FARM CREDIT

FRAUD PROTECTION AWARENESS SERIES

Fraud Tip #3 – Invoice/Vendor Fraud

A highly successful and prevalent scam in use today is Vendor/Invoice Fraud. These scams are similar to the CEO Email Scam we covered in Fraud Tip #1 emailed earlier this year, in that they rely on "social engineering" – manipulating a person into doing something. They also depend heavily on the scammer's email hacking and research skills to become familiar with the targeted company.

Invoice/Vendor Fraud

The basis of these scams is exceedingly simple:

- A scammer contacts a company employee – by email, fax or telephone – pretending to be a vendor. The scammer "informs" the employee that the vendor's bank account number or address has changed, so that subsequent payments will then be unknowingly routed to a bogus account (for wires or ACH payments) or address (for checks).
- In the email version of this scam, the fraudster might use a vendor's compromised email account. In other cases, the scammer might create a spoofed email account – a fake email account that closely resembles a legitimate one. For example, the email address tom@company.com could be spoofed as *tom@c0mpany.com*, where a zero (0) is used in place of the O in company.

Why Invoice/Vendor Fraud is Effective

- *A scammer with hacking skills can manipulate email accounts.* The scammer can read communications to and from vendors and craft an email strikingly similar to what a vendor might write.
- *Scammers do their research.* They send emails or place calls to find out exactly who is responsible for invoices and vendor payments. They may also research the organization in general and refer to other known employees, customers or suppliers – or use industry jargon – to give the employee more confidence that the request is real.
- *Invoice/Vendor Fraud succeeds based on social engineering techniques – manipulating*

a person into doing something or giving away information by making them think they are communicating with a known and trusted contact. They prey on human vulnerabilities, targeting sincere people who are eager to fulfill a vendor's request and do a good job. Social engineering is all about establishing credibility and trust.

How to Detect and Prevent Invoice/Vendor Fraud

- Consider implementing a procedure to confirm any request for changes to a vendor's payment information by calling a known vendor representative.
- Consider requiring high-dollar invoices received electronically to be authenticated by a phone call to the vendor prior to payment. For those received by mail, authenticate by phone or email. Communicate only using the vendor's established phone number, email address and contact names on file.
- Pay attention to unusual circumstances and "red flags:"
  - Does the vendor normally contact the company using a different communication mechanism – phone, email or fax?
  - Is the individual making the request someone your company hasn't dealt with before or seems to be new to the vendor?

Although there is no certainty that a particular course of action will prevent a loss, the considerations outlined above might be beneficial to you. Please keep in mind that your company might be responsible for a loss even if it is related to a fraud perpetrated on the company. In the scenario described above, for example, because an authorized employee of the company provided the wire instruction to the bank, the company is responsible for the wire even if the employee was deceived by the fraudster.

As you consider the fraud awareness information described 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 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 to a fraud and, if a fraud occurs, your diligence might aid in a potential loss recovery.