Cybercrime & Bank Fraud:
Tips for Protecting Your Business

INVESTORS
COMMUNITY BANK

The threats are real, and they're just about everywhere. Between bank fraud — illegally obtaining money or other assets held by a financial institution using false information or pretenses — and cybercrime, which is a catch-all term for any crime committed via the internet, businesses of all sizes are finding that they need to take steps to protect themselves.

Business owners can’t afford to dismiss bank fraud and cybercrime as things that “can’t happen” to them. Establishing preventive measures to mitigate risks is a smart move that could safeguard both their businesses and their reputations. This tip sheet provides an overview of the most prevalent types of crimes businesses are vulnerable to, and what they can do to protect themselves.

BANK FRAUD

Bank fraud is nothing new, but the incidence today has reached an all-time high — according to the Association for Financial Professionals (AFP), 82% of organizations reported incidents in 2018. Here are some of the most common ways criminals perpetrate bank fraud against a business:

Impersonating a bank. Criminals set up fake companies and/or websites pretending to be a legitimate bank; they then ask for deposits.

Stolen checks. Stealing checks isn’t difficult when the checks are printed (not direct deposited) and can be done by anyone with access to mail, a mailbox store or even a payroll company. With a stolen check, a criminal can open a bank account under the name on that check and deposit it.

Forgery. Paper checks can be altered. By adding a zero, for example, a perpetrator can change a $100 check into one for $1000. Similarly, forgers can cash a check by duplicating a signature.

Fraudulent loans. A person could take out a loan in the name of your business, simply by using false documentation and a false ID.

Your banker can offer additional fraud prevention tips specific to your needs and implement procedures to help protect your finances.

Account takeover fraud. Thieves use stolen login information to access a customer’s account.

Card-not-present fraud. These are transactions made online or via phone where the cardholder does not need to present the physical card to complete the purchase.

The best ways to protect against these and other types of bank fraud are to be vigilant about:

- Using Positive Pay to help guard against check and ACH fraud.
- Keeping company checks and account numbers in a safe place and implementing safeguards like encrypted passwords and locked file cabinets
- Using a secure method of communication when you need to send account information to the bank. When requesting a wire transfer, for example, sending your information via fax or secure email are recommended options.
- Setting parameters for wire transfers such as requiring a call back to yourself or another authorized individual for verification prior to the wire being sent out.

Employees with online access and/or authorized signers on accounts should be extremely cautious of emails requesting wiring out money, changing account numbers or switching banks for payroll deposits, even if they are from the CEO or CFO, as these are most often fraudulent. Be sure to talk to your employees about precautionary procedures. Trust but verify!

CYBERATTACKS

There are other threats that fall under the more general umbrella of "cybercrime." These threats affect businesses and individuals and can be very harmful and costly:

- **60% of small companies go out of business** within 6 months of a cyberattack (U.S. National Cyber Security Alliance)
- The average small business spends **$690,000 recovering** from a cyberattack (Ponemon Institute)
- **62%** of all cyberattacks **target small and mid-sized businesses** – about 4,000 every day (IBM)

There's also the cost of downtime. With systems compromised, it's tough to conduct business as usual, and 44% of businesses estimate they could lose $10,000 or more during just one hour of downtime, according to continuum.net.

The most common type of cybercrime is called "phishing" — the attempt to obtain sensitive information such as usernames, passwords and credit card details for malicious reasons, by posing as a trustworthy entity in an electronic communication. Employees can be the weakest links in a business' efforts to protect its systems and data, often failing to adhere to proper procedures related to downloads, backups and other security measures. Criminals get to employees through social media and emails, typically, and in doing so are able to bypass the security set up to protect systems.

Once they're in your system, perpetrators infect and disrupt the system using malicious software, often referred to as "malware," or hijack data using software referred to as ransomware. With control over the data, criminals demand payment to release control back to the company. In 2016 alone there were 638 million ransomware attacks — 167 times more than the year before. Here are smart ways to protect your organization from this growing threat:

Encrypt data. Many small companies still keep sensitive customer data in simple spreadsheets and store it in the Cloud or on a company server. Encryption encodes plain text into unreadable data and provides an added measure of security by making it accessible only to authorized users.

