ARMSTRONG BANK

CORPORATE USER
PAYMENTS EDUCATION

ACH

Rules Update - *What's new for 2026?*

- **Standard Entry Descriptions** – As an effort to better identify fraudulent transactions, effective March 20, 2026, two standardized Company Entry Descriptions are being established.
  - **PAYROLL** – must be used for transactions using the PPD SEC Code that are for the payment of wages, salaries, and other similar types of compensation.
  - **PURCHASE** – must be used when debiting for an online purchase of goods.
- **Fraud Monitoring –** Beginning in 2026, the Rules will require each Originator establishes and implements risk-based processes and procedures that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses. At least annually, the parties subject to this requirement must review their processes and procedures and must make appropriate updates to address evolving risks.

  This means that businesses that originate ACH payments will be required to have practical, risk-based procedures in place to help identify ACH transactions that may be unauthorized or approved under false pretenses (such as fraud or scams). These procedures should be appropriate for your business and designed to catch suspicious activity. At least once a year, you must review these procedures and update them as needed to keep up with new and changing risks.

Fraud Monitoring Considerations – *What do I need to include?*

Your risk-based processes and procedures will be as unique as you are, but there are a few basic considerations to help with the development process.

- Put procedures in place to protect against account takeovers and other types of fraud. Make sure employees are educated on common fraud schemes, including those that come through emails, phone calls, faxes, or mailed letters.
- Train employees to slow down, question, and independently confirm any changes to payment instructions, payment methods (for example, switching from ACH to a wire), or requests that create pressure to act quickly or keep information secret.
- Remind employees never to share online banking login credentials or account information with anyone—even if the request appears to come from your financial institution.
- Verify bank account information for first-time payments by using tools such as ACH prenotes or small test (micro) deposits.
- Review your bank and ACH activity regularly, ideally on a daily basis, to quickly spot any unauthorized or unusual transactions.
- Do not rely solely on email for payment instructions. Always verify email requests using a different method, such as a phone call or a written request.
- Use Dual Control for ACH processing. This means one person creates or edits ACH information and a different person releases it to the bank, reducing the risk of errors or fraud.
- Use the correct SEC codes in ACH batches. SEC codes identify whether payments are for businesses or individuals and how the authorization was obtained. Using the proper code helps ensure correct return timeframes and reduces unnecessary returns, leading to smoother processing.

ARMSTRONG BANK

CORPORATE USER PAYMENTS EDUCATION

BUSINESS BEST PRACTICES

Business Email Compromise (could also be known as Email Account Compromise or "EAC")

Business Email Compromise (BEC) is one of the most prevalent and financially detrimental cybercrimes targeting organizations of all sizes. This type of attack capitalizes on the widespread reliance on email for both personal and professional communication. In a BEC scheme, criminals send fraudulent emails that appear to originate from a trusted source, making a seemingly legitimate request. Examples of BEC could include an email that appears to be from a familiar vendor that contains an invoice with updated payment details or an email that impersonates an employee requesting a change to their payroll deposit account information. These scams have resulted in significant financial losses and reputational damage for the affected businesses.

Recommended Prevention Tips

- Use dual-verification or authentication outside of email communication to verify requests for account information changes.
- Verify that the sender's email address matches the email address on file for that sender.
- Be alert for misspellings of the address domain for example: **abc-organization.com** instead of **abcorganization.com**.
- Avoid providing login credentials or personal identifiable information (SSN, account information, etc.) by email.
- Monitor your financial accounts on a regular basis for irregularities, such as missing deposits.

What to do if you have experienced BEC?

Immediately reach out to our Treasury Operations department at 888-221-2265 for assistance.

Learn More

EPCOR Corporate User Webpage: https://www.epcor.org/wcm/Corporate_User/wcm/Corporate_User.aspx
NACHA Business Email Compromise Response Plan: https://www.nacha.org/system/files/2024-07/Business%20Email%20Compromise%20Action%20Plan.pdf
EPCOR YouTube Small Business Fraud Series: https://www.youtube.com/playlist?list=PLVyjCXE5rUTHDCDCZWgIB0ksM-FtTLq0U