

# **FRAUD MONITORING**

**NEELY D. DUNCAN, CPA, CFE, FCPA**  
Lane Gorman Trubitt, PLLC  
2626 Howell St. Suite 700  
Dallas, TX 75204

State Bar of Texas  
**GOVERNANCE OF NONPROFIT ORGANIZATIONS COURSE 2011**  
August 18-19, 2011  
Austin

**CHAPTER 21**



## **NEELY DUNCAN, CPA, CFE, FCPA**

Lane Gorman Trubitt, PLLC  
2626 Howell St. Suite 700  
Dallas, TX 75204

### *Areas of Focus*

Non-Profit (including Healthcare related entities), A133 – Single Audits, Employee Benefit Plans, Continuing Care Retirement Communities, Healthcare Consulting, Forensic Consulting/Expert Witness/Attorney Work Product

### *Experience:*

Neely served four years in the United States Navy. One year as a State Auditor for Virginia. In excess of ten years of auditing experience in public accounting. Her responsibilities include planning, risk assessments and completion of audit procedures, supervision of staff and reviewing of workpapers, financial statements and attending board as well as audit committee meetings after completion of audit. Neely also performs forensic work related to various cases as well as consulting for healthcare practices.

### *Academic Background:*

Old Dominion University – Bachelors in Accounting

### *Professional Association:*

Board Member, Texas Society of Certified Public Accountants

NPO Conference Committee - Chair

Emerging Practice Issues Committee - Member

Ethics Task Force - Member

Board Member, Arthritis Foundation - Assistant Treasurer

Planned Giving Committee - Previous Member

Walk Committee - Member

Dallas Society of Certified Public Accountants - Member

Professional Leadership Program - Previous Chairman

Not-for-Profit Study Group - Planning Committee Member

Scholarship Committee - Member

Association of Certified Fraud Examiners - Member

Philanthropy Committee - Member

Scholarship Committee - Member

Nominating Committee - Chair

American Institute of Certified Public Accountants - Member

2007 Recipient of the “Young CPA of the Year” award, Dallas CPA Society

Previous Treasurer, Association of Independent Living

Center for Nonprofit Management Education Series - Planning Committee

### *Licensed In:*

Texas

### *Contact Information:*

214.461.1437

nduncan@lgt-cpa.com



TABLE OF CONTENTS

I. INTRODUCTION..... 1

II. FACTS ABOUT FRAUD PER THE SUMMARY OF FINDINGS ..... 1

    A. Overall Statistics and Observations:..... 1

    B. Occupational Fraud ..... 1

        1. Asset Misappropriation..... 1

        2. Corruption Schemes ..... 2

        3. Financial Statement Fraud ..... 2

III. CONTROL WEAKNESSES THAT CONTRIBUTED TO FRAUD PER THE 2010 ACFE REPORT..... 2

    A. Per the ACFE 2010 Report, the control weaknesses that contributed to fraud were as follows: ..... 2

    B. Per the ACFE 2010 Report, behavioral red flags displayed by perpetrators: (the top items listed in the study)..... 3

    C. Motives for Fraud – Why do they do it? ..... 3

    D. Why do Organizations let the Perpetrator off the Hook? ..... 3

        1. Fear of notoriety. Many organizations fear the effects of negative publicity if they file an official report about insider theft. The damage to a nonprofit organization’s reputation can create a breach of trust with the public and ultimately destroy the organization..... 3

        2. Fear of legal action. The organization may be threatened with civil and criminal action by an offender. For example, someone caught with their hand in the till may threaten to sue for defamation, false arrest, violation of privacy, wrongful termination, etc. .... 3

        3. Concern about personal safety. Workplace violence has become more common recently and employers are understandably wary of prosecuting thieves who threaten personnel with bodily injury..... 3

