November 2023

Private Foundations Bulletin

Protecting Your Foundation from Disbursement Fraud

By Thomas J. DeMayo, Partner, Cybersecurity and Privacy Advisory and Eric J. Hillman, CPA, Senior Manager

Disbursement fraud, either electronic or check based, continues to be a prevalent and increasing threat to private foundations. Over the years, we have worked with numerous foundations that fell victim to this crime. While losses continue to mount, the positive news is that there are many key controls that can be implemented both internally and in combination with your banking and custodial institutions to mitigate this risk. In this article, we will explain the common tactics used and the key controls your foundation should consider implementing.

Business Email Compromise

Business Email Compromise (BEC) has been one of the primary drivers of electronic fund transfer frauds. BEC is when an attacker gains access to either a grantee's, vendor's, or internal employee's mailbox that has a role in the disbursement or receivables process and leverages that access to facilitate the malicious deviation of payments. The process remains predictable, which means that the implementation of select controls can have a significant impact on risk reduction.

The common process is as follows:

1. A vendor's, grantee's or internal employee's mailbox is compromised by a cyber attacker. This typically occurs from the organization being phished.
2. The attacker reviews the mailbox searching for specific pending transactions. This ensures that the foundation to be targeted is expecting a pending transfer from the now- compromised entity.
3. The attacker preps the compromised mailbox by placing rules in the mailbox to ensure that emails to the targeted foundation are directed automatically to a different folder and not the inbox. This ensures that the communications will remain hidden.
4. The attacker emails the targeted foundation with updated payment instructions.
5. The attacker may also call the foundation to break the call-back process the foundation may have implemented.

Key controls to implement:

1. Ensure that any changes to ACH payment information from a vendor or grantee requires a call-back process to that vendor or grantee on a known good number This means that as part of the vendor or grantee setup, the establishment of the key contacts and numbers is critical. Do not follow any instructions in the email, inclusive of numbers to call.

2. With the evolution of artificial intelligence (AI) and the ability to clone voices, employees need to be educated that voice alone is not sufficient; this is inclusive of instructions internally or externally. Being that caller ID can be spoofed, in combination with voice alterations, a call-back to the known good numbers is critical. For example, policies have to be well-defined and communicated that if what appears like a call from the CFO to modify payment instructions, or bypass disbursement

controls, the CFO must be called back as well.

3. Ensure that the call-back procedures are well documented and communicated to all staff. One of the issues we see is that many foundations have implemented this policy; however, it may not be consistently followed.

Unauthorized Access to the Banking Institutions

Attackers will use various methods to attempt to gain access to the foundation's banking institutions. Once access is obtained, the attackers will attempt to transfer funds. Access is typically obtained through the use of compromised credentials. These credentials may be obtained from either the foundation employee being socially engineered (e.g., phished), using weak passwords and/or using the same password across multiple sites.

Key controls to implement:

1. Employees need to receive consistent security awareness training, inclusive of phishing testing, no exceptions.

2. Employees should be educated on the creation of strong passwords, inclusive of such behaviors as not using the same password across sites.

3. Multi-factor authentication should be enabled.

4. Separate initiators and approvers should be defined and enforced by the system. Should an attacker obtain access, this will be the key control to stop the movement of the funds.

ACH Debits

Many foundations may not realize that by default with most banking accounts, any individual with your bank account numbers can trigger an ACH debit. We usually give the example that when you lease a car and set up automatic payments from your bank account with the lessor, you don't do anything to let the bank know that the lessor is now authorized to withdraw the funds. In most situations, a foundation will have a minimal number of vendors that would ever need to perform an ACH debit.

To mitigate this risk, the key control is to establish with your banking institution an ACH Debit Block/Filter. This will require you to inform the bank what entities are allowed to ever initiate an ACH debit; any vendor not explicitly listed will be blocked.

Check Fraud

Over the last year, check fraud has become rampant and widespread. This typically occurs from checks being stolen in the mail and altered. While many foundations have moved to primarily electronic payments, checks are still actively utilized.

Key controls to implement:

1. Positive Pay – With the implementation of positive pay, you will be required to provide the bank your check runs. When the bank receives a check to cash, it will inspect the check received to ensure that the details match what was provided in the check run. If the details do not match, the check will not be cashed. When setting up positive pay, make sure the bank is checking not only the dollar amount, but the payee. While many foundations have implemented positive pay, we have experienced foundations that have still been a victim of check fraud because of not including the payee's name to be matched. When checks are stolen, the only field that may be washed is the payee, leaving the dollar amount the same. Without including the payee's name in the check, the dollar amounts will match and the check will be processed.

2. Reverse Positive Pay – Some foundations find that the process of uploading the check runs to be cumbersome based on the small volume of checks they may produce. As an alternative, the banking institutions will usually also offer reverse positive pay. Unlike positive pay, which requires you to upload your check run, reverse positive pay does not. With reverse positive pay, the bank will alert you of the checks presented for payment. You will need to approve or reject any check presented within a set window of time. Should you not approve within the required time period, the check may

be auto- approved or denied based on your setup.

3. Check Blocks – With many foundations going to complete electronic payments, especially on some of the accounts, the need to produce checks does not exist. To eliminate the risk, you establish a check block with the bank. This will eliminate the risk of fraudulent checks from those accounts.

In Conclusion

Private foundations should continuously evaluate their exposure to cyber risk and the methods employed by the criminals that target them. The ever-evolving landscape of AI is one area on the forefront that should be seriously considered when assessing cyber risk exposure. We recommend foundations consider evaluating their cyber insurance coverage in conjunction with cyber risk exposure, particularly that of breaches and fraud incidents resulting from artificial intelligence.

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
Partner
eballotte@pkfod.com

Scott Brown, CPA
Partner
sbrown@pkfod.com

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

Anan Samara, EA
Partner
asmara@pkfod.com