Avoiding Embezzlement Embarrassment Or Worse

By Ralph Q. Summerford, CFE, CPA, CVA,
and Robin E. Taylor, CFE, CPA/ABV, CVA, CBA

An entity can lose twice in an embezzlement case. Consider these 10 actions to avoid even more revenue loss during the fraud examination and litigation.

Joe Mancha, an independent CPA, determined that deposits into the bank account of Shelby Building Supply were shorted by $285,000. He wrote a report stating the company's controller, Julie Mays, was responsible for the loss.1 The owner of Shelby Building Supply, Max Aiken, filed a proof of loss with the insurance company and recovered the policy limits of $25,000 - the maximum allowed under the policy. But Max also wanted a "pound of flesh" because he knew Julie had gambled all the money away and he would not be able to collect the loss.

Max turned the matter over to the local district attorney who took the case to the grand jury, which promptly returned an indictment. During the trial, with no more evidence than Joe Mancha's schedule and Max's testimony at trial, the jury only took 10 minutes to return an acquittal against Julie. And now there was big money at stake - Julie filed a defamation suit against Shelby Building Supply, Max, and Joe, in which she claimed - among other things - mental anguish and damage to her reputation. She asked for $1 million in damages. Julie's husband also filed a suit against the men and the company and claimed damages from "loss of consortium." He only wanted $300,000. The employer (along with its owner and accountant) were faced with double jeopardy - they were about to lose twice.

When an employee embezzles, the employer loses on several levels. Not only has the entity suffered a financial loss, but there is a loss of trust. To make matters worse, the way the case is handled can determine if there will be an additional loss of revenue when it is litigated. Here we will review what I consider 10 of the most important considerations in an embezzlement fraud examination that may keep save an entity from more than embarrassment.

Top-ranked Financial Crime

According to Safechecks (www.safechecks.com), embezzlement has been the top-ranked financial crime for more than 30 years. Recent studies indicate that employee embezzlement accounts for the majority of employer losses through employee fraud. The size of the losses is staggering. In a 2003 global PricewaterhouseCoopers survey, the respondents' average loss per entity for asset misappropriation in a two-year time period was US$1,388,731.2 The U.S. Chamber of Commerce estimates the annual cost of employee theft alone at more than $40 billion in the United States. Embezzlements can occur in entities of any size and sophistication. Elaborate systems of internal control are often installed. Even those systems can be ineffective when an employee is in collusion with another employee or an outside vendor.
The fraud examiner can do much to maximize the potential for a happier ending through properly structuring the investigation. These 10 considerations are not necessarily listed in order of timing or importance. All of them are important and the timing of many considerations will overlap. Obviously,

because each embezzlement assignment is unique, you will emphasize some points over others and you will add considerations not on this list.

No. 1. Contact the Insurer
The employer's insurance company should be contacted immediately. The fidelity or employee theft premiums may have been paid, but many employers fail to actually read the policies. Failure to put the insurer on notice of a potential loss can void the coverage in some cases. Most policies I have seen have a 30- to 60-day notice provision. Although a proof of claim is not required to be filed until months after the notification, the failure to notify the insurance company when the insured could reasonably have expected there may be a loss can void the coverage. Also, many policies will pay for the investigation or at least a portion. Fraud probably is an unusual event for the entity's management so it will have little experience and will need guidance. The episode will be highly emotional so it is very easy for them to overlook basic steps.

I examined a case in which a trusted employee stole from the entity and was later caught but after restitution was placed back in her same position of authority. The entity never informed the insurer and legal authorities and so unknowingly violated the employee theft provisions of its insurance policy. When the employee later slipped back into her old ways and stole again, there was no insurance coverage for the crime even though all premiums had been paid because the provisions of the policy requiring notification clearly had been violated.

Also, consider the statute of limitations. Being a day late in a civil matter can mean no recovery.

No. 2 Contact Legal Counsel
The employer should be urged to immediately contact competent legal counsel to discuss the situation. This is not a place for self-diagnosis or amateur lawyering. An attorney who handles general corporate matters is not the person to handle this situation. The best bet is someone who has practiced in this area with experience either as a prosecutor or in a district attorney's office. By mishandling an embezzlement case, many entities find that they can lose twice: the employee has stolen but his or her rights were violated during the process of the investigation. The second loss can be more painful than the first especially if the entity has to write a check to the supposed "victim" and cannot fully recover the fraudster's ill-gotten gains.