        4. Compassion for the offender. In many cases leaders have a difficult time taking appropriate action when they have a sense of compassion for the circumstances facing the embezzler. For example, the bookkeeper may claim that he stole from your nonprofit because he needed to purchase medication for a sick family member. This is especially prevalent in religious organizations. .... 3

IV. TEN CONTROLS THAT CAN BE EASILY IMPLEMENTED TO HELP PREVENT AND DETECT FRAUD IN YOUR NONPROFIT ORGANIZATION..... 3

    1. Tone at the Top..... 3

    2. Controls over Payroll..... 4

    3. Controls over Disbursements..... 4

    4. Controls over Bank Reconciliations ..... 5

    5. Controls over Receipts..... 6

    6. Physical Safeguards..... 6

    7. Electronic Controls ..... 6

    8. Hiring Procedures ..... 7

    9. Credit Cards..... 7

    10. Controls to Help Detect Potential Financial Statement Fraud..... 7



## FRAUD MONITORING

### I. INTRODUCTION

Fraud monitoring and internal controls are essential concepts that all not for profit organizations struggle to stay on top of and in compliance with best practices. Based on an unscientific sampling of not for profit organizations a lack of internal controls and an understanding of fraud risks can pose a significant risk to such organizations and board members. The purpose of this paper is to summarize our experience as auditors and board members in the not for profit sector as it relates to internal controls and fraud monitoring.

The fact that dishonest people would steal from nonprofit organizations should come as no big shocker.

Financial reporting fraud in the nonprofit sector looks much different from that in the for-profit world. A for-profit is trying to make money; however, in the nonprofit world, the goal of an organization is to run programs that are designed to accomplish a mission and not based on generating profits for shareholders.

### II. FACTS ABOUT FRAUD PER THE SUMMARY OF FINDINGS<sup>1</sup>

#### A. Overall Statistics and Observations:

“It is estimated that the typical organization loses 5% of its annual revenue to fraud. When this is applied to the estimated 2009 Gross World Product this amount translates to a potential total fraud loss of more than \$2.9 trillion.

The median loss for organizations was \$160,000. Nearly one-quarter of the fraud cases involved losses of at least \$1 million.

The fraud occurred a median of 18 months before being detected.

Small organizations are disproportionately victimized by occupational fraud. These organizations are typically lacking in anti-fraud controls compared to their larger counterparts, which makes them particularly vulnerable to fraud.

The industries most commonly victimized in the study were the banking/financial services, manufacturing, and government/public administration sectors.

---

<sup>1</sup> These statistics can be found in the Association of Certified Fraud Examiners *2010 Report to the Nations on Occupational Fraud and Abuse* (ACFE 2010 Report-as referenced throughout the article). This study is based on data compiled from a study of 1,843 cases of occupations fraud (defined below) that occurred worldwide between January 2008 and December 2009. All information was provided by the Certified Fraud Examiners (CFEs) who investigated those cases. The fraud cases in the study came from 106 nations – with more than 40% of cases occurring in countries outside the United States.

Fraud perpetrators often display warning signs that they are engaging in illicit activity. The most common is living beyond their means and experiencing financial difficulties.

More than 85% of fraudsters in the study had never been previously charged or convicted for a fraud-related offense.

The highest levels of fraud occur in the age range of 31 to 45 years old and, generally, the median losses tend to rise with the age of the perpetrator.

Losses also tended to rise as the perpetrators' tenure increased. Employees who had more than 5 years of tenure with the victim organization caused a median loss of more than \$200,000.

52% of all perpetrators had a college degree and were predominantly male

According to the 2010 ACFE Report, tips were the most common detection methods, catching nearly three times as many frauds as any other form of detection. 40% of the cases reported were initially detected by tips from employees, customers, vendors, competitors and acquaintances.

### B. Occupational Fraud

Occupational Fraud is defined as “the use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”

Per the study, occupational fraud is much more likely to be detected by tip than by any other means.

The ACFE 2010 Report states there were three primary categories of occupational fraud used by individuals to defraud their employers: Asset Misappropriation, Corruption Schemes, and Financial Statement Fraud.

