Preventing employee fraud and theft

MARKEL®

Preventing employee fraud and theft

Yes, it CAN happen to you

No one wants to think that their employees are going to defraud their organization of valued resources but it happens all too often. Many perceive that employee embezzlement only happens to a small minority of organizations and then only to those with vast resources that have enough money to afford the loss but actually one out of three business failures are as a result of employee theft according to the U.S. Chamber of Commerce. Most cases of misappropriation of funds involves a trusted employee who takes money from an unsuspecting organization. Honest, hardworking organizational leaders have been deceived and lost tens and even hundreds of thousands of dollars. The leader's mistake was that they trusted too much. If you think it can't happen to you and your organization, then your organization is probably very vulnerable. So no matter the size of your organization, you should be vigilant about employee theft and take some steps to prevent it.

Employee theft and fraud can happen in many ways:

- Stealing from petty cash funds
- Using a business credit card for personal purchases
- Changing deposit statements
- Writing a business check for personal expenses
- Applying for a business credit card for themselves
- Inaccurately recording cash transactions or payments and taking them
- Creating fake invoices and rerouting the payments
- Creating bogus customers, vendors or transactions
- Creating a forged bank account in the name of the organization and redirecting disbursements to it
- Having the mail, bills, or payments sent to a different address
- And more … (these are just a few examples)

How do you know it's happening to your organization?

It's a good practice to proactively be on the lookout for employee theft. You can do this by looking for warning signs in individual employee actions and the financial documents you regularly receive. Some of the employee actions that should raise your suspicions and give you cause to look further into what they are doing include:

- Someone refusing to take time off or vacations
- Someone working unusual, late or excessive hours
- Someone that has close relationships with accounting employees or cash-handling employees
- Someone that "selflessly" takes on more "duties" – often financial duties
- Someone with a lifestyle well above their salary level
- Someone that insists on handling routine clerical tasks below their position (a manager for instance)
- A lack of separation between different office responsibilities
- Someone with drug and alcohol abuse issues
- Someone with evidence of persistent borrowing, bad check writing, or compulsive gambling

You can also look into bookkeeping and financial reports for some financial signs that things may not be right. Some of these signs can include:

- A considerable petty cash fund
- Inconsistencies or gaps in accounting information
- Missing paperwork, invoices, or distributions
- Discrepancies between reports and bank statements
- Overdue accounts payable notices from contractors, vendors, etc.
- Lack of invoices, receipts, or purchase orders for supplies
- Unsolved shortages of supplies, stamps, or petty cash
- Curious patterns in bank deposit statements

There are many opportunities for employee theft within most any organization so it's far better to be proactive in your business practices than to deal with the unfortunate consequences of theft. As is often said, "An ounce of prevention … is in all likelihood worth several pounds of cure." There are many things your organization can do to help lessen this risk. Review your current business practices against these (as best fits your organization) to insure you have policies and procedures in place to guard against theft.

Steps you can take

Foster a positive work environment

A work environment where employees feel valued may cause them to think twice before engaging in dishonest work practices.

Create an atmosphere of zero tolerance

Create a code of conduct echoed by senior management that makes it clear that that fraudulent activity is not tolerated. Further heighten anti-theft awareness by implementing policies and procedures for all financial functions to prevent and deter employee theft. Communicate them regularly and enforce them with no exceptions. This practice of prevention is one of the most cost effective measures you can take and is significantly less expensive than trying to recoup employee theft losses.

Good hiring practices

Preventing employee theft starts with making smart hiring decisions and not to hire employees who have stolen previously. To do this, take ample time to conduct as many of the following checks as you can.

Screen potential employees

Generally speaking, avoid nepotism and do not hire the friends or relatives of your employees. Make sure that your job applicants aren't related to your staff before you hire them. This may undo checks and balances you have in place by allowing related employees too much access to your business assets.

Conduct background checks

Before hiring anyone, you should find out as much as you can about your candidate by conducting a background check. By doing this you can find out about their previous work experience, criminal history, and credit information. Be sure to use a reputable company to perform this service for you, usually at a nominal fee.

