

SECTION 1

Not-For-Profit Organizations: Four Consistent Areas of High Risk Embezzlement: Who Does It and When

Not-For-Profit Specific Issues

WHEN AUDITING CPAs audit an organization, they are required to have a good understanding of the nature of their client's business to enable them to evaluate risk factors that could lead to embezzlement and to suggest corrective action accordingly. Obviously, business environments vary according to the nature of the business, because the risks banks face are substantially different from the risks an automobile dealership faces.

Although auditing CPAs, internal auditors, and management should continually strive to reduce embezzlement risks of the not-for-profit organization as a whole, history has shown that a typical nonprofit has extremely high fraud risk in four specific areas, those being:

1. Checks *mailed* to the organization's offices from members, advertisers, and the like
2. Printing expenses
3. Postage expenses
4. Personnel-related expenses including wages, payroll taxes, and employee fringe benefits

This book will address these areas in greater detail in later chapters, but because of the high likelihood that a knowledgeable person could take advantage of weak internal controls in these four areas, it is important to understand why these areas are so susceptible to fraud and why basic corrective action must be taken.

2 Preventing Fraud in Nonprofit Organizations

Checks Mailed to the Organization:

Issue: Not-for-profit organizations in general are unique in that they are *widely known by their acronyms* by both their members and the public! For example, the American Medical Association is referred to as AMA, the National Rifle Association is called NRA, and so forth. The vast majority of nonprofits are known by their acronyms.

Risk: When members, advertisers, and the like remit payments to nonprofits, often the remittance check will be made payable simply to the organization's acronym rather than the full name of the entity.

What could an individual with access to checks do to perpetrate a fraud? Simply open an account in another bank using a clever variation of the legitimate organization's name, with the same acronym. For example, someone at the American Crayon Association (ACA), could open an account for the nonexistent Apple Collectors Association (another ACA) at another bank and easily divert checks payable to ACA to the second account.

Suggestion: 1. Utilize the bank's Lockbox Service whereby members and contributors are provided with remittance envelopes, and checks are mailed directly to and deposited by the organization's bank rather than mailed to the organization. This service effectively eliminates the risk associated with diverting checks made payable to an acronym because employees never come into contact with these checks.

Important—see "Lockbox" in Section 3 of this manual for an in-depth discussion of this service.

2. On invoices, dues billings, and the like, request checks be made to the full legal name of the organization rather than its acronym.

Printing Expenses:

Issue: In most not-for-profit organizations, the primary product is the printed word (magazines, newsletters, books, brochures, etc.) and printing expense is typically a substantial portion of the overall budget, and in that respect, susceptible to fraud.

Risk: Because printing is such a major portion of the budget, the organization must be vigilant in monitoring internal controls over printing, to avoid ghost printing vendors and collusion between printers and key staff.

Suggestion: Ensure the organization has thorough and continually updated Approved Vendor Files. These files should include detailed information such as legal entity name, remittance address, street address, contact name, federal identification number, emergency numbers, and so on. This information is vital to auditing CPAs and internal auditors when reviewing records.

Important—see “Ghosts on the Payroll and Ghost Vendors” in Section 4 of this manual for more in-depth discussion.

Postage Expenses:

Issue: As with printing expenses, not-for-profit organizations typically have a substantial budget for postage (and freight), because they would probably have, at a minimum:

- First class mail
- Business reply mail
- Bulk mail
- Media mail
- Second class mail
- Postal permits

Additionally, nonprofits often also do business with:

- Mail and fulfillment houses
- Commercial couriers such as UPS, FedEx, and the like

Once again, because of the high volume of mail that a typical not-for-profit experiences, the organization must be vigilant in ensuring that postage funds are not diverted.

It is a simple matter for knowledgeable persons to “sell” organization postage to another party, divert postage for their own use, prepare checks to nonexistent mail houses, open up accounts using clever variations of commercial couriers’ acronyms or names, and so forth.

Suggestion: It is imperative that postage expense be monitored very closely and routinely by auditing CPAs, internal auditors, key staff, and others.

Important—see the “Postage Issues” and “Ghosts on the Payroll and Ghost Vendors” in Section 4 of this manual for in-depth discussions and recommendations.

