ALLIANCE OF SCHOOLS FOR COOPERATIVE INSURANCE PROGRAMS

ASCIP

On The Alert!

Date: May 8, 2020
Attention: **URGENT – All ASCIP Members**
Affected: School Finance
Applicability: K-12, Charter Schools, & Community College Districts

Bank & Wire Fraud On the Rise - School Funds at Risk!

Over the past few months, numerous ASCIP members/partners have experienced Electronic Funds Transfers (EFT) fraud schemes, with some incidents having significant financial impacts. In one case, a phone call was received from a third party pretending to be a known vendor executive. Most other incidents began with a fraudulent email received by a senior-level employee, which quickly involved other staff. These emails contained commonly used language, familiar company logos, similar email addresses, sender names and signatures, which did not raise suspicions to the legitimacy of the requests.

EFT refers to the electronic transfer of money from one financial institution to another including banks, your county office of education and the State Local Agency Investment Fund (LAIF). Electronic transfers include Automated Clearing House (ACH) transactions, wire transfers, electronic checks, credit/debit card payments, payroll direct deposits, ATM activities, and mobile apps such as Venmo. All methods are fast and generally safe to send and receive payments for the purchase of goods and services. Recently, though, electronic transfers are becoming a leading way for savvy perpetrators to take advantage of Districts.

Tips to Avoid Becoming a Victim of EFT Fraud:

- Beware of sudden changes in vendor practices; for example, if a vendor contact suddenly asks to be contacted via their personal email address when all previous correspondence has been via company email.
- Carefully review and verify that email names and extensions are accurate and legitimate. Perpetrators often add an additional letter to the email address, or change the extension from ".edu" or ".com" to ".org" or ".us".
- Never initiate changes or process payments based solely on an email communication or phone calls.
- Implement a call-back verification process for sensitive items such as payments for large sums, to new vendors or making changes to existing vendors. Use previously known telephone numbers, not the number provided in the email request. This includes verifying a change of mailing address to avoid mailing a check to the wrong address.
- Consider financial security procedures for verifying EFTs, by adding additional two-factor authentication such as having a secondary approval.
- Consider setting a limit on the dollar value of allowed EFTs.
- Do not use the "Reply" option to respond to emails relating to payment directions. Instead, use the "Forward" option and either type in the correct email address or select it from your email address book to ensure the intended recipient's correct email address is used.

Please contact your ASCIP risk services consultant at (562) 404-8029 for additional assistance.