First American Bank & Trust

PAYMENTS NEWS
FOR TREASURY CUSTOMERS

4th QUARTER 2022

BE ALERT, PROTECT YOUR ACCOUNT AND DON'T BE THE VICTIM OF FRAUD

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 we rely on email to conduct business—both personal and professional. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like in these examples:

- A vendor your company regularly deals with sends an invoice with an updated mailing address.
- 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.

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:

Law enforcement has found that the top three sectors commonly targeted in BEC schemes are the following:

1. manufacturing and construction (25% of reported BEC cases);
2. commercial services (18%);
3. real estate (16%).

Fraudsters typically tailor their methods to specific industries based on the likelihood of success. For example, BEC scams, especially those targeting financial firms, continue to leverage common methods of impersonating 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 be with 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

⚠ **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.

⚠ **DON'T CLICK ON 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.

⚠ **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.

⚠ **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.

⚠ **SET UP MULTIPLE SECURITY PROCEDURES:** Set multiple security procedures with your financial institution and never disable them.

⚠ **VERY 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.

⚠ **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.

⚠ **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.

⚠ **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.

⚠ **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.

NACHA RULES CHANGE ON MICRO-CREDIT VALIDATION There are Nacha Rules ("Rules"} that

are now in effect that you should understand specific to validating account information. Micro-credits are used to test the validity of an account and one of the ways Originators of WEB debits are validating the account as a fraud tool prior to initiating future WEB debits. This Rule defines Micro-Entries as ACH credits of less than $1, and any offsetting debits, for account validation. There are two phases of this rule with the first phase that became effective September 16, 2022. This Rule

- Requires that credit amounts must be equal to, or greater than, debit amounts, and must be transmitted to settle at the same time.
- Originators must use **"ACCTVERIFY"** in the company entry description field.

- Company name must be easily recognizable to Receivers and the same or similar to what will be used in subsequent entries.

The second phase becomes effective March 17, 2023, requiring Originators to use a commercially reasonable fraud detection system to validate the account. Stay tuned for more details on upcoming Nacha Rules.

WE WISH YOU A SAFE AND HAPPY HOLIDAY!