Don't let fraud steal your business

Four best practices to defend it

Small businesses are twice as vulnerable to fraud as larger businesses[1], yet many owners neither place enough importance on fraud prevention, nor take the most basic steps to adequately protect their business.

Occupational fraud, email phishing, internet attacks and a host of business scams fill the news with stories of increasingly sophisticated fraud schemes. According to the Association of Certified Fraud Examiners (ACFE), small businesses are particularly vulnerable to fraud attack, experiencing occupational fraud at almost twice the rate of larger businesses.[1] Even with this high risk, small business owners aren't paying enough attention to fraud protection. SunTrust surveyed 532 small business owners in 2018 and found that protecting business assets placed second to last on their list of business priorities. Forty-six percent said they were not very concerned about fraud, and 79 percent did not take the most basic steps to reduce fraud exposure.[2]

But ignoring fraud won't make it go away. The ACFE reports that a typical business will lose an average of 5 percent of their annual gross revenues to fraud.[1] SunTrust Research of 532 businesses in 2018 found that in the past two years, 15 percent of small businesses were fraud attack victims. One in 5 of all small businesses experienced a fraud of greater than $15,000 with 10 percent of frauds being $50,000 or more. Fourteen percent didn't recover any of the fraud, and 1 in 4 owners recovered less than half of the stolen funds.[2]

Occupational fraud - employee theft or misuse of a business's resources

Phishing - emails appearing to be from reputable companies that induce employees to reveal sensitive information, passwords and credit card numbers

Social engineering - psychological manipulation resulting in actions to divulge confidential information

Internet attack - takeover or ransoming of websites using data obtained via phishing, spyware or malware

The financial loss from fraud tells only part of the story. Fraud can damage company reputations and wreck relationships with customers, suppliers and partners. Fraud recovery can take precious time and energy away from running your business. Business owners who ignore the risk of fraud and neglect fraud precautions, do so at their peril.

Small Business Fraud by the Numbers SunTrust Research Findings[2]

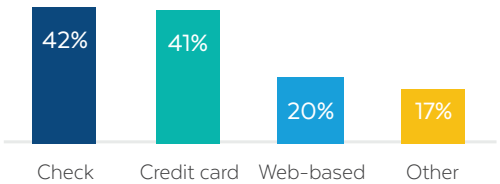
Fraud presents a persistent threat

of small businesses experienced fraud in the last 2 years

Fraud strikes are concentrated in a few areas and can have a devastating financial impact

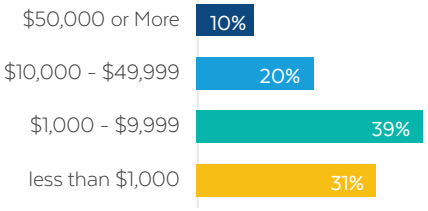
Source of fraud

% of small business owners who experienced fraud:



Amount of fraud ($)

% fraud incidents:



SunTrust®

Getting ahead of fraud

Business owners can easily implement practical steps to reduce fraud risk. Many of the business practices that prevent fraud have the added benefit of making a business run more efficiently and smoothly. That's great news for busy business owners who won't have to miss a beat on their business plans as they reduce their risk of fraud.

Assuming that fraud won't happen to you or your business is risky. Take a few simple steps to prevent fraud, mitigate damage if fraud strikes and preserve your business.

4 best practices to defend against fraud and keep your business on track

#1 Eliminate checks and "electronify" payments

What portion of your financial systems are automated?

Why it matters:

Paper transactions increase the likelihood of fraud, reduce staff efficiency and challenge efforts to be "green." Forty-two percent of all fraud crimes come from checks, making check fraud the number one deception method.[2] Stolen blank check stock, altered check amounts and use of false vendors are a few ways that paper checks are easy fraud prey. Removing paper from workflows presents a significant opportunity for many small businesses. Shifting accounts payable from checks to electronic methods like cards and online bill pay minimizes the cost and distraction of tracking down checks while providing greater visibility into current cash status and projected changes.

How to handle:

Secure blank check stock: Don't leave your checks unattended or in unlocked cabinets. Keep all checks under lock and key with guidelines for who can access them and how checks are recorded. Reconcile check stock and usage frequently.

Pay electronically: Save time, money and reduce check volume by implementing widely available online and electronic payments methods.

- Online bill pay services allow for secure bill payment without check processing risks.
- Wire or ACH payments are additional options to avoid checks.
- Credit cards – some available with individual employee spend limits – can control spending and enable online reporting for easier reconciliation and spending review.
- Online payroll systems with direct deposit eliminate the need for paper checks and provide greater control over payroll tasks.

#2 Build fraud-resistance into your business

Is fraud prevention part of your company's culture?

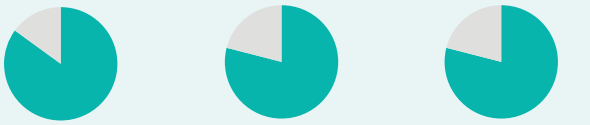
Why it matters:

The attention that a business owner devotes to fraud sends a powerful signal to employees about its importance and prevention. Structuring work and carrying out day-to-day responsibilities with an eye toward fraud prevention can stop fraud from happening. Several business routines will minimize loss, improve employee performance and security, and positively affect your overall business prosperity.