#### 1. Asset Misappropriation

According to the 2010 ACFE Report “Asset misappropriation schemes were the most common form of fraud in the study by a wide margin, representing 90% of cases — though they were also the least costly, causing a median loss of \$135,000. Financial statement fraud schemes were on the opposite end of the spectrum in both regards. These cases made up less than 5% of frauds in the study, but caused a median loss of more than \$4 million — by far the most costly category. Corruption schemes fell in the middle, comprising just under one-third of cases and causing a median loss of \$250,000.”

According to the 2010 ACFE Report there are three major areas of asset misappropriation: Fraudulent Disbursements, Cash Theft and Inventory and Other Assets.

a. Fraudulent disbursements are an asset misappropriation scheme that involves an employee

making a distribution of company funds for a fraudulent purpose. Some examples of fraudulent disbursements are register disbursement schemes, forging company checks, billing schemes, submission of false invoices, doctoring time cards, false refunds, voided sales, check tampering, payroll schemes, expense reimbursement schemes, fictitious vendors, overbilling, ghost employees, commission schemes, and false voids.

**b.** Cash theft consists of such things as skimming, lapping, and cash larceny.

Skimming is the removal of cash received prior to entry in an accounting system leaving no audit trail.

For example, employees may steal sales or receivables before being recorded on the books by selling a good or service to the customer, collecting the payment, but never recording the sale on the books. This is why various fast food restaurant chains post a notice for customers to contact management if they do not receive a receipt. This is a compensating control to offset this type of potential asset misappropriation scheme as it would alert management that an employee may be skimming sales.

Lapping involves stealing a donor's contribution and concealing the theft by applying the payments of other donors to the first donors account. For example, Jason initially pockets half of a \$10,000 contribution, but records the total contribution as \$10,000. Before any questions arise, the remaining \$5,000 balance is paid using funds diverted from another contributor. Lapping requires a great deal of time and effort, and all of the balls must be kept in the air to prevent detection.

Cash larceny is when an employee intentionally takes the employer's cash. For example, larceny schemes may include theft of incoming cash, theft of currency on hand, theft from the organizations bank deposits, and altering cash counts.

**c.** Asset misappropriation – inventory and other assets are when the employees steal items such as inventory, fixed assets, intellectual property, equipment, supplies, and other non cash items. Some examples include misuse of inventory and other assets, falsifying incoming shipments, physical padding, theft of inventory and other assets, purchasing and receiving schemes, and altered inventory records.

**2. Corruption Schemes**

According to the 2010 ACFE report, corruption involves the employee's uses of their influence in business transactions in a way that violates their duty to the employer for the purpose of obtaining a benefit for themselves or someone else. Some examples of corruption schemes are bribery, illegal gratuities, kickbacks, bid rigging schemes, diverting business to

vendors, overbilling schemes, hidden interests, and transfers at other than fair market value.

**3. Financial Statement Fraud**

Financial statement fraud is the deliberate misrepresentation of the financial condition of an enterprise accomplished through the intentional misstatement or omission of amounts or disclosures in the financial statements to deceive financial statement users.<sup>2</sup>

Some common examples of financial statement fraud are recording fictitious revenues, overstating/ understating assets, overstating/ understating revenues, understating liabilities, concealing over-budget results, concealing liabilities, inappropriate capitalizing of expenses, misclassification of assets/liabilities as long term instead of current, timing difference schemes, failing to disclose significant related party transactions, failing to disclose noncompliance with debt requirements or lack of waiver of noncompliance from lender, misclassifying restricted donations to mislead donors or charity watchdogs, holding records open beyond the period end in order to inflate revenues, failing to correctly report obligations for deferred compensation or retirement benefits<sup>1</sup>, and inaccurate fair market valuations.

