How to Protect Your Business from Corporate Fraud

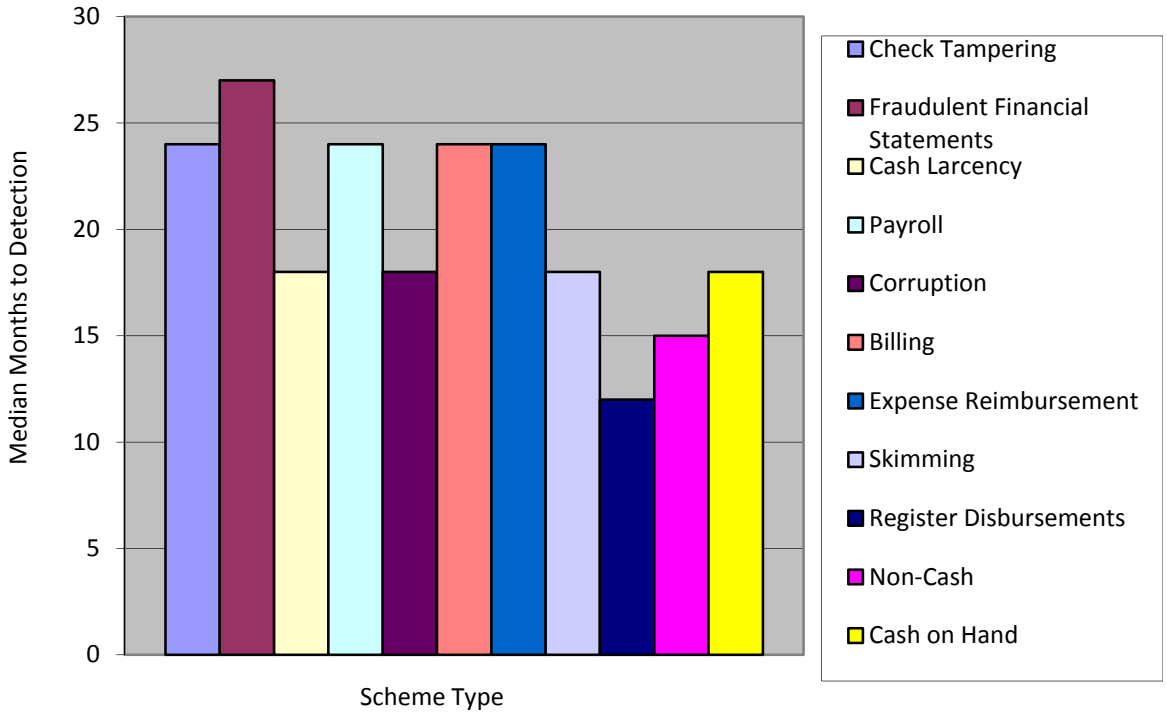
By Joel Charkatz, CPA, CVA, CFE

Fraud in the workplace is a serious problem for all organizations; most common thefts involve cash. Most fraud is ongoing with the average length of the crime being 18 months from inception to discovery. Studies indicate fraud is committed most often by well-educated professionals in senior positions and is affected by conditions within the organization. While a system of internal controls can certainly deter fraud from occurring it does not always prevent it entirely.

In a report to the Nations on Occupational Fraud & Abuse, it was found that:

- There were 1,388 cases investigated in 100 countries with 43% of the cases found in the U.S.
- Certified Fraud Examiners estimate $3.5 Trillion global annual fraud losses.
- The median loss is $140,000.
- Small businesses average losses of $200,000.
- Large companies average losses of $127,000.
- An average of 5% of annual revenues are estimated to be lost to fraudulent activity.
- 20% of investigated fraud in the report caused at least $1 million losses.
- 22% of fraud is committed by accounting department personnel.
- 12% of fraud is committed by upper management/executives.
- Twice as many males vs. females commit fraud.
- 87% of fraudsters are never charged or convicted.

Median Duration of Fraud Based on Scheme Type



The industries most commonly victimized by fraud include but are not limited to; financial services (17%), government services (10%), manufacturing (10%) and healthcare services (7%). The industries with the largest median losses from fraud are mining ($500,000), real estate ($375,000), banking ($232,000), manufacturing ($200,000) and insurance ($216,000).

The profile of a typical perpetrator usually falls into one or a few of the following categories:

- 1-5 years with the company (46%)
- 6-10 years with the company (27%)
- Know the company very well
- Possible personal problem with debt, drugs and/or gambling
- Have the access and opportunity
- Violates their fiduciary responsibility to the company

