

How to Protect Your Small Business From Fraud

7 min read



GrowthForce CEO Talks Small Business Fraud Risk on the Nurture Small Business Podcast.

Key Takeaways

- **What Is Fraud?:** Merriam-Webster defines fraud as the "intentional perversion of truth in order to induce another to part with something of value or to..."
- **Takeaways From ACFE's 2022 Fraud Statistics:** \$4.7 trillion is projected to be lost to fraud globally in 2022...
- **Watch Out for These Fraud Red Flags:** According to the 2022 ACFE report, 85% of fraudsters displayed red flags. These warning signs that indicate the potential for committing fraud include...

In an interview with Denise Cagan on her podcast, [Nurture Small Business](#), GrowthForce's Founder and CEO, [Stephen King](#) discussed fraud.

He put it simply from the start saying, "Fraud destroys lives," and King wasn't wrong.

Staggering amounts of money are lost every year around the world to fraud that occurs within businesses, and the losses are so great that they're significant enough to put most small businesses out of business. What's more? Small businesses are the most susceptible to fraud.

During their conversation, King answers Cagan's very pertinent questions about fraud, how it affects small businesses, and what business owners can do to protect their companies, their reputation, and their passion.

More of a listener? [No problem- listen to the full episode here.](#)

What Is Fraud?

Fraud Definition: Merriam-Webster defines fraud as the "intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right [1]."

In the workplace, businesses are most susceptible to internal fraud which is committed by employees, executives, or other insiders.

The Top 3 Types of Business Fraud Schemes

There are countless ways a fraudster could attempt to steal from your business. In the interview, King discussed the three most common types of fraud schemes.

1. Billing Fraud

In a billing fraud scheme, an employee submits personal, fictitious, or inflated invoices for services or goods to the company. The employee might send the invoices from a fake company. They might also create new invoices or remit multiple payments to an existing (non-compliant) vendor.

Separation of duties is key to preventing billing fraud. The person handling receivables shouldn't also be opening the mail and approving payments. Likewise, the person writing the checks should not be the person reconciling the accounts. Every step of the payables and receivables processes should be performed by a separate employee.

Read More: [Cybersecurity Precautions CEOs Need to Take Now to Avoid Lost Profit](#)

2. Payroll Fraud

Payroll fraud can occur in several ways. The most simple form of payroll fraud happens when employees submit fake time (hours they didn't actually work).

Payroll fraud can be more complex, too. For example, a bookkeeper processing payroll could pad the company's payroll taxes, sending extra money to the IRS. At the end of the tax year, they credit the excess to themselves and collect a hefty tax refund check, courtesy of the company's excess payroll taxes.

3. Employee Expense Fraud

The third most prevalent form of workplace fraud is employee expense fraud. This type of fraud involves fraudulent reimbursement requests made by employees. The expenses might be overstated, fictitious, or inflated by adding a zero. Sometimes, fraudster employees will submit the same receipts or expense requests multiple times.

To help combat this type of internal fraud, King suggested using Expensify for submitting and approving receipts and Bill.com for paying.

Small Businesses are the most vulnerable!

Statistics from a recently published report by the Association of Certified Fraud Examiners (ACFE) titled "Report to the Nations, 2020 Global Fraud Study on Occupational Fraud and Abuse" illustrates why occupational fraud poses such a significant threat to small businesses (those with fewer than 100 employees).

66% OF CASES REPORTED WERE COMMITTED BY EMPLOYEES WORKING IN THE FOLLOWING SIX DEPARTMENTS:

ACCOUNTING, OPERATIONS, SALES, EXECUTIVE MANAGEMENT, CUSTOMER SERVICES, & PURCHASES

REPORTED CASES OF FRAUD TOOK APPROXIMATELY:

14 MONTHS BEFORE DETECTION

89% OF FRAUDSTERS ARE FIRST-TIME OFFENDERS WITH CLEAN RECORDS

Fraud Scheme Rate, by Size of Victim Organization		
Scheme, Median Loss	<100 Employees	100+ Employees
Billing, \$100K	30%	17%
Check Tampering, \$110K	22%	6%
Skimming, \$47K	15%	9%
Expense Reimbursement, \$40K	20%	13%
Non-Cash, \$70K	16%	19%
Cash on Hand, \$25K	13%	10%
Payroll, \$90K	17%	7%
Cash Larceny, \$90K	13%	6%
Financial Statement Fraud, \$975K	14%	10%

21% FRAUD CASES EQUALED/EXCEEDED **\$1MM** IN LOSSES

THE TYPICAL SURVEYED ORGANIZATION LOST **5%** OF ITS ANNUAL REVENUE TO FRAUD AT A MEDIAN LOSS OF **\$150,000** PER CASE

\$4.5 TRILLION ESTIMATED ANNUAL GLOBAL LOSS DUE TO FRAUD

54% OF BUSINESSES NEVER RECOVER ANY FRAUD-RELATED LOSSES

Be proactive: steps you take today could prevent you from becoming a statistic in the future!