According to the 2010 ACFE Report, “the median duration – the time period from when the fraud first occurred to when it was discovered” – was 27 months, the longest of all scheme types.

**III. CONTROL WEAKNESSES THAT CONTRIBUTED TO FRAUD PER THE 2010 ACFE REPORT**

Antifraud controls appear to help reduce the cost and duration of occupational fraud schemes. Victim organizations that had controls in place had significantly lower losses and time to detection than organizations without controls.

**A. Per the ACFE 2010 Report, the control weaknesses that contributed to fraud were as follows:**

- lack of internal controls - 37.8%,
- override of existing internal controls - 19.2%,
- lack of management review - 17.9%,
- poor tone at the top - 8.4%,
- lack of competent personnel in oversight roles - 6.9%,

---

<sup>2</sup> This information was taken from the *Fraud Examiners Manual* written by the Association of Certified Fraud Examiners, Inc.

- lack of independent checks/audits - 5.6%,
- lack of employee fraud education - 1.9%,
- lack of clear lines of authority - 0.8%,
- lack of reporting mechanism - 0.6%.

**B. Per the ACFE 2010 Report, behavioral red flags displayed by perpetrators: (the top items listed in the study)**

- Living beyond means – 43.0%
- Financial difficulties – 36.4%
- Control issues, unwillingness to share duties – 22.6%
- Unusually close association with vendor/customer – 22.1%
- Wheeler-dealer attitude – 19.2%
- Divorce/family problems – 17.6%
- Irritability, suspiciousness or defensiveness – 14.1%
- Addiction problems – 11.9%
- Refusal to take vacations – 10.2%
- Past employment-related problems – 9.3%
- Complained about inadequate pay – 7.9%
- Excessive pressure from within the organization – 7.5%

**C. Motives for Fraud – Why do they do it?**

Some motives for fraud are bonuses, raises, promotions based on reported results, positive performance evaluations and retaining their job based on reported results (especially with downsizing in our current economy).

Other motives are to obtain bank financing or meet bond/loan covenants, (which have become more restrictive since 2008), inflating program accomplishments, and misleading information regarding organization capabilities or staff qualifications/certifications.

Also, conflicts of interest, trying to impress watchdog groups, disgruntled employees and organizations experiencing financial difficulty, can all be potential motives for perpetrating fraud.

A personal incentive to engage in fraud in a nonprofit organization may include the concealment of personal expenditures.

**D. Why do Organizations let the Perpetrator off the Hook?**

Many organizations let the perpetrator off the hook because of fear of reputational damage, fear of an employee lawsuit, concern about the personal safety of themselves or their employees, and compassion for the offender.

**1. Fear of notoriety.** Many organizations fear the effects of negative publicity if they file an official report about insider theft. The damage to a nonprofit organization’s reputation can create a breach of trust with the public and ultimately destroy the organization.

**2. Fear of legal action.** The organization may be threatened with civil and criminal action by an offender. For example, someone caught with their hand in the till may threaten to sue for defamation, false arrest, violation of privacy, wrongful termination, etc.

**3. Concern about personal safety.** Workplace violence has become more common recently and employers are understandably wary of prosecuting thieves who threaten personnel with bodily injury.

**4. Compassion for the offender.** In many cases leaders have a difficult time taking appropriate action when they have a sense of compassion for the circumstances facing the embezzler. For example, the bookkeeper may claim that he stole from your nonprofit because he needed to purchase medication for a sick family member. This is especially prevalent in religious organizations.

What most nonprofit organizations fail to realize is not prosecuting the offender sets a bad precedent that could encourage fraud by other employees.

**IV. TEN CONTROLS THAT CAN BE EASILY IMPLEMENTED TO HELP PREVENT AND DETECT FRAUD IN YOUR NONPROFIT ORGANIZATION.**

Based on more than a decade of experience with the nonprofit sector, I recommend implementing the following ten controls to help prevent and detect fraud in a nonprofit organization.

