WELLS FARGO

Commercial Banking

2023 Payments fraud update

Fraud concerns keep companies up at night

78% Companies that perceive **fraud threat levels** have increased in the past year

Source: Strategic Treasurer & Bottomline, "2023 Treasury Fraud & Controls Survey Report"

Once vs. 100% is how often **payment fraudsters need to succeed** in their attempts, compared to the **vigilance employees must maintain.**

Source: Abnormal Security, H1 2023 Email Threat Report

Organizations of all sizes, all industries, are targets for payments fraud. Keeping pace with the ever-changing fraud landscape is vitally important for corporate treasurers and finance professionals.

As fraud techniques become more sophisticated, strong internal controls, ongoing education, targeted technologies, and open communication with your bank can help mitigate your risk and provide peace of mind.

Ransomware steals the headlines, but BEC poses a greater risk

What is Business Email Compromise (BEC)?

Also known as imposter fraud

A fraudster impersonates a vendor, a company executive, or another trusted trading partner, ultimately tricking you into making the payment to them.

This kind of fraud is very hard to detect because you have been deceived into actually being the one making the payments.

FBI fraud complaints in 2022

~22,000 Business Email Compromise

9x greater

Less than 2,500 Ransomware

Source: Federal Bureau of Investigation, "Internet Crime Report 2022"

8 in 10 companies reported actual or attempted **BEC losses, totaling . . .**

Over $2.7 billion in fraud losses in 2022

Source: Federal Bureau of Investigation, "Internet Crime Report 2022"

+13% **increase** compared to 2021 fraud losses

Checks remain the most vulnerable payment method

Paper items present more opportunities for fraudsters, from mail theft to altering dollar amounts or forging signatures. Even blank check stock becomes a valuable commodity in the hands of bad actors.

63% Companies that **experienced check fraud** in 2022

Source: Association of Financial Professionals, "2023 AFP® Payments Fraud and Control Survey"

Turbulent times create ideal fraud opportunities

Any disruption to "business as usual" gives bad actors cover to pursue payments fraud. During these events, company resources may be deployed elsewhere or distracted, making it more challenging to spot and mitigate potential fraud. As threat levels rise, companies must increase their vigilance and take extra precautions to avoid becoming fraud targets.

Examples

- COVID-19 pandemic
- Natural disasters
- Industry turmoil

When innovation occurs, fraudsters follow

53% Companies concerned about **potential fraud risks of faster payments**

Source: Strategic Treasurer & Bottomline, "2023 Treasury Fraud & Controls Survey Report"

Faster payments require a new approach

Irrevocable transactions and speed of settlement make faster payments a growing target for fraud.

Recovering funds paid in error or due to fraud becomes more challenging with real-time payment networks.

As your company adopts new methods, set up clear criteria for when to use real-time payments. Document and train employees on required approvals, reconciliation timeframes, and other controls that will mitigate your risks.

Artificial Intelligence makes spotting fakes more difficult

Deep fakes, ChatGPT, and other AI technology are elevating the quality of fraudsters' attempts. The bad grammar, spelling errors, and poor design of past communications are no longer clear giveaways.

Unfortunately, fraudsters can take the same tools developed to ease our workload and deploy them for malicious purposes.

Scams improve in quality

Bad actors can now engineer hyperlinks that display one address, but take you to another. "Evil Proxy" servers attempt to break down two-factor authentication.

Four ways to protect your payments

In the fight against fraud, there's no silver bullet. You're best protected when you and your bank use a layered security approach. Be at the ready with these fraud prevention best practices. Remember, in the fight against payments fraud, your employees are your greatest asset—and your biggest cybersecurity liability. While your staff must be right 100% of the time, threat actors need to be right only once (and they know it).

Set up strong internal controls

- Implement dual custody on all online payment services (ACH, wire transfer, foreign exchange) and user administration management
- Set dollar limits for initiating payments or using money movement services
- Deploy two-factor authentication to access your corporate network and initiate payments—according to recent AFP research,[1] this is one of the most effective techniques for preventing both BEC and account takeover (ATO) fraud
- Notify your bank immediately when an authorized signatory or approver on your accounts leaves your company
- Establish a process to discontinue payments entitlements for retiring or departing employees

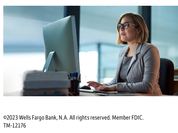
1. Source: Association of Financial Professionals, "2023 AFP® Payments Fraud and Control Survey"

Take a preventive approach

- Never give out passwords, PINs, PINs plus token codes, or other authorization credentials, especially if you receive requests via phone or email from individuals outside your organization
- Validate all payment requests using known sources for contact information
- Reconcile your accounts daily to detect suspicious activity
- Lock your check stock and signature stamps in a secure location
- Update your antivirus and antispyware software and firewalls regularly

Train (and retrain) employees

- Educate payments staff regularly on how to detect, prevent, and report BEC, phishing, and other fraud schemes
- Deploy frequent communications to remind employees they are the first line of defense against fraud



Be active with your bank

- Work with your relationship manager to add fraud prevention solutions such as Fraud Manager, ACH Debit Block, Positive Pay, and Account Validation Service
- Notify your bank immediately if your contact information (name, phone number, email, password) in Wells Fargo Vantage[SM] changes without you initiating the change

©2023 Wells Fargo Bank, N.A. All rights reserved. Member FDIC.
TM-11276