Business Fraud: How To Identify and Prevent It



IN THIS ARTICLE

- What Is Business Organization Fraud?
- What Is the Most Common Type of Fraud in Large Businesses?
- What Is the Most Expensive Type of Fraud?
- Why Is Fraud in Small Businesses So Common?
- Identity Theft and Fraud in Small Businesses
- The Best Way to Avoid Fraud?

Running a business is challenging enough. The last thing you should have to worry about is fraud. But fraud is a serious issue that continues to impact businesses of all sizes.

According to The Association of Certified Fraud Examiners (ACFE), U.S. businesses will lose on average 5% of their gross revenues to fraud, with small and privately owned businesses the most at risk.

Though small business fraud is usually a result of lax internal control or lack of employer knowledge in ways to prevent fraud, it’s not only employees or staff that pose a threat.

Without proper oversite, hackers and online thieves can steal confidential company information, while both owners and executives can also pose a risk.

The best way to manage fraud is to put safeguards in place that work to eliminate fraud.



What Is Business Organization Fraud?

Business organization fraud can be as straightforward as an employee helping themselves to petty cash, to your chief financial officer running a scam. In general, corporate fraud schemes generally fall into these common categories:

1. **Asset Misappropriation**

   This includes stealing, falsifying expense reports, and stealing non-cash assets.

   Asset misappropriation accounts for the majority of fraud cases annually and can include stealing petty cash, making unauthorized purchases on a company credit card, or transferring money from a company bank account into a personal account.

   Asset misappropriation can also include stealing office equipment, inventory, or supplies.

2. ## Payroll Fraud

   Payroll fraud includes submitting inaccurate time sheets, paying unauthorized or fraudulent overtime, or paying unauthorized bonuses.

   Though payroll fraud is most likely committed by the payroll department, there are many known cases of employees or even departments submitting inaccurate overtime hours and bonuses for payment.

3. ## Financial Statement Fraud

   Though financial statement fraud is relatively rare, it usually occurs with publicly held companies that purposely withhold details on their financial statements.

   However, this can also happen with smaller businesses that try to produce fraudulent financial statements to obtain a loan.

   Financial statement fraud can carry substantial penalties, including returning any loans obtained under fraudulent pretenses, and even a prison sentence, particularly if the loan was from the federal government.

4. ## Tax Fraud

   Tax fraud can be directly tied to financial statement fraud, with owners doctoring financial statements to avoid paying taxes. Of course, not paying taxes at all, or tax evasion is also considered a crime, with significant repercussions courtesy of the IRS.

5. ## Corruption

   a much more intricate scheme than the first two, corruption typical corruption charges include bribery and extortion. Usually seen in larger companies, corruption can occur when a high-level executive accepts bribes or funnels money without the knowledge or consent of others.



The best way to prevent business fraud is to put the necessary internal controls in place. Good fraud prevention measures can help reduce your fraud risk and keep your company safe from both internal and external financial crime threats.

What Is the Most Common Type of Fraud in Large Businesses?

According to the Association of Certified Fraud Examiners, the most common type of fraud found in large businesses is asset misappropriation.

Asset misappropriation simply means that employees are stealing funds or company assets. Typically, these are employees in high-level positions that have access to bank accounts and other company assets.

The best way to prevent asset misappropriation in your company is to implement internal controls that safeguard company assets.

It’s also helpful to observe your employees for any warning signs such as a change in attitude, or a sudden desire to work long hours when no one else is in the office.

What Is the Most Expensive Type of Fraud?

The most expensive type of fraud is financial statement fraud, with a median loss of nearly $600,000. Financial statement fraud occurs when fraudulent financial statements are created in an effort to mislead investors and lenders.

Though the Sarbanes-Oxley Act of 2002, which expands reporting requirements for publicly held businesses was created as a result of the shocking bankruptcy of energy giant Enron, there are companies that continue to try and game the system by creating false or altered financial statements.

One of the biggest contributors to white collar crime, financial statement fraud is typically found in publicly held businesses, though with recent loans available from the government due to Covid-19, small business owners have also been active participants in financial statement fraud.

Financial statement fraud does raise some red flags that should be investigated. Some of the things you should keep an eye out for:

- An obvious surge in profit at year-end
- A proliferation of bonuses paid based on performance alone
- Revenue growth while cash flow remains low
- Significantly out-performing the competition

Why Is Fraud in Small Businesses So Common?

Big businesses aren't the only ones prone to fraud. Small businesses experience fraud much more frequently, though typically at a lower level.

For small businesses, the risk often lies in a lack of internal controls. In very small businesses, owners may not be familiar with accounting processes and procedures and may fail to implement controls simply because they have no knowledge of them.

