Q4 2025

Payments Newsletter

For Treasury Customers

Business Email Compromise: The Billion-Dollar Cyber Threat Every Company Must Address

Businesses worldwide are encountering a rapidly growing cybersecurity threat: Business Email Compromise (BEC). This sophisticated form of cyberattack has become one of the most financially damaging crimes, targeting companies of all sizes to steal sensitive information and funds.

What is Business Email Compromise?

Business Email Compromise is a type of cyberattack in which criminals use email fraud to manipulate employees, executives, or financial teams into transferring funds, providing access to sensitive accounts, or disclosing confidential data.

Hackers often impersonate trusted individuals (such as CEOs, vendors, or business partners) by using tactics like phishing, domain spoofing, or email account takeovers.

BEC attacks are particularly dangerous because they rely on social engineering rather than malware. This makes them harder to detect with traditional cybersecurity tools.

Common Scenarios of BEC Attacks

- **Invoice Fraud:** Cybercriminals impersonate vendors or suppliers, requesting payment for fake invoices.
- **Executive Impersonation:** Hackers pose as senior executives and instruct employees to make urgent wire transfers.
- **Payroll Diversion:** Attackers trick HR departments into redirecting an employee's paycheck to fraudulent accounts.
- **Gift Card Scams:** Fraudsters request bulk purchases of gift cards, claiming it’s for corporate purposes.

How Companies Can Protect Themselves Against BEC

Given the sophistication of BEC attacks, businesses must adopt a multi-layered approach to defend against this threat.

- **Employee Awareness and Training:** Since BEC attacks rely heavily on social engineering, employee education is the first line of defense. Regularly train staff to recognize phishing emails, verify unusual requests, and avoid clicking on suspicious links. Ensure that employees understand the tactics used by attackers and know how to respond.
- **Implement Multi-Factor Authentication (MFA):** MFA adds an additional layer of security by requiring users to verify their identity through multiple methods, such as a password and a mobile authentication app. This makes it significantly harder for hackers to gain access to email accounts, even if credentials are compromised.
- **Verify Requests Independently:** Encourage employees to double-check financial requests or

changes to payment details by contacting the requester via a known, trusted communication channel, such as a phone call, rather than replying to the email. Avoid relying solely on email for sensitive financial transactions.

- **Secure Email Accounts and Enforce Strong Passwords:** Ensure email accounts are protected by strong passwords and encryption. Regularly monitor for unauthorized access and implement security tools to identify suspicious activity. Consider using anti-phishing software to flag malicious emails before they reach employees.
- **Adopt Domain-Based Authentication Protocols:** Set up domain-based email authentication protocols, such as DMARC, SPF, and DKIM, to prevent email spoofing. These measures help verify that incoming emails are genuinely from the claimed sender.
- **Limit Access to Sensitive Information:** Restrict access to financial accounts, payroll systems, and other sensitive data to only those employees who need it. This minimizes the risk of unauthorized transfers or leaks.
- **Create a Response Plan:** Develop a clear response plan for BEC incidents. Employees should know whom to contact and what steps to take if they suspect they've been targeted. Quick action can prevent financial losses or reduce their impact.

The Human Factor: A Key Vulnerability

Human error remains the most common entry point for attackers. Cybercriminals count on employees to act impulsively or fail to verify requests. By combining technology with ongoing employee education, businesses can significantly reduce the risk of falling victim to these attacks.

By fostering a culture of cybersecurity awareness and implementing robust defenses, businesses can stay one step ahead of cybercriminals and ensure their financial security.

Get Prepared for the Upcoming Nacha (Network) Rules: Company Batch Header Requirements — Effective March 20, 2026

Reduce ACH Fraud Risks: PAYROLL and PURCHASE Descriptions Are Coming Soon: As part of the ACH Network's ongoing efforts to reduce fraud and improve the recovery of funds, two new rules will take effect on March 20, 2026. These amendments introduce standardized Company Entry Descriptions — "PAYROLL" and "PURCHASE" — to bring greater transparency to transactions and strengthen risk mitigation. Here's what you need to know to stay compliant and protect your business.

REQUIRED DESCRIPTION	DETAIL
PAYROLL	This description must be used for PPD credit entries related to wages, salaries, and similar compensation payments. It allows Receiving Depository Financial Institutions (RDFIs) to monitor payroll activity more effectively, potentially supporting logic for early funds availability and helping reduce payroll fraud risks.
PURCHASE	This descriptor applies to WEB debit entries (and certain TEL entries under Standing Authorization) for e-commerce transactions, including recurring purchases first authorized online. While ODFIs are not required to verify the accuracy of the descriptor, its standardized use can enable better identification of e-commerce transactions.

Effective Date and Early Adoption

The rules officially take effect on March 20, 2026, but Originators may begin using the descriptors sooner. This provides flexibility for businesses to update systems and processes ahead of the compliance deadline.

