Top 10 Ways Employees Steal From Their Employers

According to the Association of Certified Fraud Examiners, total business fraud in 2009 was $2.9 trillion dollars; small business, defined as less than 100 employees, accounted for 30% of all frauds or $870 billion dollars! The median loss at small businesses was $200 thousand dollars and was typically taken over a two or three year period. 82% of small to mid-size businesses report they have experienced employee theft. We all want to believe it can't happen to us, but with these numbers, the odds are very much against us.

The vast majority of employees are honest and hardworking. Unfortunately, it may only take one dishonest employee to put your business in serious trouble or even destroy it. The methods used are only limited by a dishonest employee's creativity. Don't assume you can "profile" an employee thief. Many frauds are perpetrated by long-term employees that no one ever thought could be involved in fraud.

One of my favorite fraud stories is about a parking lot outside Britain's Bristol Zoo. Allegedly, for 25 years, 7 days a week, approximately $500 was collected in parking fees every day. The attendant never took a day off and then one day he didn't show up for work. When the zoo called the city about a replacement, they were told he was not a city employee and the zoo was responsible. The zoo was shocked that the attendant was not a city employee because he certainly was not a zoo employee! At $500 a day, 7 days a week for 25 years, that equates to $4.6 million dollars! Although the veracity of this story has been challenged, the lesson to be learned rings true. Many times a fraud may be right under our nose and we may not see it! Be professionally skeptical, follow up on anomalies, and respect your instincts.

I think we can broadly characterize most employee fraud into 10 categories. If you know what broad types of fraud schemes exist and have some basic knowledge of internal control, perhaps it can help you prevent employee fraud at your company.

I'll provide the broad categories here and then briefly explore each of them in additional detail.

1. Help Yourself!
2. Fake Documents
3. Fake Vendors or Fake Employees
4. Misapplying Customer Remittances
5. Bribes, Bid-Rigging, and Kickbacks

6. Purchasing Goods for Personal Use with Company Funds
7. Data Manipulation
8. Fraudulent Expense Reports
9. Manipulate the Machines
10. Salami Fraud

Know that many controls are easy to establish while others may be too elaborate or expensive for your business. For smaller businesses, it's sometimes difficult to properly segregate duties for good internal control. Think hard about this because it's a major reason smaller businesses are hit so hard by employee fraud. Segregation of duties between employees having physical control of your assets and recordkeeping for those assets is absolutely critical.

Regardless of the amount of time and money you spend, you'll never be able to be completely fraud-proof your company. Having said that, employee theft is a crime of opportunity. If you take small, simple steps, you can create a healthier internal control system and help discourage employee fraud at your company.

Top 10 Ways Employees Steal From Their Employers

Method 1- Help Yourself!

Many times security and controls are so poor, employees simply walk out the door with your cash, inventory, or other assets. Ignoring fraud or denying it can happen at your company is foolish and is inviting loss.

Number one, establish physical access controls. Segregating and restricting access to high value inventory should be considered. If you have high value inventory, especially small items like jewelry, you should physically segregate it and lock it up. You should establish physical control and limit employee access to a small number of employees. Ideally you should set up the control so all employee access is through a card reader that logs time, place, and employees in and out. All inventory removed should be logged with time, purpose, requisition and job/order number and requisitioning employee. Limiting access to inventory will reduce loss potential, both in terms of theft occurrence and severity.

Is your facility protected with card keys? This technology is relatively cheap and can tell you exactly who went where and when. If all employees do not need access to all areas of your facility, the system can be set up on a need to access basis. Can you control regular building egress so that employees will all have to leave at one exit which can be monitored, as opposed to employees “going out the back door?”

By the way, a favorite trick of dishonest employees is to take inventory out the back door and put it in the dumpster for retrieval after hours. To foil this, it doesn’t take much effort to simply lock the dumpster at the end of every day.

Do you take a physical inventory annually? Large inventory shrink may be a sign of employee theft. Unexplained empty boxes in the warehouses?

Periodic inventory cycle counts may also help uncover problems. Cycle counts are simply counting a portion of the inventory on a rolling basis. Don’t publicize a schedule in advance but conduct the counts regularly and try to count it all at least once a year.

When was the last time you did a fixed asset inventory? Do you know what you currently have? Have the fixed assets been tagged or otherwise identified as

company property? Do you have procedures for disposal of excess or obsolete fixed assets? All fixed asset disposals or sales should require appropriate documentation and approval. Accounting should get notification so they can adjust the records. They can also compute a gain or loss on disposal which should be known in advance of the sale or disposal.

If you utilize anti-theft tags, think about who has access to the tools which can remove the tags. Again, a simple roadblock that may discourage a casual theft.

With today's technology, it's easy and inexpensive to put in cameras in key locations at your facilities. This should not only help reduce employee theft but increase facility security and help protect your employees.

Can your office employees walk out the door with your cash? What are your check signing procedures? For a smaller company, perhaps the owner/CEO signs all the checks. This may provide some protection but it's hardly fool-proof. Larger companies may utilize check signing machines which afford some protection as long as the signing meter is controlled and logged. In no event should you permit employees to utilize rubber stamps to sign checks.

In accounts payable, once the checks are signed, they should be mailed out directly to the payee and not be returned to the check requisitioner. Consider having your accounts payable checks taken directly to the post office. I once worked at a company which gave the outgoing checks to the mailman as he delivered the incoming mail. Unfortunately, the mailman had itchy fingers and stole some of the checks, altered them for his own benefit and then cashed them. After that episode, one designated employee hand carried the checks directly to the post office every day.

Can an employee write themselves a check and cover it up by making fictitious accounting entries? Know that banks can't be counted on to authenticate check signatures. You need to set up job responsibilities such that the person having custody of an asset also does not have recordkeeping responsibility.

Smaller companies should consider having bank and credit card statements sent directly to the business owner's home address. This may help internal control if the owner scrutinizes the spending each month before doing the bank reconciliation. Are bank reconciliations done promptly and reviewed?

For petty cash, utilize an imprest system. Keep the cash under lock and key and make one employee responsible. When the funds needs to be replenished, the cashier should produce receipts to substantiate the fund replenishment and so accounting can make the appropriate journal entries.

Diamond Graphics, a Minneapolis company, was recently bilked out of $1.9 million dollars by their accountant. Apparently he was able to divert accounts payable checks intended for certain vendors to his personal bank account. Because he had control of the books and the checks, he was able to conceal the fraud for years by making fictitious accounting entries.

Ask Callan Western Sales, a Los Alamitos, California sporting goods store, if separation of duties is a good idea. Authorities say that a clerk there was given access to company checks and on-line bank accounts and stole $400,000. The indictment alleges that the clerk attempted to cover her theft by altering records and intercepting company credit card statements. Authorities say that financial pressures forced the family owned company to close in 2007. The owners didn't notice the fraud until after the business was forced to close.

Who's watching your accountants?

Top 10 Ways Employees Steal From Their Employers

Method 2- Fake Documents

This is one area where technology can work against you. Even an employee with low technology skills can easily get a printer and create fake documents which could fool an expert. Document falsification typically may include checks with altered payees or amounts, fake voided checks, fake or duplicate purchase orders, invoices, receiving documents, or altered time cards.

Your internal control needs to be developed with a good understanding of your work flow and processes.

One technique that can help you enhance accounts payable internal control is a "three way match." This refers to matching an invoice with a receiving document and a purchase order before an item is paid in accounts payable. The more documents that need to be forged, the lower the probability.

Most banks offer "Positive-Pay" checking accounts. Basically when you run your payables you transmit a control file to your bank with check numbers, payees, and amounts. As the checks clear, the bank matches the clearing checks to your control file. If an amount or payee does not match, you are immediately notified and you may elect to pay or bounce the check.

Unique form numbering schemes may make documents tougher to falsify and easier to spot fraudulent documents.

Accounts payable should only pay from an original invoice with an original authorizing signature of the person approving the payment. Again, once checks are signed, they should be mailed out directly and not returned to the check requestor.

Duplicate payments may be a sign of fraud. Your accounts payable system may be able to automatically check for potential duplicate payments by comparing invoice numbers, vendors, amounts, and purchase orders. You should scan the payment register and look for document number sequences that don't look right. There are companies that will come in and do an accounts payable audit to check for duplicate payments. Many of these audits are priced on a contingency basis and you may only have to pay for the audit if they detect and recover duplicate payments.

Sales return documents, voided sale documents, and credit/discount documents may be falsified to steal money from your company. For example, an employee may record a sales return for a return that never happened. If your system is not properly controlled, the employee could then direct the refund into their own pocket. You need to make sure you have proper segregation of duties to prevent this.

A former accountant at Ikea issued himself refunds for purchases made by customers. In less than one year he was able to steal $400,000. Basic return controls could have prevented this fraud. Refunds should not be processed until returned goods are received back in the warehouse.

Analysis of spending variances to budget and prior year can help root out fraud. In addition, a regular analysis of all balance sheet accounts may help detect fraud, if not deter it. If employees know that accounts are regularly analyzed and variances and anomalies are investigated, they may be discouraged from perpetrating a fraud.

Always analyze your processes and methodologies with a keen eye toward segregation of duties. The general rule is that asset custody (cash, checks, inventory, and other assets) and recordkeeping for those assets should always be done by different people.

Top 10 Ways Employees Steal From Their Employers

Method 3- Fake Vendors or Fake Employees

Many frauds are based upon setting up fake employees or fake vendors with an unscrupulous employee pocketing the payments made to them.

Who controls your accounts payable vendor master file? What are the policies and procedures to set up a new vendor? Again, think about separation of duties. No one person should be able to set up a new vendor, approve a payment to that vendor, and conceal it by making fictitious accounting entries.

Many fake vendor schemes utilize a variation of the name of a common, well known vendor. For example, instead of "Common Vendor, Inc.," an unscrupulous employee may set up a vendor called "Common Vendor" and it likely would not arouse any suspicion. If a fraudster can establish a fake vendor and direct payments to that vendor, they may be able to then pocket the money without anyone noticing in the absence of other internal controls. A simple review of the vendor master file would show two nearly identical vendors which should then be investigated. That's not to say it's clearly an indication of fraud, but it may be.

A former Quest Diagnostic manager was able to steal $1.2 million dollars by setting up fake companies, fake invoices, and fraudulent expense reports. He was caught during a review of the accounts payable system when someone became suspicious of some fake vendor names the perpetrator had established. When they investigated the suspicious vendors, they found that the addresses did not match the name. Be wary of vendors that do not have a physical address. If you're really sharp, a quick look at Google Maps may substantiate that the new vendor exists and resides where they claim to. Other business directory searches may further substantiate whether the business is legitimate or not. Some thieves may go to extraordinary lengths so you may even want to make sure the owner of the company isn't one of your employees!

What are your procedures for establishing new employees? How are checks or pay receipts distributed? Paychecks or pay receipts should not be distributed by the same person that controls the employee master file and/or runs the payroll! If an independent person distributes the checks or pay receipts and has an extra check left over, then the "ghost employee" scam may be caught and stopped. Again for both fake vendors or

fake employees fraud schemes, analysis of your spending to budget and prior year may help prevent or detect this type of fraud.

Top 10 Ways Employees Steal From Their Employers

Method 4- Misapplying Customer Remittances

Think of this type of scheme as robbing Peter to pay Paul. Or think of it as the employee/company version of the classic investment Ponzi scheme. It basically involves deliberately mis-applying customer receipts in an attempt to disguise missing money. A classic case is to steal customer A's remittance and then apply Customer B's remittance to A's account, apply Customer C's remittance to customer B, etc. (AKA, check lapping).

An employee of CCU Associates embezzled $1.3 million dollars over a 25 year period through a lapping scheme. He was caught and is currently serving a 15 year prison term.

An administrative assistant at Beverly Hospital stole $230,000 from Sodexo, a hospital vendor through a lapping scheme. The scheme unraveled when the hospital decided to change vendors. As Sodexo was working through the final payments due them, they discovered there were many invoices they showed unpaid which the hospital claimed had been paid. When the checks were traced, the fraud was discovered.

Although lapping is a common fraud technique, it is rather clumsy and may be easier to detect than some other frauds. Require all employees to take vacation or make sure you have mandatory and periodic job rotation. This type of fraud requires high maintenance and when the perpetrator is absent, it may quickly unravel and be discovered.

You should also segregate recordkeeping and opening of mail containing customer remittances. At a minimum, one employee, with no other recordkeeping responsibilities, should open all the mail and make the bank deposit. In most companies there is no reason that the accounts receivable person needs the live check. If they really must have the check, have the other person make them a copy. You cannot mix recordkeeping and asset custody in one person! If you have enough incoming check volume, consider a bank lockbox. The bank will open your mail, deposit the checks and then send remittance data to your accounts receivable staff to update your records. As an added benefit, a lockbox will generally speed up the availability of your cash.