



Mar 16, 2023

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[William T. Repasky](#)

[Robert W. Dibert](#)

[Gene F. Price](#)

WARNING – Banking Crisis Could Fuel Increase in Cyber Fraud Schemes

Bank customers currently overwhelmed by mitigating risks associated with accounts, fund recovery and operational issues caused by cash flow and liquidity disruption face another type of vulnerability—cyberattacks. Fraudsters exploit current events as part of their schemes to defraud.

As many depositors, borrowers, individuals and businesses alike are increasingly anxious about the safety of their bank deposits and loan accessibility, you can be sure that fraudsters will not let the present banking crisis go to waste. You should anticipate a new wave of phishing attacks and business email compromise (BEC) attacks.

In response to this anticipated wave due to the failure of Silicon Valley and Signature banks, the federal Cybersecurity and Infrastructure Agency (CISA) warned businesses and consumers to “[e]xercise caution in handling emails with bank-related subject lines, attachments, or links. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to any failed bank.”

Failed Bank Phishing Attacks

Phishing attacks come in many forms. It is possible that new attacks will direct individuals and businesses to verify the safety and soundness of their deposits. Otherwise, they may appear to be coming from a bank or credit union—or perhaps a banking authority like the Federal Deposit Insurance Corporation (FDIC)—asking for the submission of confidential banking information, to download an attachment or providing a link that takes the potential victim to an official looking website. While these attacks may be made by emails, they could also be made by SMS text (“smishing”) or by telephone call (“vishing”).

Handling Bank Phishing Attacks

- Banks, credit unions and governmental agencies (like the FDIC, NCUA or the IRS) never send unsolicited email, texts or phone calls asking for sensitive banking information. Nor will they threaten to withhold deposit insurance from you if you do not respond to such a message.
- Any person who says they, for a fee, can guarantee insurance for your deposits or improve your accounts' deposit insurance rights under the law may be a scammer.
- Never download software or open attachments contained in unsolicited emails. Fraudsters are very good at creating a false sense of urgency. They are also very good at impersonating the look and formatting of banking and governmental webpages.
- Whenever an email, text or telephone call concerning your banking relationships seems suspicious, step away from the communication and verify its authenticity. This can often be done as simply as contacting your neighborhood bank branch or calling your banking relationship manager. Lastly and on this point, do not attempt to verify a suspicious email by calling any telephone number found in that email. Often, fraudsters have a call answer center to assist in their schemes.

Business Email Compromise Attacks

BEC is a criminal scheme where a fraudster impersonates a bank or vendor to trick a person or a business into sending money by wire or ACH transfer to the fraudster's own account. BEC emails typically say that a longtime vendor or some other trusted business (like a bank, attorney or real estate closing office) has changed its banking information for an upcoming payment that is due.

BEC emails can look perfectly legitimate and can look like they are coming to you from a trusted source. BEC attack emails often claim great urgency to compel the target victim to take action quickly. But if victims fall for the scheme and send payments by wire or ACH to the instructions in the fraudster's BEC email, then funds will be deposited into the fraudster's account. Wire or ACH payments made mistakenly are often impossible to reverse.

In today's environment where individuals or businesses are concerned about federal deposit insurance coverage for their funds on deposit, it may be prudent to deposit available cash balances among several banks. If a fraudster should learn of pending funds transfers, they may send emails trying to trick the customer into using the fraudster's account information in the wire or ACH transfer instructions. Company staff responsible for implementing a deposit-distribution strategy must be especially vigilant, as they will be favored targets for BEC attacks.

Handling BEC Attacks

- Never accept an email or text message at face value, especially if it claims that someone has changed their banking account information. A rule of thumb could be to assume that no one ever changes their bank account in the middle of a deal or ongoing relationship.
- Always confirm supposed payment instructions by calling a person you have dealt with before at the bank or vendor. Again, do not use any phone number supplied in a suspicious email, as fraudsters route those calls to others in on the scam.
- For businesses, create a culture of skepticism. In other words, make sure your staff members, who have the authority to originate payments, are educated about BEC risks and feel empowered to seek confirmation whenever suspicious money transfer instructions are received.

If you discover that you have become the victim to a phishing or BEC attack, minutes matter in terms of your ability to get the fraudulent transaction reversed and the funds restored to you. Please immediately call your bank or credit union, law enforcement and your contacts at Frost Brown Todd.

Related Coverage

- [*Silicon Valley Bank Parent Company Files for Bankruptcy*](#)
- [*Bank Failures Lead to Uncertainty in Cash Management Arrangements*](#)

- [Failed-Bank Response Team: Borrower and Lender Perspectives](#)
- [Banking Failures Raise Access and Long-Term Regulatory Questions](#)
- [Frost Brown Todd Launches Coordinated Effort to Support Clients Following Bank Failures](#)
- [Crucial Underwriting Considerations for LHTC Investors in the Wake of Bank Failures](#)

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.