BANC OF CALIFORNIA

Payments Fraud: Business Email Compromise

Tips to Protect Yourself and Your Business

At Banc of California, we take the security of your personal information and your banking transactions seriously. As part of our Fraud Prevention program, we are raising awareness of sophisticated payment fraud scams that leverage business and personal email accounts in the commission of fraudulent wire transfers. The financial industry is seeing an increase in business email compromise scams, referred to as BEC. BEC scams target companies that conduct electronic payments. Companies of all sizes are being targeted by cybercriminals located around the world.

What is Business Email Compromise (BEC)?

Business Email Compromise is a scam targeting individuals who have the ability to make payments. In these scams, cybercriminals gain access to an employee's legitimate business email through social engineering or computer intrusion. The criminal impersonates the employee, often a senior executive or someone who can authorize payments, and instructs other employees in the company via email to transfer funds to an account controlled by the fraudsters.

Example:

- A fraudulent email is received by an employee from what appears to be a legitimate source (i.e. CEO or CFO) requesting a new payment be created, or changes be made to an existing payment
- The targeted individual executes the new or altered payment instructions
- The funds are sent to the fraudster instead of a legitimate payee

Fraudsters are clever; employees must always be wary and on the lookout for suspicious activity, and businesses must leverage internal controls to guard against unauthorized payment activity.

See next page for best practices to protect against BEC scams

BANC OF CALIFORNIA

Best Practices to Protect Against BEC Scams

1. Educate Your Employees

You and your employees are the first line of defense against BEC, and should educate yourselves about warning signs, safe practices, proper procedures for funds transfers, and responses to a suspected takeover.

Potential Fraud Indicators:

- Funds transfer requests marked “urgent” or “confidential”
- Abnormal payment activity
- Changes to a vendor’s banking information
- Sudden changes in contacts

Additionally, there are many schemes beside Business Email Compromise, and the FBI and the US Treasury are great sources to research suspicious activity:

https://www.fbi.gov/scams-and-safety/common-fraud-schemes

https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets

2. Protect Your Online Environment

- Do not use unprotected internet connections
- Encrypt sensitive data and keep updated virus protections on your computer
- Use complex email passwords and change them regularly

3. Require Alternative Communication Channels to Verify Significant Requests

- If the payment request was received by email, confirm the payment instructions by phone before approving
- Always validate contact information with your internal system, as fraudsters may append different phone numbers to payment instructions
- Recognize that your business partners may have been compromised as well

4. Require Approvals for Payment-related Activity

Requiring one employee to enter information and another to approve the entry adds a checkpoint to the payment process and reduces the possibility of a non-authorized payment. Each employee should question the payment and pay close attention to payment details.

Examples:

- Require all vendor changes to be entered, reviewed and approved by separate people
- Require all electronic payments to be entered and approved by separate people

5. Always Monitor

- Review Past Payment History
  - Payments usually follow a pattern; be on the lookout for deviations from the norm
- Perform Bank Reconciliation Frequently
  - If a fraudulent transaction was processed, this will help you uncover it faster
- Monitor Vendor Changes
  - Vendor address and banking information does not change frequently, so request supporting documentation to confirm any changes

If you fall victim to a business email compromise scam:

- Contact Banc of California Client Services immediately to notify us about the fraudulent transfer
- Contact your local Federal Bureau of Investigation office immediately; they may be able to freeze or return the funds if notified quickly
- File a complaint, regardless of dollar loss, at www.IC3.gov

For additional questions regarding fraud, please contact Client Services at 877-770-BANC (2262) or your Relationship Manager.

bancofcal.com