Personnel Expenses:

Issue: Risks associated with personnel-related expenses are obviously not unique to nonprofits, and all businesses have a high risk in this area. Why? Typically upper management rarely is aware of the detail

4 Preventing Fraud in Nonprofit Organizations

associated with processing payroll, calculating Social Security and Medicare, calculating federal and state income tax withholding, and other areas related to payroll.

When management is unaware of the detail associated with processing payroll, they are highly susceptible to payroll fraud.

- Suggestion:**
1. Always ensure that *two* employees are involved with processing payroll, and both employees sign the payroll detail attesting accuracy.
 2. Consider direct deposit of employee pay. Direct deposit requires bank account numbers, creating an audit trail.
 3. Have either the auditing CPA or internal auditor pay a surprise visit to the organization to check the accuracy of payroll, ensure there are no ghost employees, and so forth.

Important—refer to ghost employee and other personnel-related information in this handbook for greater in-depth discussion and recommendations.

Summary

Although there are obviously other areas of risk such as travel expenses and the like, it is clear that the four areas noted in this chapter are of paramount importance when evaluating the risk associated with a typical not-for-profit. Published operating ratio reports for nonprofits consistently report that if a nonprofit is victimized, there is a high likelihood that one of these areas is involved.

The Perpetrators: Who They Are, Why They Do It, and How They Are Caught

In the real world of embezzlement, the perpetrators rarely fit the stereotypical image of someone capable of concocting and carrying out fraud schemes. Rather, they are almost always someone *above suspicion!* The stories of internal theft being carried out by the innocent-appearing young man who sings in the choir or the older woman whom you can count on to remember everyone's birthday are actually the norm. Embezzlers are of any age, sex, race, religion, and income bracket.

Why? Despite the appearance of honesty, you can never be sure of what is going on in someone's personal life, and desperate people are capable of taking desperate action. For example, it is probable that you have no idea that a fellow employee may:

- Have a gambling issue
- Have an alcohol problem

- Have a substance abuse situation
- Be experiencing financial difficulties
- Have expensive medical bills
- Or—enjoy living life on the edge!

There are, however, a few profiles that warrant the attention of management:

Who They Are, Why They Do It

The Disgruntled Employee Employees who have been passed over for promotion, demoted, reprimanded, or been the subject of disciplinary action often feel they have a justifiable grievance against the organization. People in this situation often feel they have nothing to lose if they are caught in wrongdoing. Additionally, they often rationalize their actions and feel they are justifiably righting a perceived wrong, and they convince themselves they have done nothing wrong.

The Stressed-Out Employee People experiencing a personal crisis such as a divorce, serious illness, or death in the family often become desperate. It is worth repeating that desperate people often take desperate actions.

Employees Living above Their Means Employees living an extravagant lifestyle well above their income level are always suspicious. Money needed to fund this lifestyle had to come from somewhere!

The Employee Who Never Takes a Vacation It is unnatural and unhealthy for people never to take time off. Unfortunately, the reason for this behavior is often that they can't risk having someone else sit at their desk, look at their mail, or answer their telephone because they are hiding something.

Employees Who Are Unnaturally Compulsive about Their Job Responsibilities As in the case of the employee who never takes a vacation, employees who refuse to share their work with anyone, hide their work, or take work home could also be covering something.

Employees Experiencing Financial Difficulties People who can't meet their debts and are stretched too thin financially are always of concern. When this situation comes up, consider helping the individual by providing personal financial counseling.

Unfortunately, people sometimes find themselves in dire circumstances. Often this occurs through no fault of their own. There may be health issues, financial difficulties, layoffs, or elderly parents needing assistance. Always remember that desperate people will take desperate action.

Note: Occasionally check where people cash their paychecks. A bank or credit union is the typical place. If an employee owes money, you may see an endorsement

6 Preventing Fraud in Nonprofit Organizations

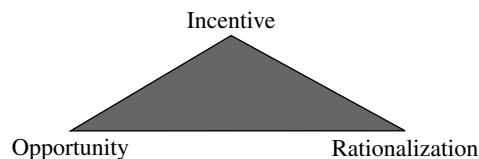
over to a private citizen. You may even see checks cashed at liquor stores, pool halls, bars, or other odd places. Or an employee may be using an expensive check-cashing service. Be alert. This may indicate an employee with problems. So a simple review of paycheck endorsements is imperative.

