How to Prevent Employee Theft

In these tough economic times, trends indicate the frequency of employee theft has increased for nonprofit organizations. We've provided some simple steps that your organization can take to ensure you are shielded as much as possible from instances of employee theft. In addition, you will be able to review three real-life claims examples that illuminate the challenges that nonprofit organizations face regarding employee theft.

1. Selecting the Right Employee

One of the most basic steps in preventing employee fraud is not to hire employees who have stolen previously. Before hiring anyone, you should conduct a background check to find out as much as you can about the employee's previous experience with employers and law enforcement. Each organization must decide whether the time and expense of such background checks is worth the return. It is always a good practice, but, at a minimum, you should check the background of any employee who will have constant access to cash, checks, credit card numbers, or any other items that are easily stolen. Before hiring an employee, you should check as many of the following as possible:

Past Employment Verification
Even though most employers will only verify position and dates of employment, you can usually tell by their tone of voice what they think of the employee. Also, ask the previous employers whether the applicant is eligible for rehire.

Criminal Conviction Checks
Most public records services (such as Nexis or ChoicePoint) have criminal conviction records for almost every large county in the U.S. If not, you may go to the courthouse and search the criminal conviction records in the criminal courts division of the employee's county of residence (or other counties in which he or she previously resided).

Drug Screening
Many organizations are now conducting drug screenings for potential hires as well as current employees. People who are frequent drug users can be more prone to theft or fraud.

Reference Checks
Amazingly, very few employers actually call the references a candidate provides. Most operate under the theory that someone wouldn't provide a bad reference. However, many times people will list important-sounding individuals as references with the hope that you won't call. And, people often assume, incorrectly, that a former supervisor or co-worker will provide a good reference.

Education and Certification Verification
It is always a good idea to verify a person's education. Also, if the person claims he has a license or other certification, call the issuing organization to verify it. It is not that unusual for someone to claim a certification or license that has actually been revoked due to a disciplinary action. Most licensing or certification organizations, including the Association of Certified Fraud Examiners, will tell you if any disciplinary action has been taken against a particular member.

Get the Consent of the Candidate
Numerous federal and state laws, such as the Fair Credit Reporting Act, govern the gathering and use of information for pre-employment purposes. Many of these laws require that you obtain written consent from the candidate before gaining some types of information listed above. It is also a good idea to obtain a signed authorization and release from a potential candidate. Consult with your human resources and/or legal department to ascertain the laws applicable to your organization and to obtain the proper authorization forms.

2. Policies and Procedures that Help Deter Fraud

Developing anti-fraud programs can be one of the most important things that you can do for your organization. Prevention, in the long run, is always cheaper than recovering your losses.

Perception of Detection

Employees who perceive that they will be caught engaging in occupational fraud and abuse are less likely to commit it. Increasing the perception of detection may well be the most effective fraud prevention method. Internal controls, for example, do little good in forestalling theft and fraud if their presence is not known by those tempted to steal. This means letting employees, managers, and executives know that managers are actively seeking out information concerning internal theft.

Proactive Programs
Becoming proactive in your anti-fraud efforts can be one of the most effective steps that you can take to prevent fraud. Some of the programs cost very little, while others require a cost commitment, although most anti-fraud programs will more than pay for themselves.

Employee Education
Every organization should have some mechanism whereby to educate executive level staff, finance department staff and other employees about fraud. This can be done as a part of employee orientation, or it can be accomplished through memoranda, training programs, and other intra-organization communication methods. The goal is to make others within the company your eyes and ears. Any education efforts should be positive and non-accusatory. It should be emphasized that illegal conduct in any form eventually costs everyone in the organization through lost productivity, adverse publicity, and decreased morale.

Auditing for Fraud
Developing audits that focus on high-risk areas for fraud is something that many organizations have found to be effective in their anti-fraud program. Not only have they identified fraud, but fraud decreased in subsequent audits. Some of the areas that are good areas for fraud audits are:

- Expense reports
- Payroll
- Purchasing
- Sales
- Accounts receivable
- Customer complaints
- Cash
- Suspense accounts

Enforcement of Mandatory Vacations
Many internal frauds require manual intervention, and are therefore discovered when the perpetrator is away on vacation. The enforcement of mandatory vacations will aid in the prevention of some frauds.

