Vendor Changes – July 18, 2024

In Ohio, we have heard of several schemes to ***redirect payments in fraudulent ways***.

We are highlighting portions of the Auditor of State bulletin on this topic now. Attached is the full bulletin for your review. Also, the internal control manual is being updated for this topic. We will review the updates during the annual Making Numbers Count training.

Some of the procedures in the internal control manual and in the bulletin are specific to financial payments and are highlighted below to increase awareness now.

For departments who are requesting changes to a vendor or employee contact information:

NEVER make a change to vendor or employee's contact information or banking information without ***independent verification***. ***In-person communication*** is always the best practice for verifying identity and contact information. Never use email to verify change requests.

We will require in-person verification for change requests for payment information where possible. It is the best practice to also use a second person verification where the vendor is not personally known by the paying agent. ***We will ask for the person or department which deals with the vendor to verify the identity and confirm the change request.***

If distance prevents verifying identity and contact information in-person, use only an ***independently verified contact person and telephone number***. Do not use contact information from a change request; instead, find a phone number from a validated source such as a prior invoice or a regularly updated employee or vendor contact information listing. Another source for a valid telephone number is searching for the company's known website.

When using a telephone call to validate the identity of an employee or vendor contact, always ask the employee or vendor a question related to past experiences or conversations that only he/she would know the answer to.

With the form required for a new vendor or a change with a vendor, we will require a secondary approval (internally) for all ***payment requests, payment instruction changes, or vendor contact information***. ***Please see the attached form, which has been updated to require two signatures at the departmental level.***

The payment change initiation and payment approval functions should be segregated.

For certain employee changes, there will also be a need for secondary approval, such as with bank verifications.

• We will ***provide continual training and education*** over policies, procedures, protecting personal information, and recent cyber and phishing threats so that employees can identify fraud schemes before taking compromising actions. This is accomplished with the annual cybersecurity training, with communication about the internal control manual, and with other communications and meetings.

• We will use ***layers of authentication and security*** such as a financial institution's positive pay, ACH positive pay, and ACH Debit Block programs.

Some of the procedures and practices within the bulletin are covered in the annual cybersecurity training.

Here are procedures and practices for everyone to follow:

• With emails, **p*ay close attention to the name of the employee or vendor*** – oftentimes cybercriminals make subtle changes to names to make you think you are communicating

with a legitimate or known person/vendor. For example, can you spot the subtle difference between these two emails schoolsolutions@gmail.com vs.schoolsolutiions@gmail.com? The second email address included an extra "i" in the vendor's name.

• ***Was the email or invoice unexpected?*** Unless you are expecting an email, never click on links or open attachments without first verifying the authenticity of the message.

• ***Does the email or invoice come with a sense of urgency including a positive (reward) or negative consequence for not acting quickly***? This is a red flag.

• ***Targeted attacks may arrive when criminals know the CEO or high-ranking official is not available to confirm requests.*** By following social media posts, criminals may choose to act when, for example, your executive is on a cruise.

Take time to review emails for red flags.

If you have any questions, please reach out to Bev Hoskinson in the County Auditor's Office. Please let us know if you have any questions about the bulletin, procedures, or form.