STERLING NATIONAL BANK

WHITE PAPER

Business Fraud Prevention: 7 Strategies That Work

As a business owner, focusing on the big picture is a priority. Business administration often takes a back seat to generating revenue and managing client needs. And, that's what fraudsters count on. They use your distraction to their advantage. It only takes a few moments for fraudsters to identify vulnerable areas within an organization. Owners must maintain safeguards to the administration of the business if they expect to protect their bottom lines.

According to the Association of Certified Fraud Examiners, total losses to occupational fraud in 2018 exceeded $7 billion, with a median loss of $130,000 per incident. New start-ups and small businesses are most at risk, but big companies and corporations aren't immune. Business fraud prevention strategies can be implemented quickly and go a long way to protect against external and internal theft.

HERE ARE SEVEN EFFECTIVE TACTICS THAT CAN HELP REDUCE YOUR EXPOSURE TO FRAUD.

1 Review your accounts often.

Most businesses review their accounts at least quarterly, but that isn't enough to protect against business fraud. Check your accounts daily. Look for transactions that fall outside of standard business practices. If you spot suspicious activity, don't ignore it. Look closely to verify the transaction. The sooner you challenge questionable activity, the lower your risk of substantial loss.

2 Report missing checks immediately.

As you review your accounts, you may come across missing checks. Unless you report the missing checks immediately, your business could miss out on fraud protection from your financial institution. If multiple forged checks clear your bank account, you generally only have 30 days from the statement date to find the error and let the bank know.

Fraud prevention services like Reverse Positive Pay can also help to protect your accounts from check fraud. Businesses that write a high volume of checks should consider enhanced solutions like Check Positive Pay to safeguard accounts.

3 Train employees to spot scams.

Internet scams, such as phishing, fake antivirus offers, and untrustworthy links, are a frequent occurrence in our personal as well as our professional lives. Fraudsters can target company email and even portray themselves as a top executive to trick employees into revealing non-public information. These are known as "business email compromise" attacks, and they can be a significant risk to companies large and small. To improve your defense against fraudulent attempts, invest in a training program to teach employees how to spot and avoid scams like these.

4 Don't skip software updates.

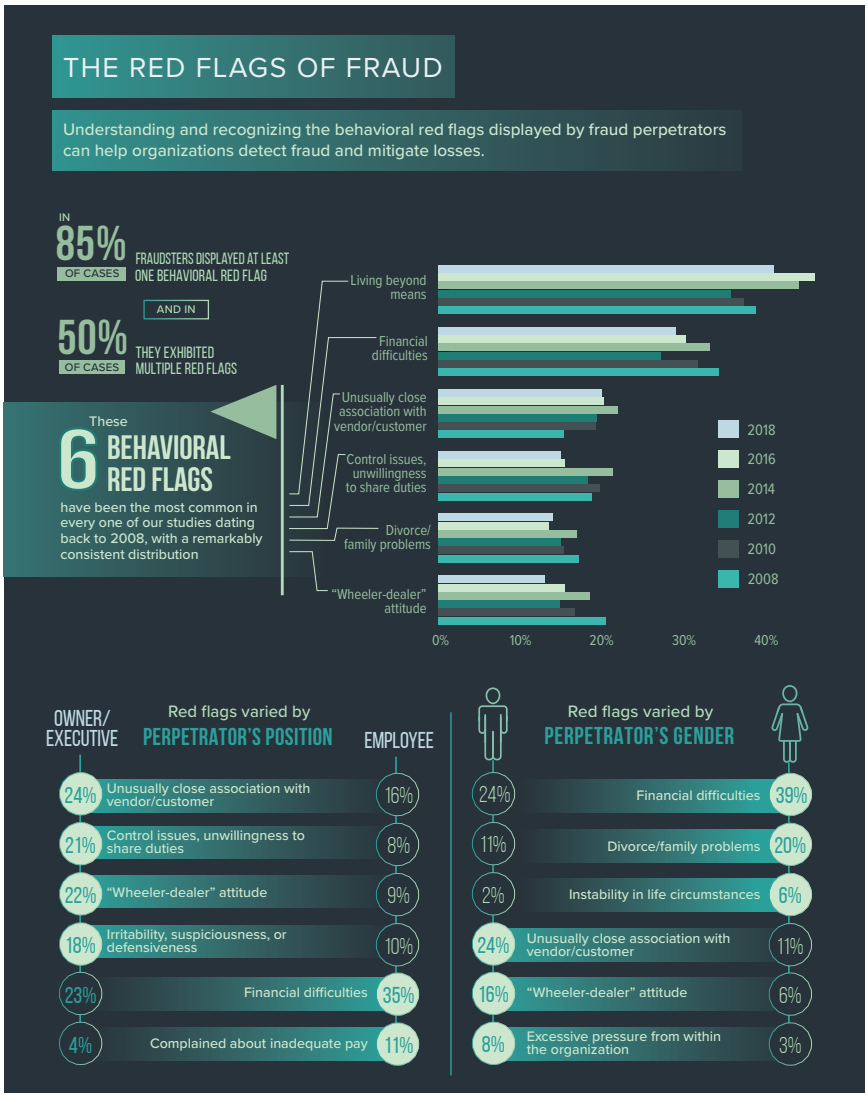
Firewalls and antivirus software can be the first line of defense against attempted criminal behavior, but not if it's outdated. A firewall can detect and stop malicious activity while an antivirus program can keep computer viruses from spreading the infection throughout the organization. System updates often contain security vulnerability fixes that can keep out prying eyes.

5 Get to know your employees.

According to the Kroll Global Fraud and Risk Report 2019/20, 39% of fraud stemmed from leaks of internal information. This makes getting to know your employees more important than ever. If you notice an employee living beyond their means, having an unusually close association with a vendor or customer, or being unwilling to share duties, those could be red flags.

Perform background checks as part of the new hire process, paying particular attention to those who will have financial responsibilities. Implement data access limits to prevent employees from accessing data they don't need. This may reduce the temptation to steal credit card numbers or other sensitive information from customers.

Source: Association of Certified Fraud Examiners. (2018). The Red Flags of Fraud. Retrieved 2020, February 26, from https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2018/The-Red-Flags-of-Fraud.pdf



6 Perform routine audits.

Audits should be a regular part of business operations. Routinely monitoring parts of your company that deal in cash, refunds, product returns, inventory management, and accounting functions can help stop fraudulent activities.

If you suspect fraud, a certified fraud examiner (CFE) can help. CFEs are trained professionals that focus on fraud detection. They can uncover fraud and theft, identify illegal accounting practices, tell you the amount of financial loss your business suffered, and provide documentation to help with recovery efforts.

7 Separate accounting functions.

By not separating accounting duties, you're putting your business at a higher risk of fraud. Small businesses are especially susceptible to this type of fraud since they may have only one person who manages all activities associated with bookkeeping, client receivables, payment of invoices, and management of petty cash.

Separate accounting duties by having at least two people handling financial tasks. For example, never have the same person who authorizes payroll write or issue paychecks. Another option is to outsource to a virtual CFO at an accounting firm.