PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

March 2023

Private Foundations Special Bulletin

Banking Crisis Ripe for Cyber Criminals – Don't Fall Victim

By Thomas F. Blaney, CPA, CFE; Christopher D. Petermann, CPA; and Eric J. Hillman, CPA

Recent history has shown that events of crises often lead to an increase in cybersecurity crimes. On Friday, March 10, 2023, Silicon Valley Bank became the second largest bank failure in U.S. history. The bank collapsed in just over two days' time, following a massive surge in requests for withdrawals from their depositors. On Sunday, March 12, 2023, a nearly identical "run" on bank deposits occurred at Signature Bank, causing the bank to fail and enter receivership with the Federal Deposit Insurance Corporation (FDIC). While the Federal Reserve Bank has announced that all deposit accounts held at these banks will be fully guaranteed, the entire banking and capital markets are in a decidedly fragile state, suffering from a highly skeptical and fearful consumer base. Given the uncertainty and overall ramifications of these bank failures, the markets are being thrust into an immediate crisis.

Such a crisis provides a ripe environment for the opportunist cybercriminal. As private foundations are significantly endowed institutions actively participating in the banking and capital markets, we offer them the following considerations and reminders to ensure they protect their assets and workforce.

Social Engineering

As Thomas DeMayo, leader of the Firm's Cybersecurity and Privacy Security group previously communicated during the Coronavirus pandemic, events that trigger emotional distress or curiosity are key themes for cybercriminals to use in creating social engineering campaigns. A social engineering campaign is an act through a social mechanism – be it email, phone calls, text messages, etc. – that is designed to manipulate the victim into performing an action, e.g., clicking on a link, opening an attachment, or disclosing information. For these types of attacks to be successful, they must trigger an emotional response with the target.

As private foundations evaluate any exposure with its partner banking institutions, it's critical to remind your employees to be cautious of emails with links or attachments that potentially implicate their partner banking institutions in the ongoing crisis. The following scenarios are examples of how the crisis could be leveraged by bad actors to manipulate your employees:

- A phone call and/or email from a purported investee contact claiming the foundation's deposits are at risk and additional information is required to process future redemptions as needed. An attachment requesting new banking information is shared in the email for the foundation's employee-victim to open, now providing access to the foundation's systems to the criminal.

- A message from a fraudulent charity or active grantee soliciting support from the foundation in response to losses incurred from uninsured deposits.

- An email from a spoofed news outlet claiming a partner banking institution has failed or a collapse is impending. A link is supplied to access an article for the victim to click to read the additional details. While the act of clicking alone may sound benign, that is enough for the cyber criminals to infect your systems, steal data, or hold you hostage with ransomware.

- An email claiming to be from the foundation's President or the COO with an updated list of approved vendors and banking partners as a response to mitigate supply chain disruption from the ongoing banking crisis. The memo is provided in an attachment that needs to be opened. The act of clicking on the attachment and opening the document could be enough in and of itself to become compromised.

Remind your employees that when receiving any messages that reference the banking system to ***Pause, Inspect and Think*** (PIT) before acting. Remind and encourage them to control their emotions and not to let their fear or curiosity drive their response. It is critical that you also have someone who the employees can reach out to if they have questions about the communication and want to confirm its legitimacy. If you have standard methods of communicating significant issues, such as posting the information to your intranet, remind employees of these methods.

Grantee-Level Cyber Risk

Organizations of all sizes are susceptible to cyberattacks in the form of phishing, ransomware, business email compromises and many others. At a minimum, cyber risk and fraud should become one of the highest priority agenda items to assess at the grantee level, particularly during an ongoing banking crisis. A foundation's management and Board should assess their grantee's cyber risk for potential cyberattacks and determine the necessary steps to take to mitigate such risk. Awareness of cyber risk at all levels can help prevent and detect a fraud. Addressing cyber risk at the grantee level starts at the foundation and should be incorporated into the foundation's initial and ongoing due diligence procedures.

Ensuring the foundation's grant funding is properly safeguarded once received at the grantee level is critical to programmatic success and should be addressed with the same care as if the funding was still maintained in the foundation's accounts. Proper controls, hotlines and codes of conduct are considerations that can guard your grantees from potential fraud risks and should be considered as "check-in" items with the grantees during ongoing due-diligence and monitoring procedures. In addition, assessing the grantee's susceptibility to social engineering schemes should be incorporated into the "check-in" procedures.

Contact Us

We welcome the opportunity to answer any questions you may have related to this topic or any other accounting, audit, tax or advisory matters relative to private foundations. Please call 212.286.2600 or email any of the Private Foundation Services team members below:

Thomas Blaney, CPA, CFE
Partner, Co-Director of Foundation Services
tblaney@pkfod.com

Christopher Petermann, CPA
Partner, Co-Director of Foundation Services
cpetermann@pkfod.com

Joseph Ali, CPA
Partner
jali@pkfod.com

Elizabeth Gousse Ballotte
Principal
eballotte@pkfod.com

Scott Brown, CPA
Partner
sbrown@pkfod.com

Raymond Jones, Sr., CPA
Partner
rjones@pkfod.com

Anan Samara, EA
Principal
asmara@pkfod.com