# FRAUD AND EMBEZZLEMENT

Frank Sommerville, JD, CPA
fsommerville@nonprofitattorney.com

## I. THE SCOPE OF THE PROBLEM

According to the US Chamber of Commerce, up to 30% of all workers will steal from their employers at some point in their career. Further, 75% of the time the theft will go unnoticed.

According to the Association of Certified Fraud Examiners (www.acfe.com), 12.2% of the thefts occur in the not-for-profit sector, with the average nonprofit loss of $120,000 per incident. Billing schemes are the most frequent form of fraud, and nonprofit organizations account for 46.6% of all cases. Just under half of all the frauds occurred in organizations with less than 100 employees.

## II. RED FLAGS

Here are the most commonly recognized red flags of theft or embezzlement:

A. Unusual drop in revenues

B. Unusual increase in expenses

C. Disorganized records

D. Missing documents

E. Duplicate payments to vendors

F. Employee re-writing records for the sake of neatness

G. Employee working excessive overtime

H. Employee refusing to take vacations

I. Employee refuses a promotion

## III. COMMON TECHNIQUES

A. Billing Schemes -- The employee sets up a fictitious vendor and writes checks to that vendor. The employee then endorses the check and cashes it.

B. Checks Payable to Cash -- The employee records the check as being payable to a known vendor, but really makes the check payable to cash. The employee then cashes the check.

C. Pays Personal Debts -- The employee pays a vendor for their personal obligations. For example, the employee uses the same telephone company as the employer. The employee pays both bills with a check from the employer.

D. Employer Credit Cards -- The employee charges personal items to the employer credit card. The vendors may appear to be usual and customary for the employer.

E. Skimming -- The employee takes cash from offering plates and pockets the money. Another form of skimming occurs when the employee asks the member to pay him or her directly for a particular item. Sometimes the employee will record a discount for a particular item and only deposit the discounted amount while retaining the discount for themselves. Skimming occurs in about 25% of cases.

F. Fictitious Employees -- The employee adds a new person to the payroll, but cashes the new employee's paychecks.

## IV. PREVENTION

To prevent employee theft, one must understand the Fraud Triangle. These three factors appear in virtually all cases and were first identified by Joseph T. Wells, founder of the Association of Certified Fraud Examiners. Prevention techniques need to deal with all three factors. First, internal controls are lacking providing the opportunity for the employee to carry out their theft. Second, pressure exists on the employee to misappropriate cash. Frequently, these pressures are external from the employer. Excessive indebtedness or keeping up with the Joneses are frequent pressures that are present in employee theft cases. Third, the employee possesses a frame of mind that allows them to intentionally misappropriate the cash and justify their dishonest actions (rationalization).

Identifying potential embezzlers is relatively easy. They are always the person that everyone would least expect to steal from them. Most embezzlers are trusted employees and operate above suspicion. Typically, they are long time employees within whom their supervisors have a very high level of trust.

A. Opportunity -- The employee knows that they are not accountable to anyone for their actions. Prevention demands that all employees be accountable for all of their actions. Accountability looks like this:

1. Require two signatures on each check and do not pre-sign any checks.

2. Make sure the employee who writes checks or makes deposits does not open or balance the bank statements. I suggest that bank statements be mailed to an off-site Board member for opening and review.

3. All credit card statements should be reviewed and approved by a Board member or senior management who does not have a credit card.

4. Require Board member or senior management approval to add a vendor or employee to the accounting system. A report of added vendors or employees should be sent to the treasurer monthly.

5. Require all employees to take at least a one week vacation every year.

6. Smaller organizations can use a web based accounting system that is accessible by the treasurer and outside CPA firm at all times.

7. Adopt a whistleblower policy.

8. Have at least two offering counters at all times and rotate count teams every week.

9. Deposit the offering as soon as possible after receipt into a 24 hour deposit slot at your bank.

B. Pressure -- The employee feels the need for more money. To become aware of potential sources of pressure, the employer should:

1. Observe the lifestyle of their employees by reviewing the types of cars being driven and types of trips being taken.

2. Develop and maintain relationships with the employees so that you become aware of what is occurring in their personal lives.

3. Be aware that frequent trips to gambling centers by relatively low paid employees create pressure.

4. Be aware of employees that are living above their means.

5. Be aware that pressure increases when children are starting college.

6. Be aware that pressure increases when siblings or spouses are more financially successful than themselves.

C. Ethics -- Most embezzlers rationalize their theft. Frequently, they think that they will repay the money once their circumstances change. Sometimes, they justify the thefts by claiming that they are under compensated for the job that they are performing. In other words, the nonprofit owes them the money and they are simply fairly compensating themselves. To prevent ethical issues:

1. At the least annually have a discussion with employees regarding high ethical standards.

2. Set a good example and follow the highest possible ethical standards.

3. Stress business ethics in every day transactions.

4. Adopt a code of ethics and follow it.

## V. WHAT TO DO WHEN YOU DISCOVER A POTENTIAL ISSUE

A. Call your attorney. You will need to discuss the options available to the church. The attorney will likely be part of the team created to investigate. He/She will help you determine whether to terminate or suspend the suspect. They will guide you regarding the fiduciary responsibilities of those in charge to prevent such embezzlement. They will also will assist the congregation in determining when to bring in law enforcement.

B. Consider engaging a Certified Fraud Examiner ("CFE") to investigate the charges and document the losses. You can find a CFE at http://nf.acfe.com/eweb/dynamicpage.aspx?site=ACFEWEB&webcode=CFEDirectory.

C. Do not confront or otherwise tip of the suspect. If they believe that you have caught them they will likely destroy key evidence of their embezzlement. There will be a time to confront them but it will be after you have gathered all the evidence and have changed their passwords so that they cannot destroy their tracks.

D. Do not discuss publicly. Please be aware that the church can be sued for defamation or invasion of privacy for even making the accusation outside a privileged context. This can only be discussed in a formal called meeting with your Board or in conversations with the congregation's attorney.

E. In most cases, it will be in the best interest of the congregation to bring criminal charges against the individual. The congregation should not be deterred in bringing charges because the individual is repentant or even offering to pay back the amount stole. The only way to alert other employers of the risk is to bring the charges. Otherwise, the individual may go to another congregation and repeat the scheme.