Fraud Prevention Checklist for Small Businesses

11 Ways to Minimize the Risk and Impact

HARLAND CLARKE® | PAYMENT SOLUTIONS

Fraud can have a devastating impact on small businesses. Prevention and mitigation strategies can mean the difference between a thriving enterprise and a shop closing its doors.

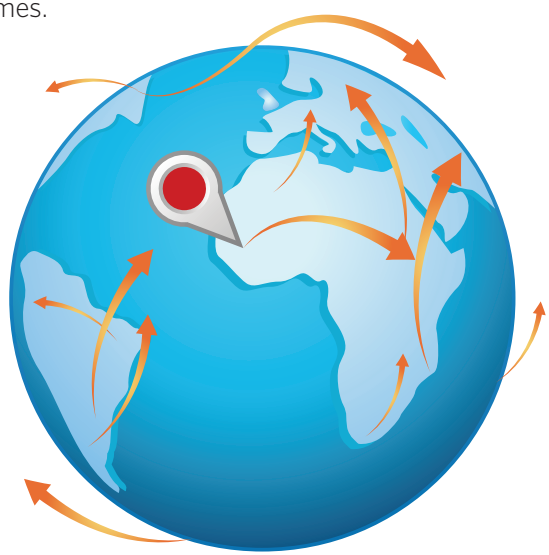
Fraud incidents tend to disproportionately affect small business, since the relative size of a financial loss makes up a much bigger chunk of revenues compared with larger organizations. For companies with fewer than 100 employees, the median loss is $147,000, compared with $100,000 for companies with 1,000 to 10,000 employees, according to a 2012 study by the Association of Certified Fraud Examiners (ACFE).[1]

Compounding the problem is the duration of fraud. Because small businesses are less likely to spend the time and money needed to reduce risk, fraud is more likely to endure for longer periods before being detected.

As a group, small businesses are plainly unprepared. For example, only 19 percent of businesses with fewer than 100 people conducted fraud training, compared with 59 percent of companies with 100 or more people, according to ACFE.[2] Smaller businesses have fewer fraud controls than larger organizations, and become victims more frequently as a result: 32 percent of companies with fewer than 100 employees reported fraud, according to the ACFE study.[3] That compared with just 20 percent of companies with 100 to 1,000 employees, and 21 percent for organizations with 10,000 or more employees.[4]

Fraud From Every Direction

Businesses in general face numerous fraud vulnerabilities. On the low-tech side, fraudsters can skim money from a business before it is deposited and recorded on the books. Other tricks include fictitious invoicing, bogus reimbursements, check tampering and payroll schemes.



On the technological side, small businesses have for years faced the threat of hackers, with common intrusions such as malware and viruses. But the nature of attacks has changed. In the past, hackers meant to destroy data and show off their abilities. But now, they seek to go undetected so they can steal company trade secrets, customer credit card numbers, customer information and vendor records. Another growing area of exposure includes identity theft, where thieves steal business information such as tax identification numbers and wreak havoc by drawing out loans in a company's name. Criminals also target a business's customer records in order to sell their identities on the black market. Meanwhile, mobile devices, spanning various operating systems, have introduced new vulnerabilities to in-house networks, giving perpetrators new entry points.

[1] *"Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study," Association of Certified Fraud Examiners.*
[2] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*

The good news is, small businesses can implement policies, procedures, and safeguards that can increase detection, minimize losses, and ensure effective resolution of fraud. Consider these 11 low-cost strategies that could significantly reduce the risk and impact of fraud for your business:

Strategies Toward Prevention

1. Be thorough when hiring. Internal staff accounts for 76 percent of fraud, according to consulting firm PwC, so your ability to protect your business starts with recruitment. Conduct due diligence when hiring new employees, including phone calls to former employers, where a brief call can reveal a lot about a prospect. Background checks using online services are an inexpensive way to confirm the information job candidates share in their applications. The checks also help identify any candidates with criminal backgrounds.*

2. Establish a code of conduct. Employees are less likely to cross the line if they have a strong sense of company rules and expectations. Make sure to establish a formalized code and communicate and distribute it to employees. Outline the repercussions employees will face for transgressions such as not following financial controls or ignoring basic protocols. Enforce the code consistently to send a strong message that there is zero tolerance for violating it and to help deter bad behavior.