To do this, you must first receive the job candidate's written consent before obtaining certain information. Federal and state laws, including the Fair Credit Reporting Act, govern the collecting and use of information for pre-employment hiring decisions. You need to receive a signed authorization and release form from a job candidate to do a background check. You can usually get these forms from the company doing the background checks.

Drug Screening

Since people who are frequent drug users are often more disposed to fraud and theft, many organizations complete drug screening for job candidates and existing employees.

Check as many of the following as possible:

- **Contact the references**
  Many employers don't follow up with the references the job candidates provide. Many think that the applicant wouldn't provide a bad reference. Some candidates may list a respectable-sounding reference thinking you won't call them. And many incorrectly assume that the reference(s) they provide will provide a good reference. By calling the references, you have an opportunity to have a conversation about the candidate and learn more about them such as work ethic, personal opinion, their honesty, and trustworthiness along with their perceived strengths and weaknesses. Often checking references will provide you with a good initial "picture" of your potential employee.
- **Verify the information the job candidate provided**
  Your background check vendor can verify employment history along with education and any licensure indicated on the job candidate's employment application. It is not unusual for a candidate to "embellish" one of these or even claim they have possession of a certificate or license when actually one may have been rescinded due to a disciplinary action.
  It also may be a good idea to contact past employers yourself. Most won't do more than verify your candidate's dates of employment and job position but you can often identify their opinion of the employee by the tone in their voice. You may also want to ask the previous employer if your candidate would be eligible to be rehired.
- **Criminal History**
  Again, your background check vendor can look to find any criminal conviction records. There are a number of databases they can search to provide you with this information. Consult with your background check vendor to determine which data bases you want searched and how much information you will need based on the position being filled. These searches generally look for criminal convictions in federal, state and county records and can go back as many as 5 to 7 years to any of the applicant's previous county of residence and county of employment (if different).

Prevention strategies

The old saying that the person most likely to embezzle from your organization is a long-term accounting employee or a trusted colleague still holds true. The absence of opportunity can turn into trust in the workplace. All managers should let employees, supervisors and even executives know that all managers are tasked with seeking out any information regarding internal theft. Employees who believe they will be caught participating in theft and financial abuse may be less inclined to commit it. Increasing employees' belief that they will be caught may be your best theft prevention method. When supervision is lax, theft and fraud are more apt to occur. However, if you do let your employees know you have internal controls to quickly identify theft, then you greatly reduce your chances of eliminating employee theft.

Have proactive programs in place

Taking a proactive approach towards reducing employee fraud can be a most effective way to prevent internal theft. Some efforts will have minimal cost while others may require more of an investment, even though most of these deception prevention efforts will have a positive return on your investment. Other things you can do include:

Keep an eye on daily activities

There are a number of ways to keep an eye on daily activities:

- Have fingerprint readers to log into financial computers
- Use computer user tracking software
- Routinely back up computer records (at least daily)
- Do not allow the same employee who creates the financial records to back them up
- Make sure that you have all of the passwords to all of your computer systems
- Make sure no one can change any of these passwords and effectually lock you out

Employee education

Every proactive program should have a system in place to educate all levels of employees about financial fraud and embezzlement prevention. This can take on many forms and be included during new hire orientation, during regular department meetings, bulletin board postings and other routinely used communications methods. The objective is to have everyone be observant. The education should be positively focused and emphasize the organizations emphasis in legally

Create a separation of duties

Separate all of the functions related to bookkeeping and finances whenever possible:

- Run all receipts and disbursements through a checking account
  - Put any money that comes into your organization into checking accounts, and
  - Take any money that leaves your organization out of a checking account (This provides records of monies coming in and going out that cannot be altered because it is controlled by the bank.)
  - Have the bank account(s) reconciled at least monthly
- Have different employees assigned to receive checks and others to enter them into the accounting system.
- The person(s) who process checks should not be authorized to sign checks or to make electronic payments.
- Always use pre-numbered checks and require that amounts and payees be manually entered.
- Keep blank checks locked with restricted access.
- Have someone assigned to regularly (but unpredictably) review bank statements, cancelled checks and other statements such as company credit cards. Many perpetrators know when audits are coming and can alter or misplace records. Surprise checks can provide a significant deterrent.
- Books kept by one person should be reconciled by another staff member.
- Adopt a policy of escalating approval for expenses.
- To ensure there are no abnormalities, review online banking transactions frequently.
- Audit your books regularly. Use an unrelated third party to review your accounts and books on a regular basis. This can include spot checks and full reviews.