Prepare for fraud strikes from inside your organization[2]

The simplest fraud prevention actions are the least likely taken[2]

% owners do NOT take this action:



85% do NOT separate duties

79% do NOT educate employees

79% do NOT secure check stock

How to handle:

Simple precautions can save you from future fraud trouble

- Research who you hire – Conduct due diligence with thorough interviews, references and past employer calls. Don't skip formal background checks: they're required to build a trustworthy team.
- Separate duties – Don't give any single employee too much authority. Structured separation of duties with financial checks and balances avoids concentrating too much power in one person and gives you and your employees the confidence that business finances are being handled correctly.
- Educate employees – Set up training sessions to teach employees how they can help prevent fraud with diligence and adherence to operational guidelines, roles and responsibilities.

More precautions can add more security

- Conduct frequent reconciliation of accounts – Only half of small business owners review bank statements, credit card charges and accounting books.[2] Frequent reconciliation identifies financial red flags early. Online banking services provide transaction, balance and utilization reporting for easier reconciliation.
- Fraud audits - Reduce risk and uncover weaknesses with audits and reviews by your CPA. Regular fraud audits signal your commitment to reduce fraud and keep your business secure.

SunTrust®

#3 Keep data and computer security on "high alert"

Do you have security resources to protect your hardware, software and data?

Why it matters:

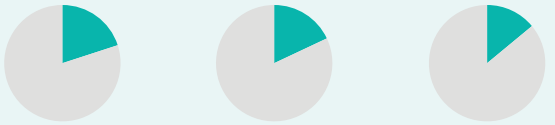
While fraud at large companies makes the headlines, it is smaller companies that are often on a cybercriminal's radar. Computer crime is opportunistic, and small companies have valuable data, but fewer resources to devote to protection. That makes you a target for a hacker's probing for security weaknesses. A case in point is the massive Target data breach which began with the infiltration of a small HVAC contractor's computers.

Cyberfraud accounted for over half of the fraud small businesses experienced in the last few years, yet close to half of all businesses do not secure their computers with passwords. Fifty-five percent of those who do use passwords, don't change them periodically.[2] Putting simple basic precautions to work in your company is the first step to protect your data and financial systems from cybercriminals.

Protecting electronic systems and data shrinks fraud risk

Protecting electronic systems and data shrinks fraud risk[2]

% type of cyberfraud experienced:



20% Web-based

18% Malware

14% Phishing/Social engineering

How to handle:

- Educate your employees – Hold sessions explaining malware, phishing and basic cyberthreats. Provide cybersecurity guidelines on staying secure online and how to avoid email phishing attempts.
- Secure your hardware and software – Put password protocols into place for all computers, routers and programs, including requirements for frequent password changes. Ensure all software is updated to the latest versions for the most current security protection.
- Implement virus protection software – Protect against malicious threats with easy and inexpensive virus protection programs.
- Consult with an IT security professional – Reinforce the importance of fraud protection messages and secure assistance for more complex operations.

SunTrust®

#4 Control damage if attacked

How well have you insured your business and yourself against fraud?

Why it matters:

A serious fraud attack can be catastrophic for your business. A ransomed website, infected server or compromised bank account can be as much of a disaster as a flood or fire. When a disaster strikes, an estimated 40-60% of small businesses never reopen their doors, and 90 percent fail within a year if they can't reopen within 5 days of an event.[3] Fortunately, there are simple protection measures that can shield your company from fraud and secure your finances.

Companies neglect to insure themselves against fraud losses

How to handle:

- Insurance – Talk to your business insurance provider to learn more about the types of policies that cover your industry and business type. Most common insurance that can cover fraud or theft include:
  - General Business Policy: General, professional and/or product liability cover the most common lawsuits brought against businesses. Typically, protection against fraud or theft is limited or non-existent.
  - Crime Insurance: Protects from losses from business-related crime such as fraud, embezzlement, forgery, misrepresentation, robbery or theft.
  - Cyber insurance: Covers recovery after a cyber-related security breach or similar event.
  - Data Breach Insurance: Protects against loss or theft of sensitive, personally identifiable data.
  - Errors and Omissions: Protects service organizations against negligence or other advisory claims. Coverage can provide limited protection when fraud affects the quality of customer work.
- Separate personal and business finances – After a fraud attack, you may need access to cash or credit quickly. Mixing personal and business funds can lead to cash reporting inaccuracies that leave owners short of funds for basic business operations and daily living expenses. Thirty-six percent of owners don't make separation of personal and business funds a priority.[2]

Add protection to your business

Put in place the fraud protections you need today to help keep your business strong, healthy and positioned for success.

Don't let fraud steal your business.

- Drop by your SunTrust branch
- Call us at 800.752.2515
- Visit suntrust.com/bizbestpractices

[1] 2018 Report to the Nations on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, April, 2018.
[2] SunTrust conducted research with 532 small business owners ranging from $100,000 to $2,000,000 in annual revenue during the first quarter of 2018.
[3] Business Infographic, Federal Emergency Management Agency (FEMA), https://www.fema.gov/media-library/assets/documents/108451, accessed 8/2/2018.

SUNTRUST®