No. 3 Deal with 'Alleged' Perpetrator
Once an employee is suspected of embezzlement or even caught, at least three courses of action are possible:

- terminate the employee immediately;
- place the employee on administrative leave with or without pay; or
- do not confront the employee until evidence is developed.

Management (especially owners) will usually prefer to terminate immediately. If the assumption is wrong about the perpetrator, the entity can easily be facing a suit for wrongful dismissal, slander and/or libel. I prefer to get the investigation underway and discover evidence of sufficient predication before termination. Additionally, under common law, employees have a duty to cooperate with employers in a legitimate investigation. If the person is still employed there is a good chance you can actually get bank and tax records from the perpetrator to prove the fraud. The circumstantial evidence can go a long way in proving a case and gives the fraud examiner the best chance to remain in contact with the perpetrator and uncover the full fraud scheme or schemes.

The entity's policies or contracts should dictate if it places the employee on leave, which it should do

only after sufficient predication exists for a fraud examination.

I always want the employee available because we may uncover fraud faster through interviews than forensic examination of boxes of documents. Sometimes during the course of an interview the suspect implicates other employees on other past frauds.

Try to avoid exposing the employer to defamation claims. Was this really embezzlement? Was a crime really committed? Incompetence can often appear to be criminal. Avoid jumping to conclusions but criminals can often hide behind cloaks of incompetence and they often wear their outer garments so well!
The entity should not prematurely disclose information to the wrong parties. This is especially damaging when it does not know the full extent of the fraud and the number of perpetrators.

No. 4 Prepare Action Plan
Here is a dangerous mistake: jumping into an assignment with little or no planning. An embezzlement fraud examination can be complex so organized documentation is necessary. A proper plan does the following:

- maximizes efficiency;
- ensures that you do not overlook important steps of the investigation;
- documents compliance with professional standards regarding planning, supervision and due professional care;
- speeds completion of the written report at the close of the investigation;
- allows the fraud examiner to recall pertinent details of the work at a later date. (The actual testifying may occur several years later. "I'm sorry, I can't recall" is not the answer you want to provide in court.); and
- allows greater efficiency on future assignments as a reminder of what works and what does not.
  The approach to an embezzlement case is to follow the steps in a typical fraud investigation - examine documents and then interview:
- neutral, third-party witnesses;
- corroborative witnesses;
- co-conspirators; and
- the suspect.

You can conduct most of the document examination covertly without placing everyone (including the suspect) on notice. Reviewing the documents can produce fruitful evidence of the crime, which you can use during interviews to guide the examination.

The timing and order of the interviews are crucial. Once you start interviewing, everyone knows the examination has begun. Talk first with managers who may be directly affected by the loss or those that may be useful in the investigation. Tell them that they should not disclose any of the information that you have to tell them.

If you have not identified the suspected perpetrator, you will need to cast a wider net and bring in all individuals who may have had the opportunities and access to commit the fraud, which will provide documentation that you did not single anyone out for discriminatory scrutiny.

No. 5 Act Quickly
Direct observation rarely catches employee theft. Usually a tip or specialized audit procedure uncovers embezzlement. The perpetrator's scheme or schemes likely have been ongoing. The financial impact may be material and will probably be greater than first suspected. The employer must move quickly

to stop the damage.

No. 6 Know Employer's Rights and Responsibilities
The employer has a right to conduct a fraud examination and a responsibility to stockholders to investigate and seek to recover losses by theft. The complex series of laws dealing with employee rights in the workplace does not necessarily have to hamper the examination. The rules must simply be followed. (See the next section.) However, the employer must treat all employees consistently. An inconsistent track record can later be used against the employer.

No. 7 Know Employee's Rights and Responsibilities
Read the employee handbook. It may outline the employee's rights in such situations and his or her responsibilities. Generally, an employee has a fiduciary duty to comply with the employer's investigation of their possible fraudulent acts. Failure to do so can lead to termination of employment.

