Wire Transfer Fraud: It Could Happen to You

If you're caught in a scam, be sure to follow these steps.

By Jesse Daves

In recent years, there has been a surge in fraud schemes designed to trick organizations into sending wire transfers to bank accounts set up for this fraudulent purpose. The scenario below has become all too familiar.

The Scam

An employee – we'll call her Jessica – was out of town when she received an urgent request from her organization's executive director – Scott – to send a wire transfer to a vendor. She read the e-mail on her cell phone and quickly replied that she would handle it as soon as she could get to her laptop to connect to the bank's website. When Jessica asked for the vendor's invoice, Scott replied that he would provide it later in the week when he got back to the office. Jessica initiated the wire transfer with the bank for $154,290.

The following day, Jessica received a second e-mail from Scott requesting another wire transfer to the same vendor to pay the balance of the invoice. Once again, Jessica initiated the transfer.

A week later, Jessica followed up with Scott in the office to get the invoices supporting the two wires she sent. Scott was confused by Jessica's questions, as he was unaware of the invoices or the wire transfers. He relayed his concern to the organization's board of directors, who immediately launched an internal investigation. The board wanted to know exactly what happened. Were employees willing participants? Were similar disbursements made in the past? How could the organization prevent this in the future?

Six Crucial Investigation Steps

When learning about a scheme of this type, an organization should work with a seasoned investigative team and follow the steps below to remediate the fraud.

1. PRESERVE & PLAN

Early in an investigation it's critical to identify sources of relevant data. Sources include computers, e-mail messages and attachments, mobile devices, network files and logs, and various accounting records. Once you identify the sources

> "A fraudster's strategy relies on employee fallibility."

of information, develop a preservation and analysis plan, including proper "chain of custody" procedures. Make certain that evidence is properly preserved to maintain its integrity and defensibility.

2. INTERVIEW

A fraudster's strategy relies on human error and employee fallibility. It's imperative to learn the level of employee participation, if any, in the scam. Be sure an investigative team interviews employees to determine whether they're witnesses, victims, or part of the scheme. As a result of these interviews, investigators may decide to investigate some employees further. They may need to conduct background checks to discover if other factors influenced decisions made by employees. An investigation should also include a review of an organization's internal controls. It's important that you collaborate with counsel to address legal concerns involving employees, privilege issues, and whistleblower matters.

3. ANALYZE

Analyzing the following data points is vital:

- **wire** transfer activity and related accounting records
- **e-mail** messages and attachments
- **network** files, logs, and traffic
- **mobile** devices
- **computers** and hard drives
- **phone** records
- **Internet** research related to domain registration
- **policies** and procedures related to disbursements.

An investigation should also rule out possible malware or other malicious software that may have resulted in an unauthorized intrusion.

4. COMMUNICATE

Communication with board members is essential, including regular updates about the investigative approach and findings. Board members will be keen on finding answers – particularly about the internal control environment and the security measures surrounding the funds.

5. RECOVER

How much effort is warranted to recover funds lost in a fraudulent wire transfer? Fraudsters have become adept at disguising ownership of e-mail addresses (domains) and bank accounts, especially those residing in foreign jurisdictions. Decide if insurance coverage, under fidelity bond or computer crime polices, may be a better option than recovery efforts. You can also file a report with the Federal Bureau of Investigation to be considered among the growing number of reports filed each year by organizations that are similarly defrauded.

6. REMEDIATE & PREVENT

In the scam described above, while there was no indication that the wire transfer fraud was perpetrated by insiders, several internal control deficiencies contributed to the organization's financial loss. To prevent a recurrence, it's important to uncover what happened, determine who was involved, identify the potential for recovery, and create a remediation plan to avoid similar fraud events in the future. Successful remediation plans include the following steps:

- **Close gaps** in the control environment.
- **Employ monitoring tools** to detect intrusion.
- **Initiate training** and education programs.

Jesse Daves (jdaves@bdo.com) is a director in the global forensics practice at BDO Consulting.

Manage Your Risks

Use these articles at NonprofitWorld.org to safeguard your organization from fraudulent schemes:

Don't Get Caught by Phishing Schemes (Vol. 35, No. 2)

Cybersecurity: Not Just for Home Depot Anymore (Vol. 34, No. 4)

New Internal Control Guidance: What You Need to Know (Vol. 28, No. 1)

Workplace Identity Theft: Curing the Latest HR Headache (Vol. 25, No. 5)

Want to Avoid Fraud? Look to Your Board (Vol. 28, No. 5)

Setting Up a Control System for Your Organization (Vol. 16, No. 3)