Require employees to take their vacation days and time off

An employee that refuses to let someone else do their job should raise some suspicions. All employees should be required to use their time off to refresh and renew. When they are off you have an opportunity to check what they have been doing to ensure accurate recordkeeping and to certify what they are doing is in accordance with your organizations policies and procedures.

Enforce regular work hours

Don't allow employees to take home financial work. This only opens unnecessary opportunities for fraudulent behavior.

Eliminate petty cash

Employees who embezzle often start with lesser amounts from a petty cash fund. If the employee believes they are able to do this without being caught, the amount they steal will often grow to a much larger amount. Eliminating petty cash does away with this initial cash influence.

Be observant

It is not uncommon for employees who embezzle from the company to use this money to make improvements in their lifestyle that would otherwise not be possible. This could include expensive clothing, high-end cars, lavish vacations and extravagant home improvements to mention a few. Managers should be trained to be on the lookout for these and other signs.

Establish a reporting system

Implement a system that encourages employees to make a report of any suspected theft. Every employee should know how to report suspicious, unethical or illegal behavior. Be sure that your system allows your employees to do this anonymously and without fear of recrimination for good faith reporting. This system could also include a confidential hotline for reporting criminal behavior.

Prosecute employee who steal

If your organization has been a victim of employee theft, prosecute the employee(s) involved. Your employees need to see the consequences for embezzling from your organization. Failure to prosecute sends the wrong message to everyone.

Have adequate insurance

Contact your insurance agent and review how much employee dishonesty insurance your organization has – and needs. This employee dishonesty coverage is designed to cover a number of employee acts of dishonesty including credit card fraud, forgery, unauthorized electronic transfers, alteration of records and counterfeit fraud to mention a few. Surprisingly, many organizations are underinsured in this area.

If you suspect embezzlement

If you suspect that embezzlement is occurring within your organization, contact an independent certified public accountant (CPA) to obtain an independent and neutral investigation and opinion about your suspicions.

If you have to tell any employee about this suspected theft to further along the investigation, be certain to tell them that this information is confidential and should not be shared. It is important that everyone involved in the investigation maintains the strictest confidentiality to avoid notifying the potential thief and potential character assassination claims. Any employees brought into this investigation should be warned that violating this confidentiality will also result in their employment termination.

When ready, interview the suspected employee last. Be certain to have a witness present. Ask for an explanation for the discrepancies you've uncovered. Never accuse an employee of stealing in front of anyone else as this could lead to a defamation lawsuit against you if your claim cannot be proven. It's a good practice to also have an independent CPA or fraud investigator present during your interview.

If you confirm that embezzlement has taken place, immediately suspend the employee. Don't give your employee an opportunity to come up with a false excuse, destroy evidence, cover-up what they have done or to take away incriminating information before being terminated. You do not want to give them an opportunity to fabricate some charge against you in order to coerce you into not reporting them to law enforcement.

Notify law enforcement officials right away if you are sure of your suspicions. Doing this sends a very strong message to your other employees about how serious you consider such a crime and your intentions to prosecute employee theft.

You may also want to consider contacting an attorney to review your claim to determine if any third parties may also have any responsibility in your loss. A liable third party might be an auditor or accountant who should have detected the theft beforehand, a bank teller that accepted a forged record or document or even other coconspirators of the embezzler.

Conclusion

No one wants to think that their organization will be the victim of employee theft but it happens frequently. Your organization will be better served by recognizing that it can indeed happen and taking proactive measures to minimize the threat.

Sources:

www.uschamber.com
www.asae-aon.com
www.entrepreneur.com
www.thehealthlawfirm.com
www.quickbooks.intuit.com
www.completecontroller.com
www.score.org
www.americanbar.org