November 2023

On the Lookout

Cash Management Security Tips

FRAUD PREVENTION

As the holiday season approaches, businesses become more vulnerable to cyberattacks and fraud attempts as fraudsters take advantage of increased online activity, holiday vacations, and the rush caused by increased business or year-end activities.

In this Security Alert, find more information on some of the most prevalent fraud threats today, including mail theft and check washing under **Highlight on Check Fraud**, and the continuing threats of **Business Email Compromise** and Man in the Middle attacks.

In a rapidly changing digital environment, online scammers are constantly finding new ways to compromise businesses, but good security practices go a long way in mitigating these threats. View additional tips and recommendations under the **System Security Health** section.

October 2023 celebrated 20 years of Cybersecurity Awareness Month, a dedicated time to raise awareness and educate ourselves on how to protect our online data and privacy. Many government organizations and financial communities publish helpful fraud prevention and cybersecurity information in October. Refer to the **Cybersecurity & Fraud Prevention Resources** section for links to some of the best resources available.

INCLUDED IN THIS ISSUE

HIGHLIGHT ON CHECK FRAUD

> ***"Checks continue to be the payment method most vulnerable to fraud."***
>
> In a recent survey of hundreds of treasury practitioner members conducted by the Association of Financial Professionals (AFP), 63% of participating Financial Institutions report that their organizations faced fraud activity via checks. 75% of organizations currently using checks do not plan to discontinue issuing checks. [1]

In a recent analysis of fraud data compiled between July 1, 2023 and September 30, 2023, we found that check fraud accounted for over 40% of fraud incidents reported by PCSB Bank customers.

Mail Theft & Check Washing

One of the most common forms of check fraud is mail theft and check washing, a scam where fraudsters steal checks from a mailbox, "wash" the check to remove the payee and amount information, and issue the check for a different payee and a potentially higher dollar amount. Businesses often do not notice they are victims of this type of fraud unless they are closely reviewing their paid checks for changes to the originally issued check, or until they are notified by the intended payee.

What Can I Do?

Secure Your Checks

Dropping checks in less secure locations such as mailboxes with larger openings or accessible areas where mail is left for a letter carrier, makes it easier for fraudsters to fish for checks. Safeguarding your mailing process or bringing mail to the Post Office ensures checks are not stolen to perpetrate check fraud. Ensure that any checks you have in your possession are properly secured and, for remote deposit checks, destroyed after a deposit is processed.

Review Paid Checks

Use check viewing tools available in online banking to ensure paid checks were processed for the appropriate amount and to the intended payee. Paid checks can be viewed online and through the mobile app.

Switch to Electronic Payments

Checks are payment types that are particularly susceptible to fraud as they expose the payor's account number and bank routing number. The security of this information is in the hands of each individual that touches the check. Electronic payment options such as ACH transfers send account information through secure channels and include additional security benefits such as dual control and electronic notifications.

Enroll in Check Positive Pay

Check Positive Pay with Payee Verification is a service that allows businesses to reconcile expected checks they have issued and catch potentially fraudulent items. Report your issued checks to the bank to validate the check number, date, amount, and payee name of checks as they are presented to the bank for payment. Any checks presented to the bank that were not reported by your company will be presented to you for your review. Contact your Cash Management representative for more information.

Report Suspected Fraud

Report any suspected fraud to one of your bank representatives for advisement and to ensure your business is not vulnerable to additional fraud attempts.

Report any instances of mail theft to local law enforcement and to the US Postal Inspector's Office: https://www.uspis.gov/report

[1] https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

ALSO LOOK OUT FOR…

While Check Fraud is the most prevalent form of payment fraud, precautions against all types of fraud is essential to mitigate risk and prevent potential losses. Look out for the two common forms of fraud below.

Business Email Compromise

Business Email Compromise (BEC) is a scam in which a perpetrator gains access to your company's email system or impersonates a person of authority within the organization (such as the business owner or CEO) and emails a request to an unsuspecting employee instructing them to initiate an Online Wire or ACH payment.

Research conducted on over 450 treasury practitioners by the AFP found that 65% of organizations were victims of payments fraud attacks or attempts in 2022. Of those organizations, 71% were victims of BEC.[2] The FBI's Internet Crime Complaint Center (IC3) reports 2022 losses from BEC fraud exceeded $2.7 billion.[3]

Man in the Middle

Man in the Middle attacks occur when a perpetrator penetrates a payment recipient's network and sends an email masquerading as them to request a change to payment instructions, resulting in payments routed to a fraudulent account.

A common example of this occurring is when a company receives an email that a vendor has recently changed banks and would like the company's next payment to be made to the new banking instructions included in the vendor's email. Since this type of fraud can use details from an existing legitimate relationship, it is very hard to detect without further verbal verification.

[2] https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud
[3] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

PREVENTION METHODS AND TOOLS

The steps and tools described below can help prevent most forms of electronic payment fraud.

Educate Employees

Employees are the most important and last line of defense against fraud at your company. Employees are able to detect suspicious activity based on their knowledge of the company and its activities. Encourage all employees to take their time, think about what they are doing, ask questions, and trust their instincts. Below are some "low-tech" tips for combatting fraud.

