DECEMBER 2024

PCSB bank The Incredibly Neighborly Commercial Bank

CASH MANAGEMENT SECURITY TIPS

ON THE LOOKOUT

BEC is a scheme where fraudsters pose as legitimate known sources to request payments or gain sensitive information. For example, a fraudster may:

·Use email addresses or websites with slight variations of legitimate email addresses or companies to mislead recipients into thinking they are interacting with the legitimate business.

·Send links or attachments that install malware to gain access to business data including passwords and/or financial information.

·Send spear phishing emails that appear to be from a trusted source to trick recipients into revealing sensitive information in order to carry out the scam, or request payments.

ALWAYS Confirm Payment Instructions

When a payee requests payment instruction changes for ACH or Wires, the Bank recommends following up with the payee in person or by calling a known phone number to verify requested changes PRIOR to modifying payment instructions. This additional step can assist in safeguarding your payments as Businesses and Financial Institutions continue to see an increase in Business Email Compromise (BEC).

The Federal Bureau of Investigations (FBI) began researching BEC in 2013. Over a decade later, it remains one of the most widely used methods of attack utilized by fraudsters. Fraudsters perpetuate fraud by exploiting the sense of security people associate with familiarity, whether that be a known email address or recognizable email format. The best way to combat BEC is for businesses and their business partners to have a thorough and dependable verification process in place for exchanging payment information. Fraudsters target all parties involved in a transaction from the payee to the bank, ultimately making us all allies in preventing fraud.

Dual control offers an added layer of protection that is recommended by the Bank to protect unauthorized payments from being made via ACH and Wire products. Dual control may not prevent fraud attempts through BEC, but it gives businesses another opportunity to catch and question any new or updated payment instructions

Micro-Entries

Businesses with ACH services can use micro-entries to validate payee accounts before originating larger dollar transactions. This makes micro-entries are a great tool to use when confirming new or updated payment instructions.

How can I use micro-entries to verify an account?
When you receive new or updated payment instructions, you can send a micro-deposit then use a confirmed contact method to have the payee verify the payment was received BEFORE sending any additional funds. This process confirms that payment instructions came from a legitimate source and the addition/update was implemented correctly.

Additionally, best practice is to be particularly suspicious of last-minute and urgent requests to change payee account details. A standard process where creating micro-entries when adding or updating payee account information, and an alternate process that requires additional reviews or validations if microdeposits are skipped, helps prevent online banking users succumbing to the pressure often applied by fraudsters.

What is a Micro-Entry?

A micro-deposit is an ACH Credit (and any offsetting ACH Debit) under $1 containing "ACCTVERIFY" in the Company Entry Description for the purpose of verifying an account. Credit amounts must be greater than or equal to debit amounts, and be transmitted to settle simultaneously. Micro-entries are also known as micro-deposits or test transactions.

Electronic Payment Services Reduce Check Fraud

Although the use of checks has declined, check fraud remains on the rise. Checks are a fast and easy way for fraudsters to gain information and funds. While the Bank offers services to help prevent check fraud, reducing the number of checks you issue and utilizing alternative payment methods is the most effective way to reduce the risk of check fraud. If issuing checks, the Bank strongly advises against placing them in the mail.

The Bank offers a variety of Electronic Payment services that are safe and convenient alternatives to checks. Discover more about these services in our Electronic Payments Comparison document.

CONTACT US
PCSB Bank Cash Management
(914) 248-4401
cashmanagement@mypcsb.com
pcsb.com

PCSB bank The Incredibly Neighborly Commercial Bank

Online Banking Access Reviews

Did you know it is best practice to perform frequent reviews of your company's Cash Management Online profile?

Following the steps outlined below regularly will help to mitigate unauthorized account access, reduce losses should fraud occur, and assist the Bank in maintaining the most up to date contact information for you and your online banking users.

- Verify that email addresses and phone numbers are correct for all users.
  - Ensures users are able to receive critical updates from online banking.
  - Keeps the bank's contact information for your users up to date.
- Remove users who have transitioned to other roles, left the company, or otherwise no longer need access to online banking.
  - Ensures that access to sensitive information or activity is limited to applicable roles and responsibilities within your organization.
  - Reduces the number of online banking users that could be targeted for fraud, such as account takeover attempts.
- Review ALL user's payment permissions.
  - Confirm all users permitted to create payments should continue to have that responsibility. Reconsider users who are permitted to create payments but have not done so since the last review performed.
  - Verify user's payment limits are still acceptable for their role.
  - Verify that there are enough backup users to perform critical duties such as payment approval.
- Review last login date of users in Locked Out and Deactivated status.
  - Reconsider access for users who have a login date greater than 90 days and are locked or deactivated.
- Require all online banking users perform cybersecurity and fraud prevention training.The Federal Trade Commission (FTC) site offers FREE videos and quizzes you can share to help inform or remind your users about different types of fraud and how to prevent them.