Fraud Risk Associated with Remote Staff

SHAWN H. MILLER, CPA, CFE | CALIBRE CPA GROUP, PLLC
JEREMY ZISSMAN, CPA | FISCAL STRATEGIES 4 NONPROFITS, LLC

Summary

Let's discuss how having finance staff working remotely increases fraud risk.

Risks

- Lack of supervision
  - How many accounting employees are on staff? Normally one or two.
  - The limited number gives rise to little or no supervision.
  - Board oversight is minimal or non-existent

Risks

- Remote access to all software
  - All software is either cloud or network based and without readily accessible support, remote employees tend to take actions that may not be in their best interests.

Risks

- Ghost/scam emails
  - Fraudsters can easily target the unaware accounting staff through false emails that look real or through ghosting a real contact.
  - The expected result of this activity would be for the accounting staff to change the bank account to that of the fraudster and have the accounting staff disburse funds to that account.
  - Don’t be fooled and realize the fraudsters are both smart and experienced in their practices

Risks

- Limited training
  - With remote staff rarely visiting offices, training is virtual and normally infrequent as it is hard to deliver over Zoom

Controls

- Frequent interaction via zoom or other source with supervisor
  - By ensuring all remote staff have access to and support from supervisors and other knowledgeable staff, their confidence and knowledge can be increased, and this alone may be sufficient to prevent any fraudulent activity

Controls

- Significant training for all finance staff
  - Review process to ensure complete understanding of what to and what NOT to do
  - Questions that should be asked to ensure understanding
  - How to do any necessary research
  - Payee/bank verification should occur frequently to confirm no unusual ror fraudulent activity has occured,.

Controls

- Frequent interaction via zoom or other source with supervisor
- Significant training for all finance staff
  - Review process
  - Questions that should be asked
  - How to do any necessary research
  - Payee/bank verification
- IT review of remote access
  - Review of security
  - Review of log in process
  - Phishing email training

Controls

- IT review of remote access
  - Review of security protocols and regular scans should be performed to confirm no unauthorized access has occurred
  - Review of log in process and routine password change protocols in place
  - Phishing email training through online education and test emails to confirm employees are not prone to click on bad emails

Case Studies

- Bank account changes for vendor payments to fraudulent payee
  - An email may be received PURPORTING to be from a vendor when in fact it is not. Included may be the following message:
  - "As a result of a bank audit, we have a new bank account that you should now use to ACH us our remittance. Our new bank account # and routing # are ……."

Case Studies

- Ghost/Phishing email scams: False email insertion into valid email conversation
  - Are these email addresses the same:
  - phishing@notarealemail.com
  - phishing@N0TAREAIEMAIL.COM
  - Be alert for familiar email addresses MISSPELT and email addresses that are in CAPS when the original is NOT.

Contact

Fraud Risk Associated with Remote Staff

Shawn H. Miller, CPA, CFE | Calibre CPA Group, PLLC
202.721.1712 | smiller@calibrecpa.com

Jeremy Zissman, CPA | Fiscal Strategies 4 Nonprofits, LLC
jzissman@fiscalstrategies4nonprofits.com