3. Educate your employees. Your staff must be aware of all the ways a company's financial health and reputation can be compromised, and why it is important to follow the rules. Show them the stakes for not doing so: lost income and possible layoffs, or even a complete shutdown of the business. Conduct seminars and circulate emails on the latest issues. Tap resources such as your financial institution for advice.

4. Keep close tabs on finances. Check bank and credit card statements monthly and know how much it costs to run your business, as well as how much money is coming in. Sign up for text and email alerts. Look for inconsistencies. Make sure to separate responsibilities, such as having one person open checks and log them in, while another employee writes checks so that there's a clear separation of duties with handling money. Compare the check log to reconciled statements.

5. Bolster computer security. Even basic measures can deter criminals who are looking for easy targets. Protect your network with firewalls and anti-malware products. With the proliferation of mobile data, you must also develop a strict policy on what type of data is accessible from tablets and smartphones so that the proper controls are in place to prevent intrusions. Protect your network by using long passwords that have random sequences, upper and lower case, and letters and numbers. Consider adding additional ways for users to authenticate themselves than just a user name and password.

6. Be aware of regulatory changes. Pay close attention to local, state and federal requirements for protecting customer information and reporting fraud. Take the regulations seriously, as penalties and fines could add to your losses in the event of fraudulent activity.

7. Use checks with security features. Check fraud continues to be the leading type of business payment fraud.[5] Taking the responsibility of preventing it is not only good business sense,

*This information does not constitute legal advice. Please consult a legal professional.

[5] *"2012 AFP Payments Fraud and Control Survey," Association for Financial Professionals.*

but also recognized as a best practice.[6] Use checks with security features such as holograms, thermochromic heat-sensitive ink, chemical reactive paper and a true watermark. These added elements make duplication difficult for fraudsters.

8. Have employees switch positions. Also make sure to rotate job responsibilities so that one person does not remain in a sensitive position for a long period. In addition, make sure employees take vacation, so that substitutes fill in. This will serve as a barometer for any suspicious activity in the company.

9. Use a fraud detection monitoring service. Having a set of eyes on the business can help detect fraud so you can minimize the damage. Fraud detection services can track a host of business credentials such as debit and credit card numbers, bank account numbers and payment cards. These services can also send you emails and text alerts to inform you of suspicious activity.

Strategies for Mitigation

Given the rampant nature of fraud nowadays, small businesses also need to plan for the day it happens. Consider these ideas for alleviating fraud's impact:

10. Subscribe to a fraud remediation service. Fraud is all too common, so be prepared. Subscribe to a service that fights on your behalf. You need an advocate who can respond to identity fraud as soon as it happens. The average fraud incident takes 33 hours to resolve, so advocates help save you precious time and minimize productivity losses of impacted workers. Advocates can determine the threat, investigate acts by unknown parties or employees of the business, and spearhead the investigations needed to prepare cases and speed the path to a resolution. So consider a service that also helps you care for your affected employees by providing personal fraud counseling, research and remediation.

11. Look to experts to implement a response plan. Your business may need to communicate news of a security breach and handle crisis management. Work with a recovery service that can provide an action plan for the critical first 48 hours after the discovery of fraud. You will likely need to help employees and customers after a breach with services such as free credit monitoring, research to uncover additional identity issues, and creation of an online portal for victims. These services should also provide identity theft protection for a large number of victims and for a period of up to two years after the breach. Look for vendors that offer customized websites for victims to enroll in fraud and credit monitoring.

[6] *Universal Commercial Code, revised 1993.*

Don't Wait — Start Now

Unfortunately, the threat of fraud is here to stay, so small-business owners must be diligent in reducing risk. The median fraud duration for all businesses was 18 months in 2012, according to the Association of Certified Fraud Examiners.[7] That means owners must act now to put the right measures in place in order to lower the odds. But they need not go it alone. Financial institutions offer a great partner to help small businesses integrate fraud prevention and mitigation into their workflows. Financial institutions have deep experience working with small businesses and can offer a variety of prevention, detection and remediation services to help prevent fraud and minimize its impact.

[7] *"Report to Nations," ACFE.*