Anticipated Benefits

- Enhanced fraud prevention through better identification of transaction purposes.
- Improved monitoring capabilities for receiving institutions, particularly for payroll transactions and e-commerce debits.
- Standardized data can help streamline risk management practices and improve the overall quality of ACH transactions.

Frequently Asked Questions (FAQs) to assist you in preparing for the change

Is the use of the new Company Entry Description "PAYROLL" mandatory for all Originators?

Yes, starting March 20, 2026, all PPD credit entries for wages, salaries, and similar compensation must use "PAYROLL" in the Company Entry Description field.

Does this requirement apply to payments for contract (1099) employees?

Yes, payments to contract workers that qualify as compensation fall under this rule.

Why is the "PAYROLL" descriptor required?

The descriptor helps RDFIs monitor payroll transactions more effectively, enabling early detection of fraudulent activity such as payroll redirection schemes.

Can Originators use additional descriptive text in the Company Entry Description field?

Yes, Originators may use the remaining characters in the field for additional information, provided "PAYROLL" or "PURCHASE" is present as required.

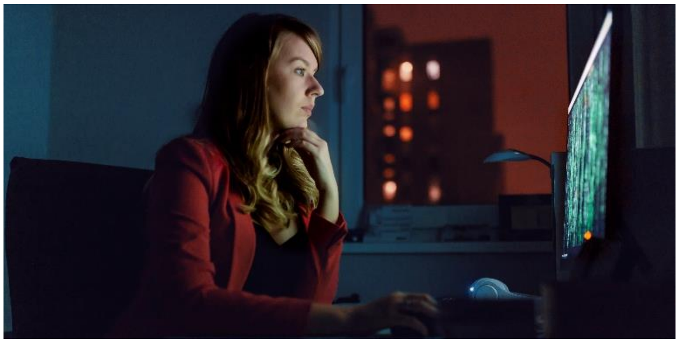
Are receiving institutions required to monitor transactions with the descriptor "PAYROLL"?

No, receiving institutions are not obligated to act on transactions bearing the "PAYROLL" descriptor, but the amendment provides intelligence that RDFIs may choose to leverage for monitoring or funds availability.

If you have any questions about these rules or need assistance with implementation, reach out us today!

How to Prepare

- **System Updates:** Work with your third-party service providers and internal IT teams to ensure systems you use to create files (e.g., Wave, Quickbooks, Gusto, etc.) can accommodate the required Company Entry Descriptions. This includes updating software to automatically populate the correct descriptors for applicable transactions.
- **Policy Review:** Review your organization's internal ACH policies and procedures to align with the upcoming changes.
- **Early Adoption:** Consider implementing the descriptors before the mandatory deadline to ensure a smooth transition and avoid last-minute compliance challenges.



Stay Ahead of ACH Fraud: Preparing for New Monitoring Rules

Starting in March 2026, Nacha is introducing new fraud monitoring requirements that will impact Originators, Third-Party Service Providers (TPSPs), Third-Party Senders (TPSs), and ODFIs with high ACH origination volumes. As a Treasury Management or Cash Management professional, understanding these changes early will help your business stay compliant.

What’s Changing?

- **Phase 1 (Effective March 20, 2026):** Applies to ODFIs and non-consumer Originators, TPSPs, and TPSs with 6 million or more ACH originations in 2023.
- **Phase 2 (Effective June 19, 2026):** Expands to all remaining non-consumer Originators, TPSPs, and TPSs.

What’s Required?

- Entities must establish risk-based processes and procedures to identify ACH entries initiated due to fraud.
- Processes should be tailored to the entity’s role in the ACH Network and reviewed annually.
- ODFIs can consider fraud monitoring steps already implemented by other participants (e.g., Originators and TPSPs) when designing their own procedures.

Fraud Scenarios to Address

The rules highlight False Pretenses, including frauds involving:

- Business Email Compromise (BEC)
- Vendor impersonation
- Payroll impersonation
- Account takeover schemes

These scenarios focus on payments induced by misrepresentation but do not cover scams involving fake goods or services.

How Should You Prepare?

Evaluate Current Processes

If your business already monitors for fraud in WEB debits or Micro-Entries, you may be ahead of the curve. However, you should assess whether your current systems can handle expanded fraud detection responsibilities for other transaction types.

Collaborate with Us

We may reach out to discuss compliance requirements or request proof of your fraud monitoring procedures. Be proactive in asking questions and seeking guidance to ensure your systems align with the new rules.

Begin Planning Now

The effective date may seem far off, but preparing early can help avoid last-minute compliance challenges.

Stay Informed

These rules are part of a broader initiative to reduce fraud and improve ACH transaction quality. We will continue to provide information on additional rules changes or clarifications.

Anticipated Benefits

- **Enhanced Fraud Prevention:** Expanding monitoring responsibilities across more ACH participants improves detection of fraudulent activity, especially in credit-push payments.
- **Improved Transaction Quality:** Risk-based monitoring reduces fraud attempts, leading to a cleaner ACH Network and better outcomes for all participants.

Warm Wishes for a Joyful Holiday Season!