Takeaways From ACFE's 2022 Fraud Statistics

The Association of Certified Fraud Examiners just released the results from their most recent study, *Occupation Fraud 2022: A Report to the Nations* [2], which looks at 2,110 real-life case studies across 133 countries and 23 major business industries. Some of the key findings from this report include:

- \$4.7 trillion is projected to be lost to fraud globally in 2022.
- 5% of revenue is estimated to be lost to fraud every year.
- The median loss per case is \$177,000.
- The average loss per case is \$1,783,000.
- On average fraud results in \$8,300 lost each month.

- The average case goes on for 12 months before detection.
- Fraud hotlines significantly reduce the impact of fraud.
 - Companies with hotlines have a median loss of \$100,000 over 12 months.
 - Companies without hotlines have a median loss of \$200,000 over 18 months.
- 49% of cases occurred due to either a lack of controls or the override of existing controls.

How to Protect Your Small Business From Fraud

Fraud is an enormous problem for business owners. Unfortunately, small businesses that likely can't afford losses to fraud are the most susceptible to fraudsters. To safeguard your business from the very serious consequences of workplace fraud, you must be proactive about protecting your business.

Read More: [What If The IRS Knocks On My Door? How To Handle An Audit Of Your Business.](#)

Watch Out for These Fraud Red Flags

According to the 2022 ACFE report, 85% of fraudsters displayed red flags. These warning signs that indicate the potential for committing fraud include:

- Living beyond one's means (39%)
- Financial difficulties (25%)
- Unusually close association with a vendor or customer (20%)
- Having issues with control issues or being unwilling to share duties (13%)
- Defensiveness, irritability, or suspicious behavior (12%)
- Intimidation or bullying (12%)
- Family problems or divorce (11%)
- Exhibiting a "wheeler-dealer" attitude (10%)

Perform Background Checks on Applicants

In addition to keeping an eye out for red flags, King also recommended performing background checks on new applicants which might reveal red flags in their past. However,

according to ACFE's 2022 report, only 6% of fraudsters had previously been convicted of fraud.

Read More: [Major Failure in the C-Suite: CEOs Need to Take More Caution In Cybersecurity](#)

Establish Internal Controls

As King mentioned during the interview, 89% of fraudsters are first-time offenders [3]. So, even if your applicants pass their background checks, it does not necessarily mean that you should trust them implicitly. Small businesses are built on trust between employees and their employers. However, trust cannot and should not be blind in business. The fact is, you shouldn't trust anyone, and it's best for your business and your employees if you establish controls as if you do not trust anyone.

Establish systems of internal controls by separating duties within your bookkeeping and accounting processes. As King explained it simply, "The person who writes the checks should never reconcile the bank account."

He explained that in order to establish a true separation of duties, you need at least three people on your back office team: one person to approve transactions, one person to pay, and one person to record and reconcile the accounts. The first person can be you, the business owner or manager, the second person is usually a bookkeeper, and the third person should be a controller.

The issue is that most small businesses can't afford to hire both a bookkeeper and a controller, and whenever one person is handling two out of three steps of the transaction process, it leaves the business vulnerable to a high risk of internal fraud.

Consider Outsourcing Your Back Office

If your business can't afford to establish adequate internal controls with in-house bookkeeping and accounting staff, then the owner should consider outsourcing their back office processes to a third-party provider who is required to get approval from the business owner before any transactions are carried out or any changes are made (such as salary raises or additions to the payroll roster).

Outsourcing is a highly effective strategy for small and medium-sized businesses to mitigate fraud risk, while also unburdening themselves with the constant demand of

back-office tasks. Outsourcing is not only less expensive than hiring a three-person, in-house team, but it is also more reliable, as you're guaranteed coverage in the event of vacations, employee illnesses, or turnover. Plus, you don't have to attempt to hire high-quality back-office staff during the Great Resignation (one of the worst labor shortages ever).

Your Business Could Be Next: Implement Fraud Prevention Strategies Now

King explained that any small business that ever wants to be a big business needs to operate the way a big business would, and that means eliminating policies based on the honor system and replacing them with strategies to prevent fraud. If you don't already have fraud prevention measures baked into your accounting system, operations, policies, and procedures, then now is the time to take action – before you sustain a major loss as a result of internal fraud that could have been mitigated.

Read More: [What If The IRS Knocks On My Door? How To Handle An Audit Of Your Business.](#)

To hear Stephen King's full interview on the *Nurture Small Business* podcast, you can listen [here](#).

[1] <https://www.merriam-webster.com/dictionary/fraud>

[2] <https://legacy.acfe.com/report-to-the-nations/2022/>

[3] <https://legacy.acfe.com/report-to-the-nations/2020/>