

Identifying and Preventing Fraud

A Practical Approach to Protecting Your Organization

Many executives believe fraud simply cannot happen in their organization. They have seemingly “good and honest” employees that have been with the organization for many years and have the latest in financial accounting software. Nonetheless, it *is* possible theft may be occurring. Sometimes people are forced by their situation or tempted by an opportunity that has developed to take advantage of the circumstances. A one-time small theft is not that damaging, but a recurring effort or a major breach can be catastrophic.

Unfortunately, fraud is not an isolated incident. It occurs more often than it is caught and the offenders are often people you would least expect. Some “interesting” fraud facts note that:

1. **86%** of identified fraud occurs in organizations that lacked internal controls or did not follow or test them with any frequency.
2. **39%** of fraud occurs in organizations with less than 100 employees.
3. **12 months** or longer is the average length theft occurs.
4. **71%** of cash fraud incidents involve fraudulent disbursement of company checks.
5. **\$500,000** is the median fraud loss per scheme when collusion between an employee and manager are involved.

Review Key Areas to Identify “Red Flags”.

Below is a list of potential warning signs. If these conditions exist, it does not *necessarily* mean illegal activities are occurring, but they are indicators something could be wrong. If you find any of these conditions in your organization, it should make you feel uncomfortable. At a minimum, implement steps to reduce the potential for future theft. If some of these conditions exist and your business has not been producing the profits you felt it should, you may want to consider a fraud audit. Some of the signs are:

1. **Sloppy bookkeeping.** This should be a big red flag. Either it is a sign of possible theft or a poorly run department.
2. **No cash receipts.** If cash receipts are part of the operations but deposits do not reflect any cash or minimal cash, then a problem does exist.
3. **Lack of timely deposits.** All receipts should be required to be deposited daily. This control is critical in preventing “lapping schemes” where future receipts are used to cover current deposit shortages. Without daily deposit requirements, checks for the next day may be substituted for the cash that was pocketed. As months pass, journal entries may be made to correct any imbalances and the theft can go undetected.
4. **Summarized totals.** Totals without supporting details should be investigated. Summarized receipts look nice and clean, but they create the opportunity to “pocket” cash by not having to account for each transaction. The detail should include cash and checks received separately in each remittance. An individual independent of the

- collection process should verify the cash and check that daily deposit amounts are in agreement with the underlying detail.
5. **Customer calls.** If a customer calls asking why their check has not been cashed or reports that they paid in cash but are getting collection notices, those are clues that something is wrong.
 6. **Lack of “separation of duties”.** Unless you are the owner, the same person should not deposit the receipts, pay bills, reconcile accounts, and keep the books. It puts too much responsibility on one employee and too much trust in their behavior.
 7. **Changes in balances.** If general ledger balances are historically consistent but a certain account balance shows significant changes, then it is worth investigating.
 8. **Journal entries.** Although they are part of the accounting process, their frequent use to correct imbalances or adjust the same accounts should be reviewed.
 9. **Not enough management attention.** This creates the opportunity for theft. Management’s performance of random checks (even if minimal) will deter some people from taking the risk.

What is the Profile of Someone Who Commits Fraud?

Who is more likely to be the person to steal from an organization? The young unskilled worker, the church-going father of three, the single office manager or the “trusted employee”? All are prime suspects given the right opportunity, access, personal convictions, and current financial situation. The truth is you cannot tell which employee is likely to commit fraud. Even “good” people make poor decisions if they are in a trusted position and perceive an *opportunity*, feel financial *pressure* or can *rationalize* their actions. Some steal because of a health issue that is creating mounting debt, while others suffer from an intensive addiction to drugs, alcohol, shopping or gambling. Whatever the reason, anyone may be capable of this behavior in the proper situation.

There are plenty of ways people justify “taking a little extra”. Theft can be as simple as coming in late and going home early. Everyone feels underpaid, so cutting a few corners makes it seem less painful. An employee may leave early to reduce the commute time or take excessive sick days. Thirty minutes a day at a fully loaded cost of twenty dollars an hour is a loss of \$2,500 a year. In a business with fifty employees, the loss potential could be \$125,000 annually or the equivalent of two to three people.

Fraud is not limited to employee theft. There are other types of losses to consider. For example, a cashier may allow friends access to a park district or theater event without paying admission. Was a loss really incurred if these same people would not have attended had they been required to pay the admission? When a physical product is not involved, potential losses related to service dollars are harder to comprehend. If a retail employee observes a shoplifter but does not report or try to stop it, does that constitute a fraudulent act? A policy may exist requiring employees to report shoplifting but enforcement may be lax.

How Can You Implement an Effective Prevention Program?

One method of defusing theft is a random monitoring policy. A thorough and objective policy can be promoted to employees as a focus on job protection and creation of a safe and healthy work environment. Everyone should understand that monitoring of controls and processes does not constitute a personal accusation on any one individual. Any employee's activities and duties may be subject to random monitoring as part of the overall ongoing evaluation of system controls to maintain internal strength and balance. In today's environment, most employees welcome efforts to create a safer, more stable work environment.

There is always someone smart enough to defraud the organization. With just a little thought and planning any employee can attempt to divert funds, steal supplies or merchandise, "pad" expense accounts, and create fictitious invoicing and billing schemes. Ongoing monitoring and evaluation of a well-developed system of internal controls can be extremely effective in reducing the risk of fraud. You may increase your chances of identifying fraud sooner and even deter individuals from attempting fraudulent activity.

Not sure how to get started? If your organization has not addressed internal control issues or you feel you do not have the in-house skills to evaluate your systems, please call us. We can review your overall control environment and provide written recommendations that are appropriate for you.

Written by Tom Ahlbeck, CPA and Principal at Ahlbeck & Company 847.824.4000.