ACH and Wire Payments:
Internal Control Best Practices for School Districts

School districts are increasingly moving away from paper checks in favor of ACH transfers and wire payments. The benefits are real -- electronic disbursements are faster, less expensive to process, and eliminate much of the manual work associated with cutting and mailing checks. However, this shift also increases the opportunity for fraud and cyber attacks. Cybercriminals actively target local governments, including school districts, through fake vendor requests, spoofed emails, and unauthorized transfer schemes. A single control gap can result in a significant loss of public funds. The following best practices address the key controls and safeguards every school district should have in place.

Vendor Onboarding

Setting up a new vendor to receive electronic payments should follow a clearly defined process and not be handled informally. At a minimum, every new vendor should complete a standardized onboarding form and provide a current IRS Form W-9 before any payment is issued. The most important step is independently confirming the vendor's banking details -- not by relying on what was submitted in the enrollment request, but by contacting the vendor directly using a phone number sourced from your own records or a publicly listed directory. Email alone should never be accepted for receiving vendor banking information! Business office staff should also review the existing vendor master file for duplicate entries, similar names, or accounts registered under initials rather than a full legal business name, all of which can be indicators of fictitious vendor activity.

Vendor Banking Information Changes

A request to update an existing vendor's account or routing number deserves the same level of scrutiny as adding a brand new vendor. The change should be submitted on a formal request form, and the new banking details must be confirmed by reaching out to the vendor at a phone number already on file with the school district. A second employee not involved with processing the request should independently review and approve the documentation before anything is updated in the system. The school district should also allow a reasonable waiting period between approving

the change and issuing the first payment to the revised account, giving staff an opportunity to catch errors or identify manipulation before funds leave the school district. Every change should be documented with a clear record of who requested it, who reviewed it, and when it was approved.

Online Banking and Payment Controls

No single employee should have end-to-end control over an electronic payment. Every ACH batch and wire transfer should require two separate employees to complete two distinct steps -- one to enter and submit the payment, and a different person to review and authorize its release. If not already utilizing, school districts should highly consider Positive Pay and ACH debit blocking or filtering, which can prevent unauthorized transactions from clearing the bank. Additionally, school districts already utilizing Positive Pay should ensure they are receiving the highest level of verification service that their banking institutions offer (including the verification of payee name on all checks, ACH payments, and wire payments). Online banking activity should be reviewed each business day by someone who is not directly involved in processing payments, and any system alerts or unusual items should be documented and followed up promptly. Dollar thresholds that trigger escalating levels of review or board notification are also worth establishing.

Segregation of Duties and System Access

Proper segregation of duties is one of the most fundamental controls in any payment environment. The employee responsible for maintaining the vendor file or entering banking details should be a different person than the one who initiates or approves payments. Access to financial systems and online banking portals should be limited to what each staff member actually needs to do their job, and those permissions should be reviewed on a regular basis to confirm they remain appropriate. Every user with access to banking systems should be required to authenticate through a multi-factor method -- an authenticator app or hardware token provides stronger protection than a text message code. System sessions should require re-authentication at the start of each workday or even more frequently.

Policy, Oversight, and Ongoing Vigilance

Good controls only hold up over time when they are backed by written policy and consistent oversight. Every school district should have a formal electronic payment policy that details the school district's overall process and controls, including but not limited to: who is authorized to be involved in the process, what approvals are required, what approval thresholds may apply, how vendor banking changes are handled, and what steps to follow if something goes wrong. The Board of Education should receive regular reporting on ACH transfers and wire activity, including transaction volumes, dollar totals, and any exceptions requiring follow-up. Perhaps most importantly, the school district should identify in advance who is responsible for contacting the bank, filing the appropriate reports, and communicating with leadership if a fraudulent transfer is suspected -- working through those questions for the first time after a loss has already occurred is not a position any school district wants to be in. All staff with access to the district's network and email should receive periodic training to recognize phishing attempts and email fraud, and the school district's cyber liability coverage should be reviewed annually to confirm it adequately covers electronic payment fraud risks.

Electronic payments are not inherently riskier than paper checks, but they do require a different and more deliberate set of controls. School districts that take the time to formalize these procedures, train their staff, and hold themselves accountable through regular oversight are far better positioned to detect and prevent fraud before it causes lasting financial harm.

Written by: Brendan Nelson, CPA – Partner, R.S. Abrams & Co., LLP

Phone: 631-234-4444

Email: bnelson@rsabrams.com