Ransomware steals the headlines, but BEC poses a greater risk

What is Business Email Compromise (BEC)?
BEC also known as dumpster fraud.
BEC is a sophisticated social engineering attack that uses manipulated emails to trick employees into giving away sensitive information.

Companies reported actual or attempted BEC losses, totaling ~22,000.

Fraud concerns keep companies up at night
Companies concerned about potential fraud costs of faster payments.

Companies that perceive risks of faster payments have adopted stronger internal controls that will mitigate your risks.
In the fight against fraud, there’s no silver bullet. You’re best protected when you and your bank use a layered approach.
When innovation occurs, fraudsters follow.

Related: 2023 Payments Fraud and Control Survey
Source: Association of Financial Professionals, “2023 AFP® Payments Fraud and Control Survey”

4. Companies that perceive faster payments are challenging to spot and mitigate potential fraud. As threat resources may be deployed elsewhere or distracted, making it more challenging to spot and mitigate potential fraud.


FBI fraud complaints in 2022

The bad grammar, spelling errors, and poor quality of fraudsters’ attempts.
Deep fakes, ChatGPT, and other AI technology are elevating the quality of fraudsters’ attempts.

Deeper fraud attempts, lower success rate.
Artificial Intelligence makes spotting fakes more difficult.

Faster payments require a new approach
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 how to recognize legitimate requests versus those made by fraudsters.

Take a preventive approach

FBI fraud complaints increased in 2023

Increase compared to 2021 fraud complaints

Companies that perceive faster payments have adopted stronger internal controls that will mitigate your risks.

Do not give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.

Never give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.

When innovation occurs, fraudsters follow.
When your company adopts new methods, set up clear criteria for when to use real-time payments. Document and train employees on how to recognize legitimate requests versus those made by fraudsters.

Take a preventive approach

Your company has adopted new methods, set up clear criteria for when to use real-time payments. Document and train employees on how to recognize legitimate requests versus those made by fraudsters.

Train (and retrain) employees

- Educate payments staff regularly on how to detect, prevent, and respond to potential fraud.
- Implement and enforce a process to discontinue payments entitlements for retiring or departing employees.
- Deploy frequent communications to remind employees to always verify the authenticity of requests before taking any action.
- Lock your check stock and signature stamps in a secure location.
- Reconcile your accounts daily to detect suspicious activity.
- Never give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.
- Conduct periodic reviews of all payments made to ensure accuracy and legitimacy.

Better, faster, stronger internal controls

- Implement and enforce a process to discontinue payments entitlements for retiring or departing employees.
- Deploy frequent communications to remind employees to always verify the authenticity of requests before taking any action.
- Lock your check stock and signature stamps in a secure location.
- Reconcile your accounts daily to detect suspicious activity.
- Never give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.
- Conduct periodic reviews of all payments made to ensure accuracy and legitimacy.

Set up strong internal controls

- Implement and enforce a process to discontinue payments entitlements for retiring or departing employees.
- Deploy frequent communications to remind employees to always verify the authenticity of requests before taking any action.
- Lock your check stock and signature stamps in a secure location.
- Reconcile your accounts daily to detect suspicious activity.
- Never give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.
- Conduct periodic reviews of all payments made to ensure accuracy and legitimacy.

Set up strong internal controls

- Implement and enforce a process to discontinue payments entitlements for retiring or departing employees.
- Deploy frequent communications to remind employees to always verify the authenticity of requests before taking any action.
- Lock your check stock and signature stamps in a secure location.
- Reconcile your accounts daily to detect suspicious activity.
- Never give out passwords, PINs, PINs plus token codes, or other authentication credentials, especially if you receive requests via phone or email from individuals outside your organization.
- Conduct periodic reviews of all payments made to ensure accuracy and legitimacy.

53% Companies concerned about potential fraud costs of faster payments.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.

Turbulent times create ideal fraud opportunities
Any disruption to “business as usual” gives bad actors cover.