Vendor Impersonation Fraud

What is it?

Vendor Impersonation Fraud can occur when a business, public sector agency or organization, e.g., a municipal government agency, a school district, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the contractor or construction-related company. Although any business entity could be the target of this type of social engineering attack, public sector entities seem to be specifically targeted because their contracting information is oftentimes a matter of public record.

How It's Done

- Fraudster monitors a business, public sector agency or organization for publicly available contractor or vendor information.
- The fraudster poses as a legitimate vendor or contractor to request updates or changes to payment information, or change of payment method.
- Then the fraudster, sends an email, form, or letter resulting in the business or agency transferring funds to an account controlled by the fraudster or a money mule.

Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- ✔ Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume this is a cybersecurity issue.
- ✔ Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, pressure to take action quickly, and any change of payment method (e.g., ACH to wire).
- ✔ Be old-fashioned! Verbally authenticate any payment changes via the telephone.
- ✔ Review accounts frequently.
- ✔ IInitiate payments using dual controls.
- ✔ Do not provide nonpublic business information on social media.
- ✔ Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.
- ✔ Make vendor payment forms available only via secure means or to known entities.
- ✔ A company domain should always be used in business emails.
- ✔ Require changes to payment account information be made or confirmed only by site administrators, and use methods like verification codes to existing contacts.
- ✔ Do not ignore calls from a financial institution questioning the legitimacy of a payment.