidence, such as ledgers, checks, and bank statements, computer files and hard drives are at equal risk for corruption or deletion if not preserved in a timely fashion. Often, users have remote access into the business systems, and in some cases have access directly into their individual workstations, depending on the level of technology, sophistication, and authority involved. Once the computer hard drives have been deleted or physically stolen from the computers, recovering the files becomes much more difficult, if not impossible. Having reliable and secure backups of the drives creates a secondary plan in the event files are deleted or computer drives are deleted. However, if the backup tapes and drives are under the control of the same person or individuals potentially involved in the matter, both the computer drives and the backups are at risk of theft or destruction. Beating suspects to the punch by imaging the drives, making a backup, or taking possession of their computer will provide the best scenario for finding electronic evidence, if any exists.

Before setting out to preserve any potential electronic evidence, answers to a few questions may help. Are the computers desktops or laptops? Does the target use any other electronic devices, such as a hand-held phone or BlackBerry, to access his files and e-mails? The mobility of computers can create many issues and concerns—first and foremost, physically locating where the devices exist at any point in time. Chances are if the target uses anything but a desktop, his laptop and devices remain with him at all times. If the laptop is not at the organization, it will make it difficult to seize it or make an image of the hard drive without the user's knowledge.

Remote access to the organization's systems, files, and information may need to be disabled to the target once the investigation has been initiated. Knowing all the means the target has available to gain access will help ensure all points of access have been disabled, preventing the target from secretly accessing and deleting key files and information, or worse, stealing company information, such as client and customer lists or trade secrets, before being terminated.

FRAUD FACTS

The sophistication of an average perpetrator has likely been raised by what has been termed the *CSI* effect. In essence, individuals have been watching episodes of crime and forensic shows on television, and have learned what things are important in investigating various types of crimes. Much information is also available to a perpetrator through the Internet. One example is with software and technology available to remove files and evidence from computer hard drives. Wikipedia, the Internet-based encyclopedia, includes the term *anti-computer forensics*, which is defined as ''a general term for a set of techniques used as countermeasures to forensic analysis.'' Much more information is included by Wikipedia in its definition, providing would-be perpetrators with knowledge that could aid them in preventing detection and recovery of supporting evidence.

LEARNING POINT

Legal counsel plays a very important role in every fraud investigation. First and foremost, no privilege exists between a client and an accountant, or a client and a fraud investigator. Any and all communications and procedures performed for the client will be wide open for discovery, and worse, the potential will exist that the very professionals retained to help the client resolve a matter could become witnesses against the client. To help ensure that all communications, procedures, and information are protected from discovery, the client should engage counsel to direct the inquiry or investigation. The accountant, fraud investigator, computer forensic specialist, and anyone else brought into the case should then be engaged directly by counsel. In order to preserve the privilege between the client and counsel, all communications should be directly to counsel, and all work performed should be clearly marked *confidential* and *attorney-client privileged.*

In many investigations, issues are identified within the victim organization beyond those relating to the fraud matter being investigated. In most cases, the discovered information could prove detrimental to the organization, and therefore may need to be protected by maintaining it as confidential. Having been engaged as a consulting expert directly by counsel will help preserve the information from being disclosed. Conversely, if counsel changes strategies later in the investigation and decides to disclose the same fraud professional as an ''expert'' for trial purposes, counsel does so at the risk that any and all information collected and discussed from the inception of the matter will be discoverable. This is something to keep in

(*Continued*)

mind and discuss with counsel before getting too far into the matter and preparing a well-documented file—potentially to be used against the client.

Second, issues will be encountered during an investigation, some more predictable than others, requiring legal advice. It is not uncommon for allegations to be raised by the target regarding the conduct of the victim organization. In searching for evidence you could encounter locked desks and cabinets within the control of targeted employees. Can you access the locked areas, or is there an expectation of privacy? The target may need to be placed on administrative leave. A whole host of legal issues may need to be contemplated, and having counsel engaged and available to provide direction and advice will preserve the integrity of the investigation.

''Is the human resource department involved in this matter at this point in time?'' Tim indicated the human resource director was informed of the matter earlier in the day, and that she would be available as needed all weekend as well to discuss how to deal with the matter.

LEARNING POINT

Equally important to counsel is the involvement of any human resources personnel within the victim organization. In smaller companies and organizations, no such resources typically exist, and a client would be wise to have counsel cover these areas of concern as well.