A U.S. employee has certain rights to privacy, which may be open to interpretation and state law regardless of a company policy. They also have rights under the provisions of the Employee Polygraph Protection Act and the Fair Credit Reporting Act, among others. Ask an attorney for details. (For the latest on European Union employee and employers rights legislation visit http://europa.ev.int/index_en.htm.)

Also, U.S. employees have constitutional rights and the right to sue their employers under certain circumstances. The Fourth Amendment to the U.S. Constitution prohibits unreasonable searches and seizures. The Fifth Amendment provides that a person cannot be compelled to give information that might incriminate him. The Sixth Amendment provides that a person has the right to an attorney and to confront the witnesses against him.

The gerenal rule is that the U.S. Constitution does not limit the powers of private employers in conducting a corporate investigation. However, that rule is subject to several limitations. Although a private employer usually cannot be sued for a violation of the Fourth, Fifth, or Sixth Amendments, these provisions still have important implications for the fraud examiner. Some form of "(U.S.) state action" must be involved when an employee sues and employer for the violation of a constitutional right. (State action is involved during any investigation by a state or federal entity, including investigations of their own employees.) There are no rules regarding when an investigation can be considered to involve U.S. state action. However, the following examples could be considered to involve state action:

- investigations conducted by a private company but at the suggestion of the state or federal authorities;
- investigations begun by a private company that later are taken over by or expanded by state or federal authorities;
- joint investigations with or aided by state or federal authorities;
- investigations conducted by a private company that are required by state or federal law; or
- searches or interrogations conducted by outside investigators who are off-duty state, local, or federal authorities.

If a private entity conducts an examination in accordance with U.S. federal laws, the entity's internal investigation may or may not be considered state action.

For example, in the case of Skinner v. Railway Labor Executives Ass'n, 489 U.S. 602 (1989), the U.S. Supreme Court found that a private railroad acted as an agent for the government when it complied with the provisions of the Federal Railroad Administration Act in administering drug tests to its employees. Under the regulation at issue, the railroad was required by law to conduct the test and the

Federal Railroad Administration was authorized to receive the test results.

If a company is conducting an investigation pursuant to such federal laws as the Securities Exchange Act of 1934 or the Foreign Corrupt Practices Act of 1977, the company should be aware of the possible implications of state action. Therefore, obtain legal advice before taking any adverse action against an employee.

No. 8 Secure Data

The employer must take immediate steps to preserve data. Fraud deals with issues of "intent" and proving intent is generally through circumstantial evidence. Evidence that goes to the issue of intent must be gathered and preserved.

Data to be secured includes anything that the employee touched in his or her role at the organization. Steps may include the following:

- Mirror the hard drives of the computer used by the employee at the office or plant preferably without the employee's knowledge. This will provide a complete snapshot of the data on the drive and allow it to be reviewed at a later date without destroying the integrity of the underlying data.
- Mirror copies of the hard drive server in the entity's network.
- Secure copies of all electronic backups in the network and local drives.
- Secure original data, including printed copies of ledgers and subsidiary journals, vendor invoices, bank statement and contents, etc. All documents should be cataloged. Electronic data is great but ultimately it is just a tool to lead us to the original source documents. The original documents must be protected.
- Secure floppy diskettes that the employee may use to keep selected data off hard drives.
- Search the employee's desk and office. This is the entity's property that the employer legally can search at any time. Even though many employee handbooks communicate that employer right, be sure to review your plans with the entity's attorney.
- Once an employee is notified that he or she is the subject of the investigation, the employee should not be allowed to touch computers or remove anything other than personal items from the office. The employee should be accompanied while in the office and walked from the premises. The timing of such notification is a separate issue.

Do not overlook the employee's home computer. Even if it is owned by the entity, you may be able to gain legal access to the computer if you suspect it contains entity information and software. The employee may have been able to remotely dial from his or her office to this home computer so coordinate cutting off access to both computers. Disconnect all access to all computers from the employee's office as well as any access the employee may have from a remote site. Also, be sure to obtain the employee's passwords and modify them so they cannot be reused. Because the employee may know the passwords of others in the organization, it is a better idea to have everyone change their passwords to prevent the unauthorized access or destruction of computer.

Once you secure the data, you have access to the employee's files including all current emails and deleted messages, which can be brought back to life with data recovery software. Some embezzlement frauds become so complex (such as lapping and kiting schemes) that a fraudster needs a separate computer file to organize the scheme. A skillful technician can break a protective password on the file.

