Broadalbin-Perth Central School District

Online Banking

Report of Examination

2020M-144

Table of Contents

Report Highlights

Audit Objective

Determine whether the Broadalbin-Perth Central School District's (District) Board and District officials ensured online banking transactions were appropriate and information was secure.

Key Findings

The Board and District officials did not adequately safeguard online banking transactions. Officials did not:

- Adopt a comprehensive online banking policy.
- Monitor online banking user compliance with the District's acceptable computer use policy (AUP). As a result, five of the six online banking users were allowed to access nonbusiness websites prohibited by the policy.
- Provide IT security awareness training to all online banking users.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt a comprehensive online banking policy.
- Monitor computer use to ensure compliance with District policies.
- Provide IT security training to all IT users.

Background

The District serves the Towns of Broadalbin, Perth, Johnstown, Mayfield and Northampton in Fulton County, the Towns of Edinburg, Galway and Providence in Saratoga County and the Town of Amsterdam in Montgomery County.

The District is governed by a seven-member Board of Education (Board) responsible for the general management and control of financial and educational affairs. The District Superintendent serves as the chief executive officer responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The Superintendent, Assistant Superintendent for Business Operations (Assistant Superintendent), Treasurer and administrative assistant are responsible for overseeing and performing online banking activity.

Quick Facts	
Online Banking For the Audit Period	
Interfund Transfers	357
Total Interfund Transfers	$72.5 million
Electronic Disbursements	301
Total Electronic Disbursements	$46.1 million
Users	6
Bank Balances as of January 31, 2020	$12.1 million

Audit Period

July 1, 2018 – January 31, 2020

Online Banking

How Should Officials Safeguard Online Banking Transactions?

Online banking provides a way to directly access funds held in a district's bank accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. School districts can disburse or transfer funds by electronic funds transfers (EFTs), provided that the governing board enters into a written agreement with the bank.

An EFT is the electronic transfer of money from one bank account to another, either within a single bank or across multiple banks, through computer-based systems without the direct intervention of bank staff. EFTs consist of different types of payments, such as wire transfers commonly used for bond payments, investments or other large settlements and other electronic transfers used for small-dollar and recurring transactions, such as federal and State payroll tax payments.

GML requires that a school district's agreement with its bank describe the manner in which electronic transfers will be accomplished and identify the names and numbers of bank accounts from which transfers may be made and the individuals authorized to request transfers. Also, GML requires school districts to implement a security procedure that includes verifying that payment orders are for the initiating district and reviewing payment orders to detect errors in transmission or content.

To safeguard cash assets, a board must adopt policies and procedures to properly monitor and control online banking transactions. A comprehensive written online banking policy clearly identifies district approved online banking activities district officials will engage in, specifies employees' titles authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of online banking activity.

In addition, officials must properly segregate the duties of employees granted access to the online banking applications to ensure that employees are unable to perform all financial transactions on their own. It is also essential that bank accounts be monitored by someone independent of the transaction for unauthorized or suspicious activity at least every two or three days.

District officials should limit the number of users authorized to execute online banking activities and the number of computers used. Authorized online banking users should access bank accounts from one computer dedicated for online banking transactions to minimize exposure to malicious software.

Officials Did Not Adequately Safeguard Online Banking Transactions

The District entered into a written online banking agreement with their financial institution to allow officials and key employees to complete electronic banking transactions. However, we found that the Board did not adopt an online banking policy that defines the type of online

banking activities allowed or the procedures for authorizing, processing and monitoring online banking transactions.

Officials properly segregated the duties for processing online banking transactions by limiting employee access to specific functions and bank accounts and requiring the Treasurer to obtain secondary approval, in the online banking application, for wire transfers and automated clearing house (ACH) payments from the administrative assistant or Assistant Superintendent. However, we found that the option to perform EFTs to foreign countries was not disabled.

The Treasurer told us that EFTs to foreign countries were not disabled because the District had processed a one-time electronic international transfer to a foreign country. In June 2019, the District processed an international wire transaction for the purchase of a 3D printer, which we determined was for a proper purpose. However, disabling international wire transfers when not needed would provide additional controls in securing District funds.

In addition, District officials did not ensure that a dedicated computer was used for online banking transactions. Instead, six online banking users (employees) accessed the online banking application from their assigned District computers, which they used for all other work-related activities, including connecting to the Internet. To the extent possible, authorized users should access bank accounts from one computer dedicated for online banking from a wired network to minimize exposure to malicious software.

How Does an AUP Secure and Protect a District's IT Systems?

A school district should have an AUP that defines the procedures for computer, Internet and email use. The policy should describe what constitutes appropriate and inappropriate use of IT resources and the board's expectations concerning personal use of IT equipment and user privacy.

Internet browsing increases the likelihood that users will be exposed to malicious software that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to data including personal, private and sensitive information (PPSI)[1] and IT assets by monitoring Internet usage and by configuring web filtering software to block access to unacceptable websites and help limit access to sites that comply with a district's AUP. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, acceptable use policies or standard security practices.

Monitoring for AUP compliance involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Automated mechanisms may be used to perform this process and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

1 PPSI is any information to which unauthorized access, disclosure, modification or destruction – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers (students), third parties or other individuals or entities.

In addition, officials should require employees to sign acknowledgement forms to indicate they read the district's AUP and are aware of what was expected of them, and to acknowledge they would be held accountable to the policies and procedures outlined in the AUP.

