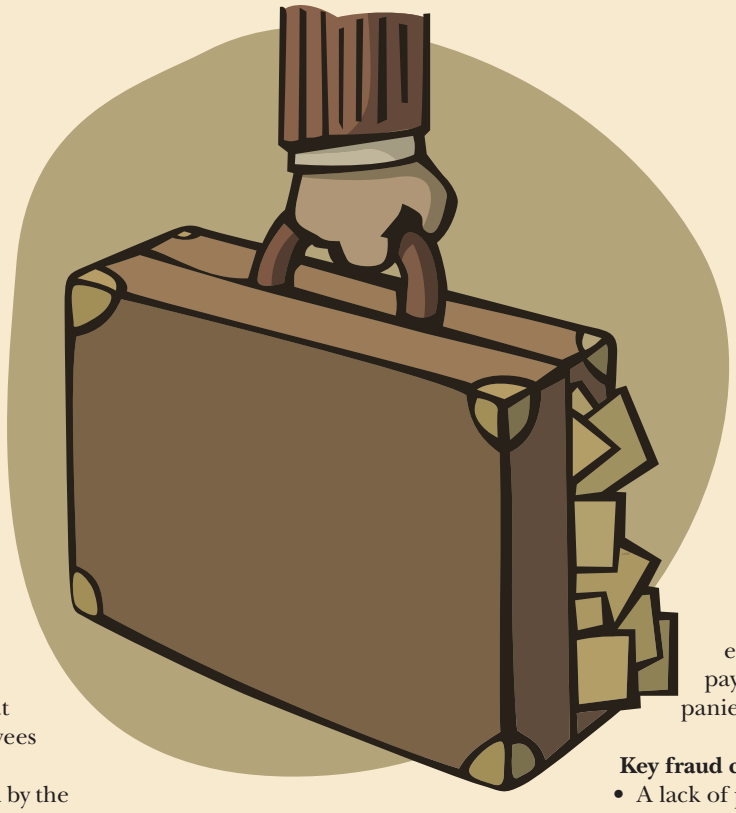
OCCUPATIONAL FRAUD & ABUSE

A CLEAR AND PRESENT DANGER TO YOUR BUSINESS

Brian Mohlenhoff, CPA, CFF and George Uhl, CPA, CFE, CFF MDD Forensic Accountants



The U.S. Chamber of Commerce estimates that occupational fraud costs U.S. businesses more than $50 billion annually and that one-third of business failures are directly related to employee theft. The Chamber also estimates that 75% of all employees have stolen from their employers at least once and half of these employees have stolen repeatedly.

Statistics from a study conducted by the Association of Certified Fraud Examiners[1] show that no company is immune to occupational fraud and that the cost of fraud is significant. Companies that do not have good internal controls in place are losses waiting to happen, while companies that already have controls in place need to assess them periodically to assure they continue to minimize the risk of fraud.

Occupational Fraud generally falls into the following three categories:

Asset misappropriation schemes are the most common form of fraud, accounting for 87% of fraud cases; however they also have the lowest loss amounts.

Corruption schemes occur when an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer.

Financial statement fraud schemes take place when an employee intentionally causes a misstatement or omission of material information in the organization's financial reports.

The following cases are actual examples of occupational fraud. The companies range in size from twenty to more than 500 employees. In each case, their management never thought they would be a victim of fraud, and therefore, never saw a need to review or assess internal controls. They all thought fraud was something that happened to "other companies."

DURATION OF FRAUD: 18 MONTHS
COST TO COMPANY: $300,000

A manager at a tire company distributed paychecks to his employees on a weekly basis. The manager received the paychecks each week from the payroll service company and then passed them out to employees. After another employee noticed that the manager locked his door for a few minutes every time the payroll checks were received, she became suspicious and reported this to her manager. The company ultimately discovered that several former employees were still receiving paychecks, some of whom had left the company years ago. To facilitate the fraud, the perpetrator used his access to edit payroll records and passwords to falsify hours and thus, paychecks, for previous employees. He then took the paychecks to check cashing companies to redeem them.

Key fraud contributors:

- A lack of proper internal controls
- Not observing proper separation of duties
- Not regularly monitoring payroll records for ghost employees
- Not requiring that employees regularly change system passwords
- Allowing the manager who passed out checks to accept them from the payroll service company
- No fraud hotline for employees to report suspicious behavior

DURATION OF FRAUD: 4 YEARS
COST TO COMPANY: $215,000

A 10-year accounting clerk working for a supplier to the automotive industry was in charge of preparing checks for vendor payments. After several years on the job and added responsibilities, which included the ability to make entries in the company's general ledger, she began to issue checks to herself and forge the authorized signatures. To conceal the fraud, she recorded the fraudulent checks as Use Tax in the ledger and noted the payee as "Confidential Vendor."

Key fraud contributors:

- No procedures in place to review cancelled checks and verify that the vendor listed in the accounting system matched the vendor on the check
- No review to ensure proper support for all disbursements
- No sequential review of checks to assure that all checks were accounted for was conducted by a manager prior to the checks being issued

DURATION OF FRAUD: 1 YEAR
COST TO COMPANY: $115,000

A newly promoted controller at a printing company was in charge of overseeing all accounting functions and reported directly to the CEO. As part of his responsibilities, the controller was made a signatory for company issued checks. To commit the fraud, the controller established a bank account for a fictitious company and then began issuing company checks to the fictitious vendor. Although one of the company's controls was to require two signatories on all checks, the second signatory was a subordinate of the controller, and the subordinate employee was directed to sign the checks even though they lacked proper documentation. Additionally, rather than setting up a separate vendor account for the fictitious vendor, the controller made the payments under various existing vendor accounts. The fraud was ultimately discovered when one of the customers received a statement showing several payments made by the printing company to the fictitious company under this customer account.

Key fraud contributors:

- Too much responsibility given to the controller
- The second signatory was a subordinate of the controller
- Lack of formal communication channels to report potential fraud
- No secondary review by another employee to assure all payments were properly documented

As you can see, fraud is not limited to a specific industry, company or employee. It is far reaching and impacts all types of organizations, regardless of whether they are large or small, public or private, for profit or not-for-profit. Furthermore, due to limited resources, statistics show that smaller companies may be at a higher risk for fraud. Below are some steps that any organization can implement to help them keep their resources safe.

CREATE A SEPARATION OF DUTIES

While a smaller firm may have a more difficult time with these procedures, owner involvement in the process is a good alternative. A larger firm should be able to easily implement internal control procedures. A good place to begin is organizing the firm's banking responsibilities so that all invoices for services are issued out of one office by a billing person, with all cash collections and deposits being handled by another office. Additionally, all money received is sent and deposited in a different office from where invoices are issued or where the bills are paid. Finally, the monthly bank account reconciliation is performed in a third office. While performing the bank reconciliation, part of this process is verifying the checks that have cleared the bank have been posted to the ledger account. If a check does not appear on the ledger, this should be investigated so the amount can be posted and to verify it was not a fraudulent check.

UTILIZE AN "EXPERT FEE FUND"

Very similar to the attorney Trust Account, this is where a firm is asked to disburse funds on behalf of insurance carriers and review and pay expert fee invoices for a particular case. As these assignments have increased in quantity, we have worked on implementing ways to prevent theft as employees and partners have the ability to disburse funds. Some general protocols for protection of the funds in these types of accounts include:

- Two partners should act as signors; employees should not have check signing privileges.
- Partners need to review all requests for payments, including copies of invoices, etc.
- A partner should reconcile the account to review for "additional" checks or amounts and check that seem "out of place." Taking it one step further, a partner not overseeing or signing the checks for disbursements should perform the reconciling function.
- A documentation audit should be performed periodically to verify proper substantiation has been received for disbursements.

Additionally, to prevent the creation of "ghost employees," make sure that the payroll functions are each performed in a different office or by a different employee. An additional review should be conducted by a partner.

STOP EXPENSE ACCOUNT ABUSE

To ensure employees don't take advantage of their expense accounts, operate with a corporate American Express card; all corporate charges are billed to a master account that is paid directly by the firm. Each month, all expenses should be reconciled. If an expense is not reported on an expense account, the employee should be questioned and the expense accounted for.

On a quarterly basis, review the expenses by scanning the entries and look for any out-of-the-ordinary charges or vendors and investigate. These extra steps should be taken so that certain employees will think twice before acting.

CONSIDER USING OUTSIDE RESOURCES

A firm can engage an outside professional accountant to interview the employees who handle the above tasks, review the internal controls you have in place and recommend changes to the controls based on your individual business, staff levels, operations and degree of owner involvement. They will be able to provide an outsider's view and comments on your procedures in place, as well as judge the employee's responses to questions regarding their duties. Also, a firm can have a partner or owner do a high-level review of the monthly financial statements, checking for anything out of the ordinary.

Remember: a few simple procedures and some extra time can go a long way in ensuring a firm does not become a victim of fraud.

Brian Mohlenhoff is a CPA and Partner in MDD's Parsippany, N.J., office. He also holds the Certified in Financial Forensics designation. His forensic accounting acumen has been utilized by businesses ranging from sole proprietorships to Fortune 500 entities. He has served as both a fact and expert witness in several litigation cases.

George Uhl is a CPA and Partner in MDD's Dallas, Texas, office. He also holds the Certified Fraud Examiner and Certified in Financial Forensics designations. He has provided his expertise on a number of litigation cases and has served as both a fact and expert witness. He has testified in support of his findings and also on opposing expert findings.

[1] The Association of Certified Fraud Examiners' "2012 Report to the Nations on Occupational Fraud and Abuse"