Fraud Tip ~~Friday~~ Tuesday:
Scams Perpetrated by Cybercriminals Capitalizing on the Collapse of Silicon Valley Bank

Following the collapse and federal takeover of Silicon Valley Bank (SVB) on Friday, March 10, scam artists wasted no time preying on SVB's customers. Research and law firms have blogged about the following three scams which have already surfaced since the collapse of SVB just last week. **It's very unlikely that these specific scams will directly touch our customer base. However, it is always best to be educated and vigilant in today's current environment:**

1. **Reports have surfaced of an email scam that initially targeted SVB customers when news first broke, and has only increased in volume following the bank's failure and takeover.** In the scam, fraudsters posing as companies that previously banked with SVB notify them that because SVB cannot accept payments, they should wire future payments to a different bank. The fraudsters own the bank account that is provided in the new wire and payment instructions. The high visibility of the federal takeover makes these communications very convincing. Victims are already skittish about sending money to SVB and eager to instead send their payments to a bank that has not collapsed. The deceptive emails include details such as account numbers and names of individuals within the company that is purportedly making the wire instruction change. However, the wire transfer instructions included in the email are fraudulent and will direct funds to an account controlled by the scammers.
   Everyone should always use an abundance of caution when receiving emails requesting wire transfers or changes to wire instructions, whether they involve SVB or any other financial institution. One should always verify the request by contacting the person making the request directly using a phone number obtained from a reliable source, like the company's official website. Do NOT rely on telephone numbers or email addresses provided within the email that contains the wire change instructions.

2. **At least a dozen phishing websites emerged right after the collapse, developed by Threat Actors to impersonate SVB.** They have domains which, at a glance, look like they could be SVB's. They've launched malicious campaigns to, among other things, set up a bogus reward program to trade cryptocurrency for USD 1:1. It simply pushes the victim to expose their crypto wallet at which point their funds are stolen. In some cases, simply scanning a QR code on an offer compromises the user's wallet.

3. Many businesses which bank with SVB are struggling to make payroll and keep their business running while their accounts are frozen. **Several fraudulent "private investment groups" have offered to buy SVB customer's verified claims of their frozen account balances for CASH to be paid out within 24 hours.** Sadly, the best-case scenario of this situation is that they're offering loans to struggling companies at exorbitant interest rates. Worst case is they're stealing all of their company info, their funds, and their futures, and their problems just got exponentially worse.

Again – it's not likely that any of these scams will touch our customer base, but during this volatile timeframe, it's always best to be more diligent with the transactions that we make. If at any time something gives you any concern, just ask your supervisor to take a look at it with you. Thank you!

Legence® Bank Member FDIC