**1. Tone at the Top**

The first and most important thing the board can do is set the control environment, also known as “setting the tone at the top”. All employees, executives and board members need to understand the organizations policies and procedures and the repercussions of not following them.

In my experience, I have seen that this applies to everyone except the Executive Director or the President of the Board. If the top executives do not lead by example and set the right tone for the organization, it gives employees the impression they don’t have to follow the rules either.

The employees tend to rationalize that if the top person does it then it must be okay for them to do it as well. They may start cutting corners or not providing receipts for expense reimbursements because the executive does not do it.

The area I have seen the most abuse in my experience is executives not providing receipts for expense reimbursements, not submitting timesheets, and not having their company credit card statements reviewed.

The nonprofit organization should have a written policy stating the organization's position and how fraud perpetrators will be dealt with. This should be emphasized during new-hire orientation and re-emphasized, at a minimum, annually. A simple email circulated by the Board President or Executive Director will remind employees of the policy and help prevent and detect fraud.

Smaller companies especially should have a policy of job rotation and enforced annual leave since many frauds require the person to maintain continuous, manual intervention. However, it does not do anyone any good if you force vacation and then the work sits until the person returns. This control is only effective if someone reviews information while that key employee is out. Several types of fraud require the fraudster have several balls in the air that are easily discovered when the person committing the fraud has an illness or can't control the situation for a period of time.

It is vital for management to emphasize the importance of ethics and controls at staff meetings, board meetings, and volunteer events and demonstrate enforcement ALL of the time. Leadership must communicate clearly the organizational mandate that fraud will be not be tolerated and those that steal will be dealt with harshly.

As noted in the 2010 ACFE Report, over 49% of frauds are detected by tip and therefore we highly encourage a whistleblower policy/ hotline. This does not need to be an extravagant, expensive ordeal, simply giving employees direct access to a board member, without the fear of retaliation or retribution may be enough. The employees should be encouraged and reminded of this policy at a minimum annually. A simple email by a board member to all employees would be an easy, effective method.

## 2. Controls over Payroll

Payroll controls at small organizations are actually considered to be viewed as more controlled because everybody knows everybody. It tends to be more difficult to create a fictitious employee and actually pay them for any length of time.

However, where most abuse happens pertains to the controls over employees' timesheets, especially for those employees who work on an hourly basis. It is important that a manager or supervisor familiar with the employee's duties review their timesheet for accurate labor charging before the timesheet is approved. A rubber stamped approval is not going to

be effective in preventing or detecting payroll fraud in the organization.

Using a payroll service can assist in ensuring compliance with payroll laws and regulations and deter fraud by having an independent third party review the payroll.

Encourage all employees to use direct deposit. This eliminates the need for checks to be printed and signed, nor are you or your Executive Director signing his/her own check. Many banks offer free checking accounts as an incentive for people to use direct deposit.

Use a separate bank account for payroll. We recommend the nonprofit organization establish the second account as an imprest payroll account, whereby the account has a zero balance and transfers are made from the main account as needed for the payroll checks and payroll taxes. This account limits access to the main operating account for both the payroll service center and employees. Additionally, fraud or errors on the part of the bank and payroll service will show up sooner. This will also alert you if someone has changed the amount on the check or tried to cash it.

Ensure adequate segregation of duties as much as possible to ensure the same person is not able to prepare, post, reconcile, pay, makes changes to master file, and enter the payroll into the general ledger.

Keep in mind the fact that many times fraud starts where an individual receives an inadvertent "overpayment" in the form of a paycheck or reimbursement. If an overpayment makes its way through your accounting system and into the pocket of an employee, he or she may believe that future overpayments will also go undetected.

## 3. Controls over Disbursements

### A. Require two signatures.

This is a good policy so that someone sees the big checks. This ensures two people are involved in the process. Both required signatures have to agree on the expenditure. It is more about setting the right tone than about preventing theft.