Targets of investigations should be subject to employment policies and procedures of the victim organization. Hopefully, formal documents in the form of employment handbooks exist and were issued to the employees, with signed acknowledgments obtained, evidencing the target's receipt of the policies. However, informal memos and e-mails may be the only form of documented policies in less sophisticated organizations. Employment policies often come into play in every investigation. Were employees put on notice that their e-mails, Internet activity, and all other electronic activity would be monitored and reviewed? What about defining appropriate versus inappropriate use of their computers? How about their phone usage and monitoring for personal use of company resources? Any mention of employees' expectation of privacy with their workspace areas? How about return of

(*Continued*)

(*Continued*)
company materials, property, computers, keys, and proprietary information upon termination of employment?

Targets of inquiries and fraud investigations are often placed on paid administrative leave pending the outcome of the investigation. This should be done to preserve both the integrity of the individual as well as the integrity of the investigation. Who will talk with the employee and place her on paid leave? How will the measure be documented in the employee's file? What happens when sufficient information and evidence is collected to terminate the individual's employment? Who is best to handle all aspects and requirements of termination, other than human resource personnel?

Most interesting is that many targets of a fraud investigation fire back allegations and counterclaims at the victim organization, forcing the organization to assume a defensive posture while on the offense of pursuing the original claim against the target. Claims of harassment, hostile workplace environment, and wrongful termination are common, regardless of the fact that the target may have stolen a significant amount of money from her employer. Individuals will also battle for unemployment benefits and funding of their retirement accounts even after admitting they stole money or assets from the organization. It is best to anticipate these issues and have the resources (counsel and human resources) on board as part of the investigative team to timely respond to any of these types of claims.

''What do you want to see happen, and on what timeframe are we dealing?'' Tim stated he wanted first and foremost to ensure that any evidence supporting or negating the allegations is preserved, to minimize the need to solicit replacement information from third parties at the high costs banks and other financial institutions were charging. His timeframe was as soon as possible.

LEARNING POINT

Matters can be investigated in different ways, applying different strategies, and procedures can be modified and performed based on the desired goals or desired outcomes of the stakeholders, or victims. It is important to have an initial discussion at the onset of an investigation into a potential fraud matter identifying different investigative options. Criminal prosecution may be

(*Continued*)

desired from inception, or may be left for later discussions based on the evidence identified. Yet in other matters, criminal prosecution will be taken off the table and not desired. Restitution may be the biggest desired goal, but strategies and efforts to accomplish that goal may be hindered by the victim's desire to keep the matter out of the public eye. Access to information will become an issue as subpoenas and search warrants will not be options for collecting much-needed evidence. Knowing what the victim may be considering in the form of desired outcomes if in fact the fraud allegations are substantiated will help identify how the matter will be investigated, and the means and measures that will be available.

Equally important is managing a client's expectations. Fraud investigations take time, and educating a client up front that these matters are not resolved and adjudicated in weeks or months will help set the client's expectations from inception. Information requests could take weeks, and when received, often prove incomplete, leading to further subpoenas and court hearings. I always tell clients that a typical case could take three to six months to fully understand and investigate, and that no case is ''typical.''

The sense of urgency should be placed on two initial areas: preserving critical potential evidence and securing assets, bank accounts, investments, and other means for restitution. Once both of these areas have been addressed in a timely fashion, there is time to perform a thorough and objective investigation of the facts to form a conclusion based on the procedures performed and evidence collected.

• • •

I told Tim I would be available any time during the weekend, and thought it would be best to assemble a meeting with the executive director, human resource director, and outside counsel to discuss the matter and identify a strategy on how to resolve the allegations. Tim said he would call the other individuals and would target having a meeting Sunday afternoon, with the goal to identify a plan to be executed Monday morning. He thanked me for being available to support him on the matter.

I waited in anticipation for a call from Tim the rest of Friday night and Saturday morning, knowing he wasn't the type who was going to sleep or rest himself until the meeting was established and things were in motion.

Just before noon Saturday morning, as I packed our gloves, baseballs, and bats into my trunk to head to the park for some family baseball practice, my cell phone rang. I knew before I reached it that it was going to be Tim calling me. I was right. Tim indicated he had reached the others, and that with all their schedule conflicts throughout the weekend, the earliest we could meet was Monday morning at his office. I told Tim I would be there bright and early, ready to act as needed based on the outcome of the meeting. I told him to try to enjoy the rest of his weekend, knowing he probably wouldn't, and to call me anytime if anything changed.