ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS
ASCIP

On the Alert!

Date: November 02, 2023

Attention: ASCIP Members

Affected: Administrators, Legal, Risk Management, Faculty & Staff

Applicability: K-12 Districts, Charter Schools, & Community Colleges

YOU COULD LOSE MILLIONS OF DOLLARS IN WIRE TRANSFER FRAUD!!

Over the past few months, several ASCIP members and partners have been victimized by electronic fund transfer (EFT) fraud crimes. Most of these incidents started with fraudulent emails directed to district employees (a practice known as phishing). These emails had familiar logos and similar email addresses, sender names, and signatures, which did not raise suspicion about their legitimacy. In one case, a phone call was received from someone masquerading as an existing vendor's executive (a practice known as vishing). District employees processed the requests without additional verification or confirmation of their legitimacy only to find out later that the emails were fraudulent.

EFT (Electronic Funds Transfer) and EFT Fraud

EFT refers to the electronic transfer of money from one financial institution to another, including institutions such as county offices of education and the state Local Agency Investment Fund (LAIF). It includes activities like ACH (Automated Clearing House) transactions, wire transfers, electronic checks, credit/debit card payments, payroll direct deposits, ATM activities, and mobile apps such as Venmo. All are fast and generally safe ways to send and receive payments. However, they are becoming a leading way for criminals to steal funds from districts. The good news is districts do have tools and methods to protect themselves.

Tips to Avoid Becoming a Victim of EFT Fraud

Engineering controls

- Implement Positive Pay for all checks and Automated Clearing House (ACH) transactions. This is an online banking fraud mitigation service that allows Districts to manage ACH debits and credits posted to your business account via filters and blocks.
- Use a verified Vendor/Supplier Portal for entry and validation of critical information (name, address, bank account, tax ID number).
- Use a secured Employee Portal where employees enter initial and requested changes to critical information, such as bank account information, which needs secondary approval from another employee.
- Use multi-factor authentication with all these and other critical systems.

Administrative controls

- Ensure that District employees who have control over District EFT disbursement are restricted to approvals only with the co-approval of another authorized employee (i.e., a two deep approval process).
- Implement a call-back verification process. Receive verbal communication using trusted information on file regarding all changes on critical information. Even better is to use video confirmation with a service such as Zoom or MS Teams.
- Be wary of sudden changes in vendor practices or information on file. Carefully review and verify that email names and extensions are accurate and legitimate, including single letter changes or changes in the email extension from ".edu" or ".com" to something else.
- Always perform a pre-note validation transfer (or test deposit) with blind confirmation for all new vendors or vendors change requests in electronic banking information.
- Set limits on the dollar value of allowed EFTs.
- Do not use the "Reply" or "Reply All" options to respond to emails related to payment directions. Instead, use the "Forward" option and type in the known email address from your system of record.
- Implement regular training of District employees in fraud prevention practices.

Please contact your ASCIP Risk Services Consultant or our Risk Services team at RM_Info@ascip.org for questions or to discuss further.