The fact that the two people signing the checks both know someone else is looking at it as well is a good deterrent against fraud. If you require two signatures on checks, but have trouble getting both signatures and consequently have blank checks signed, have the board change the policy to only have a signatory for checks up to a specified amount.

B. Never sign blank checks or have checks made out to cash. We also recommend blank checks be kept in a locked box or cabinet accessible only to those with proper authorization. Additionally, the blank checks should be inventoried periodically.

C. Ensure appropriate segregation of duties by reviewing procedures and controls related to cash disbursements. For instance, the responsibility or authority to approve disbursements, sign checks, receive and review unopened bank statements and cancelled checks, and prepare/review bank reconciliations should not all reside with one individual. This condition could provide an opportunity for misappropriation of funds and concealment of such activity. In order to mitigate this condition, we recommend that someone other than the bookkeeper/accounting person review unopened bank statements and cancelled checks. This control usually takes no more than an hour each month and provides a supervisory control that can help prevent or detect improper or unauthorized disbursements.

D. Once management signs the checks, they should never be returned to the preparer for mailing. In order to reduce the risk that checks could be altered after being signed, we recommend that once checks have been signed, they are immediately mailed by someone with no access to the accounting records and not returned to the preparer. Check signing is not the only way to get the treasurer or another board member involved. Have the bank statements and cancelled checks sent directly to the treasurer. The treasurer can review the checks and the endorsements. Check signers(s) should double check that the amount and the vendor name and address on the invoice match the amount and vendor name and address on the check. In this age of computerization, “autofill” often inserts the wrong amount or payee, so it is important for there to be a double check.

Unless they routinely do it every day, the executive director or treasurer should randomly open a day’s mail. If the executive director does this every day, he or she should delegate this task. Make mail opening a group activity with two or more people involved with one person responsible for opening the mail and another for recording incoming checks.

E. Use two separate bank accounts for your organization. One should be the main account into which funds are deposited. The second should be a subsidiary account that all checks are written against. When checks are written, there should be a transfer from the main account to the subsidiary for the necessary amount. As a result, the subsidiary account will have a balance only large enough to cover checks that are written (also the entity can set up positive pay). Only a board member or specifically appointed person should be allowed to authorize transfers from one account to another. Using this system, embezzlement or other irregularities will cause an overdraft. Instruct your bank to notify you immediately when an overdraft

occurs. Problems are easier to solve a few days after they occur as opposed to weeks or months later.

F. Limit advances and reimbursements to staff for supplies. Set up accounts with the vendors the nonprofit organization prefers and limit authorized purchasing to only those establishments. Remember to remove employees from the list of authorized purchasers when they leave the organization.

Verify the list of authorized purchasers at each store on a regular basis. Set appropriate limits for authorized purchasers on all accounts based on the employee’s job description and responsibilities.

Review the vendor list in your accounting system periodically for reasonableness. Also review the controls in place regarding who is authorized to establish an account with a new vendor.

Using current technology, anyone can create a professional looking invoice. Avoid paying fraudulent invoices by requiring the employee who received the goods or services to sign the invoice and state the purpose of the expense on the invoice. The signature should be on the actual document, not scribbled on a Post-it note. Post-it notes can be removed easily.

#### **4. Controls over Bank Reconciliations**

A. Bank reconciliations should be completed on a timely basis, reviewed by a third party, and initialed by the reviewer. This creates an appearance of detection even if the person reviewing is not an accountant.

We recommend reconciling all bank accounts within 10 days of receiving the bank statement. Ensure that the reconciliation is reconciled to the General Ledger as well as the checkbook.

The absence of adequate source documentation can be a red flag that an insider is defrauding the organization.

B. Inactive bank accounts can be susceptible to misuse by someone seeking to misappropriate cash. Thus, we recommend management determine if the inactive accounts are necessary and close them if not.

