

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

**SMALL BUSINESS**

# Protecting Small Businesses from Fraud

The ways small businesses have been handling their bookkeeping and accounting for years are quickly becoming obsolete. Antiquated and manual processes leave small businesses vulnerable to fraud from both the inside and the outside.

Aug. 13, 2020



Many small businesses like to think that their size insulates them from fraud. In reality, though, the opposite is true – small businesses are big targets for would-be fraudsters. According to the [ACFE Report to the Nations](#) (Copyright 2020 by the Association of Certified Fraud Examiners, Inc), small businesses are two times more

likely to experience billing and payment fraud and four times more likely to experience check and payment tampering as compared to their larger counterparts. Too often, small businesses lack the necessary security measures to protect against fraud, making it easier for perpetrators to breach the company's financial systems.

The ways small businesses have been handling their bookkeeping and accounting for years are quickly becoming obsolete. Antiquated and manual processes leave small businesses vulnerable to fraud from both the inside and the outside. Reducing fraud starts with understanding your vulnerabilities and instituting the changes needed to secure your business.

## **Top Vulnerabilities Facing Small Businesses**

Business vulnerabilities go far beyond someone trying to steal your credit card number or login credentials for financial sites, though those things still happen. Fraudsters routinely steal bank information from paper checks and use it to make fraudulent transactions. At businesses without stringent approval processes, employees or outside infiltrators can send illegitimate invoices through AP and receive payment through a shadow company. Scammers are also spoofing employee identities to make fake transactions seem legitimate and even blame the fraud on innocent staff members.

Even the most business-savvy small business owners can fall victim to fraud. Barbara Corcoran, of "Shark Tank" fame, was **scammed out of nearly \$400,000** in an email phishing scheme. Using a spoofed email address for Corcoran's assistant, the scammer sent a fake invoice to Corcoran's bookkeeper, provided legitimate-seeming answers to the bookkeeper's questions, and obtained payment. Although news coverage didn't disclose the internal processes Corcoran's company had in place for invoice approvals, the scam illustrates a classic example of how more robust workflows for processing and approving invoices will help stop fraudsters, who are constantly evolving their tactics.

These external actors aren't the only drivers of fraud at small businesses. Internal vulnerabilities leave small businesses open to fraud every day. Think of your current bookkeeping workflows and who controls them. Many small businesses use a long-time bookkeeper or office manager, who is the only person who knows the business's login information, links, and processes for completing crucial bookkeeping tasks. What happens if that person leaves or can't work? When the sole handler of AP is gone, it can take businesses weeks to sort out their processes and set up new, secure procedures, and that's if they have an expert AP vendor assisting with recovery. In

contrast, if you use controlled, automated AP solutions from the start, it's easy to delete users and set new users up in designated roles with the appropriate access rights.

## **Top Three Reasons Companies Are Resistant to Change**

Accountants hear the same reasons time and time again for why clients don't want to change the way they handle bookkeeping and AP. These reasons, though, are easily debunked.

- 1. *I don't want people seeing my business on the cloud.*** The cloud doesn't let people see your business, especially if you use automated accounting software that lets you limit who can view or access specific information. What does let people see your business? Vulnerable and outdated processes that allow them to gain access to your bank account.
- 2. *The cloud isn't safe.*** Nothing is 100% secure, but the cloud is far more secure than manual processes. Paper records and local desktop files can be lost in any number of ways, including fire, flood, theft, or hardware failure. Cloud applications, in contrast, include sophisticated security protocols, and cloud providers have teams dedicated to installing and updating security patches. Cloud-based applications offer lower risk when it comes to maintaining your sensitive financial data.
- 3. *Our company made an investment in QuickBooks 10 years ago, so we're already using solid accounting software.*** Desktop software platforms need to be updated regularly. Just as you're constantly upgrading and updating your smartphone and personal devices, you need to stay on top of your accounting and other business software. Any investment in security is ongoing. A benefit of cloud-based applications is that they usually work on a subscription basis and include constant security updates and upgrades with new security features.

Society has changed, and new fraud schemes surface all the time. Small businesses must adapt along with them and always be prepared for the unexpected.

## **Time for Change**

Businesses can't run the same way they did 20 years ago. Those that resist change do so to their own detriment.

It's not just the scammers who are evolving. Your customers and vendors are also changing how they do business. Therefore, your business must also adapt, even if it's

in steps. Particularly in the time of COVID-19, businesses need to be paying extra attention to infrastructure security as virtual work capabilities are now mission-critical.

Start by cutting out inefficiencies and high-contact tasks such as sending paper checks. Focus your staff on high-value work that requires human input, as opposed to data entry and other routine tasks. Moving to cloud-based accounting tools removes tedious, manual processes and creates small efficiencies that can have significant, positive effects on company cash flows and more.

## **Six Critical Moves to Make Right Now**

The good news is that there are a number of changes small firms can start implementing today to stop fraud in its tracks.

1. Create audit trails that track every click and every dollar down to the individual who performed the action.
2. Establish checks and balances to control the movement of funds. Ensure that the same person taking payments isn't also responsible for making payments; if that's not possible, add oversight.
3. Use smart, automated workflows to remove manual tasks from your processes.
4. Shift to online tools that enable virtual work. If your processes rely on your team sitting together, you need to make major adjustments to accommodate the realities of the new normal.
5. Build a long-term relationship with a trusted strategic advisor who knows your business, can help you make big decisions, and can advise you on issues related to technology workflows.
6. Don't take anything for granted. The last 20 years have shown us that anything can happen, from major global events to more localized natural disasters. Your business must be prepared for whatever occurs. Recent global events have highlighted how critical it is for people to be able to conduct business remotely. Ideally, you've put those tools and processes into place so you can use them in times of crisis. Be prepared with technology that will work to your advantage and reduce impacts on your company.

Fraudsters will continue to attack small businesses, but your business doesn't have to be their next big payday. By recognizing your vulnerabilities and instituting the changes and new technologies necessary to address them, you'll be positioned to handle the threats that arise in the future.

=====

Shelly Lingor is a partner at [GunnChamberlain, P.L.](#), a Jacksonville, Florida-based boutique accounting firm that prides itself on using technology and community relationships to help clients accomplish their goals and grow their businesses. With 25 years of experience in the accounting industry and a long-standing passion for the growing field of cloud accounting technology, Lingor leads the firm's tech division that offers virtual accounting services as a clear path to growth.

Jeannie Ruesch works as the director of marketing at [Bill.com](#) and has been in the accounting industry for more than seven years. She previously worked at Xero and The Sleeter Group. She has more than 20 years' experience in brand creation and strategy, design, social media development, demand gen, and customer marketing. She's a tech geek at heart, an author, an award-winning graphic designer, and loves finding ways to help customers solve problems.

Small Business • Technology • News

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2023 Firmworks, LLC. All rights reserved