No. 9 Perform Background Check of Suspect

Background and credit checks allow the identification of "need" and "greed" as possible motivations for the fraudster. Still, provisions of the U.S. Fair Credit Reporting Act usually require notifying the employee that the check is being made. We usually notify all employees in a department or group

that we may be performing checks and we also advise them they have a right to receive copies.

No. 10 Remember Iceberg Principle
Fraud is like an iceberg. What is seen may only be a small part of the whole. Many others may have been involved in the fraud scheme. Often, the toughest frauds to detect are those involving collusion with others within or outside the entity. For example, a common embezzlement scheme involves the use of fictitious vendors or consultants. Any employee with the authority to approve payment of an invoice can perpetrate such a scheme.

Admitted fraud likely follows the 10 percent rule: A fraudster's first admission is only a small part of the whole story. The true fraud (the other 90 percent) may be greater, broader, and longer than you originally envisioned.

Preventing Embezzlements
Here are some ways to help prevent entity embezzlements:

- Review hiring policies to keep people of questionable background from making it to the payroll.
- Restrict access to employee master files to prevent "ghost employees" and improper pay rates.
- Restrict access to vendor master files with strict procedures for additions and modifications.
- Separate the cash/banking function from the accounts receivable function.
- Protect all check stock and destroy obsolete stock.
- Mail vendor checks. Do not return them to the operating units that requested the payments.
- Reconcile bank accounts on a timely basis. Parties issuing the checks and handling deposits should not be allowed to perform the reconciliations.
- Rotate personnel or functions in critical financial areas on a regular basis.

A Delicate Balance
An effective embezzlement investigation requires the interplay of several diverse elements. There must be a balance between the rights and responsibilities of both the employer and the employee. The days of effective do-it-yourself legal representation and fraud investigations are over for employers. CFEs can help employers keep their equilibrium and avoid even more revenue loss during the case's examination and litigation.

Ralph Q. Summerford, CFE, CPA, CVA, *is president of Summerford Accountancy, P.C., a litigation support firm in Birmingham, Ala., that specializes in fraud examinations and forensic accounting. His email address is: ralph@summerfordcpa.com.* ***Robin E. Taylor, CFE, CPA/ABA, CVA, CBA****, is a partner in the Birmingham, Ala., office of Dixon Odom PLLC. He specializes in business valuation and forensic accounting. His email address is: rtaylor@dixonodom.com.*

1 The facts of this case are true, but the names have been changed to protect the guilty and the innocent.
2 PricewaterhouseCoopers in association with Wilmer, Cutler & Pickering, www.pwcglobal.com/extweb/ncsurvres.nsf/docid/65EC95F223DCDAD785256D4D004ECD3E

Anatomy of Embezzlement
According to Joseph T. Wells, CFE, CPA, in his book "Occupational Fraud and Abuse," embezzlement is a special type of fraud: an employee not only steals the assets but that person also violates a fiduciary duty to hold the assets for another where there is trust or a high degree of good faith. Black's Law Dictionary says, "To 'embezzle' means willfully to take, or convert to one's own use, another's money or property of which the wrongdoer acquired possession lawfully, by reason of some office or employment or position of trust. The elements of 'embezzlement' are that there must be a

relationship such as that of employment or agency between the owner of the money and the defendant, the money alluded to have been embezzled must have come into the possession of defendant by virtue of that relationship and there must be an intentional and fraudulent appropriation or conversion of the money."

The key here is the money came into possession of the wrongdoer by reason of employment or position of trust. The fraudster will be someone who is in a position of trust, often the long-term and seemingly loyal employee. Unfortunately, this injects the added issues of emotion and a sense of betrayal into the theft. Combine this with other elements spinning off the classic fraud triangle and the story of the crime takes on the elements of a classic mystery novel.
Those other elements can include:

- need or greed: unusual financial strains or other less supportable motivations create the mindset to steal;
- revenge: employees feel wronged, and see employers as unjust, corrupt or discriminatory;
- thrill seeking: taking the opportunities, employees steal because they can;
- denial: some employees rationalize their thefts as temporary loans or as entitlements based on past under-compensation; and
- addiction: dishonest employees often continue to steal until they are caught.