Job Rotation
Some frauds are detected during sickness or unexpected absences of the perpetrator, because they require continuous, manual intervention.

Surprise Audits Where Possible
All too many fraud perpetrators know when auditors are coming, and therefore have time to alter, destroy, or misplace records and other evidence. A proactive fraud policy involves using the technique of surprise audits as much as possible. It might have a significant deterrent effect.

Management Oversight

It is most common for employees who steal to use the proceeds for lifestyle improvements. Some examples include more expensive cars, extravagant vacations, expensive clothing, new or remodeled homes, expensive recreational property, and outside investments. Managers should be educated to be observant to these signs.

Minimize Employee Pressures

Pressures, such as financial hardship or family problems, can be especially difficult to detect on the part of the employees. Organizations can take steps to assist an employee who might be having difficult times.

Open-Door Policies

If employees and others can speak freely, many managers will understand the pressures and might be able to eliminate them before they become acute.

Employee Support Programs

Many progressive organizations have realized the benefit of employee support programs. Some kinds of support programs include alcohol and drug assistance, and counseling for gambling, abortion, marital problems, and financial difficulties.

Management Climate

If the style of management is conducted by objective measures rather than by subjective measures, then employees will not manufacture or imagine the performance criteria employed by management. In addition, it is obvious that management that is perceived to be dishonest will beget dishonest employees.

Monitoring Systems

Another key part of an anti-fraud program is having a reporting system for employees and agents of the organization to report criminal conduct. Confidential hotlines are one of the best ways for an organization to monitor compliance.

Reporting Programs

Each employee in the organization should know where to report suspicious, unethical, or illegal behavior. A reporting program should emphasize that:

- Fraud, waste, and abuse occur in many organizations
- Such conduct costs the organization jobs and potentially its reputation
- The organization actively encourages any employee with information to come forward
- The employee can provide information anonymously and without fear of recrimination for good-faith reporting
- There is an exact method for reporting, i.e., a telephone number, name, or other information
- The report need not be made to one's immediate superiors

Rewards

Some organizations (particularly for-profit companies) have a policy of rewarding information that leads to the recovery of merchandise, property, or money. Others offer rewards upon the criminal conviction of the person(s) involved. If a reward policy exists, strict criteria should establish reward payments, and such proposed policies should be reviewed and approved by counsel. The amount of reward paid by organizations varies from fixed fees to a percentage of the recovery. Studies indicate that rewards should not exceed a few thousand dollars. Crime Stoppers recommends rewards not exceeding $1,000.

AON

3. Claims examples – Here are some real-life claims examples to illuminate various exposures for associations.

Scenario #1

During a review of bank statements the association noticed that several check copies were missing. When the issue was discussed with the accounts payable employee her answers were vague. While the employee was out on personal time the association secured the missing checks from the bank and found that they were made payable to the accounts payable employee. This employee did not have check signing authorization and the signatures were forgeries. The association closely examined all of their bank accounts and determined that the employee was forging checks from 3 of their 5 bank accounts. After a thorough investigation the association determined that this employee forged 159 checks over a two year period, totaling over $373,000.

Scenario # 2:

The association was contacted by a bank officer who let them know about irregularities with their checking account. The bank investigated when another bank customer found cancelled checks without their account number listed on them. These checks instead showed the association's account number. The association's employee who worked in finance also did the same type of work on a contract basis for the other banking customer. The association was receiving quarterly statements that appeared on line; however, once notified of the irregularities they reviewed all of the monthly banking statements. In addition to irregular deposits, 100 checks were found payable to the employee in question. The employee did not have check signing authority and some of the signatures were forged. The employee was using the association's bank account as part of a scheme involving several companies. Money was deposited and then checks were forged and directed to this person's personal account. The loss was approximately $37,000.

Scenario #3:

An association chapter determined that a volunteer board member and committee chairman had stolen $9,000 from a checking account that he had access to and the association decided to give the volunteer 30 days to return the funds. Upon further research, the association chapter discovered this individual had taken an additional $29,000. The insurance policy for the association had specified language to extend employee theft coverage to people who are non-compensated "employees" of an association chapter. Except when involved in fund soliciting, this language provides employee theft coverage for those non-compensated individuals while performing duties of "employees". After the claim was reported to the insurance company, the association chapter confirmed they were able to recuperate all of the stolen funds from the spouse of the volunteer.