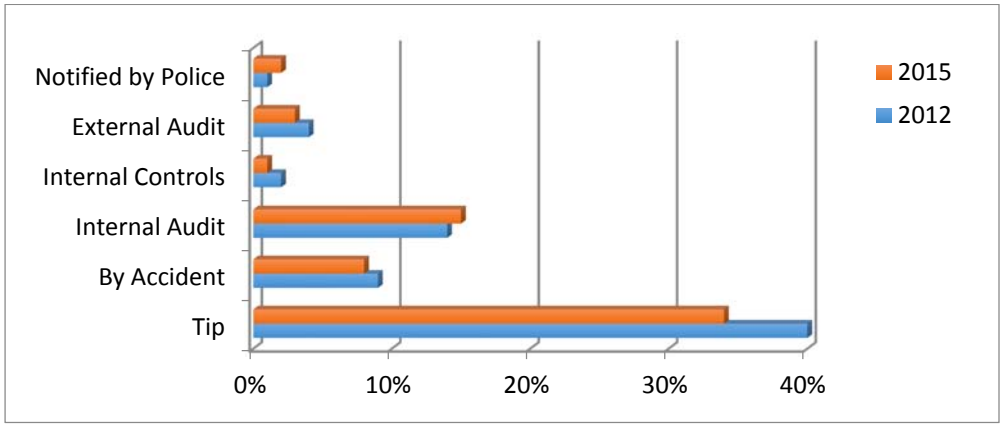
Opportunity + Motive = FRAUD

Organizational Vulnerability

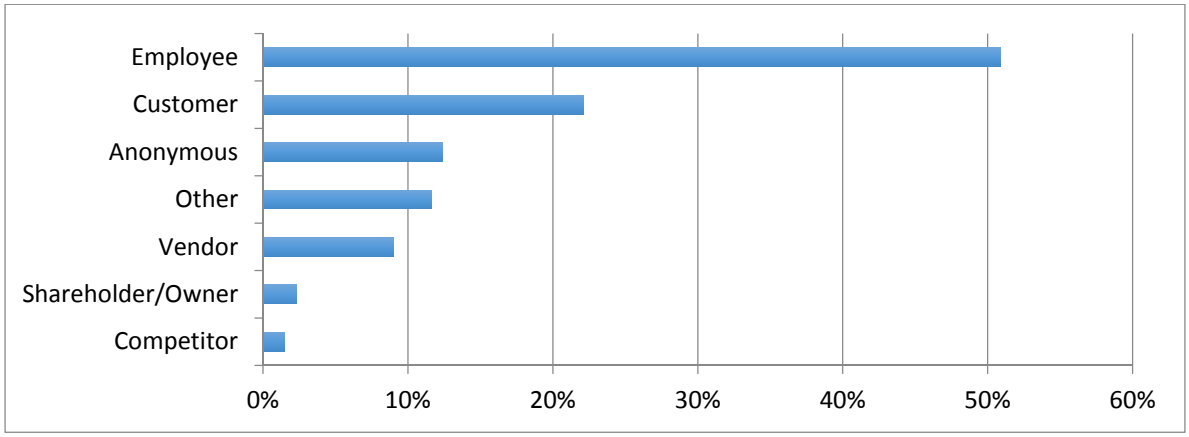
In fraud cases found within the workplace, there are almost always existing vulnerabilities that the business owner may not recognize.

- Small businesses typically have a lack of or poor internal controls.
- There are insufficient management procedures and oversight.
- One employee is handling the entire process (i.e. Accounts Receivable).
- No conflict of interest policy in place.
- Lack of checks and balances in place.
- Approval of own expense reports.

Type of Detection



Source of Tips

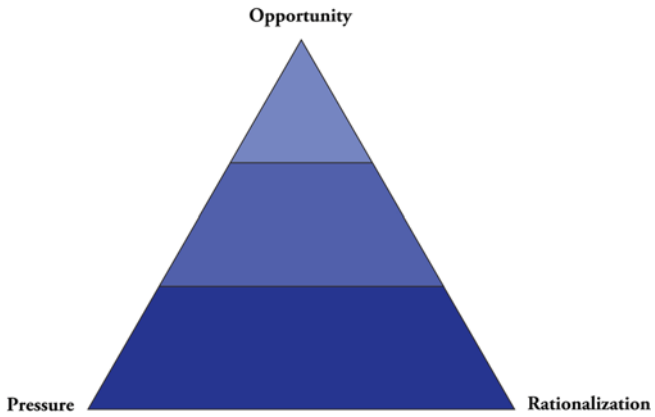


To help you detect if fraud may be present in your organization, there are general warning signs to look out for, that include:

- The general ledger does not balance (usually not an issue in today's computerized world).
- An employee is living beyond their means.

- Accounts payable sub-ledger does not reconcile with the general ledger (again, not a common issue today).
- There are excessive write-offs of accounts receivable.
- Unexplained cash discrepancies exist.
- Increased accounts receivable in comparison to sales.
- Postings to customer accounts are delayed.
- Employee is duplicating submissions.
- Altered or forged deposit slips are discovered.
- Customers are complaining about billing.
- There is a rise in "soft" costs (i.e. advertising or consulting fees).
- Vendor contact information matches the employee's address.
- Checks are voided, destroyed or missing.
- There is a delay in posting accounts receivable payments.

Fraud Triangle



Types of Fraud

Fraud exists across multiple platforms in many ways. Common types of fraud include skimming, larceny, check tampering schemes, expense account schemes, credit card fraud and financial statement fraud. We will explore each instance and what to look out for here.

