craft bank

2nd QUARTER 2023

PAYMENTS NEWSLETTER

FOR TREASURY CLIENTS

CHECK FRAUD WARNING FOR BUSINESSES: SIGNIFICANT INCREASES IN CHECK MAIL THEFT

Check fraud can take many forms, but in most cases it involves the attempt to pay for goods using stolen, altered, or counterfeited checks. The FBI reports that U.S. mail fraud, including check fraud, is the largest source of illicit proceeds in the United States, and businesses should be aware of the significant increases in checks being stolen from mailboxes and in postal service locations.

This type of check fraud generally targets the U.S. mail to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Business checks are inherently more vulnerable, as business accounts are typically well funded, and businesses may not be aware of the fraudulent activity immediately and especially in larger accounts.

It is important that businesses remain vigilant when writing and mailing their checks and understand the significant increase in this type of fraud and the ease by which fraudsters can perpetrate such fraud.

1. **Sign up for Positive Pay Services –** Positive pay provides the tool to protect you from checks and/or ACH presented for payment so you can determine which checks and/or ACH should be paid or rejected. As there is a short window to return any unauthorized entries (24 hours), timing is of the essence, and the use of the positive pay system allows a business client to stay in control of authorized vs. unauthorized payments. With increased fraud and corporate account losses, this tool benefits you and protects your money from being stolen.
2. **Review Your Account Daily** – It is important for businesses to review their accounts daily to ensure that transactions posted to the account are authorized and any unauthorized activity is reported to the financial institution immediately.
3. **Promptly Pick Up Mail** – Don't leave letters and packages in your mailbox or at your door for any length of time.
4. **Inquire About Overdue Mail** – If you do not receive a check, credit card, or other valuable mail you're expecting, contact the sender as soon as possible to inquire or put a stop payment on the check.
5. **Don't Send Cash –** Don't risk sending cash in the mail.
6. **Arrange for Proper Pick-Up of Mail –** If you cannot be at your office or home office to receive a package, arrange for prompt pickup.
7. **Use Hold-for-Pickup Service** – When shipping packages, use the hold-for-pickup option, and the recipients can collect the package at their local post office.
8. **Request Signature Confirmation** – When mailing something important, consider requesting signature confirmation for the intended recipient.
9. **File a Change of Address** – If you move your office location, make sure you file a change of address with the postal service, and let your financial institutions know as well.

EMAIL COMPROMISE (BEC): DO YOU KNOW WHO IS ON THE OTHER SIDE OF A PAYMENT REQUEST?

Business email compromise (BEC) — also known as email account compromise (EAC) — is one of the most financially damaging online criminal schemes. This type of crime exploits the fact that individuals rely on email to conduct business — both personal and professionally. In a BEC scam, criminals send an email message that appears to come from a known source, often from someone from within the same company such as a CEO, COO, or other management position making a legitimate request for payment:

- A request to pay a vendor (known vendor but with different payment instructions)

- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A request to pay a client for overpayment.

Businesses continue to be the targets of fraudsters' attempts to access sensitive information for the purpose of transmitting funds out of the business account. While businesses may already have internal controls against such fraud, it is imperative to be on the lookout for these types of attacks, as fraudsters are getting bolder and more strategic in their quest to steal funds from businesses of all sizes. There are different types of compromised email scams, including:

The key for fraudsters is to impersonate a company's executives (e.g., CEO, CFO, COO) to discourage employees receiving the fraudulent payment instructions from challenging or confirming the order. Fraudsters will typically use excuses such as "in a hurry to get the payment out," "at a funeral and can't receive a phone call from bank to validate payment," or "boarding a plane, and I don't have cell reception to validate the wire transfer." Don't be the victim of such trickery.

Other BEC warnings of fraud:

- Poor grammar and spelling
- Suspicious responses from customers and vendors
- Last-minute wire transfer requests of changes to a recurring wire transfer payment
- Missing signature line
- Customer states they cannot be reached via phone
- Software expiration notification (e.g., Microsoft, McAfee, etc.)
- Target emails to individuals responsible for handling wire transfers within a specific business.
- Spoof emails that very closely mimic a legitimate email request (e.g., "Code to admin expenses" or "Urgent wire transfer")
- Fraudulent email requests for a wire transfer are well worded, specific to the business being victimized

FRAUD PREVENTION TIPS

1. **DON'T SHARE SENSITIVE INFORMATION ONLINE:** Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
2. **DON'T CLICK ON AN UNSOLICITED EMAIL:** Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing) and call the company to ask if the request is legitimate.
3. **EXAMINE EMAIL ADDRESSES:** Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
4. **BE CAREFUL ABOUT DOWNLOADING**: Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
5. **SET UP MULTIPLE SECURITY PROCEDURES:** Set multiple security procedures with your financial institution and never disable them.
6. **VERIFY PAYMENT REQUEST IN PERSON OR OVER THE PHONE WITH PEOPLE YOU KNOW:** Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
7. **DON'T BE PRESSED TO SEND MONEY:** Be especially wary if the requestor is pressing you to act quickly. Stop, validate, and proceed with caution.
8. **TRAIN ALL EMPLOYEES:** it is important to train all employees on these attacks. Remember, it only takes one employee to click on a link and approve a payment.
9. **DON'T DO BUSINESS SOLELY FROM AN EMAIL:** If you receive a fraudulent email and email a payment instruction based on this email, you are opening yourself up to significant risk. Slow down, authenticate the request, and discuss internally with management. Fraudsters depend on you NOT to verify the request/instruction to send a payment.
10. **CONTACT US IF YOU FEEL YOUR ACCOUNT HAS BEEN COMPROMISED:** Timing is of the essence with fraud. It is important that you report any unusual activity and/or request immediately so that we can turn off any payment channel that has been compromised.