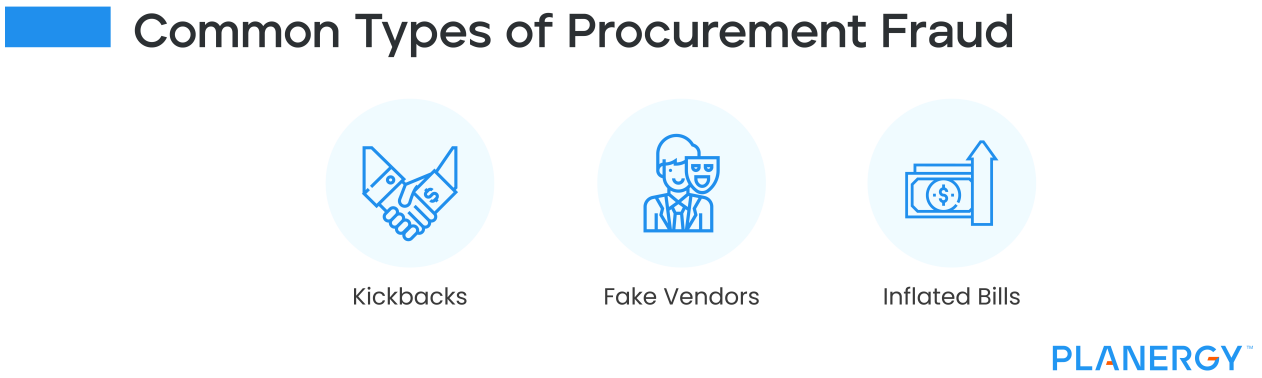
Another risk in small businesses is having one employee do multiple tasks such as

signing checks, processing payments, making bank deposits, and handling payroll.

Another risk is procurement fraud. While a low risk for smaller companies, once your company begins to grow, the risk of procurement fraud grows as well.

Here are a few areas where procurement fraud is likely to occur:

- **Kickbacks** – this happens when employees collude with vendors to up the cost of a product and receive cash or goods in return.
- **Fake Vendors** – If you don't have a proper procurement process in place, including procurement software, you run the risk of paying fake vendors for products or services never received.
- **Inflated Bills** – with the proper safeguards in place, it's easy for employees to approve inaccurate or overly inflated invoices.



Ways to spot procurement fraud include consistently mismatched invoices, unusually low bids, and employee/vendor relationships.

Procurement isn't the only area where small businesses are vulnerable. Embezzlement is another problem for small businesses and can be done in numerous ways, with the number one way simply not ringing up the sale and then pocketing the cash.

Skimming, usually found in all-cash businesses, is taking a percentage of the money from the total received.

Forged checks, altered checks, and even payroll fraud are just a few of the things that small business owners need to protect themselves against.

Identity Theft and Fraud in Small Businesses

In 2020 alone, there were almost 17 million cases of identity theft in the U.S. alone. But it isn't only individuals that are at risk for identity theft. Small business owners have recently become the latest target, with a 46% increase in the number of business identity theft cases reported in 2020.

While larger businesses have more controls in place to prevent identity theft in the business, small business owners are often vulnerable to these attacks.

In most cases, thieves are after confidential business information such as a federal tax identification number, which allows them to impersonate the business, enabling them to open lines of credit, credit cards, or even obtain loans.

Business identity theft is not going away, so it's important that small business owners become aware of the risks and put the proper security measures in place to prohibit thieves from obtaining their financial information.

The Best Way to Avoid Fraud?

The best way to prevent business fraud is to put the necessary internal controls in place. These steps should include some of these anti-fraud measures:

- ### Segregation of Duties

  Never have a single employee handle all of your accounting duties. If one employee enters new vendors and cuts checks, another employee should review the printed checks or ACH/electronic payments and sign the checks.

  This may be difficult for very small businesses, but in cases where you don't have enough employees to properly segregate duties, at the very least, you need to review all new vendor information and all payments made by the business.

Implement Three-Way Matching for Accounts Payable

The three-way matching process matches an invoice with a purchase order and shipment/receiving information. All three must match, or an investigation is necessary.

Investigate Financial Statement Discrepancies

When reviewing your financial statements, spend some time digging deeper into anything that looks amiss. Whether it's an overstated expense or a lower-than-expected bank balance, take the time to dig deeper. While it may be nothing, you won't know if you don't look.

Do a Background Check on Your Employees

Sometimes simply checking references isn't enough. Performing a criminal background check on potential new hires is important.

Just be aware that most cases of fraud involve someone without a criminal history, so a clean background isn't a guarantee, nor a reason to not put additional safeguards in place.

Don't Focus Only on Finances

There are other ways that employees can defraud your business, including stealing products and supplies and even sensitive information.

Make sure that all confidential documents are locked in a safe or away from the office, and shred any documents that you don't want others to have.

Keep Computers Secure

If you don't have the proper measures in place to keep your computer data secure, you open yourself to not only internal fraud, phishing scams, and business identity theft.

Whether your software is on your desktop or on the cloud, if the proper precautions aren't taken, you make your company vulnerable both

internally and externally to online scammers.



Business fraud isn't going away anytime soon. But good fraud prevention measures can help reduce your fraud risk and keep your company safe from both internal and external financial crime threats.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our Accounts Payable Automation Software page to see how PLANERGY can automate your AP process reducing you the hours of manual processing, stoping erroneous payments, and driving value across your organization.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts