Kumar P. Setty, BS, MS, MBA

Several months ago I received a phone call from my old college roommate Ricardo (not actual name). I was happy to hear from my friend. When I asked him how things were going, he mentioned that he was working very hard but he didn't seem to be reaping the harvest of his labors. As an auditor who has worked on many fraud cases, I immediately became suspicious and I asked my friend if he had been a victim of a potential fraud. Ricardo then indicated that he had some misgivings regarding his office manager, Julie (not actual name). Julie, a single mom with an 8-year-old son, worked as an office manager for Ricardo's dental practice. Julie's husband had passed away several years before she had obtained her job. She had lupus, which was a long-term health issue for her. The medications for Julie's condition were partially covered by her insurance policy so she accrued large and frequent out-of-pocket expenses. These expensive medications were required to stabilize her symptoms. Since Julie was young, she would have to continue her purchases of the expensive medications for treating her condition.

After a month, Ricardo then recounted the following story in a phone conversation: *I met Julie during an interview for a position as a receptionist. She seemed ideal for the position. She worked for me for about a year until I had to hire an office manager. She knew what she was doing, she seemed diligent and she also had a talent for understanding the operations necessary for running my dental practice. I offered her the position and she accepted my offer. I placed a tremendous amount of trust in her and I delegated to her the task of examining and processing insurance payments on a daily basis. She had full access to the computer, mailbox and office suite. I have a small operation, so it wasn't feasible to spread the duties among additional staff. In retrospect I should have handled the key duties that involved accounts receivable and payables.*

Another year had passed and I was wondering why my office didn't seem like it was growing, yet I was working very hard. I noticed small things like insurance claims that were closed without payment, and a lack of organization in the accounting. I asked Julie a couple of times about the sloppy accounting and lack of practice growth. She told me that because many patients had switched insurance providers, she had to close claims from the previous insurers to bill the patients. I asked her for the records of the billings and she told me no one had told her how to do it and didn't think to record the billings. Basically she supposedly sent the patients a bill and left the amount as unpaid on the accounts. I got upset that the accounts were a mess, but I didn't suspect that she was stealing.

Several months later I got the gnawing feeling that something was not right. I confronted her and asked for an explanation. She denied any wrongdoing and said that no one showed her how she was supposed to account for the payments and receivables. This was not true. I let it go for some time. I waited for a day when no one was in the office and I called a sample of the insurance providers in the patient accounts with closed claims that had no payments attached. I asked for cancelled checks and found out that a lot of the checks didn't have my rubber stamp on the back, but had a handwritten account number.

I contacted that bank where the checks were being deposited, but was told that no information would be given about the accounts without a request from the police. I then confronted her again with the evidence and she finally broke down and admitted to the theft. I let her continue her explanation and she stated that she was undergoing severe financial hardship, lack of family support, medical expenses, and that she was doing it for her son.

What Causes Employees to be Fraudulent?

Most frauds are the result of several factors that can be illustrated by the Fraud Triangle (a trademarked term from American Institute of Certified Fraud Examiners). At each of the vertices of the Fraud Triangle, there are 3 factors: pressure, opportunity, and rationalization. In this particular case, there were several "pressures" that were compelling Julie to commit the fraud. The first pressure was Julie's health condition and the resulting prescription expenses accrued along with other treatments. Other pressures were that she was a widowed mother and that her salary as an office manager most likely could not cover her medical expenses, her parental obligations, and her lifestyle.

Julie's "opportunity" presented itself when she noticed the volume of insurance claims being

processed. Upon seeing the cash flows she must have been tempted enough to consider how these payments could be diverted to her for her financial benefit. Since Julie had physical access to the office suite, had primary access to the incoming and outgoing mail, and was responsible for the entire claims process, she had ample opportunity to divert funds from the insurance company to her personal account. Since there were no checks or reconciliations performed by the owner, Julie was able to cover her tracks.

Julie's "rationalization" was rooted in the fact that she was undergoing financial hardship due to a long-term medical condition, she is a widowed mother, and her salary was not enough to meet her obligations. Rationalizations present themselves in varying degrees and varying forms. She may have thought that she was "borrowing" the payments meant for the owner and that she would defer repayment of the funds to a future date.