Perform Cybersecurity and Fraud Prevention Training at Least Annually

The Federal Trade Commission (FTC) site offers FREE videos and quizzes you can share to help inform or remind your employees about different types of fraud and how to prevent them. These tools reiterate daily practices that help prevent fraud, such as:

- How to create strong online banking credentials, and steps to keep credentials safe
- The dangers of links or files from unfamiliar sources, and how to handle them
- Best practices for securing physical devices with sensitive information
- The importance of keeping your computers and security programs up to date
- The importance of virus protection software on ALL computers

Always Verify Requests for Changes

Any time you receive a request to change payment routing instructions (ABA/routing number, account number/IBAN) use a trusted contact method, preferably a contact method that is different from how you received the request, to verify the details BEFORE making any changes. For example, if a vendor contacts you via email to update their account details, contact the vendor using a known phone number to confirm. This process is very effective in preventing BEC and Man in the Middle fraud.

Take Time to Ask Questions

- **"Does this payment make sense?"** – Did you receive a request from a local vendor to change their account details to a bank out of state or out of country? Does the recent invoice look different from previous invoices, or is the amount significantly different from previous invoices?

- **"Does it fit with the company's normal activities?"** – Did the request imply urgency that requires you to rush, or skip normal processes and procedures? Did the request come from an unexpected source or leave off teammates who are usually involved in the process (such as an executive reaching out to you, and only you, for the first time to request a change)? Was the request received outside of normal business hours?

Cash Management Online Security Features

Your Cash Management Online (CMOL) service comes with multiple security features to help prevent payment fraud.

Dual Control

This feature requires that a second person reviews and approves all payments before they are approved for processing. This feature helps prevent unauthorized payments from processing if internal fraud or an account takeover occurs. A second pair of eyes also helps catch typos or other mistakes in payment instructions.

Split Authentication

This feature provides advanced protection through the use of payment-specific credentials to help prevent payments fraud in the event of an account take over. When enabled, the credentials used to login to CMOL must be different from the credentials used to create, edit, and approve payments. For example, a user logs into CMOL with Secure Browser and then is prompted to complete multi-factor authentication to create a wire.

Payee Creation/Change Notification

CMOL sends a notification through its Subscription service any time a new payee is saved, or when bank details (ABA/Routing Number or Account Number/IBAN) are updated for an existing saved payee. This feature helps notify the company if unauthorized changes are made to payee details. It can also be used to inform other departments within the company of legitimate payee changes that they too may need to make.

Status Change Notifications

CMOL sends a notification through its Subscription as ACH and Wires change status. Users select which status(es) to receive notifications about. For auditing purposes, these notifications can also be delivered to users who are not allowed to create payments. This feature helps keep the company informed about all ACH and Wire payments created to help detect potentially fraudulent transactions.

SECURE BROWSER

The CMOL Secure Browser is an award-winning product that protects your online banking sessions with layered security features.

Multi-factor Authentication

The Secure Browser uses an authentication method recommended by most payment processing regulatory bodies and cyber security organizations.

Encrypted Keyboard Driver

All keystrokes performed in the Secure Browser are encrypted to keep your data safe in the event that there is malicious software already on the PC trying to capture sensitive information.

SSL Certificate Site Verification

The Secure Browser validates the SSL certificate of every site, every time you access it to prevent being redirected to an unauthorized website.

Self-Assessment

The Secure Browser performs a self-assessment each time it is launched to ensure that it’s files and folders have not been tampered with. If a file or folder has been unexpectedly altered, the browser will prevent access to online banking sites.

ADDITIONAL RESOURCES

Cybersecurity & Fraud Prevention Resources

Cash Management Sales Manager

Contact your Cash Management Sales Manager for more information on fraud prevention services available to you.

Internet Crime Complaint Center (IC3) https://www.ic3.gov/

A division of the FBI, this site provides comprehensive reports of reported internet crimes, consumer and industry alerts, information about common and emerging scams, and more. If you are a victim of an internet crime professionally or personally, use this site to report this incident.

Federal Trade Commission (FTC) https://www.ftc.gov/

This site provides valuable, easy to understand information and tools for businesses large and small to learn about and prevent various types of fraud.

Cybersecurity & Infrastructure Security Agency (CISA) https://www.cisa.gov/

This site provides information and updates targeting cybersecurity and information security professionals. Resources include publications, virtual workshops, and in-person training.

Cyber Security Insurance Policy

In addition to taking steps to prevent fraud, you can also help protect your company against losses in the event fraud occurs.

Cyber Security Insurance (also known as Cyber Liability) policies protect businesses against financial losses due to system hacking, ransomware attempts, and data breaches at your company or a vendor where your data is stored.

Coverage can include forensic services to investigate breaches, help navigating regulatory obligations and customer communications, reimbursement of lost income due to business disruption, and more.

Speak to your insurance agent for additional details on cyber security insurance and how you can protect your company.

PCSBbank®

Member FDIC

CONTACT US

PCSB Bank Cash Management

Support: (914)248-4401

Sales: (914)248-4385

cashmanagement@mypcsb.com

www.pcsb.com