Employees Who Have Drug Problems People who become addicted to drugs will do almost anything to support their habit, obviously including stealing from their employer. The best way to approach this is to suggest counseling. This type of person should never, of course, be put in a position handling money, checks, and so forth.

The Employee with a Gambling Problem Most gamblers, of course, are responsible individuals, but people with a gambling problem, particularly illegal gambling through bookies, are a real danger. These people “borrow” money to place bets and intend to repay the “loan” with their winnings, which of course rarely happens. When these people get in over their heads, particularly with the criminal element, they find themselves in a desperate situation and, once again, desperate people will resort to desperate actions.

The Fraud Triangle

To preview the Fraud Triangle noted in “Statement of Auditing Standard No. 99”, Section 2 of this handbook:



Incentive: The scenarios described above are examples of the “Incentive,” the starting point for fraud.

Opportunity: Too much trust, poor internal controls, lack of supervision by supervisors, no financial audit by independent CPAs, and the like, all create opportunity for fraud. The basic purpose of effective internal controls is to remove the opportunity for fraud.

Rationalization: After a period of time, the perpetrator actually convinces himself that he is not stealing, but rather self-correcting a perceived wrong such as a pay discrepancy or the like.

How They Get Caught

Just as profiles of embezzlers surprise people, so does uncovering fraud.

Despite belief to the contrary, *most fraud is discovered by accident and due to unanticipated work interruptions*, and not during the course of a CPA's financial audit!

Here is how fraud is uncovered:

- During the course of a CPA's financial audit: 2%
- As the result of an internal audit: 18%
- By whistleblowers: 30%
- By pure luck: 50%

Let's break down each category:

CPA Financial Audit Despite belief to the contrary, it is actually unusual for an audit to uncover an embezzlement. Why? The perpetrator knows what the auditor does and does not look at, as well as what management does and does not look at. This combination, coupled with a weakness in internal controls, is the basis for the important "opportunity" portion of the Fraud Triangle. It is also important to reinforce the fact that auditors are not there to uncover fraud during the course of their audit, but rather to issue an opinion on whether or not the figures in the financial statement are presented fairly, even considering the provisions of SAS 99.

Internal Audits As you can see, the probability of uncovering fraud rises from just 2% due to a CPA's audit to 18% for an internal audit.

A good internal audit program is very effective if the procedures are followed during the period between the time that the auditors conclude field work for year 1 and return to start field work for year 2. See "The Embezzler's 'Window of Opportunity,'" later in this chapter.

Whistleblowers The probability of fraud being detected rises to an impressive 30% due to whistleblowers.

It is important to have a whistleblower program coupled with a whistleblower retaliation prohibition policy as part of any organization's administrative policies. These policies are actually a requirement of organizations subject to the Sarbanes-Oxley Act of 2002, but all organizations should give this serious consideration. (See "Whistleblowers," in Section 3 of this handbook.)

Luck Luck accounts for a whopping 50% of all reported fraud! That is correct—simply stumbling onto something or the thief's carelessness accounts for a full one-half of reported fraud!

The Finance Department

It's unfortunate, but it's a fact—*most* internal embezzlement schemes involve someone assigned to the accounting function. With that in mind, pay particular attention and be diligent when assessing a system of internal controls.

8 Preventing Fraud in Nonprofit Organizations

Think about some of the responsibilities individuals have in the typical accounting area:

- They receive the organization's checks and cash.
- They prepare the bank deposits.
- They take the deposits to the bank.
- They order checks.
- They prepare checks.
- They mail checks.
- They receive the bank statements.
- They prepare payroll.
- They prepare payroll tax deposits.
- They do the bank reconciliations.
- They prepare the financial statements.
- They prepare journal entries.
- They are the petty cash custodians.
- They prepare payroll tax returns.
- They have access to the safe.
- They activate loans and lines of credit.
- They are the sole custodians of the accounting records.
- They coordinate and arrange for payment for organization credit card transactions.
- They process credit card information from customers.
- They prepare W-2s and 1099s.
- They process credit card transactions for customers.
- They are the custodians of fixed asset records.
- They are the custodians of inventory records.
- They ultimately write off bad debts from accounts receivable.
- They record debt service transactions.
- They account for noncash expense such as depreciation and amortization.