C. The person doing the bookkeeping should not reconcile the bank accounts. Separate these responsibilities if at all possible. If you have a small staff, ask a board member to reconcile the bank statements or receive the statements directly. The executive director should review the reconciliation and bank statements periodically as well.

Make certain that someone independent of check processing receives unopened bank statements each month and reviews payees, amounts, signatures and endorsements. This person should be focused on looking for unusual transactions, amounts and payees.

D. Verify wire transfers – Have someone not involved with wire transfer requests verify all wire transfers outside of the organization.

Many nonprofits go to great lengths to protect written checks and forget about controls with regard to wire transfers.

**5. Controls over Receipts**

A. Make bank deposits daily. Use a bank lock box if you receive an influx of deposits at once, for example, if you are a membership organization with dues all due at the same time of year. It may cost less than you think. It should be used for all deposits and should be reconciled on a timely basis.

B. Verify cash logs - Make certain your cash receipts log matches the cash receipts entry in the ledger and the actual bank deposit.

C. Involve a second person in cash receipts processing – Have a second employee involved in verifying incoming receipts.

The notion underlying independent checks is that if employees know their activities are being monitored, the perceived opportunity to commit fraud is reduced. For example, when an independent manager (one with no access to donated cash) compares the cash receipts log to what was deposited in the bank, the manager is making sure that all cash received actually was deposited into the bank.

Such independent checks not only guard against employee fraud but also uncover honest mistakes. But the biggest concern with not-for-profit organizations is that incoming cash donations won't be logged in but will instead be diverted into the pockets of dishonest employees or volunteers.

D. Review the accounts receivable agings monthly. Send out second/third notices. Have someone other than the cash receipts person follow up on unusual items.

E. Another strong deterrent - install security cameras in areas where cash is handled.

F. A less-expensive but perhaps equally effective option would be to conduct “surprise” audits of cash accounts since staffers and volunteers won't have time to cover their tracks.

**6. Physical Safeguards**

Nonprofit organizations can minimize opportunities for misuse or theft by simply limiting access to physical assets and accounting records by unauthorized personnel.

Such safeguards include locked cash registers and storerooms, electronic passwords, fireproof safes, fences around buildings, and secure storage lots for equipment and materials.

Reconcile your physical inventory of furniture and equipment to your accounting records. This can be done as part of an annual office clean-up day. This will reveal if things are missing and also deter theft.

Do the same reconciliation with software licenses. Also, remove from your accounting property list obsolete or no longer used software and dispose of the old software disks and programs.

**7. Electronic Controls**

A. Run vendor addresses through an edit check to see if any match each other and/or employee addresses.

B. Protecting confidential information isn't only a business requirement – it's often a legal requirement. Employees can breach confidentiality by simply allowing someone to use their password to access company data. From there, unauthorized users can alter, delete, or steal information. Moreover, hackers pose threats from outside the organization and can gain access to company data through electronic trickery like “masquerading” and “piggybacking.” Ensure the organization has implemented proper access-control mechanisms, beyond just user-names and passwords, so that only authorized persons are able to view data, perform tasks, or both. This probably will mean creating several levels of security and, therefore, several levels of users.

C. Periodically test the backup system for your accounting data to make sure it is working properly. Otherwise, you may not find out there is a problem until the day you need the backup.

D. Provide appropriate system access – Ensure that the level of system access granted an employee is consistent with the employee's job description and responsibilities.

E. Encryption technology, which allows only authorized users to access (“decrypt”) certain information, is becoming increasingly important for companies that allow employees to use laptops, CDs, and USB keys that contain confidential data. Consider also how much proprietary and confidential information is received and stored on people's phones. Every phone should, at a minimum, have a password.

F. Other strategies include maintaining antivirus protection to detect threats and crafting policies to limit and/or control internet use to help prevent access to

infected websites. All of these strategies will help protect your company from accidental loss or deliberate theft, as well as secure the data so it can't be read if it's lost or stolen. Examples of websites typically blocked due to the threat of virus infection are Facebook, MySpace, Twitter, etc.

