PAYMENTS FRAUD TRENDS & PREVENTION

According to the Association for Financial Professionals (AFP), **79% of organizations were impacted by fraud in 2024**[1]—highlighting an urgent need for heightened awareness. At Busey, we understand that protecting your business means more than just managing your finances—it means safeguarding your assets and information from constantly evolving threats.

Your safety is our priority. Through our robust suite of Treasury Management solutions, we are committed to keeping you informed, vigilant and confident in your risk mitigation plan.

HOW BUSEY CAN HELP

Here are a few ways we can help protect you and your organization:

POSITIVE PAY SOLUTIONS

- Use Check Positive Pay to match check number, amount and payee name
- Enable ACH Positive Pay to filter and block unauthorized debits

ACH & WIRE TRANSFER CONTROLS

- Set appropriate daily/monthly limits for ACH and wire transfers
- Use temporary limit increases for one-time or occasional large payments
- Require dual authorization for all outgoing payments (ACH, wire)
- Ensure secondary authorizer is different from initiator

ACCOUNT MONITORING & RECONCILIATION

- Perform daily account reconciliation
- Use account segregation to isolate high-risk transactions
- Leverage digital banking alerts to monitor for signs of suspicious activity

AUTHENTICATION & ACCESS CONTROLS

- Require multi-factor authentication (MFA) for all banking platform users
- Immediately remove access for terminated or unauthorized employees
- Use secure portals for vendor onboarding and bank detail changes

[1]Association for Financial Professionals (2025) *2025 AFP® Payments Fraud and Control Survey Report,* Truist

WHAT IS BUSINESS EMAIL COMPROMISE (BEC)?

BEC is a sophisticated scam in which fraudsters impersonate trusted individuals—such as company executives, coworkers, vendors or bank employees—to deceive businesses into sending money or other sensitive information such as digital banking user credentials. Using techniques like phishing, email spoofing or hacking, attackers mimic or gain access to legitimate accounts and send convincing requests for wire transfers or payment changes. These scams often involve altered invoices or fraudulent payment instructions that appear authentic, leading victims to unknowingly transfer funds to the attacker's account.

MOST COMMON TYPES OF BEC FRAUD

- **79%** EMAIL SPOOFING
- **56%** DOMAIN LOOKALIKE
- **44%** EMAIL ACCOUNT TAKEOVER

MOST COMMON PAYMENT METHODS UTILIZED IN BEC SCAMS

- **63%** WIRE TRANSFERS
- **50%** ACH CREDITS
- **26%** CHECKS

REMINDER

Busey will never contact you or your employees to ask for digital banking login information—such as usernames, passwords, PINs or one-time passcodes—or request access to your device.

If you receive suspicious communication from someone claiming to be with Busey, **do not respond, click any links or open any attachments.**

ACCORDING TO THE AFP, OUT OF REPORTING ORGANIZATIONS IN 2024:

- **79%** Experienced fraud attempts
- **63%** Were impacted by BEC
- **63%** Were targeted by check fraud
- **95%** Who used positive pay found it effective for combating check fraud
- **65%** Reported that positive pay was the top means for payments fraud discovery

While your bank plays a key role in protecting your accounts, safeguarding your organization starts within.

By staying informed, training employees, strengthening internal controls and implementing verification measures, you can significantly reduce risk.

Below are some proactive steps and best practices to help you prevent fraud and protect your business.

VENDOR & PAYMENT VERIFICATION

Always perform callback verification using known contact information before updating vendor payment details

Avoid relying solely on email for sensitive payment instructions

91% of organizations found this to be effective in helping to reduce fraud

GOVERNANCE & SEGREGATION OF DUTIES

Establish clear segregation between cash management, reconciliation and approval functions

Centralize payment processes to reduce manual check issuance

87% of organizations found similar measures effective for combating fraud

ONGOING EMPLOYEE TRAINING & AWARENESS

Conduct regular training on phishing, BEC scams, suspicious behavior and how to identify spoofed emails and domain lookalikes

Train employees to question urgency and confirm requests through known, trusted channels

84% of organizations found regular training to be effective for minimizing fraud

EMAIL & NETWORK SECURITY

Use email filtering and external banners to **flag suspicious messages**

Implement strict access controls and monitor system activity

91% of organizations who adopted additional layers of network security found it helpful for reducing fraud

POLICY & RISK REVIEWS

Periodically review fraud risk exposure, especially with outsourced functions and fintech partners

Audit exception reports and **approval workflows** regularly

93% of organizations who implemented company-wide verification policies found it effective in fighting fraud

For more information, tips and resources for preventing fraud:

Scan to visit Busey's Fraud Prevention FAQs

Scan to subscribe to our Money Matters blog

Busey BANK®
Member FDIC