Without effective internal controls, any of these responsibilities, in the hands of the wrong individual, could lead to a serious problem. This problem is compounded if the person the accountant reports to is not an accountant also.

When Do They Do It? In addition to the fact that embezzlers are often above suspicion, many fraud schemes have another similarity. The time of the embezzlement is very likely the same from case to case.

And, exactly, when is that? It's always during a very large "window of opportunity." And that window is most likely to be open *between the time the CPA has left the office after concluding the audit field work for the current year, and the time he or she is scheduled to come back to start the audit for the subsequent year.*

The window of opportunity is the time that the organization has to be the most vigilant. A smart thief is not going to pursue an embezzlement scam when the auditors are on-site or due to come in. In fact, this is the time when the thief will be squeaky clean.

The Embezzler's "Window of Opportunity"

Any accountant experienced in the area of fraud investigation or forensic accounting will emphasize the vital importance of taking thorough and copious notes of every important detail relating to the investigation. Why? Notes will be extremely important in the event that the matter goes to litigation, because it may be *years* before the matter goes to trial. Obviously, people move on to other firms, people retire, and there is an understandable memory lapse over time. If good notes are taken, others can proceed because detailed information is available.

Over time, an experienced fraud examiner will notice that similarities often exist when comparing the details of various fraud scenarios. Although this is certainly not an absolute, the vast majority of embezzlement schemes share the following:

- Weak internal controls
- Too much trust
- Poor management oversight
- Lack of a financial audit
- No background checks on key positions
- Lack of independent checks on bank statements and credit card statements
- Failure to take advantage of the bank's Positive Pay service
- Failure to take advantage of the bank's Lockbox service

Another striking consistency that has surfaced over time is *when* most of the embezzlements addressed in this book occurred, and this is *between the time the auditors conclude their field work for one year and return to start their field work for the subsequent year*. Obviously, the perpetrators of a scam, regardless of how clever, will in all likelihood put the fraudulent activity on hold while the auditors are physically in the office, as they want to give the impression to the auditors that they are squeaky clean. In other words, while the auditors are on-site, there will be no ghosts on the payroll, there will be no check tampering or switching, there will be no ghost vendors, and so on.

Something to Consider

Consider having the independent CPA pay a surprise visit to the client's offices on a day while the window is open, that being of course a business day during the window of opportunity for embezzlement.

10 Preventing Fraud in Nonprofit Organizations

The Surprise Visit

The auditors will select a day for the surprise visit at their discretion. For this surprise visit to be effective, consider the following:

1. With management's permission, of course, the auditors should have the client's bank send a cut-off bank statement directly to their offices, *not* to the client's office. This statement should include copies of the front and back of checks.
2. Have the client's credit card company send a cut-off statement to the accountant's office, as with the bank statement.
3. Transaction tests:

Purchases

Prior to the surprise visit, the accounting firm should send unknown "shoppers" to the establishment, as follows:

Cash: One of the shoppers should purchase items for cash and check to see that the items were rung up properly on the cash register and that a receipt was issued for the purchase.

Check: One of the shoppers should make a purchase with a personal check and observe that procedures were followed.

Credit: One of the shoppers should use a credit card and monitor credit card procedures.

Mail: If the client sells goods or services via the mail, test the system by carefully monitoring purchases made by credit card, check, and even cash.

Internet: If the client sells goods or services via a website, make test purchases as noted above.

4. On-site work relating to purchases:
 - A. Trace the cash purchases to ensure that these transactions were not voided *after* the shopper left the premises. Obviously, if they were, a serious problem exists.
 - B. Trace the credit card purchases to the cut-off credit card statement to ensure that the proper amount was recorded to the proper card.
 - C. Thoroughly audit the check transactions by carefully examining the checks or check images. In particular, compare the test check endorsement stamps and bank clearinghouse stamps with other checks to ensure they that match and that someone hasn't opened up an account at another bank under the same or similar name as the client's business name.
5. Other on-site work:

Payroll: Thoroughly investigate new employees hired after field work was concluded, to ensure that there are no ghosts on the payroll (See "Ghosts on the Payroll and Ghost Vendors" in Section 4 of this manual).

Payroll taxes: Audit the accuracy of the payroll tax liability and actual tax deposits for federal, state, and local payroll taxes to ensure that there have been no intentional tax overpayments credited to any individual income tax withholding account.

New vendors: Organizations should have an approved and updated vendor listing examined by the auditors during field work. New vendors added to this list should be investigated by the auditors to ensure that they actually exist and that there are no ghost vendors (See “Ghosts on the Payroll and Ghost Vendors” in Section 4 of this manual).

Tip: Examine new vendor invoices carefully. Pay close attention to and investigate new vendors that show only a post office box remittance address and no street address. Not indicating a street address on an invoice is unusual and should be investigated.

Bank reconciliations, current year: Select a random bank reconciliation prepared internally by staff and check it carefully as follows:

- a. Ensure that all checks have been accounted for, and investigate any missing checks.
- b. Investigate any new or unusual bank debit memoranda. A common “window of opportunity” trick is to have insurance payments, car payments, and the like paid for by debit memoranda drawn against the checking account during this period, and canceling these prior to the auditors arriving to start field work.
- c. Investigate any out-of-sequence checks.
- d. Test deposits.

Bank reconciliations, last month of the prior year: Here is another common scam:

Someone approves a legitimate invoice for payment early in the last month of the fiscal year and forwards the approved invoice to finance for payment. An accountant prepares the check, has it signed, and mails it to the vendor, who cashes the check accordingly. This check or check image will be in the end of the month bank statement.

Unknown to anyone, the dishonest accountant intentionally prepares a second check payable to the same vendor for the same amount of money and for the same invoice, in another check run, but places this check in the office safe. Typically, the fraudulent check will be made payable to a very clever variation of the legitimate vendor’s name. For example, if the legitimate vendor is the *Acme Printing Corp.*, the second check may be made out to the *Acme Printing Co.*, and the possibility of discovering this would be very remote.

The auditors start their field work and the accountant crosses his or her fingers, hoping the auditors do not catch the double payment.

12 Preventing Fraud in Nonprofit Organizations

If the auditors *do* discover the double payment, typically they would bring it to the staff accountant's attention, and he would probably feign embarrassment over the double payment error, but would be able to produce the check for the second payment (it is still in the office safe), show it to the auditors, simply void the check, and correct the transaction by an adjusting journal entry.

At this point nothing looks suspicious to the auditors, because mistakes can happen, particularly at the end of the year when the accounting staff is busy with budgets, taxes, W-2 preparation, and so forth.

But what if the auditors *don't* discover the double payment, which is also possible? Simple—the perpetrator waits for field work to be concluded (the window of opportunity just opened), opens a bank account in the name of the payee of the fraudulent check, deposit the second check, waits for the funds to become available, closes the account out at that time, and pockets the money!

What is the possibility that the auditors will discover this? Very low, *because this transaction occurred on the prior year's records, which have already been audited!*

Tip: During the course of the surprise visit, revisit the end of the prior year's bank reconciliation and track the status of checks outstanding on that statement. In particular, compare the endorsement stamps appearing on these checks against other checks deposited by the same vendor, and ensure that they match.

Inventory: The surprise visit is an opportune time to examine inventory rather than waiting for field work to commence.

Tip: Open up and examine the contents of boxes of *inexpensive* inventory, particularly if there are any marks on the box. A common trick is for an employee to put an *expensive* item in a box for an inexpensive item when no one is looking and carefully place and mark the box. An accomplice could easily enter the establishment, pick up the marked box, and present it to a cashier for payment. The cashier would scan the bar code, charge the lesser amount, and watch the accomplice walk out of the store.

Tip: Assuming the client's type of inventory qualifies, of course, consider recommending that the client purchase a clear-plastic, shrink-wrap machine. If possible, wrap incoming inventory boxes in this clear plastic and safeguard the machine. Simply wrapping boxes in clear plastic greatly reduces the possibility of switching expensive and inexpensive items.