The simplified process for any medical practice is as follows:

1. The patient's ability to pay for a medical service is confirmed by the medical professional staff.
2. The patient receives a service from the medical professional.
3. The medical staff then compiles the information regarding the service to the insurance company and then requests commensurate payment or adjustments to the requested claim.
4. The insurance company submits a check payable to the medical practice.
5. The medical staff member or office manager deposits the checks from the insurance company into the receivables account for the medical practice.

In this particular case, Julie had total control of the entire process along with physical access to the office, logical access to records, payments and authority over bank accounts. Essentially, committing this fraud was a "slam dunk" for her. Julie simply waited for the checks to arrive by mail from the insurance company and she deposited the funds into her personal bank account. In many cases, banks typically do not care about the "payable to" field on the check. They will accept any endorsed check for deposit as long as the funds are available from the payer (the insurance company). Most banks leave it to the responsibility of the account owner to perform their own bank reconciliation and to follow up on any inconsistencies. Banks just want deposits. They don't argue about who gets the payment or who pays. Julie was able to cover her tracks by feigning a lack of knowledge of simple bookkeeping. Since Ricardo did not have time to go through the weekly deposits, this fraud persisted.

Ricardo finally checked with the insurance company and received the cancelled checks. He noticed that the checks were not endorsed by his business, but by Julie for deposit into her personal account.

Fraud's Red Flags

One common red flag for this type of fraud is if Julie never took a vacation. Many times, perpetrators of fraud do not want to take any vacation because they fear being discovered and they also fear missing out on the opportunity to abscond funds by not being present in the office. Other red flags include: adverse credit history, living beyond one's means, gambling, and health issues.

Steps to Prevent Embezzlement

In this particular case, when there are staffing constraints, it is difficult to hire additional staff members to perform periodic checks. In this particular case, it is incumbent on the owner of the business to take the additional step to perform weekly or monthly bank reconciliations where individual claims are matched to payments from the insurance company and deposits on the bank statement. If it is practical to do so, it may be feasible to institute electronic funds transfer (EFT) so that the insurance company can wire or electronically transfer funds to the payee or owner (Ricardo). Another alternative is to set up a bank lockbox so that payments (manual checks or EFT) are sent to the lockbox and are immediately deposited by a third-party into the bank account. The matching process of the claim and deposit should still be performed to ensure that all checks are received and deposited, and that the bank has recognized and confirmed all deposits.

As an alternative, it might be feasible to have 2 people trained in the payments process so that they could each take turns receiving and depositing checks. Although it is difficult to detect collusion among staff members, sharing duties makes any deviations easier to detect and this practice provides as a balance of power.

The bottom line is that there must be a system wherein critical processes are segregated as much as possible and then all payments must be verified by an additional, trusted party.

In tough economic times it is important to implement oversight processes to ensure that embezzlement is prevented or at least detected within a reasonable period of time. It is also important to understand the common drivers and motivations that would lead an employee to commit theft. Despite the fact that it is difficult to detect collusion among 2 or more employees,

the proper checks can empower a business owner to detect suspicious activities.

In situations where hiring constraints are common, a business owner can still institute processes to detect and prevent embezzlement. With a small investment in technology many of the oversight processes can be automated.

Screening potential employees is an important step in preventing the hiring of potential embezzlers. Screening criteria may include checking credit history, criminal background check, drug testing and obviously checking references from previous employers. Screening, however stringent the process may be, will not prevent a person from deciding to try fraud for the first time. In order to implement a sound system for detection of embezzlement or fraud, it is important to emphasize effort on designing an effective process to prevent fraud.

Closing Comments

It is impossible to design a foolproof method for preventing an employee from stealing from your business, but it is possible to greatly reduce the possibility of being subjected to a fraud. A combination of preventive and detective controls represents a key feature of an effective anti-fraud strategy.

Mr. Setty holds a BS in Chemical Engineering from University of Rochester (NY); a MS in Software Engineering from the Carnegie Mellon University (Pittsburgh, Pa); and a MBA from University of Illinois. He is a certified information systems auditor and oversight knowledge developer (Oversight Anti-Fraud Software), and is an active member of Mensa. With more than 10 years of experience in the areas of auditing, computer security, and fraud analysis and detection, Mr. Setty is currently employed as an Audit Manager for a consumer packaged goods company in Chicago, Ill, where he focuses on computer security, financial auditing, and fraud prevention. He also worked as a consultant for many small to large companies performing Sarbanes-Oxley compliance, auditing, fraud detection and prevention, and computer security reviews for a variety of industries. He can be reached at (312) 593-8846 or vpsetty@gmail.com
.