## 8. Hiring Procedures

A. When employees falsify their credentials, they have perpetrated a fraud against your organization.

Background checks, credit checks, exit interviews, reference checks, drug tests, past work experience checks are crucial to help prevent and detect fraud.

Fraud experts estimate that nonprofit organization can prevent about 80% of fraud by effectively screening prospective employees and volunteers.

Those with criminal backgrounds and/or who misrepresent themselves on their employment applications are most likely to commit fraud.

## 9. Credit Cards

Credit cards are a prime area for fraudulent activity within nonprofit organizations. The organization should have clear defined travel and entertainment policies and procedures.

There should be proper authorization, review and preapproval.

Credit cards should not be shared.

The limits on credit cards should be appropriate per review of the employee's job description.

Never allow personal charges for any reason on a company credit card.

Create and have a policy of per diem rates, what will and won't be accepted, what can and cannot be charged to the credit cards, etc.

Have someone on the board review key employee credit card statements monthly.

Look for unusual vendors and transactions that don't appear to have a business purpose.

Question at least one expenditure on the credit card statement each month and indicate your review/approval by initialing the statement.

## 10. Controls to Help Detect Potential Financial Statement Fraud

A. Require budget to actual and require the CFO to provide explanation of variances greater than 5% change. Require comparison to prior year with explanation of variances greater than 5% change.

B. A final report should be prepared that compares actual performance against an approved budget. Variances should be explained and, if caused by an

accounting error, corrected before the report is distributed.

C. Distribute financial reports to staff members and all department heads. A fresh set of eyes may pick up an error or a potential problem.

D. Periodically someone other than the Finance Director should look at the reports generated by the financial system. Again, a fresh set of eyes may identify a problem.

E. The Board/Treasurer should ask at least one question about the financial statement analysis each month.

---

i Web sites with information directly related to prevention or detection of fraud or addressing issues related to fraud.

American Institute of Certified Public Accountants – [www.aicpa.org](http://www.aicpa.org)

American Institute of Philanthropy – [www.charitywatch.org](http://www.charitywatch.org)

Association of Certified Fraud Examiners – [www.cfenet.com](http://www.cfenet.com)

Association of Fundraising Professionals – [www.afpnet.org](http://www.afpnet.org)

BBB Wise Giving Alliance – [www.give.org](http://www.give.org)

BoardSource – [www.boardsource.org](http://www.boardsource.org)

Charity Navigator – [www.charitynavigator.org](http://www.charitynavigator.org)

EthicsLine – [www.ethicsline.com](http://www.ethicsline.com)

Evangelical Council for Financial Accountability – [www.ecfa.org](http://www.ecfa.org)

FraudNet – [www.fraudnet@gao.gov](mailto:www.fraudnet@gao.gov)

General Accounting Office – [www.gao.gov](http://www.gao.gov)

GuideStar – [www.guidestar.org](http://www.guidestar.org)

IGNet – [www.ignet.gov](http://www.ignet.gov)

Information Systems Audit and Control Association – [www.isaca.org](http://www.isaca.org)

The Institute of Internal Auditors – [www.theiia.org](http://www.theiia.org)

Internal Revenue Service – [www.irs.gov](http://www.irs.gov)

Management Assistance Program for Nonprofits – [www.mapnp.org](http://www.mapnp.org)

National Association of College and University Business Officers – [www.nacubo.org](http://www.nacubo.org)

National Association of State Charity Officials – [www.nasconet.org](http://www.nasconet.org)

National White Collar Crime Center – [www.nw3c.org](http://www.nw3c.org)

Nonprofit Risk Management Center – [www.nonprofitrisk.org](http://www.nonprofitrisk.org)

Society for Human Resource Management – [www.shrm.org](http://www.shrm.org)

Wall Watchers' Ministry Watch – [www.ministrywatch.com](http://www.ministrywatch.com)