



Occupational Fraud

What every company needs to know
to prevent and detect fraud.



Every organization is at risk of experiencing fraud - in particular, small businesses with less than 100 employees are especially vulnerable to occupational fraud. On average, a typical organization loses 5% of its annual revenues to occupational fraud.

Most of the fraud occurring in businesses goes undetected anywhere from 17 months to 30 months depending on the type of fraud being committed. Your company should have the tools and knowledge to beat fraud before it drains your company of hard-earned and valuable resources.

This Sensiba San Filippo InfoCast™ outlines the basics on how to identify, detect and prevent fraud in your organization, as well as what you should do if fraud is found.





What is occupational fraud?

Occupational fraud is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources.

This definition encompasses an extensive range of potential frauds committed by employees, managers or executives. Occupational fraud can be as simple as an employee stealing a tool or as sophisticated as financial statement fraud.

Unfortunately, no company is immune to fraud.

Companies of all sizes, types, locations and industries are affected. The manufacturing industry has been one of the hardest hit in recent years, with the largest median losses.

THE THREE MOST COMMON TYPES OF FRAUD ARE:

- Asset misappropriation: schemes in which the perpetrator steals or misuses an organization's resources, e.g. false invoicing, payroll, check tampering, billing, expense reimbursements and skimming (cash is stolen before it is recorded).
- Corruption: schemes in which fraudsters use their influence in business transactions in a way that violates their duty to their employers in order to obtain a benefit for themselves or someone else, e.g. employees might receive or offer bribes, extort funds from third parties or engage in transactions that present conflicts of interest.

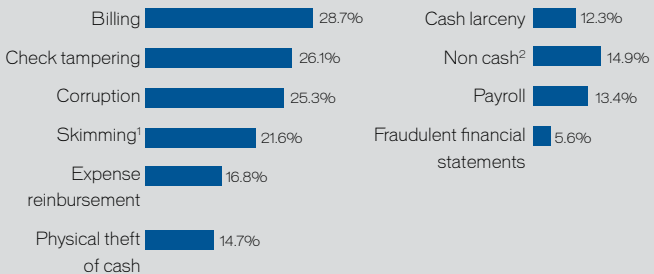


- Financial statement fraud: perpetrator intentionally misstates or omits material information from the organization’s financial reports, e.g. reporting of fictitious revenues or expenses, or the concealment of revenues or expenses in order to make an organization appear more profitable or conversely, less profitable to evade taxes.



Money Issues

Frequency of various employee fraud schemes at companies with fewer than 100 workers



¹Theft of cash before it's recorded in the books.

²Theft of equipment, merchandise, inventory or data

Note: From a survey based on data compiled from 959 cases of occupational fraud investigated between January 2006 and February 2008. The survey included 342 companies with fewer than 100 employees.

Source: Association of Certified Fraud Examiners



Detection of Fraud

Many business owners believe that if fraud is occurring in their business it will be readily apparent and quickly identified. The reality is that the accidental detection of fraud is very unlikely. Current fraud research indicates that small privately-held businesses discover fraud by accident less than one-third of the time. In almost every large, sophisticated fraud case, detection required the implementation of a properly designed internal control or a tip from an auditor or employee. Undoubtedly, there is room for improvement in every business' fraud detection processes.

PREVENT FRAUD: FIVE STEPS

So what can you do? The following five steps can provide the backbone for an environment that is more, rather than less, prone to detecting fraud in its midst:

1. Accept the fact that fraud can occur and that no company is immune. A healthy amount of skepticism is good for every business owner to have.
2. Hire the right people and perform background checks. While you may consider yourself an excellent judge of character, most fraudsters are very likeable people. Check references!
3. Let employees know that you are looking for fraud. Don't act paranoid or accuse employees of being dishonest, but do ask questions when things don't look right. At least your employees will know you're paying attention.



4. Set up general business controls:

- Control the mail by having it picked up by an employee with no financial responsibilities. Scan all financial mail for anything that looks out of the ordinary.
- Control and receive the bank statements. Review their contents before reconciling. Look for missing checks, out of sequence checks, unknown payees, checks that appear altered, or checks not signed by an authorized signer
- Control receivables by limiting access to customers' records
- Maintain access control over inventory and monitor material costs closely
- Establish an annual operating budget and compare to actual results
- Require employees to take vacations and cross-train employees over multiple functions
- Hold regular meetings with department managers
- Visit job sites and/or vendors
- Establish and communicate formal fraud policies for the organization
- Take action when fraud occurs





5. Set up industry-specific controls. No one knows your industry and your business better than you. Think as if you were going to perpetrate a number of frauds against the business and how one would accomplish them. Take action to eliminate these opportunities regardless of how unlikely they may seem.

The Perpetrators

In most detected cases of fraud, the perpetrator acted alone. In cases where two or more individuals colluded to commit fraud, the damage was four times higher than if there had only been one perpetrator.

Tenure of employees has not been shown to have a correlation with fraud. Studies show that individuals who have worked with the company for more or less than five years have similar likelihoods of committing fraud.

Most perpetrators make less than \$50K annually.

Intense financial pressures in one's personal life can be a key contributing factor for occupational fraud schemes.

College graduates or those with post graduate degrees were accountable for over fifty percent of all fraud. Research also indicates that as the education level of the perpetrator increases, so does the likely size of the fraud.

Fraud is most likely to occur in the accounting department. Accounting staff generally have the greatest access to resources and have the opportunity and knowledge to hide the fraud.



Most perpetrators are first time offenders and have not previously been punished or terminated by an employer for committing fraud.

Red Flags

Certain behaviors or characteristics may help you detect fraud. Some perpetrators become irritable, start living outside their means, encounter financial difficulties, are unusually close with a vendor, have addiction problems, are getting a divorce, refuse to take vacation, have excessive pressure, or are being secretive about work activities. It is important to know that these behaviors do not automatically mean fraud is occurring, but they are potential warning signs.





The Last Word

“Employees should be trained to understand what constitutes fraud and how it harms the organization. They should be encouraged to report illegal or suspicious behavior, and they should be reassured that reports may be made confidentially and that the organization prohibits retaliation against whistleblowers.” *Association of Certified Fraud Examiners*

Of course, you can't run a business when constantly looking over your shoulder, but by putting the right people in your organization and building an environment of healthy and appropriate skepticism, you can help your company beat the fraud odds.



SOURCES:

2008 Report to the Nation, Association of Certified Fraud Examiners
RECon News, Cherry Bekaert & Holland

For more information about occupational fraud or to discuss your organization's other accounting, tax issues or operational issues, please contact Sensiba San Filippo at info@ssflp.com.

SENSIBA SAN FILIPPO

CERTIFIED PUBLIC ACCOUNTANTS AND BUSINESS ADVISORS

info@ssflp.com

www.ssflp.com



A member of
KS International