Officials Did Not Monitor For AUP Compliance

The District's AUP requires all IT users to sign an acknowledgment form indicating that they are aware of and will comply with the AUP. However, District officials did not adequately monitor online banking users' Internet use for compliance with the AUP (the employee computer use agreement). We reviewed the web browsing histories on the six computers used for online banking and found that five of the six users assigned to these computers accessed websites for nonbusiness purposes that were prohibited by the AUP.

Five online banking users accessed websites for personal purposes, such as shopping, banking and bill paying, and other non-District related activities, such as watching videos, browsing entertainment news, and visiting sports, social networking and email websites. This occurred because District officials did not properly configure the installed web filtering software intended to restrict these employees' internet access.

> Five online banking users accessed websites for personal…shopping, banking and bill paying, and …activities such as watching videos, browsing entertainment news, and visiting sports, social networking and email websites…

In addition, officials were unable to provide us with evidence that all network users had read, were aware of and acknowledged they would be held accountable for compliance with the AUP.

The Treasurer signed an acknowledgement form and her Internet use was in compliance with the AUP. The Assistant Superintendent and the accounts payable clerk both signed AUP acknowledgment forms and should have been aware their Internet use did not comply with the AUP, while the administrative assistant, payroll clerk and District Clerk did not have a signed AUP acknowledgement form on file.

By allowing personal use of District computers, the District has an increased risk that its network and computers will be exposed to attacks and malicious software that may compromise PPSI. As a result, the District's IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse.

Why Should Officials Provide IT Security Awareness Training to Employees?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees and students. The training should center on emerging trends such

as information theft, social engineering attacks[2] and computer viruses and other types of malicious software that could compromise online banking accounts and potentially lead to significant loss of assets.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs. In addition, the training should cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; and how to respond if a virus or an information security breach is detected.

In addition, the governing board and district officials should establish a policy and written procedures that require employees to be periodically trained in IT security awareness issues and in proper use of the IT infrastructure, software and data. While IT policies will not guarantee the safety of a district's systems, without formal policies and procedures that explicitly convey the appropriate use of the district's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Officials Did Not Provide IT Security Awareness Training

The District's AUP includes provisions for orientation classes explaining acceptable use of computers and the Internet when employees are initially hired. However, District officials did not provide all users of online banking services with formal periodic IT security awareness training to help ensure they understood IT security measures designed to safeguard the District's financial assets from potential abuse or loss and understand their role in protecting IT assets.

While the Assistant Superintendent and the Director of Information Technology periodically attended formal IT security trainings and provided pertinent information to the rest of the online banking users, no formal training was provided to these users.

Because officials did not provide IT security awareness training or restrict personal use of District computers used for online banking, funds were vulnerable to online theft through unauthorized access. As a result, we reviewed all 357 interfund transfers totaling $72.5 million, all nine wires transfers totaling $16.5 million (including one international wire transfer of $1,417 for the 3D printer) and 11 ACH payments totaling $1.9 million processed during our audit period.

We found all interfund transfers were transferred within District bank accounts and all wire transfers and ACH payments reviewed were for appropriate purposes. No funds were lost during our audit period. However, if the bank accounts were attacked and funds misappropriated, as of January 31, 2020, the District could have lost up to $11.2 million.[3]

When District officials do not ensure that users understand the IT security policies and procedures and their roles and responsibilities related to IT and data security, they cannot protect the confidentiality, integrity and availability of data and computer systems. Further,

2 Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information. Phishing is sending deceptive email messages in an attempt to gather personal information or infect computer systems with malicious software.
3 This amount would include losses incurred after funds transfer fraud insurance deductions.

without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, District data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

What Do We Recommend?

The Board should:

1. Adopt a comprehensive online banking policy.

The Superintendent should:

2. Ensure that all IT users, especially employees involved in the online banking process, are provided with formal IT security awareness training.

District officials should:

3. Monitor computer use to ensure compliance with the AUP and regulations.
4. Ensure all IT users sign an acknowledgment form indicating that they are aware of and will comply with the District's AUP.
5. Designate a secured computer to be used for online banking transactions and ensure the computer is connected via a hard-wired internet connection.
6. Disable the ability to perform international wire transfers, when not needed.

Appendix A – Response From District Officials

Appendix B – Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials to obtain an understanding of online banking practices, to obtain any related policies and procedures and to determine if cybersecurity training was provided to online banking users.

- We reviewed the District's employee computer use agreement and signed acknowledgment forms on file for online banking users to obtain an understanding of the acceptable use of computers and Internet and to determine whether all online banking users had signed acknowledgment forms.

- We inquired about written agreements with banks and reviewed the documentation regarding user capabilities for electronic transfers.

- We observed online banking users' access from logon to logoff for the Assistant Superintendent, Treasurer, payroll clerk, accounts payable clerk, administrative assistant and District Clerk.

- We used specialized audit software to examine the six computers used for online banking purposes.

- We reviewed all interfund transfers for the audit period to determine whether they were made between District's accounts.

- We reviewed all wire transfers for the audit period and used our professional judgment to select a sample of 11 ACH payments from the 292 ACH payments totaling $29.5 million for the audit period (based on high and low dollar amounts, description of the transactions and bank accounts). We reviewed the wire transfers and our sample of ACH transactions to determine whether they were for appropriate purposes, and adequately supported and approved.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix C – Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/localgov

Local Government and School Accountability Help Line: (866) 321-8503

GLENS FALLS REGIONAL OFFICE – Gary Gifford, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties