FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #6 – Impersonation Scams

This is the sixth in our series of quarterly emails on payments fraud, which continues to plague financial institutions and businesses at an alarming rate. According to the 2016 Payments Fraud and Control Survey conducted by the Association for Financial Professionals, **73 percent of companies surveyed were targets of payments fraud in 2015**. Regardless of what you do, the size of your business or where it is located, payments fraud can affect you.

Impersonation scams continue to be one of the most prevalent types of payments fraud and warrant reiteration in this fraud tip. These often begin with the CEO email scam - *covered in our first fraud tip* - in which a scammer gains access to, or spoofs, the email account of a company's CEO, CFO or other executive, and requests that an ACH or wire transfer be sent to a specific bank account. However, other types of impersonation scams involving vendor invoices - *covered in our third fraud tip* - and faked customer requests are also robbing companies and their well-intentioned employees of millions of dollars every year.

We urge you to share this information with your employees so that you can better protect your business from these types of fraud scams.

Impersonation Scams

There are several variations of impersonation scams:

- **Executive Impersonation:** In this variation, a hacker takes control of the CEO's or CFO's email account, or spoofs it. Spoofing involves creating a fictitious email domain that closely resembles the actual one. For example, where a valid email address could be JDOE@COMPANY.COM, spoofed variations could use a "0" (zero) rather than a capital "O" (the letter) in COMPANY, or JDOE@COMPANY.COM, simple misspellings such as JDOE@COMPNAY.COM, or other substitutions, such as using a lower case "r" and "n" (rn) in place of the letter "m," which can be easily overlooked.

Posing as the CEO or CFO, a fraudster sends an email to a company employee responsible for payments and requests that an urgent wire or ACH be sent to a specific recipient. In some cases, these fake emails may be "forwarded" using another fake email address from another company executive to give the request the appearance of greater legitimacy. Other common factors include an emphasis on the "urgency" of the payment or its "strict confidentiality." The use of spoofed third parties, such as law firms or auditors, is also a common practice.

Acting in good faith, the employee instructs the company's financial institution to initiate the request.

- **Vendor impersonation:** Similarly, a fraudster can take control over or spoof the email account of a company vendor. In these cases, the fraudster - posing as the vendor - sends an email to inform the company that the vendor has a new bank account where future electronic payments should be sent. A bogus invoice could even be attached to the email. Likewise, the fraudster could send an email notifying the company of an address change so that check payments would be rerouted and later deposited into the fraudster's account. In addition, the fraudster could make counterfeit checks using the account information on your legitimate check as a template.
- **Customer impersonation:** Fraudsters can also take over or spoof the email account of a company's customer. In these scams, the request is often related to something other than a payment. A scammer might target a customer's email account to simply collect information that could be valuable in committing a later fraud. An easy way for the fraudster to accomplish this is through hiding malware in an email attachment or tricking the recipient into clicking a link in the email. To the fraudster, the setup of the fraud scheme is as important as the scheme itself.

Why Impersonation Scams Are Effective

- *Like most successful fraud schemes, impersonation scams are based on trust.* Impersonated emails appear to come from people and businesses that are well known and trusted by others within the company. These scams prey on human vulnerabilities by targeting an employee's desire to do a good job and fulfill an executive, vendor or customer request.
- *Often - but not always - impersonation scams succeed through computer hacking skills and manipulation of actual company email accounts.* These types of attacks are more difficult for employees to identify because the email account, but **not the email itself**, is legitimate.

- *Scammers do their research.* They send emails or place calls to determine the person or department responsible for payments. They may also research the organization, so that they are able to refer to employees, vendors, or customers and use industry jargon to give the employee more confidence that the request is legitimate.
- *Overreliance on a secure email gateway to filter fraudulent emails.* A gateway may detect spoofed emails, but it will not necessarily detect emails from accounts that have been hacked. Even spoofed emails with no detectable virus or bug may pass through.

How to Detect and Prevent Impersonation Scams

While fraud schemes are getting more sophisticated and harder to detect, there are things that you and all employees can do to better protect yourself from fraud. A few things to keep in mind:

- Carefully check the email domain portion of an email sender's address - the portion between @ and .com (or .net, etc.) - for any replacement characters, such as "0" or zero instead of the letter "O" or "I" (lowercase "L") in place of "I" (uppercase "I"). Keep in mind, there are many other character replacement variations that are commonly used.
- Validate **by telephone** using a known phone number, not the one listed on the request, or in person, **each** email-based payment request coming from a company executive, especially if the request falls outside of standard company practices (missing a payment request form or an accompanying invoice, for example). Even if these elements are present, confirm the payment with the requestor.
- Pay attention to unusual circumstances and red flags:
  - Does the email sound like typical emails you and your colleagues may have received from the CEO or other company executives in the past?
  - Does the vendor normally contact the company in a way other than email, e.g., via phone or fax?
  - Is the vendor representative someone with whom the company has not interacted in the past?

As you consider the fraud awareness information provided above, please also bear in mind your important role in the fraud detection and reporting process. Your vigilance in reviewing your accounts and transactions is vital to fraud prevention and detection. Fraud schemes - as well as loss recovery efforts and outcomes - can be complicated. Early detection and prompt reporting of a fraud incident is critical because the passage of time might adversely affect the potential recovery of a fraud loss or the outcome of a customer claim. Your attentiveness often is the first line of defense for fraud, and if a fraud incident does occur, your diligence might aid in a potential loss recovery.