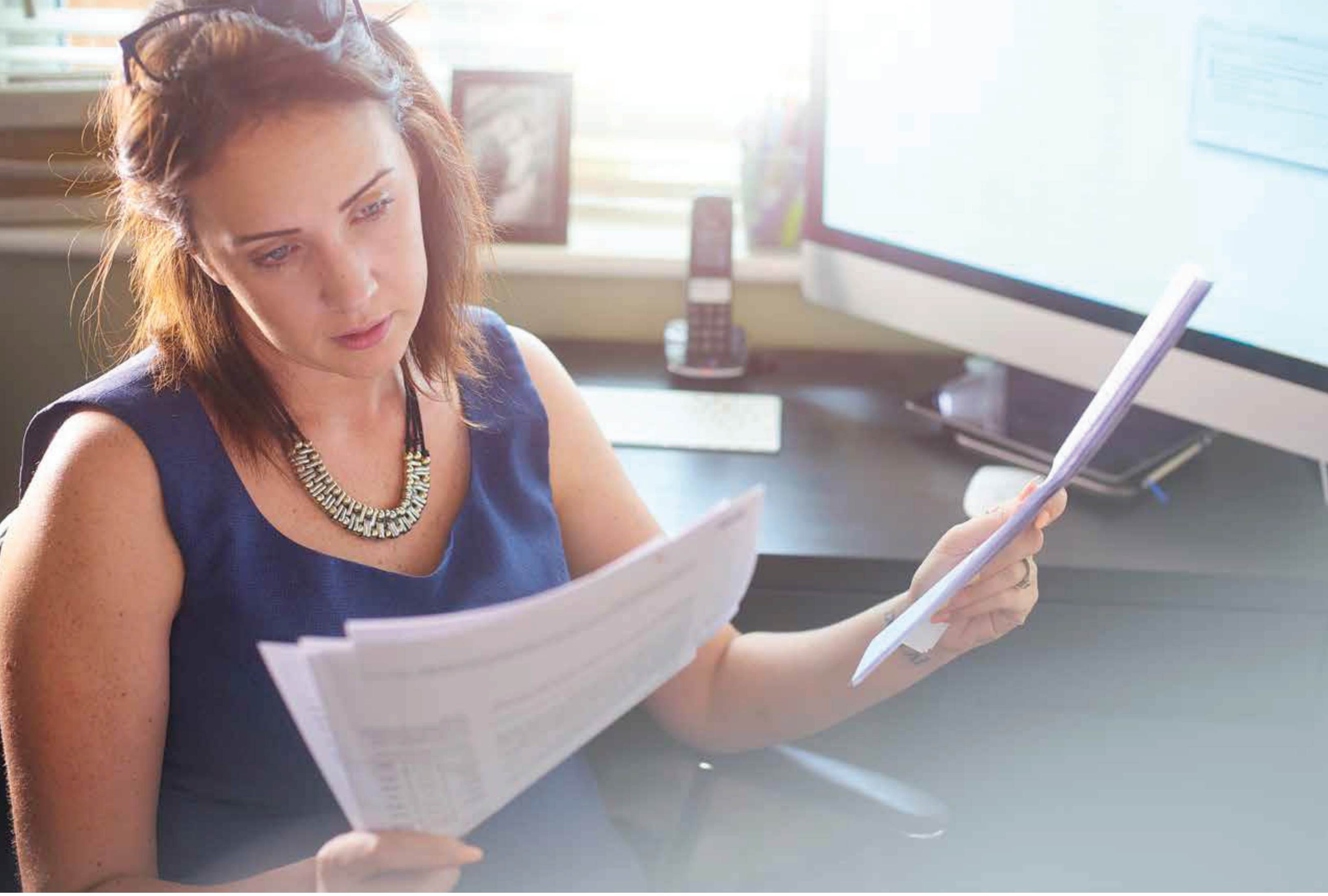
Keep systems up to date. Another way criminals access company data is through connected devices that are poorly protected. "Smart" products like connected thermostats are a way for hackers to get into systems, where they can gather data or interrupt service. Even the best operating systems need frequent updates and added antivirus and security patches. Even if a hack occurs, the consequences can be minimized if your **files are backed up daily**.

Install firewalls. Wireless routers are becoming more common, but when compared to wired routers, they're less secure, and if that wireless router is a few years old, it might not have the firewalls in place to keep criminals out. The best way to stop them from gaining access is to make your passwords hard to "crack."

Educate employees. When people understand how hackers might infiltrate the company's system they're more able to identify and report suspicious emails and avoid downloading attachments that contain viruses. Employees should know how to spot a fake (phishing) email. Telltale signs include, misspellings, grammatical errors, a sense of urgency, prizes, serious demands or threatening consequences. They should be trained to not respond to suspicious messages and not to click on links in the suspicious email.

Protocols should include a reporting method and the use of software to scan files before they're allowed to be downloaded.

Ensure vendor compliance. Vendors (like accountants and legal firms) that have access to your files can be compromised and, in turn, can increase the risk of someone hacking of your systems. Similarly, if you use third-party software for payroll or other functions, it's important to know if the company has proper security measures in place.



Don’t make the mistake of considering your company — large or small — out of reach of bank fraudsters or cybercriminals; take precautions and educate everyone in the company about mitigating threats. Reach out to a member of ICB’s Treasury Management Team if you are interested in setting up Positive Pay for your company.

Disclaimer: Views provided in this piece are general in nature for your consideration and are not legal, tax, or investment advice. Investors Community Bank (ICB) makes no warranties as to accuracy or completeness of information, including but not limited to information provided by third parties, does not endorse any non-ICB companies, products, or services described here, and takes no liability for your use of this information. Information and suggestions regarding business risk management and safeguards do not necessarily represent ICB’s business practices or experience. Please contact your own legal, tax, or financial advisors regarding your specific business needs before taking any action based upon this information.

EQUAL HOUSING OPPORTUNITY

MEMBER FDIC

Appleton: (920) 739-2660
Green Bay: (920) 884-1166
Manitowoc: (920) 686-9998
Stevens Point: (715) 254-3400
Sheboygan (Loan Production Office): (920)-451-0200
Call Toll Free: (888) 686-9998
Email: contact@investorscommunitybank.com
Website: investorscommunitybank.com

INVESTORS
COMMUNITY BANK