Skimming

Skimming is the removal of cash prior to its entry into the accounting systems. It is the most common form of fraud with a median loss of $50,000. Cash is targeted in 90% of these schemes. It is performed at the time of service through falsification of receipts and/or tampering with deposits.

Larceny

Larceny is the theft of cash after entry into the accounting system. It is also known as bookkeeping fraud. There is typically a median loss of $22,000. It involves altering deposit slips after the deposit, fraudulent payments to vendors and/or check tampering.

Check Tampering Schemes

Common check tampering schemes can involves one or multiple of the following instances:

- Forged maker: signature of authorized signer is forged
- Forged endorsement: check for third-party stolen and endorsed to legitimate payee for conversion to perpetrator
- Altered payee: alters check so that it is payable to the perpetrator
- Authorized maker: authorized signer makes check payable to self for personal purposes

Some red flags to look out for in check tampering schemes could be:

- Canceled check amount does not match books
- Missing checks
- Checks payable to employees
- Altered endorsements
- Altered payees
- Checks out of sequence
- Questionable deposit dates
- Unaccounted for cash advances

Expense Account Schemes

There are four methods in which an expense account scheme could be performed:

- Mischaracterized Expenses: legitimate receipts for non-business expenses
- Overstated Expense Reports: inflated amounts for actual expenses and keeping the difference
- Fictitious Expenses: Creation of phony documentation
- Multiple Reimbursements: Submitting expenses more than once

Credit Card Fraud

Credit card fraud is when the corporate credit card is being used inappropriately to steal goods or services from the company. This is most commonly committed by the bookkeeper or another with card access to make unauthorized purchases for personal use.

Financial Statement Fraud

Financial statement fraud is the deliberate misrepresentation of the financial condition through misstatement or omission. This involves overstating assets, revenues and profits and understating liabilities, expenses and losses.

Falsifying financial statements are not always for personal gain. It can assist the fraudster in boosting stock sales, demonstrate earnings per share, meet lender requirements and inflate purchase price for acquisitions. It also can hide the inability to generate cash flow and meet company goals and objectives. Some fraudsters use it as a way to fraudulently win performance-related bonuses.

The opportunity for financial statement fraud exists when there is:

- An absence of oversight by the Board of Directors or audit committee,

- Neglectful behavior of the Board of Directors or audit committee,
- Weak or nonexistent internal controls,
- Unusual and/or complex transactions, or
- Financial estimates that require SUBJECTIVE judgment by management.

Financial statement fraud can be identified as there are always two accounts affected and therefore two categories on the financial statements. It is very common to have fraud involve several methods. There are five classifications of financial statement fraud; fictitious revenues, timing differences, improper asset valuations, concealed liabilities/expenses, and improper expenses.

Some red flags to be aware of in financial statement fraud cases include:

- Management compensation closely tied to company's value
- Management dominated by one person or very few
- Management shows disregard for controls and policies
- Unrealistic financial goals
- Past history of illegal conduct by management

Prevention or Deterrence?

What type of measure are you taking to prevent or deter employee theft from occurring?

Prevention removes the root cause of the problem. While deterrence modifies behavior through threat of sanctions and consequences. Implementing perception of detection is when those who perceive they will be caught committing fraud are less likely to engage in it.'

Internal Controls are key to protecting from fraud. Employee education of internal controls helps to communicate enforceable policies and procedures within your business. The policies and procedures should also be reasonable across all personnel. In addition, you can have internal and external audits performed to gauge where you rank. Employee background investigations can help mitigate risks of hiring someone who may steal. Also, be sure to implement a clear delegation of duties. And provide opportunities for employees to bond to build employee commitment and enthusiasm within your company.

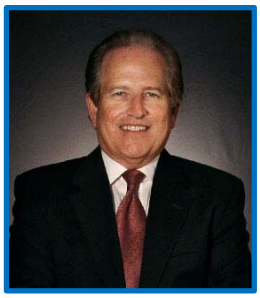
Statistics show that initial fraud detection happens commonly in one or more of the following ways

- Accident: 80%
- Tip 43%
- Internal Controls: 37%
- Internal Audit: 15%
- External Audit: 4%

In order to assist in preventing and diagnosing workplace fraud cases, here are 11 Tips for Preventing Fraud:

1. Have a Fraud Assessment conducted
2. Develop a written code of ethics

3. Lead by example
4. Establish reasonable expectations
5. Treat employees well
6. Restrict access to bank accounts
7. Regular bank reconciliations
8. Secure inventory and supplies
9. Prescreen applicants
10. Provide mechanism for reporting fraud
11. Use a Fraud Hotline



Joel Charkatz, CPA, CVA, CFE is a Shareholder with KatzAbosch, Joel has served the Maryland business community for more than 40 years. He is Chairperson of the firm's Business Valuation/Litigation Support and Forensics Group and is a member of the Medical Practice Services Group.

For any questions, please contact Joel at jcharkatz@katzabosch.com or 410-307-6400.