

The Downside of Digital Banking

Banking online has become a way of life for most of us, but it also can be an avenue for fraud. Is your district taking the proper steps to safeguard taxpayer dollars?

Computers, smartphones, and tablets have changed the way we live. For example, digital banking is now at our fingertips. Online banking customers can open accounts, transfer funds from one account to another, pay utility and credit card bills, change passwords, authorize access for additional computers, and much more. Some digital applications can even scan checks for deposit into customer accounts.

Banks benefit from the trend toward online conveniences. They send account statements to customers digitally, cutting costs associated with printing and postage. Similarly, after checks are cashed through an account, digital images are sent back to the customer, eliminating sorting, packaging, and shipping cancelled checks. These measures streamline functions and save banks both time and money.

School districts have been quick to adopt many of the efficiencies offered by their banking partners. By embracing new technologies, districts save taxpayer money by making their own operations more effective. However, while employing banking innovations does improve financial operations, administrators and board members must be cautious.

Recent cases of cyberfraud in

school districts have prompted state regulators to begin targeting online banking policies and procedures during their audits of school business operations. For example, in October 2011, nearly \$138,000 was stolen from a Vermont school district. The Washington South Supervisory Union's bank account was victimized via wire transfer. The money was deposited into 17 accounts in 10 different banks across the U.S. and the Ukraine.

In another case this past February, Vermont's state auditor issued a 77-page report documenting more than \$415,000 in school district losses. Sixteen districts experienced theft, embezzlement, or wire fraud. Of the 25 incidents reported, four losses exceeded \$40,000. The State Auditor speculates that the number and total dollar amounts of the losses may, in fact, be much larger.

Threats to online banking operations can come from within a school district or from the outside. It is important for your board to be familiar with the nature of external and internal threats. A knowledgeable board is prepared to safeguard the district's financial resources.

Threats from the outside

Cyberthieves use programs that infect

a victim's computer. The program copies keystrokes used for entering names and passwords. It then sends the information via text message directly to hackers who are usually located outside the U.S. After the hackers penetrate the district's account, they wire transfer the money to an account owned by a person known as a mule.

Mules are usually Americans hired for this work on job search websites. However, foreign nationals visiting the U.S. also are used. Most are unaware of the illegality of the transactions they are directed to perform.

After stolen money is deposited into the mule's account, it is withdrawn and forwarded via private money-wiring services to the cyberthieves' accounts, usually located in other countries. As compensation for facilitating the transaction, the mule deducts 10 percent before forwarding the balance to the designated account.

Without proper internal controls for online banking, a breach in security can result in the loss of financial resources as well as embarrassment for administrators and board members. In addition, employee and student records may be compromised. Identities are stolen when Social Security numbers, addresses, and phone numbers are downloaded. Such information is used to open new credit card accounts. This, of course, creates additional legal and financial exposure for the district.

Threats from the inside

Last year, many school district audits conducted by the New York state

Comptroller focused on online banking functions. These audits identified issues that place districts at risk for financial exploitation. They noted that opportunities for fraud are more likely to occur when unfettered access to accounts is permitted.

For example, the comptroller's office noted that in one New York state district both the treasurer and deputy had supervisory access to 11 district accounts. Without needing administrative approval, both employees were authorized to transfer money between accounts, upload direct deposit files, and make direct payments to other bank accounts. They also could purchase U.S. savings bonds, change the names and addresses listed on the district's bank accounts, and increase access rights of unauthorized users. Both were permitted to perform all duties without review, authorization, or notification of another administrator.

Nearly all district staff are loyal, dependable, and honest. But without adequate internal controls, one untrustworthy employee can take advantage of lax oversight and personally profit from district online banking transactions. This is especially true in difficult economic times.

Policy protection

Increasingly, state auditors are concerned about a lack of school board oversight regarding online banking transactions. They emphasize the need to develop policies limiting opportunities for online banking fraud.

Your board will want to review policies already in place. If necessary, update them to include online banking transactions. Be sure your policies are documented in writing. When reviewing banking policies, specify which online banking activities are permitted. In addition, identify specific job titles with authority to process transactions.

Furthermore, your board can review your administration's approval

process as well as the documentation used to verify the legitimacy and accuracy of all online transactions.

When providing oversight for your district's internal control structure, inquire whether there is any separation of duties for online transactions. This can be difficult in districts where staff is limited. However, it is essential that administrators develop procedures that mandate that at least one other person review and verify online transactions. Without this safeguard, there is increased risk that unauthorized transactions can take place.

Reviewing written procedures for accessing and exiting online banking sessions is another important area of board oversight. You will want to notice the details of how transactions are conducted. For example, when logging on to a bank website, manually enter the URL rather than use a bookmark. This minimizes the risk of accessing a fraudulent website if a bookmark has been altered. Similarly, using a search engine to access a bank's website may unwittingly lead to a fictitious site designed to illegally gain access to district accounts.

Written procedures also must outline steps to check the authenticity of bank websites during the log-on process. Banks use various safeguards such as entering random number codes generated by password devices or the use of pictures chosen by users. Information regarding the location of passwords must be safeguarded and shared only with those officially authorized to access the account.

Precautions also must be taken when leaving a banking website. After logging out, all browser activity such as Internet history, cache, cookies, or temporary Internet files should be deleted. Federal law enforcement agencies recommend that dedicated online banking computers be kept in a secure location. In addition, use of an online banking log that identifies employees conducting specific transac-

tions can ensure procedures are followed.

Beyond policy

Written policies and procedures are not enough to protect your district. Employees who conduct online banking also must receive adequate training in executing control procedures. Administrators can initially orient employees to policies and procedures and emphasize the importance of obtaining authorization when required. Periodic review will ensure all staff understand and can implement the policies and procedures.

In addition, collaborate with your banking partners when developing online banking procedures. Banks are aware of attempts to penetrate their control measures. Ask them to suggest strategies to prevent fraudulent access to both district and bank systems.

Board members and administrators must be aware of the substantial risks associated with online banking. Without thoughtful policies and effective internal controls for financial computer transactions, school districts open themselves to serious legal and financial risks. Unfortunately, you can no longer depend on an armed bank guard to protect your district's money. Cyberthieves develop strategies to steal your financial resources. Board members must develop policies and ensure that administrators implement effective internal controls to combat cyberattacks. Bank vaults may still be locked, but if you don't have the right policies and procedures, your district's money could be gone before you know it. ■

Charles K. Trainor, an *ASBJ* contributing editor, is a certified fraud examiner and certified internal auditor. He is president of Management Audit Consultants, Inc. (www.mgmtaudit.com) and served for 21 years on a school board in New York state.